# 사설 네트워크에서 IPv4/IPv6 네트워크 연동을 위한 통합 연동기 설계

이수원°, 이광희, 최훈
충남대학교 컴퓨터공학과
{swlee°, khlee}@ce.cnu.ac.kr, hc@cnu.ac.kr

# The Design of IPv4/IPv6 Interworking Function for Private Networks

Suwon Lee°, KwangHee Lee, Hoon Choi
Mobile Distributed Computing Lab, Department of Computer Engineering,
Chungnam National University, KOREA

요 약

IPv6는 기존 IPv4의 문제점인 주소 고갈 문제를 근본적으로 해결하기 위해 IETF(Internet Engineering Task Force)에서 제안한 프로토콜이다. 그러나 IPv4를 한 순간에 IPv6로 대체하는 것이 불가능 하기 때문에 IPv4와 IPv6간의 호환 및 연동을 위해 듀얼스택(dual stack), 터널링(tunneling), 프로토콜 변환(protocol translation) 등 많은 IPv4-to-IPv6 transition 메커니즘들이 고려되고 있다. 이러한 프로토콜 진화 방안들은 각 방식에 따라 최소한 한 개 이상의 많은 공인 IPv4 주소를 필요로 하며 IPv4 주소가 부족한 현재 상황에서 IPv6 네트워크와의 연동에 많은 어려움이 따르게 된다. 본 논문에서는 공인 IPv4 주소 부족 문제와 네트워크 보안의 필요성에 의해, IPv4 사설 네트워크에서 공인 IPv4 주소로 이루어진 네트워크(인터넷)와 IPv6 네트워크의 연동을 위해 단지 하나의 공인 IP 주소를 이용하여 네트워크간의 연동을 지원하는 통합 연동기를 설계한다.

## 1. 서 론

현재 세계적으로 널리 쓰이고 있는 인터넷의 기본적인 프로토콜인 IPv4는 32비트 주소체계를 사용하기 때문에 이론적으로 약 43억 개의 인터넷 주소공간을 제공할 수 있다. 그러나 기하급수적으로 늘어나는 인터넷 수요자와 이동통신의 All IP, 스마트 정보가전 서비스에 의해 사용될 IP주소의 수요가 늘어남에 따라 IP 주소 고갈문제가 발생하였고 새로운 부가 기능이 필요하게 되었다. 따라서 기존의 IPv4 문제점을 극복하기 위해 IETF (Internet Engineering Task force)에서는 IPng( IP next generation)그룹을 구성하여 IPv6[1] 프로토콜을 제안하고 차세대 인터넷 프로토콜로 채택하였다. 그러나 IPv4를 한 순간에 IPv6로 대체하는 것이 불가능 하기 때문에 IPv4와 IPv6간의 호환 및 연동을 위해 듀얼스택(dual stack), 터널링(tunneling), 프로토콜 변환(protocol translation) 등 많은 IPv4-to-IPv6 transition 메카니즘들이 고려되고 있다. 프로토콜 변환 방식과 터널링 방식은 IP 네트워크의 투명성을 제공하지 못하거나 연동을 지원하기 위해 많은 공인 IPv4 주소를 필요로 한다. 듀얼스택 방식은 IPv4/IPv6 연동 기법은 가장 간단하고 효율적인 방식이지만 프로토콜 변환, 터널링 기법 보다 더 많은 공인 IPv4 주소가 필요하다. 그러나 기술의 간단성 및 구현의 용이성 때문에 IPv4/IPv6 연동을 위한 기반 기술로 채택되고 있다. IPv4 네트워크에는 개인의 프라이버시(privacy), 보안 및 공인, IPv4 주소 고갈 문제로 사설 IPv4 주소로 구축된 많은 사설망이 존재한다. 이러한 사설망들은 IPv4에서 IPv6로의 진화가 종결되어도 네트워크 보안등 많은 이유로 여전히 사설 IPv4 네트워크를 유지하려고 할 것이다. 따라서 프로토콜 변환과 같은 IPv4/IPv6 연동 기술을 적용하기 어렵다. 본 논문에서는 사설 IPv4 네트워크에서 공인 IPv4 네트워크 연동과 IPv6 네트워크 연동을 모두 지원하는 통합 연동기를 설계한다.

°본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

## 2. 관련 연구

### 2.1 듀얼스택

듀얼스택은 호스트에서 IPv4, IPv6 프로토콜 스택을 모두 가지고 있어서, IPv4망과 통신할 때는 IPv4 프로토콜 스택에 할당 되어 있는 IPv4 주소를 이용하고 IPv6 네트워크의 호스트와 통신 할 때 IPv6 주소를 이용하는 방식이다. 듀얼스택은 호스트에 설정되어있는 라우팅 테이블을 이용하여 통신하려는 호스트에 따라 자동으로 발신지 주소 및 프로토콜을 선택할 수 있어 매우 간단하고 구현하기도 쉽다. 그러나 모든 호스트에 공인 IPv4 주소를 할당해야 하므로 부족한 공인 IPv4 주소의 낭비가 심하다.

### 2.2 터널링 방식

터널링 방식은 통신하고자 하는 양쪽의 네트워크가 IPv6 네트워크이고 IPv6 패킷을 전송하는 네트워크가 IPv4 일때 적용하는 연동 방식이다. 터널을 구성하는 방식에 따라 수동(configured)/자동(automatic) 터널링 기법[2]과 생성된 터널을 효과적으로 관리하기 위한 터널 브로커(tunnel broker) 기법[3]이 있다. DSTM(Dual Stack Transition Mechanism)[4]은 IPv6 호스트가 듀얼스택으로 구성되어 있고 DSTM 호스트가 IPv4 호스트와 통신하려 할 때 DHCPv6 호스트로부터 IPv4 주소를 동적으로 할당받아 터널 방식으로 연동을 지원한다. 이러한 터널링 방식은 IPv4/IPv6 연동 시 듀얼스택 방식보다 적은 공인 IPv4 주소를 필요로 하지만 생성된 터널을 통과하기 위해 망 경계에 존재하는 라우터의 구성정보를 필요로 하며 패킷을 캡슐화(encapsulation)해야 하므로 많은 오버헤드가 있다.

### 2.3 프로토콜 변환 방식

프로토콜 변환 방식은 서로 상이한 프로토콜을 사용하는 호스트 간에 통신을 지원하기 위해서 네트워크 장비에서 프로토콜을 변환하는 NATPT/SIIT 방식[5]과 호스트에서 프로토콜을 변환하는 BIS(Bump In the Stack)[6]이 있다. NATPT/SIIT 방식은 망 장비에서 프로토콜 변환을 위해 데이터 패킷을 수정해야 하므로 다양한 인터넷 응용을 지원하기 어렵고 데이터 플로우 식별을 위해 많은 공인 IPv4 주소가 필요하다. BIS 방식은 네트워크에 연결되어 있는 호스트를 수정하여 IPv4 응용 프로그램이 IPv6 응용 프로그램과 통신을 지원한다. BIS는 프로토콜 변환을 위해 호스트에 추가적인 모듈을 설치해야 하고 데이터 플로우를 식별하기 위해 많은 IPv4 주소를 필요로 한다.

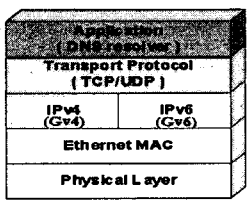
## 3. IPv4/IPv6 통합 연동 기법 설계

IPv4 사설망은 IPv4 주소 부족 문제, 보안, 프라이버시 등 많은 이유에 따라 구축되었지만 사용자에게 인터넷 서비스를 제공하기 위해 인터넷과 연동이 필요하다. 인터넷이 IPv4에서 IPv6로 진화하게 되면 IPv6 네트워크와의 연동을 프로토콜 변환 방식과 같은 연동 기법을 이용해야 한다. 프로토콜 변환 방식의 대표적 기법인 NATPT(Network Address Translation & Protocol Translation) 방식은 보안 및 프라이버시 등의 이유로 구축된 사설 네트워크에는 적합하지 않다. 본 논문에서는 사설망의 대표적인 특징인 네트워크 보안 및 프라이버시를 지원하면서 IPv4 네트워크인 인터넷과 연동을 지원하고 새롭게 구축되고 있는 IPv6 네트워크와의 연동을 지원할 수 있도록 IPv4/IPv6 통합 연동 기법을 제안한다.

IPv4/IPv6 통합 연동 기법은 듀얼스택 호스트로 구성된 로컬 네트워크인 DSPN(Dual Stack Private Network)와 DSPN 호스트에서 생성된 패킷을 전달하기 위한 IPv4/IPv6 통합 연동기로 구성된다.

### 3.1 DSPN 호스트

DSPN 호스트는 IPv4-to-IPv6 전이 메커니즘인 듀얼스택으로 구성되어 있으며 IPv4 프로토콜 스택에는 IPv4/IPv6 통합 연동기에서 IPv4 네트워크와 연결되어 있는 외부 인터페이스의 IP 주소로 설정되어 있고 IPv6 프로토콜 스택에는 DSPN 네트워크에 할당되어 있는 IPv6 사이트 로컬 (site-local) 주소가 설정되어 있다.




[그림 1] DSPN 호스트의 프로토콜 스택

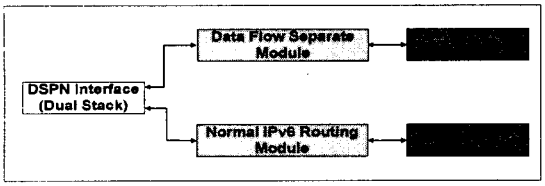
[그림 1]에서 IPv4 프로토콜에 할당되어 있는 IP 주소 *Gv4*는 DSPN을 구성하는 모든 호스트들이 공유하는 주소로 IPv4 네트워크인 인터넷과 통신하고자 할 때 호스트 라우팅에 의해 자동으로 선택된다. IPv6 프로토콜에 IP 주소 Gv6는 IPv6의 사이트 로컬 주소이며 IPv6 네트워크와 통신할 때 호스트 라우팅에 의해 자동적으로 선택되어 발신지 주소로 사용되며 DSPN 네트워크 내부의 IP 통신을 할 때에도 이용된다.

### 3.2 IPv4/IPv6 통합 연동기

IPv4/IPv6 통합 연동기는 DSPN과 다른 IPv4/IPv6 네트워크 경계에 존재하는 라우터이다. DSPN 호스트의 목적지 호스트에 따

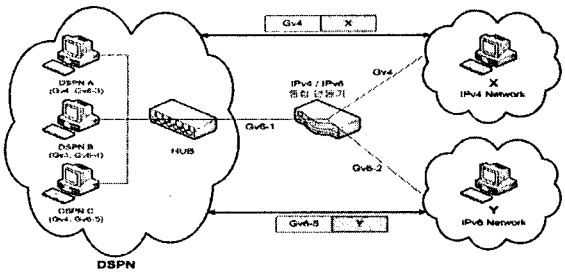
른 자동 발신지 주소 선택 기능을 이용하여 IPv4 네트워크와 DSPN의 연동을 위해 IPv4/IPv6 통합 연동기에서는 데이터 플로우 식별을 위해 데이터 플로우 식별 테이블을 구성하고 유지/관리해야 하며 외부 IPv4 네트워크에서 DSPN으로의 데이터 패킷 전달을 위해 L2 포워딩을 수행한다[7]. 이때 구성되는 데이터 플로우 식별 엔트리는 <프로토콜 식별자, 발신지 호스트 맥 주소(MAC address), 목적지 호스트 주소 (IPv4 주소), 발신지 포트 번호, 목적지 포트번호, 타임아웃 값>으로 구성된다. 또한 DSPN 네트워크와 IPv6 네트워크와의 연동을 위해 IPv4/IPv6 통합 연동기에서는 단지 일반적인 IPv6 라우팅 만을 수행하면 된다.

[그림 2]는 IPv4/IPv6 통합 연동기의 구조를 나타낸다.




[그림 2] IPv4/IPv6 통합 연동기 구조

## 4. 연동 과정




[그림 3] IPv4/IPv6 통합 연동기 동작 과정

[그림 3]은 설계된 IPv4/IPv6 통합 연동 기법을 이용해 DSPN과 IPv4/IPv6 네트워크와의 연동 과정을 보여준다.

DSPN A 호스트는 IPv4 네트워크의 호스트 X와 통신하고 DSPN C 호스트는 IPv6 네트워크의 호스트 Y와 통신한다고 가정한다. 이때 DSPN 호스트들은 통신하려는 호스트의 IP 주소를 얻기 위해 일반적인 DNS 해석 과정을 거쳐 상대호스트가 IPv4 호스트인지 IPv6 호스트인지를 알게 된다. 얻어진 IP 주소의 버전에 따라 자동으로 발신지 주소(IPv4 또는 IPv6)가 선택되고 데이터 패킷이 생성된다. 생성된 패킷은 일반 라우팅에 의해 IPv4/IPv6 통합 연동기로 전송된다. 패킷을 수신한 IPv4/IPv6 통합 연동기는 패킷의 IP 프로토콜 버전에 따라 데이터 플로우 식별 테이블에 새로운 테이블 엔트리를 추가할 것인지 일반 IPv6 라우팅을 수행할 것인지를 결정하게 된다. 예를 들어 DSPN A에서 IPv4 호스트 X로 전달되는 데이터 패킷이면 패킷 헤더 정보를 이용하여 데이터 플로우 식별 엔트리를 <프로토콜 식별자, A의 MAC 주소, Y의 IP 주소, 발신지 포트, 목적지 포트>로 구성된다. 이 식별 엔트리는 IPv4 호스트 X에서 DSPN 호스트 A로의 응답 패킷 전송을 위해 이용된다.

## 4. 결 론

본 논문에서는 보안과 프라이버시 이유로 구축되었던 IPv4 사설망 네트워크에서 IPv4/IPv6 망과의 연동을 지원하는 통합 연동기를 설계하였다. 설계된 연동기는 End-to-End connectivity를 지원하며 단지 참조에 의해 데이터 플로우를 구별하므로 라우터 포워딩 성능을 저하하지 않고, IPSec과 같은 보안 통신을 위한 프로토콜을 지원하며 단지 하나의 IPv4 주소를 이용하여 IPv4/IPv6 망과의 연동을 지원하는 특징을 갖는다.

향후 연구 과제로는 효과적인 구현을 위한 방안 모색과 양방향 통신을 지원하는 통합 연동기 구현을 위해 기존의 DNS_ALG 기능을 확장하여 구현하는 것이다.

## 5. 참고문헌

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

[2] A. Conta, S. Deering "Generic Packet Tunneling in IPv6 Specification," IETF RFC 2473, December 1998.

[3] A. Durand, P. Fasano, I. Guardini, CSELT S.p.A., D. Lento "IPv6 Tunnel Broker," IETF RFC 3053, January 2001.

[4] J. Bound, et al., "Dual Stack Transition Mechanism (DSTM)," IETF dratf-ietf-ngrans-dstm-08, June 2002.

[5] G. Tsirtsis, P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)," IETF RFC 2766, February 2000.

[6] K. Tsuchiya, H. Higuchi, Y. Atarashi, "Dual Stack Hosts using the 'Bump-In-the-Stack' Technique (BIS)", IETF RFC 2767, February 2000.

[7] Kwang-Hee Lee, Hoon Choi, "FSL3/4 on NEDIA (Flow Separation by Layer 3/4 on Network Environment using Dual IP Address," LNCS 3090, pp. 1015-1024, 2004.