IPv4 네트워크와 IPv6 네트워크 간의 연동

o
김상범, 김두석
한국통신 통신망연구소 통신망기술연구팀 데이터망제어연구실
305-390 대전 유성구 전민동 463-1
전화:(042)870-8322, 팩스:(042)870-8279

A study on the interworking between IPv4 network and IPv6

Sahng-Beom Kim, Doo-Seok Kim
Telecommunication Network Research Lab., Korea Telecom
463-1, Jeanmin-dong, Yusung-gu, Taejeon, 305-390, Korea
ksbn@kt.co.kr

Abstract

In this paper, we consider the interworking methods for Internet layer 3 protocols. The legacy protocol for Internet is IPv4(IP version 4). The ability of IPv4 is not enough for modern real time multimedia communication services. So IPv6(IP version 6) protocol was suggested to resolve the problems of IPv4. 6Bones(IPv6 Backbones) have also constructed from 1996 in many countries. The 6Bones should be interoperatable to the legacy internet. To support all data services including voice and video, IP protocol should be enhanced because the characteristics of modern network services are requiring QoS(Quality of Service) functions, plug and play, security, mobility and so on. So a new IP protocol, IPv6, has been developing to meet the requirements. In this paper, some migration methods for internets are described. We first describe the protocol compatibility problems and suggest some solutions and scenario to solve the problems.

1. 서론

기존 인터넷에서 사용하는 TCP/IP 프로토콜에서 IPv4 프로토콜이 주로 사용되어 왔다. 1970 년대에 미국방성에서 개발하고 인터넷에서 사용되어 온 IPv4 프로토콜은 보편화되었고, 비교적 안정적으로 운영되고 있다.

근래에 들어 인터넷 분야에서 음성 서비스와 데이터 서비스는 통합된 네트워크에서 제공되도록 요구되고 있고, 한편 실시간 멀티미디어 서비스가 제공되는 인터넷을 사용자가 원하고 있다. 또한 서비스 품질(QoS)[1]의 차별화에 따른 요금 책정, 단말 이동성 제공, 보안 기능 등은 인터넷 사업자가 향후 확보해야 할 기능이다.

인터넷에서 IPv4 에 대한 기능 강화가 현재 요구되고 있으며, 한편 기존 32 비트로 구성된 IPv4 주소의 고갈 문제가 현재 언급되고 있다.

인터넷 진화와 더불어 점점 가용한 IP 주소 부족 현상이 일부 지역에서 발생하고 있고, 새로운 서비스 도입에 따른 IP 프로토콜의 기능 추가가 요구되고 있다. 이에 따라 IETF(Internet Engineering Task Force) 표준화 단체에서 새로운 IP 프로토콜을 규격화하고 있으며, 이를 IPv6 라고 한다. IETF 중심으로 차세대 인터넷 프로토콜이 연구되어 왔고 1995 년에 IPv6 규격[3]을 발표하였다. 현재 IPv6 관련 규격들은 IETF draft 를 통해 계속 수정 및 보완이 되고 있다.

데이터 네트워크인 기존 인터넷이 VoIP(Voice over IP) 기능을 확보하게 되면 인터넷이 전화망과 같은 일반 음성 통신 네트워크를 수용할 수 있다. 그러나 IPv4 를 기반으로한 기존 인터넷은 만족스러운 QoS 확보가 어렵고, 근래에 시도되고 있는 실시간 멀티미디어 관련 서비스를 네트워크 상에서 제공하기가 곤란하다.

Best-effort 서비스를 특징으로 하고 있는 기존 IPv4 프로토콜 기반의 인터넷은 사용자의 급증 문제에 직면하고 있고 앞서 언급한 문제를 해결하기가 곤란하다. 이러한 문제에 대해 IETF 를 중심으로 수 년 동안 연구한 결과 IPv4 프로토콜을 IPv6 로 대체해야 한다는 결론을 내렸다.

1996 년부터 몇 개의 국가에서 IPv6 관련 프로토콜을 호스트와 라우터에 구현하여 6Bone 구축을 시도하여 왔다. 최근에는 각국의 차세대 인터넷에서 기본적으로 6Bone 을 구현하고 있다.

IPv6 관련 프로토콜이 새로운 기능을 제공해도 기존 IPv4 를 기반으로 한 인터넷과 10 년 이상 공존이 불가피하다. 따라서 IPv4 네트워크가 IPv6 로 자연스럽게 진화될 방식이 요구된다. 이를 위해 현재 IETF 의 ngtrans(next generation transition) 그룹에서 연구가 활발히 진행되고 있다.

본 논문에서는 IPv4 와 IPv6 의 연동문제에 개해 언급한다. 본 논문의 2 장에서는 IPv6 프로토콜의 특징을 IPv4 비교하여 기술한다. 3 장에서는 기존에 발표된 IPv4 에서 IPv6 로 이행되는 방식을 언급하고 그에 대한 문제점을 도출한다. 4 장에서는 IP 프로토콜의 호환 시나리오를 제시하고, 5 장에서는 결론 및 추후 연구과제에 대해 언급한다.

2. IPv6 의 특징

기존 TCP/IP 프로토콜이 기본이 되었던 IPv4 는 상당히 안정적인 측면이 있으나, 인터넷 사용자의 급증과

사용자의 새로운 서비스 요청에 직면하여 많은 문제점이 노출되고 있다.

사용자의 급증은 결국 IPv4 주소 고갈의 문제를 가져온다. 이를 위해 CIDR(Classless Inter-Domain Routing)[2], Block of 'C'[2], NAT(Network Address Translation)[2] 방식이 고안되었으나 근본적인 해결책은 아닌 상태이다.

고속으로 라우팅을 처리하는데에 있어서 IPv4 헤더의 많은 필드는 불리하게 작용한다. 근래에 새로이 요구되는 데이터 서비스 제공을 위한 기술들, 예를 들면 auto-configuration 기능, QoS 지원, 전세계적 전자 상거래를 위한 보안 문제, 호스트의 이동성 지원은 기존 IPv4 프로토콜로는 해결이 곤란하다.

QoS 와 관련된 실시간 서비스 처리 문제도 IPv4 의 문제이며, 이에 대해 IPv6 에서는 새로이 헤더에 추가된 필드인 flow label 을 통해 MPLS(Multi-Protocol Label Switching) 기법을 도입할 수 있다[3]. 최근에 등장하고 있는 VoIP, Mobile IP 의 서비스 지원에 대해서도 IPv6 가 IPv4 보다 유리하다는 견해가 지배적이다.

다음 [표 1]에 IPv4 와 IPv6 에 대한 비교를 나타내었다.

[표 1] IPv4 와 IPv6 의 비교

구분	IPv4	IPv6
주소공간	32 비트	128 비트
최대 연결 가능 호스트	40 억	3.4E38 승
주소 할당 체계	A, B, C 클래스와 별도의 D 클래스	Unicast, Anycast, Multicast
헤더 필드 수	10 개(복잡)	6 개(단순)
헤더 체크 썸	있음	삭제됨
Fragmentation 정보	데이터그램마다 있음	전송기술의 신뢰도 향상으로 옵션 처리됨
Plug & Play 기능	없음	auto-configuration 기능으로 지원
QoS 지원	헤더의 TOS 필드 외에 별도의 기능이 없음	헤더에 traffic class 와 flow label 필드가 추가됨
보안 기능	별도의 IPsec 프로토콜 요구	자체 내장
Mobile IP 수용	상당히 곤란	가능

IPv6 는 멀티미디어 데이터의 실시간 처리가 가능하도록 설계되었다. 즉, QoS 개념을 도입하여 특별한 수준의 서비스 품질을 요구하거나 실시간 서비스와 같이 특수한 처리를 필요로 하는 패킷에 대해서 flow 를 정의할 수 있도록 하였다.

IPv6 만이 지닌 특징으로 보다 강화된 보안 기능을 들 수 있다. IPv4 는 보안을 염두에 두고 설계된 것이 아니기 때문에 IPsec 이라는 보안 관련 프로토콜을 별도로 설치해 주어야 했으나, IPv6 에서는 이러한 IPsec 기능을 프로토콜 내에 탑재할 수 있도록 설계되었다. 이러한 보안 및 인증 기능은 현재 비즈니스 분야에서 국제적인 전자 상거래를 위해 빠른 도입이 요구된다.

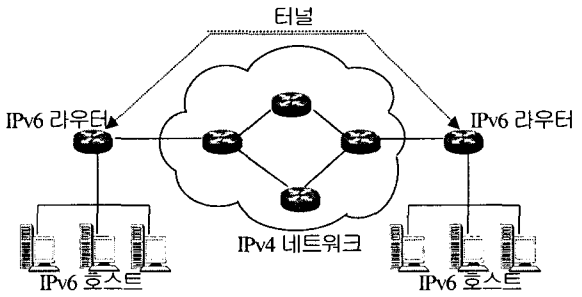
3. IPv4 에서 IPv6 로의 전이

기존의 IPv4 네트워크를 IPv6 네트워크로 모두 교체하려는 목표로 IETF 의 6Bone 계획은 시작되었다. 그러나 전세계에 펼쳐져 있는 기존의 IPv4 네트워크를 IPv6 네트워크로 진화시키는 문제가 쉽지 않다.

국제 6Bone 을 구축하는 현재의 방법은 다음과 같다. 일단 IPv6 를 사용하는 지역적인 네트워크를 아일런드로 구성하고, 6Bone 아일런드 사이를 주로 터널링 기법을 써서 기존 IPv4 네트워크를 터널로 이용하는 방법이 있다. 이 경우 QoS 측면에서 만족스럽지 못하다.

IPv4 헤더 Encapsulating 노드에서 추가 Decapsulating 노드에서 제거	IPv6 헤더	데이터

[그림 1] Encapsulation 된 IPv6 패킷

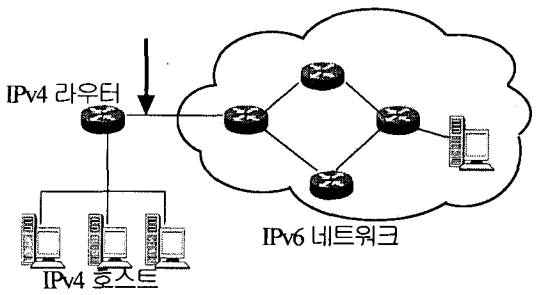


[그림 2] IPv6 터널링 방식

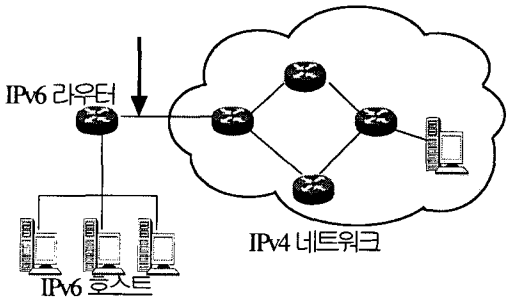
서로 다른 6Bone 에 속해 있는 호스트 간에 통신은 앞서 기술한 터널링 기법으로 해결이 가능하다. 한편 [그림 3]과 [그림 4]에 나타낸 것과 같이 IPv4 호스트가 6Bone 내의 호스트와 통신할 경우와, IPv6 호스트가 IPv4 네트워크의 호스트와 통신할 경우가 지원되어야 한다. 이를 위해 IPv6 측 주소를 IPv4 측 주소와 호환성있게 사용하자는 의견이 있다. 그러나 이러한 방식은 결국 IPv6 의 주소 공간을 32 비트로 제한시키므로 현실적이지 못하다.

[그림 3]과 [그림 4]의 화살표 위치에 주소 또는 프로토콜 변환기를 설치하여 IPv4 네트워크와 IPv6 네트워크를 연동시키는 방법이 최근 발표되고 있다. 그러

나 [그림 5]에 나타낸 IPv4 헤더 필드인 ver, TOS(Type Of Service), total length, TTL 과 IPv6 헤더 필드인 ver, traffic class, payload length, hop limit 간의 상호 변환은 가능하나 기타 필드의 변환은 곤란하다.



[그림 3] IPv4 호스트와 6Bone 내의 호스트와의 통신



[그림 4] IPv6 호스트와 IPv4 네트워크의 호스트와의 통신

IP 와 ICMP 에 대한 프로토콜 변환기[6]를 사용하여 앞서 언급한 IPv4 주소와 IPv6 주소의 매핑 문제 해결이 제안되고 있다. 이 경우 사용하고 있지 않은 IPv4 주소를 모아서 일종의 pool 형태로 저장하고, IPv6 패킷이 IPv4 네트워크로 들어올 때, pool 에 있는 IPv4 주소의 헤더를 IPv6 헤더에 대응시키는 방식이다. 이 방식 역시 IPv6 의 옵션 헤더는 변환되지 못하고 IPv6 헤더 필드의 일부 정보는 유실된다.

네트워크 주소 변환 및 프로토콜 변환기[7]는 주소 변환 뿐만 아니라 IP 와 ICMP 프로토콜 자체를 변환기에서 변경시켜야 헤더 필드 정보의 유실을 방지할 수 있다고 제안되고 있다. 그러나 이 경우에도 IPv6 의 보안 기능은 상실된다. 한편 DNS 내용의 변경도 요구한다.

IPv6 호스트에 IPv4 주소 할당기[8]는 주소 변환을 피하려는 방법이나, 기본적으로 라우터와 IPv6 에 대한 가정이 만족되어야 하고 별도 서버의 도입이 필요하다. 또한 서로 분리된 DNS 서버를 필요로 하며 DHCP 와 DNS 서버의 통신 문제를 해결해야 한다. 한편 라우터가 IPv4 와 IPv6 를 모두 지원해야 하는 단점이 있다 [9].

주소 분류 변환기[10]의 경우 IPv4 에서 IPv6 로 가는 패킷에 대한 제안된 주소 변환기가 사실상 구현이 불가능하다.

현재로서는 IPv4 네트워크가 IPv6 로 진화해 가는 과정에서 요구되는 IPv4 헤더와 IPv6 헤더 간의 변환문제에 대해, IPv4/IPv6 간의 주소만을 변환하는 것은 가능하고 이미 구현도 되어있다.

그러나 주소 정보 이외에 상이한 IPv4 헤더 필드와 IPv6 헤더 필드에 대한 모든 정보를 변환할 수 있는 만족스러운 해결책이 현재 없는 상황이다.

IPv6 헤더 구조

ver	T_class	Flow Label	
Payload Length		N_header	Hop Limit
Source Address			
Destination Address			

IPv4 헤더 구조

ver	H_length	TOS	Total Length	
identification			flag	F_offset
TTL	protocol		Header checksum	
Source Address				
Destination Address				
options				

[그림 5] IPv6 와 IPv4 의 헤더 구조

4. IP 프로토콜의 진화 시나리오 제안

성공적인 IP 프로토콜의 진화는 전체 IPv6 네트워크와 전체 IPv4 네트워크의 호환성 여부에 달려 있다. IPv6 네트워크는 점진적으로 IPv4 네트워크를 수용해 나아가야 한다. 당분간 IPv4 를 사용하는 호스트 및 라우터와 IPv6 를 사용하는 호스트 및 라우터가 공존하게 된다. 현재 IP 프로토콜을 진화시키려면 IPv4 프로토콜과 IPv6 프로토콜의 호환방식이 필요하다. 그러나 IPv4 헤더와 IPv6 헤더 간의 변환이 이루어질 때 주소 공간의 차이와 서로 다른 형태의 헤더 특성 때문에 필드 정보가 정확히 변환되기 어렵다.

대규모 네트워크에 실현 가능한 IP 프로토콜 호환 시나리오는 다음과 같다. 일단 헤더 정보 변환은 주

소와 QoS 제공에 필요한 필드를 우선하도록 한다. 6Bone 내에 추가되는 호스트와 라우터는 한시적으로 이중구조(IPv4 와 IPv6 를 모두 지원)화하도록 한다. 이중구조를 지닌 네트워크 장비가 동일한 시간에 IPv4 와 IPv6 의 2 개의 프로토콜을 함께 지원할 수 없으나[11], 6Bone 내의 호스트가 IPv4 네트워크의 호스트에 쉽게 접속하려면 이중구조를 가질 필요가 있다.

현재 소규모 네트워크에 대한 IPv4/IPv6 호환기는 부분적으로 개발되고 있으나, 아직 대규모 네트워크의 적용은 어렵다. 대규모 네트워크를 위한 시나리오는 다음과 같다.

(1) 상이한 IPv6 네트워크 간의 통신에 있어서 네트워크 사이의 IPv4 네트워크가 존재하면 터널링 방식으로 통과한다. 이 경우 손실되는 정보는 없다. Automatic 터널링, configured 터널링[11] 방식을 사용한다.

(2) 상이한 IPv4 네트워크 간의 통신에 있어서 중간에 IPv6 네트워크가 있을 경우도 IPv6 헤더 추가/삭제를 통해 터널링 방식으로 통과한다. 이 경우도 손실되는 정보는 없다.

(3) IPv6 네트워크에 속한 호스트가 IPv4 네트워크에 속한 호스트에 접속을 시도할 때 다음 절차를 따른다.

(3-1) IPv6 네트워크의 호스트와 라우터가 이중구조를 갖고 있다면 IPv4 방식으로 접속한다.

(3-2) 위의 경우가 지원되지 않을 경우, IPv4 네트워크에서는 현재 사용하고 있지 않은 IP 주소를 파악하여 헤더 변환기에서 이를 매핑 테이블 형태로 유지한다.

(3-3) IPv6 측 호스트는 접속하려는 IPv4 호스트의 IP 주소를 IPv4-compatible 주소 형태로 IPv6 헤더의 destination 주소 필드에 기록한다.

(3-4) 헤더 변환기에서 IPv6 측 호스트의 source 주소를 매핑 테이블에 있는 IPv4 주소로 대체하고 두 주소 간의 매핑 관계를 매핑 테이블에 기록한다.

(3-5) 헤더 변환기를 통해 IPv6 헤더를 IPv4 헤더로 변환한다. 이 때 IPv6 의 Traffic Class 필드는 QoS 와 관련이 있으므로 IPv4 의 TOS 필드에 매핑시킨다.

(3-6) Destination 에 해당하는 IPv4 네트워크의 해당 호스트가 sourece 호스트로 패킷을 보낼 때는 위의 역순을 따른다.

(4) IPv4 네트워크에 속한 호스트가 IPv6 네트워크의 호스트로 패킷을 보내는 경우에는 IPv4 의 32 비트 주소공간으로는 IPv6 의 128 비트 주소공간을 수용할 수 없으므로 어려움이 따른다.

(4-1) IPv4 호스트와 라우터가 이중구조를 갖고 있으면 IPv6 방식으로 접속한다.

(4-2) 위의 경우가 지원되지 않을 경우, destintion 주소인 IPv6 네트워크의 호스트의 주소가 IPv4-compatible 주소라는 것을 IPv4 source 호스트 헤더의 특정 필드를 통해 알려 온다면, IPv4 네트워크에서 보내진 32 비트 헤더를 헤더 변환기에서 128 비트의 IPv4-compatible 주소로 변환한다.

(4-3) QoS 관련 사항은 (3-4) 과정을 따른다.

(4-4) IPv4 헤더를 IPv6 헤더로 헤더 변환기에서 변환한다.

(4-5) IPv6 에 해당 호스트가 IPv4 source 호스트로 패킷을 보낼 때는 위의 역순을 따른다.

(4-6) 32 비트 주소 공간을 갖고 있는 IPv4 패킷은 128 비트의 IPv6 주소 공간의 내용을 수용할 수 없으므로 destination 에 해당하는 IPv6 주소가 IPv4 compatible 주소가 아닌 IPv4 패킷은 헤더 변환기에서 되돌려 보낸다.

5. 결론 및 추후 연구과제

본 논문에서는 차세대 인터넷 프로토콜로 인정되고 있는 IPv6 가 전체 인터넷에 자리잡기 이전에 필요한 IPv4 와 IPv6 의 공존 기간에 요구되는 진화 시나리오를 기술하였다.

대규모 네트워크에서 IPv4 주소와 IPv6 주소를 모두 관리하는 것은 복잡한 작업이다[12].

본 논문에서는 주소와 QoS 관련 필드 위주의 헤더 변환을 제안하였고, 이중구조를 갖는 경우와 이중구조를 갖지 않는 경우에 대해 IP 프로토콜의 진화 시나리오를 제시하였다.

참고문헌

[1] P. Ferguson and G. Huston, *Quality of Service: delivering QoS on the Internet and in corporate networks*, John Wiley & Sons, 1998.

[2] A. Tang and S. Scoggins, *OPEN NETWORKING WITH OSI*, Pretice Hall, 1992.

[3] S. Deering and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 1883, Dec. 1995.

[4] C. Huitema, *Routing in the Internet*, Prentice Hall, 1995.

[5] APAN, http://cache.jp.apan.net/index.html

[6] WIDE, http://endo.wide.ad.jp/index.html

[7] E. Nordmark, Stateless IP/ICMP Translator(SIIT), INTERNET-DRAFT, Dec. 1998.

[8] G. Tsirtsis and P. Srishuresh, Network Address Transition – Protocol Translation (NAT-PT), INTERNET-DRAFT, Jan.1999.

[9] J. Bound, Assignment of IPv4 Global Addresses to IPv6 Hosts (AIIH), INTERNET-DRAFT, Jan. 1999.

[10] L. Toutain, H. Afifi, Dynamic Tunneling: A new method for the IPv4-IPv6 Transition, INTERNET-DRAFT, Dec. 1998.

[10] K. Yamamoto and M. Sumikawa, Categorizing Translators between IPv4 and IPv6, INTERNET-DRAFT, Nov.1998.

[11] R. E. Gilligan and E. Nordmark, Transition Mechanism for IPv6 Hosts and Routers, INTERNET-DRAFT, Aug. 1998.

[12] T. Larder, Transition Scenarios and Solutions, INTERNET-DRAT, Apr. 1999.