IPv6 프로토콜 LAN 설계 및 구축

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

A Design and Implementation of IPv6 LAN

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 describe the design and implementation of IPv6 LAN. 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. We implemented IPv6 LAN using sTLA(sub Top Level Aggregation identifier) address and KOREN(KOrea Research and Experimental Network). Our IPv6 LAN is connected with 6TAP(Chicago), WIDE(Tokyo), and SingAREN(Singapore). We used a dedicated router, Windows 2000 PC host, FreeBSD PC host, Solaris 7 workstation and Solaris 8 workstation for IPv6 NDP(Neighbor Discovery Protocol) protocol test. 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, auto-configuration, security, mobility and so on. So a new IP protocol, IPv6, has been developing to meet the requirements. In this paper, we introduce the implementation method and configuration information of IPv6 LAN.

1. 서론

TCP/IP 프로토콜의 기본인 IPv4 프로토콜은 최근 인터넷 사용이 폭발적으로 증가하여 향후 인터넷 주소 부족 문제를 안게 되었고, 데이터 서비스에서 필요한 새로운 기술 도입이 곤란한 프로토콜이 되었다. 20 년 이상 사용되어 온 IPv4 프로토콜은 네트워크 기술의 발전과 인터넷의 사용증가로 주소 부족 문제뿐만 아니라 근래에 요구되는 데이터 서비스에서 필요한 새로운 기술들, 예를 들면 auto-configuration 기능, QoS[1], 보안, 단말기의 이동성 지원과 같은 새로운 기술 도입에 적합하지 않다.

IPv4 프로토콜의 문제점을 인식한 IETF 에서는 1992 년 2 월 차세대 IP(IPng)에 관한 제안을 공모하여, 1995 년 1 월 RFC 1752 로 "The Recommendation for the Next Generation Protocol"[2]을 발표함으로써 IPv6 프로토콜의 모습이 가시화되기 시작했다. 현재는 다수의 표준화된 RFC 문서가 새로운 인터넷 프로토콜인 IPv6 에 대해 언급하고 있다.

본 논문에서는 차세대 인터넷에서 향후 사용되어질 IPv6 프로토콜 관련 기술을 위한 실험용 IPv6 네트워크를 구축하여 IPv6 관련 실험을 하고, 그 결과를 분석한 내용을 제시한다.

차세대 인터넷의 OSI 계층 3 프로토콜에 해당하는 IPv6 에 대한 테스트 네트워크를 구축하고, 네트워킹 기술을 검증하며, 서로 다른 운영체제를 갖는 단말 간의 호환성 여부 문제가 본 논문의 기초적 내용이다. 또한 IPv6 sTLA 주소배정 방식과 IPv6/IPv4 호환기술에 대한 분석도 본 논문 내용에 포함된다.

본 논문의 2 장에서는 IPv6 특징이 IPv4 와 비교되어 서술된다. 3 장에서는 실험에 사용된 국제 IPv6 네트워크 구축에 대해 설명한다. 4 장에서는 IPv6 주소 배정 규칙에 대해 언급하고, 5 장에서는 IPv6/IPv4 호환 기술 분석 내용이 서술된다. 6 장에서는 결론 및 추후 과제에 대한 내용이 포함된다.

2. IPv6 의 특징

기존 TCP/IP 프로토콜이 기본이 되었던 IPv4 는 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)[3], Block of 'C'[3], NAT(Network Address Translation)[3] 방식이 고안되었으나 근본적인 해결책은 아닌 상태이다.

고속으로 라우팅을 처리할 경우, 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, 사용자 단말의 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[1]. 최근에 등장하고 있는 VoIP, Mobile IP 의 서비스 지원에 대해서도 IPv6 가 IPv4 보다 유리하다는 견해가 지배적이다.

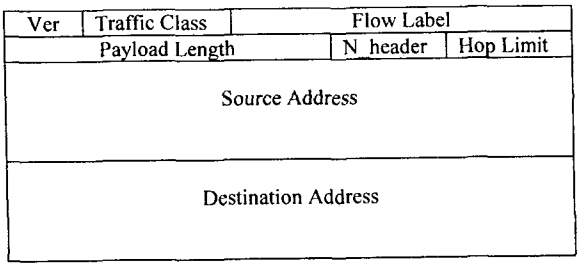
다음 [표 1]에 IPv4 와 IPv6 에 대한 비교를 나타내었다.

[표 1] IPv4 와 IPv6 의 비교

구분	IPv4	IPv6
주소체계	32 비트	128 비트
최대 연결 가능 호스트	40 억 개	3.4E38 승 개
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	헤더에서 Traffic Class 와 Flow Label 필드가 지원
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.

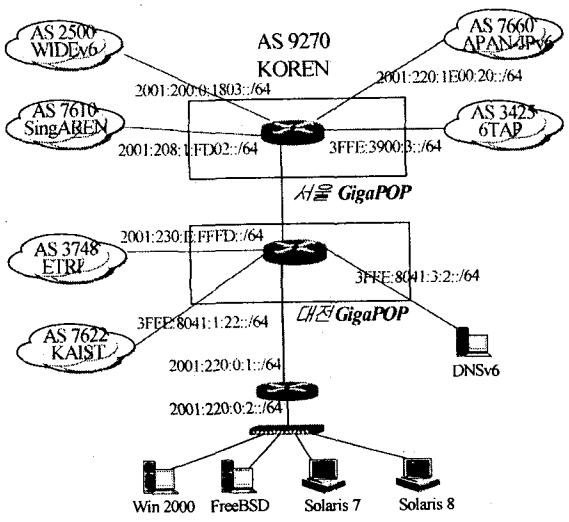


[그림 1] IPv6 헤더 구조

3. IPv6 LAN 구축

본 실험에 사용된 IPv6 LAN 의 전체 구성도는 [그림 2]와 같다. AS 9270 의 KOREN 과 연결된 실험실 LAN 은 미국 시카고의 6TAP 과 연결되어 안정적인 국제 IPv6 네트워크를 통한 실험이 가능하다.

실험에 사용된 단말은 운영체제 간의 상호운용성 파악을 위해 Windows 2000 PC, FreeBSD 3.5.1 PC, Solaris 7 및 Solaris 8 워크스테이션이 사용되었다. 실험에 따르면 단말의 운영체제 간의 상호운용성은 만족스러운 결과를 나타내었다.



[그림 2] 구축된 IPv6 LAN 구성도

IPv6 의 터널링 방식은 QoS 측면에서 만족스럽지 않은 결과를 보인다. 현재 구현된 IPv6 IGP 가 RIPv6 이고, 터널링된 IPv6 네트워크에서 한 hop 은 실제로 IPv4 네트워크에서 여러 라우터를 통과하게 된다. 결국 IPv6 터널링은 IPv4 네트워크에서 발생하는 문제를 그대로 수용하게 되기 때문에 터널링 방식은 production 수준의 IPv6 네트워크에서는 채택하지 않는 방식이다. 본 실험에 사용된 IPv6 네트워크는 native IPv6 over ATM 방식으로 구축되어 매우 안정적인 운용 결과를 나타내었다.

해외 IPv6 사이트 접속 실험에 사용된 IPv6 web 서버 목록은 다음 URL 에 있다.

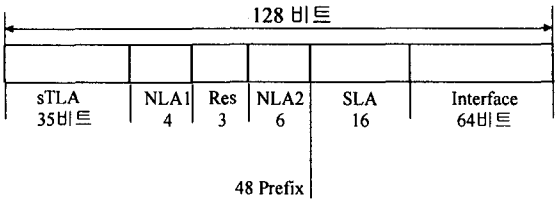
http://www.ipv6.org/v6-www.html

4. 적용된 IPv6 주소 체계

본 실험에 사용된 IPv6 주소는 ICANN(Internet Corporation for Assigned Names and Numbers) 산하의 인터넷 주소관리 기관인 APNIC(Asia Pacific Network

Information Center)에서 할당받은 sTLA 2001:220::/35 주소공간에 있는 공식 주소이다.

APNIC 은 sTLA 를 할당받은 ISP 가 주소를 배정할 때, /48 prefix 로 가입기관에 IPv6 공식주소를 배정하도록 규정하고 있다[6]. 이에 따라 2001:220::/35 sTLA 는 [그림 3]과 같은 주소체계를 수용하게 되었다.



[그림 3] 적용된 IPv6 주소체계

사용자 단말의 LAN 카드에는 MAC 주소가 정해져 있다. MAC 주소로부터 EUI-64 주소가 도출되면 이는 IPv6 주소체계에서 Interface 64 비트로 사용된다. IPv6 라우터는 128 비트의 IPv6 주소에서 상위 64 비트를 결정하여 사용자 단말에 보내준다. 이러한 과정으로 사용자 단말의 128 비트 IPv6 주소는 자동으로 설정된다. 본 실험에 사용된 라우터는 2001:220:0:2::/64 를 단말에 보내도록 설정하였다. 이러한 auto-configuration 기능은 모든 단말에서 원활히 수행되었다.

IPv6 공식주소는 현재 /35 prefix 로 ISP 에게 할당되고 있다. 그리고 /48 prefix 로 가입기관에게 주소를 배정하도록 규정되어 있다. 실제로 ISP 가 IPv6 주소 계획을 결정할 때, 고려될 수 있는 부분은 13 비트 NLA 부분으로 제한된다. 만일 한 ISP 가 IPv6 네트워크와 관련하여 여러 사업을 시도한다면, 각 사업 별로 sTLA 를 할당받는 것이 주소 체계 계획에 있어서 무리가 없다.

DNSv6 는 FreeBSD PC 에 BIND 8 방식으로 구현되었다. BIND 8 은 IPv6 에 대해 'AAAA' 구분자를 사용하고 있다. 최근에는 'A6' 구분자를 사용하는 DNSv6 가 제안되고 있으며, 이를 수용한 것은 BIND 9 이다.

5. IPv6/IPv4 호환기술

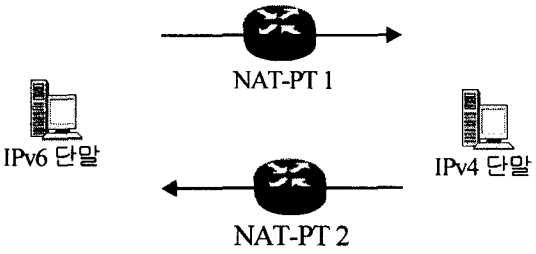
현재 다수의 IPv6/IPv4 프로토콜 호환기술이 제안되어 있다. 터널링 방식은 IP 패킷의 encapsulation 과 decapsulation 과정을 통해 IPv4 네트워크를 통과하는 기법이며, 이는 IPv6/IPv4 호환기술로 수용하기에는 곤란하다.

ISP 는 사용자 단말의 수정을 요구하지 않는 IPv6/IPv4 호환기술을 채택하는 것이 바람직하다. 이러한 IPv6/IPv4 호환기술로는 NAT-PT[4] 기술과 Transport Relay 호환기술[5]이 있다. 한편 사용자 단말의 수정을 통해 IPv6/IPv4 호환성을 확보하는 기술로서 BIS[7]가 있다.

5.1. NAT-PT 호환기술

NAT-PT 호환기술은 SIIT[8] 호환기술에서 주소할당 메커니즘이 결여되어 있는 부분을 보완한 기술이다. 그러나 NAT-PT 의 주소할당 메커니즘은 기존 IPv4 의 NAT[9] 기법과 유사하다. 따라서 IPv4 NAT 에서 발생되는 문제를 그대로 포함하고 있다.

NAT-PT 는 IPv4 주소 풀(pool)을 설정하고, 이를 통해 IPv6 주소를 IPv4 주소 풀에 있는 IPv4 주소와 매핑시키는 메커니즘이 사용되었다. IPv4 주소 풀에 있는 IPv4 주소가 모두 할당되어 IPv4 주소가 고갈되면 더 이상 IPv6/IPv4 호환은 이루어 지지 않는다. 데이터 통신의 기본이 되는 양방향성 통신 지원도 기존 NAT 와 마찬가지로 어렵다. 또한 보안성 지원도 곤란하다.



[그림 4] IPv6/IPv4 경계에 NAT-PT 가 2 개인 경우

[그림 4]와 같이 IPv6 도메인과 IPv4 도메인 사이에 NAT-PT 1, NAT-PT 2 등의 2 개 이상의 NAT-PT 가 연결될 경우, 패킷의 전달방향에 따라 전달되는 경로가 달라질 수 있다. 동일한 응용 프로그램에 속한 패킷이 방향에 따라 다른 NAT-PT 가 설치된 라우터를 통과하면 서로 다른 주소를 할당받는 경우가 발생한다. 어느 한 네트워크에서 보낸 패킷에 대한 응답 패킷의 source 주소가 다르면 패킷은 폐기된다. 이러한 현상을 방지하려면 IPv6 도메인과 IPv4 도메인 사이에 NAT-PT 기능을 가진 라우터는 하나만 설치되어야 한다. 이는 네트워크 확장성에 장애가 된다.

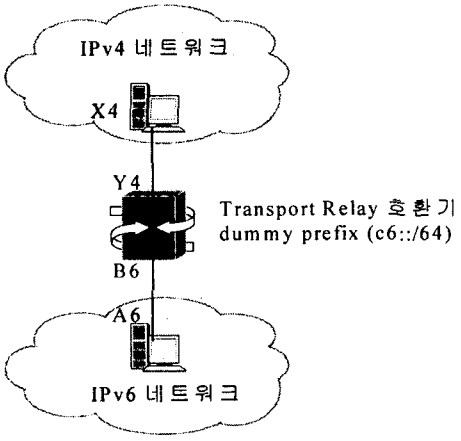
현재 사용자 단말의 수정을 요구하지 않는 IPv6/IPv4 호환기술로서 RFC 로 표준화되고 보편적으로 인정되는 호환기술은 SIIT 를 보완한 NAT-PT 기술인 상태이다.

5.2. Transport Relay 호환기술

IPv6/IPv4 호환을 NAT-PT 와 달리 IP 계층에서 처리하지 않고, TCP 와 UDP 계층에서 처리하도록 한 기술이 Transport Relay 호환기술이다. Transport Relay 호환기는 IPv6 단말과 IPv4 단말 간에 위치하여 {TCP, UDP}/IPv6 와 {TCP, UDP}/IPv4 간에 호환성을 확보한다.

네트워크의 확장성 문제는 1 차적으로 Transport Relay 호환기의 운영체제의 커널이 수용할 수 있는 connection 의 수와 프로세스가 처리할 수 있는 connection 의 수, Transport Relay 관련 프로세스의 수와

관련이 있다. 대규모 사이트에 Transport Relay 호환기술을 도입할 경우, Transport Relay 호환기를 여러 개 설치하고 서로 다른 dummy prefix를 적용하여 load-balancing을 하면된다.



[그림 5] Transport Relay 호환기 위치도

Transport Relay 호환기술은 IP 계층이 아닌 {TCP, UDP} 계층에서 정보 교환이 이루어 지므로 IPv6와 IPv4의 헤더 구조 차이를 극복할 수 있다.

[그림 5]에서 IPv4 단말의 주소가 10.1.1.1 이라고 가정하면 IPv6 단말의 주소 A6는 c6::10.1.1.1 의 목적지 주소를 지정한다. IPv6 단말 A가 IPv4 단말 X로 통신을 시도하면 Transport Relay 호환기는 일단 A로부터 들어오는 패킷을 수용한다. 그리고 우선 {TCP, UDP}/IPv6를 통해 {TCP, UDP} 연결을 시도한다. Transport Relay 호환기는 목적지 주소 끝 부분의 32 비트를 참조하여 IPv4 단말의 주소를 파악한다. 파악된 IPv4 단말의 주소는 Y4가 되고, 이 주소를 참조하여 {TCP, UDP}/IPv4를 통해 {TCP, UDP} 연결을 시도한다. 이후 {TCP, UDP} 계층을 통해 트래픽이 A 단말에서 X 단말로 흘러간다.

Transport Relay 호환기술은 IPv6 단말이 IPv4 단말에 통신을 시도할 경우에는 목적지 주소를 128 비트 공간의 끝 부분의 32 비트를 사용하면 되므로 문제없이 적용이 가능하다. 그러나 IPv4 단말이 IPv6 단말에 통신을 시도할 경우에는 DNS의 수정이 요구되며, 이에 대한 적합한 DNS 구동 방식이 지원되어야 한다.

Transport Relay 호환기술은 IPv6/IPv4 호환을 위해 특별한 DNS 서버 도입을 요구한다. 별도의 DNS 서버를 도입하지 않을 경우, 사용자 단말이 UNIX 기반 운영체제를 사용한다면 /etc/hosts 파일을 수정하여 사용할 수도 있다.

Transport Relay 시스템은 라우터에 탑재될 수도 있고, 별도의 서버를 통해 구현될 수도 있다. 이때 사용되는 라우터나 서버는 듀얼 스택 구조를 지녀야 한다.

현재 Transport Relay 호환기술은 IETF에서 공식적으로 표준화되지 않은 기술이며, INTERNET-DRAFT 상태인 기술이다.

6. 결론

IPv6 네트워크와 관련된 기본적인 표준화는 이미 IETF의 RFC를 통해 완료되었다. IPv6 프로토콜과 IPv4 프로토콜의 기본적인 차이는 NDP(Neighbor Discovery Protocol)과 ARP(Address Resolution Protocol)에 있다. IPv6는 NDP를 통해 auto-configuration, 패킷의 best path 지정, 계층 2의 주소 파악, default 라우터 리스트 작성이 진행된다[10]. 따라서 IPv6는 계층 2에 대해 독립적으로 구현된다.

IPv6 프로토콜이 지닌 많은 장점 중에서 현재 ISP에게 우선적으로 고려되고 있는 부분은 광범위한 주소체계에 있다. 네트워크의 특성상 새로운 프로토콜이 짧은 기간에 기존 네트워크에 적용하기는 어렵다. 따라서 새로운 인터넷 프로토콜이 도입될 경우, 기존 프로토콜과의 호환성 과정을 거쳐서 점진적으로 기존 네트워크의 인프라에 수용되는 방식이 바람직하다.

IPv6/IPv4 호환성 문제는 IETF의 ngtrans WG에서 계속 연구 및 보완과정을 거치고 있다. IPv6 프로토콜 사용자가 기존의 많은 IPv4의 응용 프로그램을 그대로 사용하려면 만족스러운 IPv6/IPv4 호환기법이 제공되어야 한다. 만족스러운 호환기법은 IPv6 네트워크의 확산 속도를 증가시킬 것이다.

참고문헌

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

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

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

[4] G. Tsirtsis and P. Srisuresh, "Network Address Translation – Protocol Translation (NAT-PT)," RFC 2766, Feb. 2000.

[5] Jun-ichiro itojun Hagino and Kazu Yamamoto, "An IPv6-to-IPv4 transport relay translator," Internet-Draft draft-ietf-ngtrans-tcpudp-relay-01.txt, May 2000.

[6] APNIC, "PROVISIONAL IPv6 ASSIGNMENT AND ALLOCATION POLICY DOCUMENT," Oct. 1999.

[7] K. Tsuchiya, H. Higuchi and Y. Atarashi, "Dual Stack Hosts using the "Bump-in-the-Stack" Technique (BIS)," REC 2767, Feb. 2000.

[8] E. Nordmark, "Stateless IP/ICMP Translator (SIIT)," RFC 2765, Feb. 2000.

[9] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, May 1994.

[10] S. Gai, *Internetworking IPv6 with Cisco routers*, McGraw-Hill, 1998.