

# IPv4-IPv6 주소변환을 위한 터널링 메커니즘 제안

이성협\*, 엄익준  
경북대학교 대학원 정보통신학과  
e-mail:shlee@inc.knu.ac.kr

## The Tunneling Mechanism for IPv4-IPv6 Transition

Sung-Hyup Lee\*, Ik-Jun Yeom  
Dept. of Information and Communication, graduate school,  
Kyungpook National University

### 요약

연구와 학술 목적으로 시작한 인터넷의 사용자가 급격히 증가되면서, 전세계적인 통신망을 형성하여 1970년에 시작된 IPv4의 주소체계로는 주소할당이 불가능하게 되었다. 그래서 IETF(Internet Engineering Task Force)에서는 1995년 12월에 IPv6(RFC1883)의 표준안을 제정하게 되었다[2]. IPv4에 비하여 IPv6는 주소할당 능력이 비교할 수 없을 만큼 증가되었고, IPv4의 단점을 일부 보완하여 보다 나은 주소체계를 형성하게 되었다. 하지만 기존의 IPv4의 주소체계와 IPv6의 주소체계의 호환성이 문제로 대두되었다[1]. 몇 가지의 모델로 호환성의 방법을 제시하고 있지만, 효율적이고 완벽한 방법은 최소의 비용과 가장 효율적인 터널링 방안이다. 그래서, 본 논문에서는 IPv4-IPv6 양방향 컨버터를 이용한 효율적인 터널링 메커니즘을 제안한다.

### 1. IPv4 와 IPv6 주소체계

IPv6는 현재 엔터프라이즈급 서버들 상호간이나 내부적으로 치명적인 문제를 해결하기 위한 프레임워크를 제공한다. 대규모의 네트워크에서 IPv6는 백본망 설계자들이 상당히 유동적이고 "Open-ended global routing"의 주소체계 설계를 가능하게 한다. 주요 기업이나 ISP(Internet Service Provider)들의 네트워크 밀집되어 있는 인터넷 백본망에서, 국가 또는 국제 전화체계 시스템처럼 체계적인 주소할당 시스템을 유지하는 것이 필수적이다. 대부분의 사무실 밀집형 지역의 전화 스위치들은 지역 교환을 지정하기 위해 장거리 전화의 경로는 설정하기 위해 3자리의 국가번호만이 필요하다. 이와 마찬가지로, 현재 IPv4 시스템은 인터넷 백본망에 연결되어 있는 네트워크들 사이의 데이터 전송을 위해 이러한 주소체계(haphazard)를 사용한다. 만일 이 주소체계가 없다면, 전세계에 걸쳐있는 각각의 네트워크들의 전달경

로를 백본 라우터에 라우팅 정보 형태로 테이블에 저장해두어야 한다. 현재의 IP 서브 넷 수와 인터넷 성장 속도로 비춰볼 때 라우팅 정보를 저장할 공간이 턱없이 부족하게 된다. 주소체계로 볼 때, 백본 라우터가 IP 주소 프리픽스를 사용해서 백본망을 통해서 어떤 경로를 통해 데이터가 전송되는지 결정하게 된다[2]. IPv4는 CIDR(Classless Inter-Domain Routing) 기술을 사용하면 가변적 길이의 네트워크 프리픽스를 유동적으로 사용할 수 있다. 프리픽스의 유동적인 사용으로 CIDR은 인터넷 계층적 구조의 다양한 레벨에서 상당한 "Route Aggregation"을 보장할 수 있으며, 백본 라우터가 다수의 하위레벨 네트워크들에게 수신능력을 부여할 수 있는 단일 라우팅 테이블 엔트리만으로 저장할 수 있음을 의미한다 [1]. 하지만 CIDR 라우팅의 효율성은 대규모나 과도한 계층구조에서는 보장되지 않는다. 여러 가지 경우에, Legacy IPv4의 주소들은 CIDR가 이용되기

전에 생성된다. 사실, 대부분의 IPv4 주소공간은 현재 계층적 구조로 발전되기 전에 형성이 되었다. 현재 계층적 구조의 단일화의 결과로 IPv4의 주소체계의 제한적인 면으로 인해 인터넷 주소할당이나 라우팅이 점차 모든 레벨에서 복잡해지고 있다[6]. 모든 고수준의 서비스를 공급받아야 할 객체나 개인사용자에게 문제가 되고 있다[1].

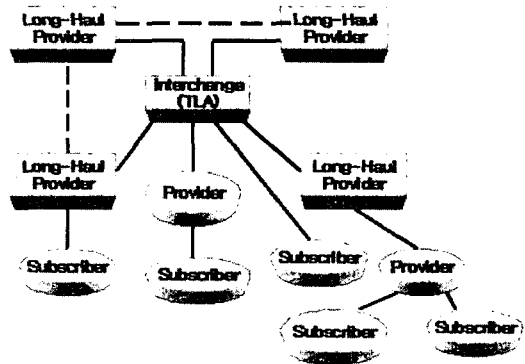
## 2. IPv4 주소체계의 문제점

인터넷 사용자의 수는 꾸준히 증가하고 있지만 IPv4 헤더의 주소구조는 고정되어 있다. 머지않아, 가용한 주소의 수가 감소함에 따라 주소의 고갈 문제가 제기될 것이다. 멀티미디어와 화상회의 같은 새로운 애플리케이션이 발전함에 따라 IP의 새로운 특성이 필요하다. 왜 새로운 IP의 개발이 필요한지에 대해 몇 가지 지적할까 한다. 인터넷 사용자의 수 증가로 IP 주소가 고갈되었다. 현재의 IP는 고정된 32비트만을 지원한다. 백본망에 있는 라우팅 테이블 또한 너무 빨리 발전하고 있다. IP 주소는 3개의 주소체계(net, subnet, host)만으로 구성되어 있으며, IP 주소 할당의 구조가 너무 거대하다. IP는 A, B, C, D 네 개의 네트워크 계층으로 되어 있다. (클래스E는 단지 특수 목적이다.) 이들 각 클래스는 네트워크와 호스트 수가 각기 다르다[5].

- Class A : 125개 네트워크, 160,000,000개의 호스트
- Class B : 16382개 네트워크, 65534개의 호스트
- Class C : 20000000개 네트워크, 254개의 호스트
- Class D : 멀티캐스트 네트워크 클래스

이뿐만 아니라, 공급자 선택성 또한 필요하다. 패킷을 전달하기 위해 특정한 공급자를 선택할 수 있어야 하며, 특별하고 신뢰성 있는 공급자를 선택하기 위해서는 인터넷의 상업적 이용이 필요하다. IP에서 멀티캐스트는 단지 서브 넷에서만 가능하다. 멀티미디어 애플리케이션에서는 이종의 서브 넷에서 다른 호스트에 주소할당을 할 수 있어야 한다. "Plug-and-Play"과 같은 이동성 제공은 특정한 환경설정이나 주소할당 체계가 필요 없이 바로 호스트에 연결이 가능함을 의미한다. 이것은 실시간의 데이터 흐름으로 호스트에 주소할당이 되는 것을 의미한다[그림1]. 이러한 특징은 화상회의와 같은 실시간 서비스에서 아주 중요하다. IPv4-IPv6에 관한 대부분의 논의는 두 프로토콜간의 주소필드 크기이다 (32비트-128비트). 하지만 중요한 차이는 충분한 라우팅 구조를 설정 가능한 발전된 계층적 주소공간을

제공하기 위한 IPv6와 IPv4의 상대적인 능력이다. IPv4는 처음으로 클래스를 기반으로 하는 주소 구조로 설계되었으며 (그림3), 주소 비트를 네트워크와 호스트로 분할했지만, 많은 하위레벨 주소들을 대표하기 위한 하나의 상위레벨 주소의 계층구조를 생성하지는 못했다.



<그림 1. IPv4 주소할당 체계 >

## 3. IPv4 - IPv6 주소변환

현재 IPv4 네트워크의 동작에 혼선 없이 IPv6를 인터넷에 어떻게 변환하는가가 문제다. 주소변환은 두 단계의 처리과정을 거칠 것이다. 첫째, 끝단에는 IPv4/IPv6용 라우터가 될 것이고, 둘째, 끝단에는 단지 IPv6용 라우터가 될 것이다. 또한, SIT(Simple IPv6 Transition)는 아래의 사항들을 제공해야한다[2].

- IPv4와 IPv6의 호스트들간의 연동 가능해야 함.
- IPv6의 라우터들과 호스트들이 거의 상호 독립적으로 인터넷에서 동작이 가능해야 함.
- 주소변환은 가능한 관리자와 일반 사용자에게 편리해야 하며, 네트워크 작업자의 이해나 작동이 용이해야 함.

SIT(Simple IPv6 Transition)는 또한 다음과 같은 특성을 가져야 한다[2].

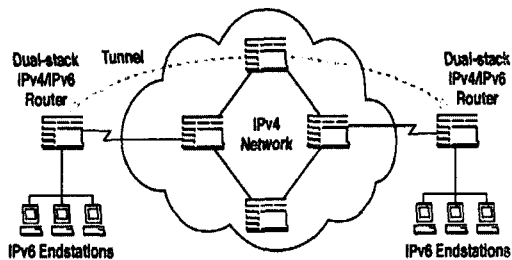
- 보다 나은 성능향상, 간편하고 쉬운 주소할당.
  - 최소한의 성능향상 특성, 적은 초기 비용 소요
- SIT(Simple IPv6 Transition)의 특성을 위해서는 동일한 메커니즘들을 제공..
- 두 가지 프로토콜로 구현하기 위한 노드들간의 직접연동과 호스트와 라우터에 이중 IP 계층(IPv4와 IPv6)의 기술을 사용.
  - IPv6의 주소 내에 IPv4의 주소를 방지하는 두 개의 IPv6의 주소 구조 보유.
  - IPv4의 라우팅 하부구조 위에 IPv6의 패킷 터널

링 메커니즘을 가져야 하며, 이 기술은 대부분의 경우에 터널 환경의 필요성에 따라 제거됨.

- IPv4와 IPv6의 헤더 내용을 해석하는 부가적인 메커니즘이 필요하고 IPv4와 IPv6에서 각기 다르게 구현.

4. IPv4-IPv6 주소변환 터널링 메커니즘

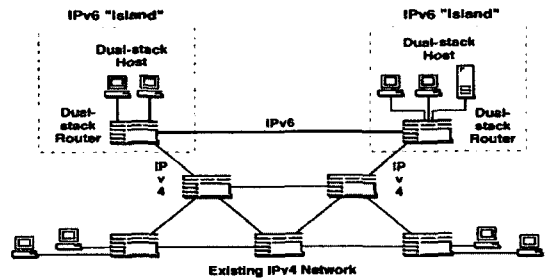
IPv4와 IPv6에서 동작하는 라우터들은 IPv4에서 동작하는 라우터들처럼 관리가 가능하다. OSPF(Open Shortest Path First)와 RIP(Routing Information Protocol)과 같은 라우팅 프로토콜의 IPv6용 버전은 이미 개발되고 있다. 많은 경우에, 관리자들은 동일한 물리적인 하부구조에서 동작이 가능할지라도 IPv4에서 분리된 IPv6를 선택할 것이다. 이것으로 개별적인 두 가지의 관리가 가능하게 된다. 다른 경우에, 동일한 영역경계, 지역, 서브 넷 조직을 사용함으로써 두 가지 구조를 결합할 수 있는 이점이 있을 것이다. 두 가지 접근 방법 모두가 이점을 가지고 있다. 분리된 IPv6의 구조는 오늘날 대부분의 기업에 제공되는 복잡하고 부적절한 IPv4의 주소할당시스템을 대체하는데 사용될 것이다. 독립적인 IPv6의 구조는 ISP 사업자들의 연결설정을 촉진함으로써 새롭고 계층적인 네트워크 주소체계를 설정할 수 있게 되었다. 이것은 라우터 상호간의 계층적 구조와 효율적인 재배열과 경로 설정이 기반이 되어야한다. IPv6를 점차 연구중인 대부분의 기구들에서는, 모든 IPv6의 호스트들이 IPv6라우터들을 각각 직접적으로 연결설정이 필요치 않은 강력한 실현성을 가진다. 대부분의 경우에, IPv4의 대양에 둘러싸인 IPv6의 섬과 같다[그림2][3].



<그림2. IPv6 섬>

다행히, IPv6의 개발자들이 IPv6가 IPv4의 네트워크들 사이에서 통신이 가능하도록 하는 주소변환 메커니즘을 개발했다. 이들 메커니즘의 필수적인 기술이 IPv4-IPv6 터널링이다[4]. 이것은 IPv4의 패킷에

IPv6의 패킷을 캡슐화하는 것이다. 터널링은 IPv4의 구성요소에 어떠한 변화도 없이 하부구조의 이점을 IPv6로 전이해서 구현 가능하다. IPv6의 구성형태의 "End-edge"상에 이중 스택 라우터나 호스트는IPv6의 패킷에 IPv4의 헤더를 첨가한다. 그리고 설정된 링크를 통해서 원래 IPv4의 트래픽으로 전송한다 [3]. IPv4 라우터는 IPv6에 대한 정보 없이도 이 트래픽을 전송한다. 터널의 다른 측면, 이중 스택 라우터 또는 호스트가 IPv6 패킷을 디캡슐시키고 표준 IPv6 주소체계의 프로토콜을 사용해서 최종

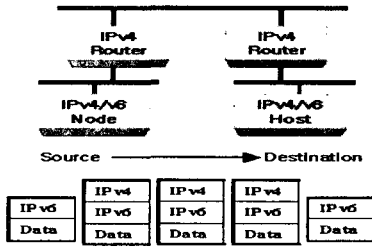


< 그림3. IPv4 네트워크상의 IPv6 터널링 >

목적지로 패킷을 라우팅 시킨다. 또한, 네트워크 관리의 필요성에 따라 IPv6 주소변환 메커니즘은 두 가지의 터널링(Automatic과 configured 터널링)을 포함한다. Configured 터널링 동작을 위해, 관리자들은 매뉴얼로 터널의 끝단에서 IPv4-IPv6의 주소 맵핑을 정의한다. 터널의 또 다른 면은, 트래픽이 완전한 128비트의 주소체계로 전송된다. 터널의 모든 점에서, 라우팅 테이블의 엔트리들은 IPv4의 주소가 터널의 통과해서 전달되는 것을 매뉴얼로 정의한다. 이것은 터널의 끝 부분에서 특정한 양의 매뉴얼 관리가 필요하지만, 트래픽은 IPv4의 라우팅 테이블의 정보가 필요 없이 동적으로 IPv4의 망을 통해서 라우팅된다. 결론적으로, 128비트의 주소를 32비트의 주소들로 일치시킬 필요는 없다[2].

4.1 기존의 터널링 방안

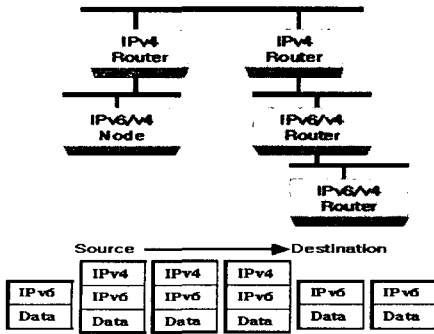
- Automatic 터널링 :이 방안은 두개의 IPv6와 IPv4의 호스트들 간에서 사용된다. 이것이 "End-to-End"다[그림3][4]. 만일 라우터가 동일한 IPv4의 네트워크영역에 IPv6/IPv4의 호스트로 IPv6의 패킷을 전송한다고 가정할 때 사용된다. 터널의 끝 부분이 목적지 호스트가 된다는 것이 중요하다[3].



<그림4. Automatic 터널링의 네트워크 구조와 패킷 구조>

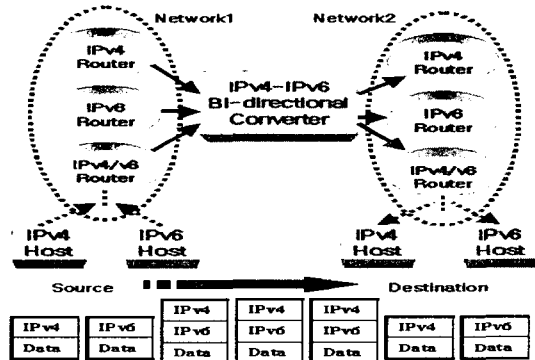
● Configured 터널링

Configured 터널링의 목적은 호스트와 터널의 끝단이 다를 때 사용된다. 이 경우에, IPv4의 헤더에 목적지 주소(터널의 끝단의 주소)가 IPv6의 목적지 주소와 간단히 맵핑될 수 없다. 터널의 끝단은 IPv6/IPv4 노드에 놓여진다[4].



<그림5. Configured 터널링의 네트워크 구조와 패킷 구조>

4.2 제안된 IPv4-IPv6 양방향성 터널링 메커니즘



<그림6. 제안된 IPv4-IPv6 양방향성 터널링의 네트워크 구조와 패킷 구조>

IPv4나 IPv6의 호스트가 네트워크1의 각기 다른 라우터들을 거쳐 네트워크2의 호스트로 패킷을 전송할 때, 출발지에서 목적지에 도달하기 위해서는 터널링을 해야한다. 본문에서 기술한 두 가지의 터널링 방안

은 목적지 호스트를 기준으로 했지만, 제안한 메커니즘에서는 호스트에서 전송된 패킷들이 라우팅되는 경로나 네트워크까지 고려했다. IPv4-IPv6 양방향 컨버터는 각기 다른 라우터를 거친 패킷들을 IP 버전에 맞게 데이터의 형식을 변환시킨다. 물론 목적지 호스트가 IPv4인지 IPv6인지를 안다는 것으로 가정한다. 목적지 호스트에서 IPv4-IPv6 양방향성 컨버터에 터널링에 필요한 정보, 즉 목적지 호스트의 IP 버전을 전송하게 된다. 이것은 약속된 메커니즘이다. 그리고 네트워크를 통과하거나 라우터를 경유할 경우 각기 다른 데이터 포맷을 가지고, IPv4-IPv6 양방향성 컨버터에서는 IPv4/IPv6의 데이터 포맷을 가지게 된다. 여기서 터널링 정보에 따라 변화된다. 어떠한 네트워크와 라우터에(IPv4 또는 IPv6) 상관없이 주소 변환이 가능하며, 이때 주소변환은 데이터 형식의 변환이 된다. IPv4와 IPv6의 확장 헤더 부분을 이용하므로 데이터의 변형이 용이하다. 제시한 메커니즘은 보다 효율적이고 가용 범위가 넓은 특징이 있다.

5. 결론

본문에서 기존의 터널링 방안들의 비효율적인 면과 적용 범위의 한계성에 대해 설명했으며 그러한 문제점들을 효율적으로 해결하기 위해 IPv4-IPv6 양방향성 컨버터를 이용한 터널링 메커니즘을 제안한 것이다. 제안된 메커니즘으로 보다 효율적이면서, 네트워크의 구성요소에는 상관없이 터널링이 수행되게 된다. 향후 연구에서는 IPv4-IPv6 양방향성 컨버터를 이용한 메커니즘의 설계와 구현이 이루어질 것이다.

참고 문헌

[1] Scott O. Brandner, Allison Mankin, "IPng(Internet Protocol Next Generation), Addison-Wesley Publishing Company, 1995.  
 [2] IETF(Internet Engineering Task Force) RFC1883, "Internet Protocol, version6(IPv6) Specification, 1995.  
 [3] Hossam Afifi, Laurent Toutain, "Method for IPv4-IPv6 Transition", ESTN Breaux, RSM Dept., 1999.  
 [4] IETF RFC2529, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", 1999.  
 [5] IETF White Paper, "IPv6", 1999.  
 [6] [Http://ganges.cs.tcd.ie/4ba2/ipng](http://ganges.cs.tcd.ie/4ba2/ipng).