차세대인터넷 전환을 위한 IPv4/IPv6망 연동 기술

The Technologies of IPv4/IPv6 Network for the Next Generation Internet Transition

2017. 10.

한국과학기술정보연구원

목 차

제 1 장 서론 및 배경

2011년 4월15일, 국내 IPv4주소 할당이 사실상 종료되면서 차세대 인터넷인 IPv6로의 전환이슈가 대두되고 있다.

현재의 인터넷 환경은 초기환경과는 다르게 지속적으로 통신기술의 발달과 통신사용자들의 저변확대, 그리고 새로운 서비스 및 다양한 서비스 요구에 의해 많은 변화가 있었지만 지금까지도 IP는 인터넷이라는 통신환경에서 중추적인 역할을 해오고 있다.

현재는 어디든 인터넷이 가능해졌고, 각종 임베디드 기기와 스마트폰이 등장하면서 유선망에서만 사용되던 인터넷이 무선 서비스에 대한 수요로 폭발적으로 증가하고 있다. 점점 다양해지는 각종 휴대형 단말을 비롯해 각종 센서 및 장치들에게 인터넷 주소가 할당되고 이들이 통신망으로 연결되어 통신하는 시나리오를 예측할 수 있다. 따라서 앞으로는 더욱 IPv4로는 도저히 감당할 수 없는 수준의 수많은 주소의 사용이 예측된다. 이에 IPv6의 128비트 주소체계를 사용하여 향후 모든 장치와 사람이 사용할 수 있도록 충분한 주소를 제공할 수 있는 IPv6로의 전환은 필수적이라고 할 수 있다.

따라서 차세대 인터넷 환경을 대비하기 위해서는 장기적인 안목을 가지고 향후 새로운 기술들에 적응할 수 있는 확장성 있는 프로토콜을 개발할 필요성이 있다. 이러한 배경에서 기존 TCP/IP의 입증된 기능들을 바탕으로 기존의 문제점을 해결하고 새로운 기술들에게 적응할 수 있도록 IPv6가 개발되어 현재 IPv6 도입 시나리오 및 각종 기반 기술들이 활발히 연구되고 있다.

본 보고서에서는 이러한 배경을 바탕으로 IPv6에 대한 간단한 개요와 IPv6 전환에 필요한 기반기술 들을 소개하고 이와 더불어 IPv6 전환에 대한 전반적인 이슈를 공유하고자 한다.

제 2 장 IPv6

2.1 IPv6 개요

IPv6는 128 비트 크기의 새로운 네트워크 주소체계를 가지는 차세대 인터넷 기반 프로토콜이며 OSI 7 Layer 참조 모델 중 네트워크 계층 기능을 구현하는 인터넷 프로토콜(Internet Protocol)이다. 인터넷 프로토콜로서의 IPv6는 주소 체계만이 아니라 네트워크 계층에서 필요한 다양한 기능의 정의를 포함한다. 따라서 막대한 수의 IP 주소를 제공할 수 있는 IPv6 주소체계는 이 IPv6 전체 표준 프로토콜 내용 중의 일부에 불과하다.

IPv6를 기반으로 하는 차세대 인터넷은 현재의 IPv4 인터넷과 전혀 다른 새로운 인터넷을 지향하기보다는 TCP/IP 체계 중 네트워크 계층(network layor)에 해당하는 IP스택(stack)이 기존의 IPv4 스택(stack)에서 IPv6 스택(stack)으로의 대체를 지향하고 있다.

IPv6에서 인터넷 프로토콜은 발전하는 인터넷 환경을 수용하기 위해 기존의 IPv4에 비해 많이 수정 보완되었다. 새 버전의 IP 주소의 형식과 길이는 패킷 형식과 함께 변화되었고 이와 관련된 여러 프로토콜이 삭제되거나 수정되었는데 IPv6의 주요 특징은 다음과 같이 요약된다.

2.1.1 IPv6의 등장

IPv4의 주소 고갈 문제 해결을 포함해 새로 그 중요도가 부각되고 있는 라우팅의 효율성, 보안 기능, 이동성 지원, QoS 보장, 편리한 인터넷 기능 제공 등을 목표로 새로 탄생한 것이 새로운 인터넷, IPv6(Internet Protocol Version 6)이다. IPv6의 등장 배경은 인터넷 주소 고갈 문제와 밀접한 연관이 있는데,

인터넷 주소 고갈 문제를 풀기 위한 임시방편으로 기존 IPv4 주소 공간을 효율적으로 재구성하는 CIDR(Classless Inter-Domain Routing), NAT(Network Address Translator), DHCP(Dynamic Host Configuration Protocol), 주소 재할당 등을 이용한 방식이 사용되고 있으나 이는 근본적인 해결책이 되지 못한다.[9]

2.1.2 IPv6의 개발 기준

IPv4의 주소 고갈 문제를 해결하고 미래를 위한 다양한 기능들이 추가된 새로운 인터넷을 개발하기 위해 IETF로부터 1993년 12월에 “IP : Next Ceneration (IPng) White Paper Solicitation"이라는 제목의 RFC 1550이 배포되었다. 이 RFC는 많은 인터넷 관계자들에게 IPng의 특정 요구 사항 또는 IPng 선택 과정 동안 고려해야 할 핵심 요소들에 관한 의견을 부탁했다. 보안 관련 견해, 대기업 사용자의 견해, 이동 통신 업계의 견해, 케이블 TV 업계의 견해를 포함하여 다양한 주제를 다루는 21개 의견이 제출되었는데 이런 문서와 백서에 대한 반응은 Scott Bradner와 Allison Mankin의 저서 IPng-Internet Protocol Next Generation[6]에서 찾아볼 수 있다. 아울러 IEEE(Institute of Electrical and Electronics Engineers)와 같은 기타 관련 조직도 IPng의 향상을 위해 의견을 제시하였다.

이들을 기반으로 IPng는 RFC 1726을 통해 그 평가에 사용될 일련의 기준을 정의하였는데, 다음과 같은 17개 기준이 제시되었다.

- 크기(scale) - 최소한 10^{12} 개의 종단 시스템(end system)과 10^{9} 개의 개별 네트워크를 식별 및 addressing 할 수 있도록 확장해야 한다.
- 토폴로지의 유연성 - 라우팅 구조와 프로토콜은 수많은 상이한 네트워크 토폴로지를 고려해야 한다.
- 성능 - 고품질 상업용 라우터는 트래픽을 그 당시 보편적이고 상용 가능한 고속 매체를 충분히 활용할 수 있는 속도로 제공해야하며 호스트는 유사한 수준의 호스트 자원을 사용하여 IPv4로 실현할 수 있는 데이터 전송 속도를

실현할 수 있어야 한다.

- 견고한 서비스 - 네트워크 서비스, 그리고 관련 라우팅 및 제어 프로토콜은 견고해야한다.
- 전환 - 프로토콜은 현행 IPv4에서 쉽게 전환될 수 있는 전환 계획을 보유해야 한다.
- 매체 독립성 - 프로토콜은 개별 링크 속도의 범위가 초당 몇 비트부터 초당 수백 기각비트에 이르는 수많은 상이한 LAN, MAN, WAN 매체의 Inter-Network에 걸쳐 작동해야 한다.
- 비연결성 데이터그램 서비스 - 프로토콜은 비연결성 데이터그램 전송 서비스를 지원해야 한다.
- 설정, 관리, 운용 - 프로토콜은 설정과 운용을 쉽게 그리고 분산할 수 있어야하며 이를 위해 호스트 및 라우터의 자동 설정이 필요하다.
- 안전성 - 안전한 네트워크 계층을 제공해야 한다.
- 이름 지정 - 어디서나 사용할 수 있는 전 세계에서 유일한 인터넷 이름을 모든 IP 계층 객체에 할당할 수 있어야 한다.
- 접근 및 문서화 - IPng를 정의하는 프로토콜과 관련된 라우팅 프로토콜은 표준 트랙 RFC로 발행되어야 하고 자유롭게 사용 가능해야 하며 구현 시 라이센스 요금이 필요하지 않아야 한다.
- 멀티캐스트 - 프로토콜은 유니캐스트 및 멀티캐스트 패킷 전송을 모두 지원해야 한다.
- 확장성 - 프로토콜은 확장될 수 있어야 한다. 프로토콜은 향후 인터넷 서비스 필요성에 맞게 진화할 수 있어야 한다. 그 뿐만 아니라 IPng 진화에 따라 상이한 버전이 동일한 네트워크에서 공존할 수 있어야 한다.
- 네트워크 서비스 - 프로토콜을 사용하는 네트워크는 패킷을 특정 서비스 등급과 연관시키고 해당 등급에 따른 서비스들을 제공할 수 있어야 한다.
- 이동성 - 프로토콜은 단말의 이동성을 지원해야 한다.
- 제어 프로토콜 - 프로토콜은 네트워크 시험 및 디버깅에 대한 기본적인 지원을 포함해야 한다.
- 사설 네트워크 - IPng를 사용하는 사용자는 기본 인터넷 인프라에서 사설

Inter-Network를 구축할 수 있어야 하며 IPng는 IP에 기반을 두거나 그렇지 않은 Inter Network를 모두 지원해야 한다.[1][3]

2.1.3 IPv6의 특성

가. 충분한 글로벌 주소

현재는 주로 PC를 이용해 인터넷뿐만 아니라 스마트 폰이나 테블릿 PC와 같은 각종 휴대형 단말을 이용하여 인터넷을 액세스하고 있다. 따라서 IPv4로는 도저히 감당할 수 없는 수많은 주소의 사용이 예측되는데 IPv6는 128비트 주소 체계를 사용하므로 미래에 모든 사람과 장치가 사용할 수 있는 충분한 주소를 제공할 수 있다. 그리고 IPv6는 언제나 어디서나 어떤 방식으로든 글로벌 인터넷 접근(특히 무선 이동 서비스)을 용이하게 하며 주소의 자동 생성 등을 지원한다.

나. 멀티캐스트(Multicast) 및 애니캐스트(Anycast) 주소

IPv4는 화상회의와 같은 실시간 통신을 필요로 하는 응용 프로그램을 위해 3계층의 유니캐스트 주소와 멀티캐스트 또는 D클래스 주소들을 제공한다. 이러한 멀티캐스트 주소 기능은 IPv6에서도 제공되는데 특히 IPv6는 멀티캐스트에 범위 개념을 도입해 멀티캐스트의 사용 및 관리의 편의성을 향상시키는 기능을 지원한다.

또한 IPv6는 애니캐스트의 그룹 유형의 주소도 제공하는데 멀티캐스트와는 달리 그룹에서 발신지에 가장 인접한 구성원만이 응답하도록 한다. 애니캐스트 주소는 매우 유용하게 사용될 수 있는데 그 이유는 애니캐스트 주소를 통해 가장 인접한 라우터나 네임 서버(name sever)에 접근할 수 있기 때문이다.

다. 인트라넷 및 인터넷의 통합

IPv6는 인터넷 및 인트라넷을 위한 통합된 어디레싱 방식을 제공한다. 이와 같은 목적을 위해 글로벌 주소 뿐 아니라 사이트 및 링크 로컬 범위의 주소를 지원한다. 사이트 주소는 인트라넷 내의 네트워크 노드를 위해 사용되며, 링크 로컬 주소는 단일 링크(라우터가 없는 소규모 네트워크)에 부착된 노드들을 식별하는데 사용된다.

라. 효율적인 LAN의 활용

IPv4가 LAN 상에서 운용될 때에는 IPv4 주소와 MAC 주소 간의 관계 및 역방향의 관계를 정해야 할 필요가 있다. IPv4는 브로드캐스트 방식의 MAC 계층 전송을 활용하는 ARP(Address Resolution Protocol)라는 보조적인 프로토콜을 통해 이와 같은 기능을 수행한다. 브로드캐스트 패킷은 모든 노드에 의해 수신되며, 모든 노드 상에서 중단(interruption)을 야기하므로 이는 시스템의 성능을 저하시킬 수 있다. IPv6에서는 ARP보다 효율적인 LAN 상에서의 인접탐색(neighbor discovery) 프로토콜을 이용하고, 브로드캐스트가 아닌 멀티캐스트 전송을 활용하여 이와 같은 비효율성을 개선한다. IPv4에서는 각 노드가 모든 브로드캐스트를 수신해야만 하는 반면, IPv6에서는 어떤 범위에서 멀티캐스트를 할 것인지를 결정한다.

마. 보안

IPv6는 전자상거래를 활성화하는 동시에 트랜잭션에 대한 대중의 신뢰도를 강화하는 새로운 서비스 및 보안 표준을 응용에 도입한다. 보안은 IPv4에서는 부가적 기능(add-on)이다. IPv4에서는 일반적으로 서버가 적당한 노드로부터 수신되고 있는지 판단하기 어렵고 발신지 주소 위장(spoofing)을 사용하여 중요한 업무 및 금융 데이터에 접근하거나 서버를 제어할 수도 있다.[2]

IPv6는 현대 기업 업무에 필수적인 인증, 보안 암호화, 데이터 무결성 보호 기능을 제공한다. IPv6 표준 기반의 인증 확장헤더는 패킷이 발신지 주소에서 안정적으로 전송될 수 있도록 보장한다. 또 다른 표준 확장 헤더는 네트워크 계층에서 종단 간 암호화를 제공하는데 이는 패킷이 조작될 가능성을 예방한다.

IPv6 보안 헤더는 호스트 간에 직접 사용하거나 추가 보안을 위해 특수 보안 게이트웨이와 함께 사용할 수 있다. IPv4 분야에서도 현재 여러 유형의 보안을 사용할 수 있지만 보안을 위해서는 근본적으로 양쪽 통신자 모두가 어떤 유형의 보안을 사용할 것인지에 대해 합의해야 하는데 이러한 공통성은 IPv6를 통해 쉽게 실현된다.

바. 라우팅

라우팅은 인터넷상의 패킷 전송을 위한 프로토콜 설계에 있어서 가장 중요한 이슈로 IPv4의 경우 클래스 C 주소에 의해 인터넷 라우터의 라우팅 테이블들이 폭발적으로 증가할 것이라는 것을 알 수 있다. 사실상 CIDR 방식이 사용되지 않는 경우 모든 단일 네트워크는 라우팅 테이블 내의 엔트리를 통보 받아야 하는데, 클래스 C 주소 블록을 사용하는 네트워크 숫자는 실로 엄청나기 때문에 라우팅 테이블은 많은 양의 메모리를 요구할 수 있다. 이에대한 한 가지 해결책으로서 CIDR 방식은 연속적인 주소들을 하나의 엔트리로 네트워크들의 블록에 통보할 수 있게 하는데 prefix를 이용해 전체 주소 비트 중 얼마나 많은 비트들이 의미를 지는 것인지를 명시함으로써 계층적인 주소할당과 라우팅을 가능하게 한다.

IPv6는 CIDR 방식의 지원을 기본으로 하며 네트워크 토폴로지와 연계된 계층적 유형의 주소 할당과 이에 따른 계층적 라우팅을 가능하게 할 수 있다.

계층적 트리의 루트에는 대륙별 주소 할당을 생각해 볼 수 있으며, 대륙 내에 차례로 ISP별, 조직별, 그리고 마지막으로 조직 내의 네트워크별 할당을 생각해 볼 수 있다. 이와 같은 모델은 라우터상의 테이블을 단순화시킬 수 있다. 또한 IPv6는 정책 라우팅이나 QoS가 포함되어야 할 가능성을 고려하고 있다. 특정한 정책을 기반으로 한 라우팅의 예로는 발신지 주소에 의해 결정된 경로 상으로 일정한 목적지로의 패킷 전송을 결정하는 라우팅을 들 수 있다. 그리고 IPv6 라우팅은 이동성을 확실하게 지원해야 한다.

사. 흐름(flow)의 개념

인터넷에서의 서비스 품질 관리를 단순화하기 위해서 흐름(flow)이라는 개념을 도입할 필요가 있다. 흐름은 일정한 방식에 의해 서로 연관된 패킷들의 연속이며 IP 계층에 의해 일관된 방식으로 다루어져야한다. 패킷들은 발신지 주소, 목적지 주소, 서비스 품질, 인증 및 보안 등과 같은 매개변수를 근거로 하여 동일한 흐름에 속할 수 있다.

흐름이라는 개념과 다른 개념들 사이에는 그 어떠한 관계도 존재하지 않는다. 예를 들어, 흐름은 몇몇 TCP 연결들을 포함할 수 있다. 또한 흐름이라는 개념은 비 연결성 프로토콜 상에서 존재하는 것이며 오류 정정과 같이 연결형 프로토콜과는 다른 목적을 지닌다. 보통 인터넷에서의 흐름은 단일노드나 노드집합을 자신의 목적지로서 가질 수 있으며, 유니캐스트 또는 멀티캐스트 흐름이 발생하게 된다. 흐름이라는 개념이 도입된 후에는 플로우 레이블(flow label)이라는 개념이 가능해지는데, 플로우 레이블을 통해 IPv6 헤더 내의 특정 필드를 예약함으로써 패킷이나 데이터그램에 표시를 할 수 있게 된다. 이와 같이 해서 IPV6는 패킷 수신 시 플로우 레이블의 검사를 통해 패킷이 어떤 흐름에 속하는지 파악하거나, 서비스품질과 관련된 패킷의 요구를 파악할 수 있는 가능성을 가지게 된다.[8]

아. 트래픽 클래스(Traffic class)

응용 프로그램이 특정 서비스 품질을 요청하지 않더라도, 때로는 주요 응용 프로그램에 의해 생성된 트래픽을 비실시간과 실시간 요구 사항 트래픽으로 차별화하는 것이 요구된다. IPv6를 사용하면 특정한 트래픽 플로우에 특수 처리를 위한 필드 값을 설정하여, 긴급하지 않은 데이터 패킷과 화상회의와 같이 고도로 민감한 실시간 응용 데이터 패킷을 구분할 수 있다. 이와 같은 목적을 위해 IPv6 헤더 내에 8비트의 “트래픽 클래스” 필드가 정의되어 있다.

2.2 IPv6 프로토콜 규격

차세대 인터넷 프로토콜인 IPv6는 IP의 새 버전으로서 IPv4를 승계하도록 설계되었으며, 다음과 같은 특징을 가진다.

2.2.1 IPv6 프로토콜 구조의 특징

가. 확장된 주소 체계 및 공간

IPv6는 IP 주소 크기를 32비트에서 128비트로 늘렸다. 이에 따라, 주소 체계가 단계적으로 증가하고, 더 많은 노드에 체계적으로 주소를 설정할 수 있으며, 자동 주소 설정이 가능해졌다. 또한, 멀티캐스트 주소에 "Scope" 필드가 추가되어 멀티캐스트 라우팅의 확장성이 향상된다. 그리고 “애니캐스트 주소”라고 불리는 새로운 주소유형이 정의되어, 그룹 내 임의의 하나의 노드로만 패킷을 보내는데 사용된다.

나. 헤더 형식의 단순화

패킷 처리 비용을 줄이고 IPv6 헤더의 대역폭 비용을 제한하기 위해 일부 IPv4 헤더 필드가 삭제되거나 확장 헤더로 되어 선택적으로 사용하게 되었다. 즉, 주소 필드로 인해 전체 기본 헤더의 길이는 IPv4보다 두 배로 확장되어 40 바이트이지만, 전체 필드 수를 12개에서 8개로 단순화시킴으로써 오히려 기본적인 처리 속도를 개선하는 효과를 가져온다.

다. 확장 및 옵션에 대한 지원 향상

IP 헤더 옵션이 인코딩되는 방식이 변했기 때문에, 포워딩의 효율성이 더욱 높아졌다. 즉, IPv4 헤더의 옵션 필드에 사용되던 헤더들이 모두 확장헤더 필드로 옮겨짐에 따라, 각 확장헤더들은 전송경로상의 모든 노드에서 처리될 필요가 없으므로 포워딩 효율이 높아졌다고 할 수 있다. 또한, 확장헤더 중에서 옵션헤더를 포함할 수 있는 헤더들은 향후 새로운 응용 서비스의 출현으로 새로운 옵션을 도입할 때 융통성을 제공할 수 있다.

라. 플로우 레이블링(Flow Labeling) 기능

송신자가 디폴트가 아닌 서비스 품질(Qos) 또는 “실시간” 서비스와 같은 특별처리를 요청하는 특정 트래픽 “플로우(flow)"에 속하는 패킷을 레이블링(labeling)할 수 있다.

마. 인증 및 사생활 보호 기능

IPv6에는 인증, 데이터 무결성 및 데이터 기밀 유지를 지원하기 위해 확장

헤더를 규정하고 있다. 즉, IPv6는 보안 기능을 반드시 구현해야 할 기본기능으로 채택함으로써, 보안 서비스 제공을 위한 효율을 향상시켰다.

이와 같은 IPv6의 기본 철학을 충족시키기 위해 아래와 같은 IPv6 패킷을 사용한다. 이 패킷은 크게 헤더 필드와 페이로드 필드로 구분되는데, 헤더 필드는 다시 기본헤더와 확장헤더로 구성된다. 기본헤더는 40바이트로 고정되어 있으며, 확장헤더는 새로운 응용들을 쉽게 수용할 수 있도록 다양한 헤더들로 구성된다.

그림 2.1 IPv6 패킷 구조

2.2.1 기본 헤더

그림에서 IPv6 기본 헤더는 40바이트의 고정된 길이를 가지면서 8개의 필드로 구성되어 있다. 각 필드의 기능에 대해서 살펴보면, 먼저 “Version" 필드는 인터넷 프로토콜의 버전을 의미하며, 여기서 IPv6 트래픽 등급을 명시해주는 필드이며, IPv4의 TOS(Type of Service) 필드와 같은 기능을 수행한다.

다음으로 IPv4 헤더에서는 없었던 “Flow label" 필드는 해당 IPv6 패킷이 속하는 흐름에 대한 특성이 있으며, 이 필드에 대한 사용 규칙은 IETF IPv6 워킹그룹에서 활발히 논의 중이다. "Payload length" 필드는 IPv6 기본헤더 다음에 이어지는 데이터들의 길이를 표시한다. 즉, IPv6 확장헤더와 상위계층 데이터의 길이이다. 이 필드의 길이는 16비트이므로 2^16(65536) 바이트만큼만 표기할 수 있다. 이보다 더 큰 경우를 지원하고자 한다면, 이 필드를 모두 0으로 채우고, 홉-바이-홉(Hop-by-Hop) 확장헤더를 이용한다. 또한, 인터넷의 모든

링크는 1,280 옥텟 이상의 MTU(Maximum Transmission Unit)를 가진 IPv6 패킷을 요구한다. 그러므로 한번에 1,280 옥텟 패킷을 전달할 수 없는 링크에서는 링크 고유의 프레그먼트와 재조립이 IPv6 아래 계층에서 제공되어야 한다.

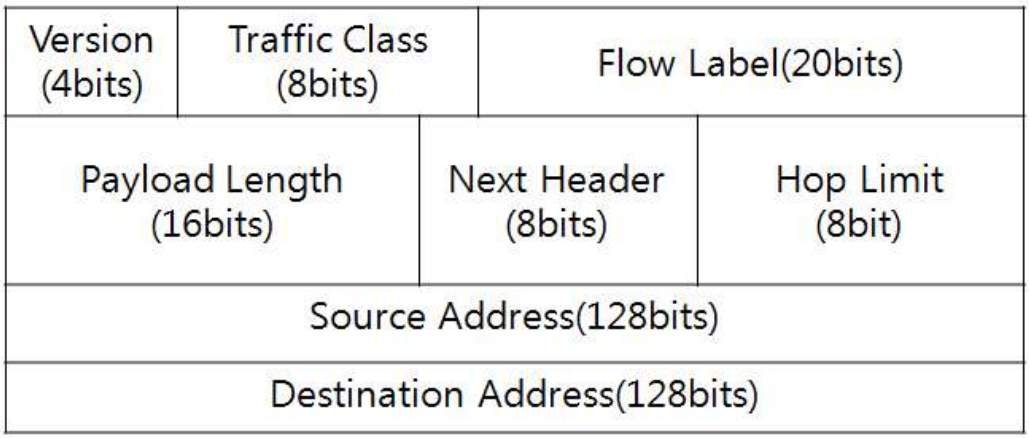

그림 2.2 IPv6 기본 헤더 구조

“Next header" 필드는 IPv6 기본헤더 다음에 위치하는 헤더의 종류를 지시한다. 예를 들어 0이면, 이어지는 헤더가 홉-바이-홉(Hop-by-Hop) 헤더임을 알려준다. 이 필드는 기타 모든 확장 헤더들에게도 포함되어, 자신 다음에 위치할 헤더 형식을 명기하기 위해 사용된다. 이처럼 모든 확장 헤더들은 자신을 식별할 수 있는 정수 값을 가지고 있으며, UDP나 TCP 등의 상위 계층 프로토콜들은 IPv4의 protocol 필드에서 사용되던 정수 값이 있으므로 그대로 이용한다. [그림2-3]은 ”Next Header"에 포함될 수 있는 값들을 표시한다. “hop limit" 필드는 IPv4에서의 TTL(Time to Live) 필드와 같은 역할을 하며, 거쳐갈 수 있는 라우터의 최대 개수를 명시한다. 다음으로 각각 128비트의 발신주소(source address)와 목적 주소(destination address) 필드가 위치한다.

0: Hop-by-Hop Options Header
2: Internet Control Message Protocol
4: Internet Protocol
17: Transmission Control Protocol
41: Internet Protocol version 6 (IPv6)
43: Routing Header
44: Fragment Header
45: Inter-domain Routing Protocol
46: Resource Reservation Protocol
50: Encapsulating Security Payload
58: Internet Control Message Protocol version 6
59: No Next Header
60: Destination Options Header

그림 2.3 "next header" 코드값

2.2.2 확장헤더

IPv6에서 선택적인 인터넷 정보들은 별도 헤더에 인코딩되는데, 이 헤더는 IPv6 헤더와 상위 계층 헤더 사이에 놓일 수 있다. 이를 확장 헤더라고 부른다. 이러한 확장 헤더들은 기능에 따라 [그림2-4]에서처럼 6가지가 있으며, 각각은 [그림2-3]에서 제시된 것처럼 고유의 다음 헤더(next header) 값으로 식별된다. 일반적으로 확장 헤더는 IPv6 패킷 내에 없거나, 하나 이상 놓일 수 있으며, 각 확장 헤더는 앞 헤더의 다음 헤더 필드에 의해 식별된다.

각 확장 헤더의 길이는 후속 헤더들이 8옥텟으로 정렬되도록 8옥텟의 정수 배이며, IPv6를 완전히 구현하기 위해 다음과 같은 확장 헤더들을 반드시 구현해야 한다. 이와 같은 확장 헤더들은 IPv4 환경에서 잘 사용되지 않았던 것으로, 확장 헤더 필드로 옮겨서 필요할 경우만 사용하게끔 함으로써 기본헤더를 간략하게 하여 일반적인 처리 효율을 높이는 것을 목적으로 한다.

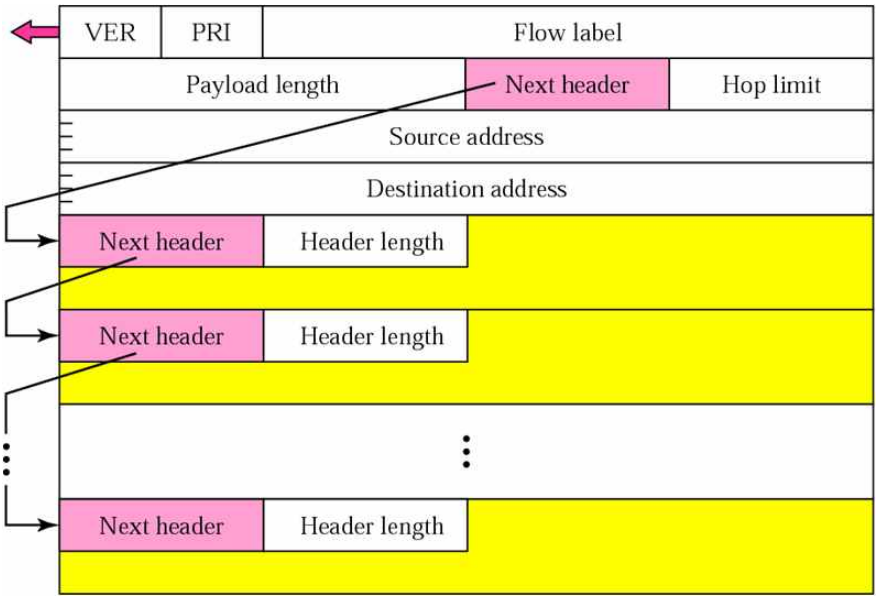

그림 2.4 IPv6 확장 헤더 형식

- 홉-바이-홉(Hop-by-Hop) 옵션 헤더 : 전송 경로상의 모든 노드마다 처리할 옵션 정보를 포함한다.
- 라우팅(Routing) 헤더 : 발신 노드기반 라우팅을 위한 헤더로 사용된다. 현재 라우팅 헤더는 목적 노드까지의 경로 상에서 반드시 포함해야 하는 중간 라우터 주소들의 목록만 포함하는 유형 0(Type 0)만 정의되어 사용되고 있다.
- 프레그먼트(Fragment) 헤더 : 프레그먼트와 재조립을 위한 정보를 포함한다. IPv4처럼 중간 노드에서는 수행되지 않으며, 발신지와 목적지에서만 사용될 수 있다.
- 목적지(Destination) 헤더 : IPv6 기본헤더의 목적지 주소나 라우팅 목록에 포함된 노드에서만 처리하는 옵션정보 또는 패킷의 최종 목적 노드에서만 처리하는 옵션 정보를 포함한다.

- 인증(Authentication) 헤더 : 망 계층에서 인증 서비스를 제공하기 위해 사용된다.
- ESP(Encapsulating Security Payload) 헤더 : 망 계층에서 기밀성 서비스를 제공하기 위해 사용된다.

확장 헤더들의 올바른 처리는 다음과 같은 요구사항들에 따라 결정된다.

- IPv6 노드는 확장 헤더가 한 패킷 내에서 몇 개가 있든, 어떤 순서로 있든 처리하려 노력해야 한다. 예외로 홉-바이-홉 옵션 헤더는 IPv6 헤더 바로 뒤에 있어야 하며, 기본적으로는 다음에서 제시하는 확장 헤더의 정렬 순서를 준수하도록 권고한다.
- 각 확장 헤더는 하나의 패킷 내에서 한번만 나타나야 하며, 예외적으로 목적지 옵션 헤더는 라우팅 헤더 앞에 한번, 상위계층 헤더 앞에 한번 씩 두 번에 걸쳐 나타날 수 있다. 또한, 상위 계층 헤더가 또 다른 IPv6 헤더인 경우 (터널링 기법)에도 확장 헤더가 한번 이상 나타날 수 있다.
- IPv6 헤더의 목적주소 필드에 설정된 노드 또는 멀티캐스트 그룹에 도착하기 전까지, 패킷 전달 경로상의 모든 노드들은 확장 헤더를 검사하거나 처리하지 않는다.
- 홉-바이-홉 옵션 헤더만이 중계 노드에서 처리되지 않아야 한다는 규정에 예외이며, 발신 노드와 목적 노드를 포함한 패킷 전달 경로 상의 모든 노드에서 검사되고 처리되어야 한다.
- 홉-바이-홉 옵션 헤더가 존재하면, IPv6 기본헤더 바로 다음에 위치해야 하며, 이를 지시하기 위해 IPv6 기본헤더의 다음헤더 필드의 값이 홉-바이-홉 옵션 헤더를 지칭하는 “0”으로 표시되어야 한다. 만약, IPv6 기본

헤더가 아닌 다른 헤더의 다음헤더 필드에서 “0”을 포함하면, ICMP 매개변수 문제 발생(Parameter Problem) 메시지를 패킷의 발신 노드로 보내야 한다.

- 각 확장 헤더의 내용과 의미에 따라 이어지는 헤더로 진행할지 여부를 결정한다. 그러므로 확장 헤더는 후행하는 헤더가 먼저 처리되는 것 없이 순서대로 처리되어야 한다. 만약, 헤더들의 다음헤더 필드에 포함된 값의 의미를 파악할 수 없는 경우, 그 노드는 패킷을 제거하고 ICMP 코드 값은 “1”(인식 불가능한 다음헤더 유형 탐색)로 하고, ICMP 데이터 필드는 원래의 패킷 내에서 인식 불가능한 값에 대한 옵셋(offset)을 담아 ICMP 매개변수 문제 발생(Parameter Problem) 메시지를 패킷의 발신 노드로 보내야 한다.

표 2.1 IPv4/IPv6 특성비교

구분	IPv4	IPv6
주소길이	32bit	128bit
표시방법	8bit씩 4부분으로 10진수로 표시 예)203.252.53.55	16비트씩 8부분으로 16진수로 표시 예)2002:0124:ABCA:DBCA:0000:0000: FFFF:4002
주소개수	약 43억개	2^{128}개(약 43억×43억×43억×43억 개)
주소할당 방식	A,B,C,D 등의 클래스단위 비순차적 할당	네트워크 규모, 단말기 수에 따른 순차적 할당
Broadcast 주소	있음	없음 (대신, 로컬 범위 내에서만 모든 노드에 대한 멀티캐스트 주소 사용)
보안	IPSec 프로토콜 별도 설치	IPSec 자체 지원
서비스 품질	제한적 품질 보장 (Type of Service에 의한 서비스 품질 일부 지원)	확장된 품질 보장 (트래픽 클래스, Flow Label에 의한 서비스 품질 지원)
Plug & Play	지원안함	지원

제 3 장 IPv6 전환 메커니즘

3.1 IPv6 전환 개요

IPv6가 IPv4 기반의 인터넷에 구현되기 시작함에 따라 검증되어야 할 중요한 이슈들 중의 하나는 바로 기존 IPv4에서 IPv6로의 자연스러운 이전을 지원해 주는 IPv6 전환 메커니즘에 대한 연구가 필요하다. IPv6 전환 기술이 필요한 이유는 IPv6 도입에 앞서 다음과 같은 몇 가지 제약사항이 있기 때문이다.

<IPv6 도입 제약사항>

① IPv6는 IPv4와 자연스럽게 호환(변환) 되지 않는다.
② 현재까지도 수 천만 개의 호스트가 IPv4 방식으로만 동작하고 있다.
③ IPv4/IPv6는 앞으로도 상당기간 상호 공존(co-exist) 할 것이다.
④ 사용자의 사용 목적에 따라 IPv6로 전환하지 않을 수 있다.

새로 구축될 IPv6 망은 IPv6 전용망이나 IPv4/IPv6 듀얼(dual)망 형태로 구성될 것이다. 일반적으로 IPv6 망과 외부의 다른 IPv6망, 혹은 IPv4 망과의 통신을 위해서는 IPv4와 IPv6망이 혼재된 통신서비스가 가능해야하며, 두 망간 통신이 자연스럽게 이루어지도록 하는 기술이 바로 IPv6 전환 메커니즘이다. 호스트와 라우터와 같은 장비에서는 IPv4/IPv6 듀얼 스택을 구성하는 방식이 가장 기본적인 IPv6 전환 방법이며, 게이트웨이에서는 IPv6 전용 호스트가 IPv4 전용 호스트와 통신하기 위해 IPv4/IPv6 변환(translation) 기술이, 망 관점에서는 IPv6 호스트가 IPv6 호스트와 통신 하고자 할 때 이 망 사이에 IPv4 망이 존재한다면, IPv6-in-IPv4 터널링 기술적용이 요구된다.[9]

3.2 IPv6 적용 시 고려사항

인터넷이라는 강력한 통신환경에서 중추적인 역할을 하고 있는 IPv4를 한번에 IPv6로 대체한다는 것은 현실적으로 불가능하다. 이것은 IPv4가 기존의 통신환경에서 비교적 잘 운용되고 있고 모든 서비스들과 애플리케이션이 IPv4를 사용하기 때문에 IPv6를 전격적으로 도입하기에는 많은 문제점들이 존재하기 때문인데 우선 가능한 IPv6 도입 시나리오와 특징은 크게 다음과 같다.

첫 번째 시나리오로서 순수 IPv6만을 지원하는 네트워크를 새로 구성하는 방법이 있다. 이 방법은 라우터를 재구성하는 것이 필요 없다는 장점이 있지만 IPv4 노드와 통신하고자 할 때 별도의 기술이 필요하다는 단점이 있기 때문에 IPv6 초기 도입단계에서는 적절하지 못하다.

두 번째 시나리오는 기존의 네트워크에 새로운 IPv6 노드들이 추가되는 방법이다. 이때 IPv6노드들은 IPv4와 IPv6의 dual protocol stack을 가질 필요성이 있고 이럴 경우 IPv4의 주소부족이라는 문제가 재발생할 뿐만 아니라 기존의 라우터들이 재구성되어야 하는 단점이 있다 하지만 기존의 네트워크를 새로운 IPv6 네트워크로 전환하는데 소요되는 비용이나 인력에 대한 부담을 줄여 자연스럽게 IPv6를 도입할 수 있는 장점이 있다.

따라서 IPv6 초기 도입단계에서는 어느 정도 IPv4와 IPv6의 혼용이 예상됨에 따라 IPv4-to-IPv6의 트랜지션 (Transition)과 상호공존 (Coexistence mechanism)을 필요로 하기 때문에 초기 IPv6망은 기존 IPv4와의 연동 및 호환을 고려하여 구축되어야 한다. 이러한 트랜지션 메커니즘 개발을 위해 IETF의 각 work group에서 활발한 연구가 진행되면서 다양한 기술들이 제안되고 있다.

기존의 IPv4에서 IPv6로의 트랜지션을 위한 트랜지션 메커니즘 중의 하나는 IPv6 도입 초기에 쓰일 수 있는 dual IPv4/IPv6 호스트로서 이 호스트에는 IPv4주소와 하나 이상의 IPv6 주소가 할당되어져 있다. 하지만 이러한 시스템은

원래 IPv6가 만들어진 중요한 이유 중의 하나인 IPv4의 주소 고갈이라는 문제가 발생하기 때문에 장기적인 관점에서는 좋은 해결방안이라고 할 수 없다.

3.3 IPv6 네트워크 전환 기술

IETF(Internet Engineering Task Force)에서 차세대 인터넷 프로토콜로 확정된 IPv6가 기존 프로토콜인 IPv4에 비해 많은 장점을 가지고 있음에도 불구하고, 세계적으로 널리 퍼져 있는 IPv4를 완전히 대체하기까지는 상당히 많은 기간이 소요될 것으로 예측된다. 따라서 인터넷 망에서 IPv4와 IPv6는 장기간 공존할 것이기 때문에, IPv4 망에서 IPv6 망으로 자연스럽게 진화시키기 위한 전환(transition)기술은 반드시 필요하다.

IPv4/IPv6 전환기술을 크게 나누면, 듀얼스택(dual-stack) 기술, 터널링(tunneling) 기술, 변환(translation) 기술 세 가지로 분류할 수 있다.

3.3.1 듀얼스택(Dual-Stack, IPv4/IPv6)

듀얼스택 기술은 하나의 시스템(호스트 또는 라우터)에서 IPv4와 IPv6 프로토콜을 동시에 처리하는 기술이다. 따라서 듀얼스택 기술을 지원하는 시스템은 물리적으로 하나의 시스템이지만 논리적으로 IPv4와 IPv6를 지원하는 두 개의 시스템이 있는 것처럼 볼 수 있다. 터널링 기술은 기존 IPv4 망을 전달망으로 사용해 섬처럼 서로 떨어져 있는 IPv6 망들을 연결시켜주는 기술이다. 변환 기술은 IPv4 망과 IPv6 망 사이의 연동 기술로 IPv6 클라이언트가 IPv4 서버에 접속할 때 또는 IPv4 클라이언트가 IPv6 서버에 접속할 때 사용된다.

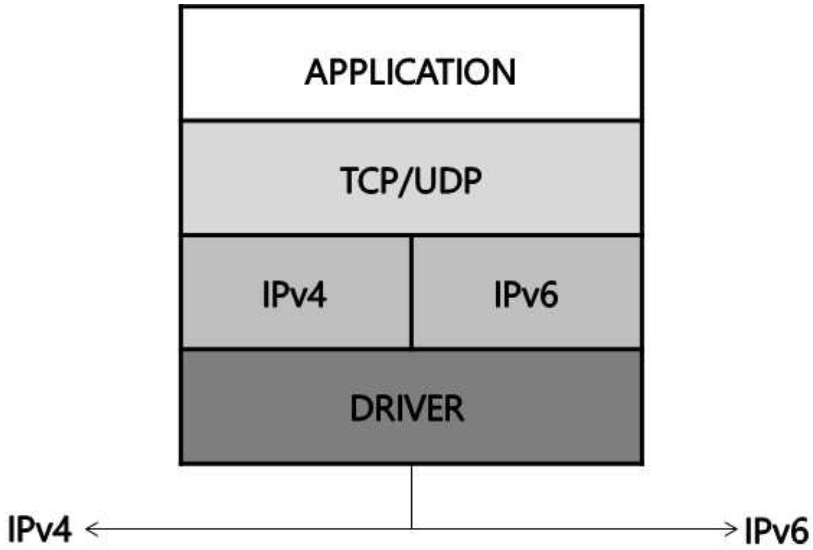

그림 3.1 Dual-Stack 구조

3.3.2 IPv6 터널링(Tunneling, IPv6-IPv4-IPv6)

IPv6 도입 초기에는 소규모 섬 형태의 IPv6 망들이 먼저 나타날 것이기 때문에 터널링 기술이 많이 활용될 것이다. 이에 따라 전환기술 중에서도 터널링 기술에 대한 표준화 활동이 가장 활발히 진행됐으며, 그 결과 지금까지 다양한 터널링 기술이 표준으로 제안됐다. 그 중 대표적인 것을 살펴보면 'Configured tunnel', '6to4', '6over4', 'ISATAP'(Intra-Site Automatic Tunnel Addressing Protocol), 'Teredo', 'IPv6 over MPLS' 등이 있다.

이 중에서 '6over4', 'ISATAP', 'Teredo' 등은 소규모 서브넷에서 사용하기 적합하며, ISP가 운용하는 대규모 망에 적용하기 위한 전환기술로는 'Configured tunnel', '6to4', 'IPv6 over MPLS' 등이 적합하다.

'Configured tunnel'은 수동으로 IPv6 망간 터널링을 설정하는 것으로 인터넷에서 흔히 사용되는 전통적인 터널링 방법과 유사하다. '6to4' 방식은 IPv6 주소에 IPv4 주소를 삽입해 IPv4 망에서는 IPv4 패킷으로 라우팅 처리되고

IPv6 망에서는 IPv6 패킷으로 라우팅 처리되는 터널링 기술로 확장성이 매우 뛰어난 장점이 있다. 'IPv6 over MPLS' 방식은 기존 IPv4 망에서 사용되던 MPLS(Multi Protocol Label Switching) 가상사설망(VPN) 방식을 약간 변형한 것으로, PE(Provider Edge) 라우터 대신에 6PE 라우터를 사용해 IPv6 패킷에 레이블을 붙여 전송하는데 기존 IPv4 망에 MPLS 기능이 있는 경우에 적용하기 적합한 기술이다.

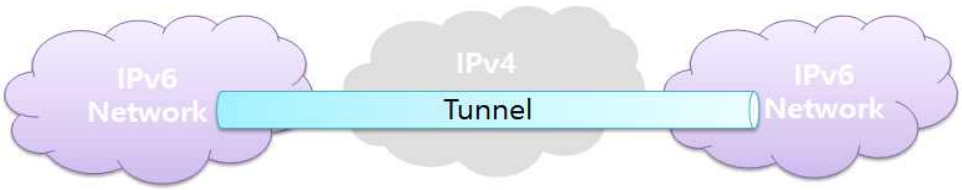

그림 3.2 IPv4 망을 경유한 IPv6 단말 간의 통신

3.3.3 변환(Translation, IPv6 → IPv4)

서로 다른 주소체계를 패킷의 완전한 재조합을 통하여 통신 가능하도록 구현하는 방식이다. 하지만 모든 통신 어플리케이션별로 특성을 호환하는 한계가 있어, 산업용등의 특정분야에 한정적으로 적용을 권장하고 있다.

- ALG (Application Level Gateway) : Application Layer에서 데이터 변환
- TRT (Transport Relay Translator) : Transport Layer에서 데이터 변환
- SIIT (Stateless IP/ICMP Translation) : Network Layer에서 데이터 변환

그림 3.3 IPv6 망을 경유한 IPv4 단말 간의 통신

제 4 장 IPv6 DNS 구축 방안

4.1 IPv6 DNS 개요

본 절에서는 IPv6 핵심기술의 하나인 DNS(Domain Name System)에 대해서 기술한다. 특히 IPv6전환 과정에서 DNS의 역할은 매우 중요하며, 이것은 기존 인터넷 사용자로 하여금 투명성 있게 IPv6를 도입할 수 있도록 하는 가장 핵심이 되는 기술이라고 볼 수 있다. 실제 128비트 주소체계를 갖는 IPv6 주소 표현은 비교적 짧은 IPv4 주소 표현에 비해서 사용자에게 불편함을 제공할 수 있기 때문에, IPv6에서의 DNS는 더욱 중요하다. 본 절에서는 DNS 프로토콜 개요와 IPv6 DNS를 구축하기 위해 확장된 내용을 중심으로 다룬다.

도메인 네임 시스템(Domain Name System)은 호스트의 도메인 네임을 호스트의 네트워크 주소로 변환 또는 그 반대의 역변환을 수행할 수 있도록 하기 위해 개발되었다. DNS는 네임체계의 하나로써 개발되었으며 현재에 이르러서는 인터넷에 필수적인 네임체계로서 자리하고 있다. DNS는 네트워크 주소를 통해 전 세계에 퍼져있는 통신망 속에서 단일한 대상을 지정하고 해당 통신대상에 접근할 수 있는 수단을 제공하는 역할을 하고 있다.

인터넷의 네트워크 주소는 32bit의 숫자로 된 IP 주소체계를 사용한다. 산술적인 단순한 계산으로는 42억 개의 IP주소가 존재할 수 있다. 이러한 IP 주소를 가지고 일일이 자신이 원하는 호스트에 접근한다는 것은 불가능하다. IP 주소를 모르는 상황에서는 해당 호스트로 접근할 수 있는 방법이 존재하지 않는다. 이것이 DNS가 존재하는 중요한 이유이다.

DNS는 네트워크 계층의 숫자 체계로 이루어진 네트워크 주소(IP 주소)와 사람이 이해하고 쉽게 기억할 수 있는 문자체계의 호스트 네임(name)을 상호 변환하여 사용할 수 있도록 매핑을 해주는 기능을 제공한다.

IPv6 DNS는 IPv6를 지원할 수 있도록 기존의 DNS 표준 프로토콜 및 관련

표준규정에서 확장된 DNS 체계이다. IPv6 DNS는 기존에 적용되어 사용되고 있는 DNS를 포함하면서 동시에 IPv6를 지원할 수 있는 확장된 DNS 체계라고 할 수 있다. 따라서 IPv6 DNS는 IPv4 영역의 DNS를 포함하고 있기 때문에 IPv4 인터넷과 IPv6 인터넷 모두 지원할 수 있어야 한다.

표 4.1 DNS S/W 확장 기능

구분	개요
resource record	IPv6 주소를 위한 AAAA RR 추가 정의
Inverse domain	IPv6 주소의 역변환 도메인으로 IP6.ARPA. 사용
Additional Section 처리절차	DNS 응답처리 절차 중 Additional Section의 IP 주소정보에 있어, IPv4 외에 IPv6 추가처리

IPv6 DNS 서버를 구축하기 위한 필요조건은 다음과 같다.

네트워크 환경 구성(IPv4/IPv6 Dual-Stack)
IPv6를 지원하는 네임서버의 플랫폼
IPv6패킷의 질의를 처리할 수 있는 DNS S/W
AAAA 등의 IPv6 확장 기능을 구현할 수 있는 S/W
도메인 및 IPv6 주소 확보

DNS는 “도메인 네임공간(Domail Name Space) 및 리소스 레코드(Resource Record)". "네임서버(Name Server)", "리졸버(Resolver)"의 3가지 기능 요소로 이루어져 있으며 DNS 구조 및 구성 요소는 그림 4.1과 같다.

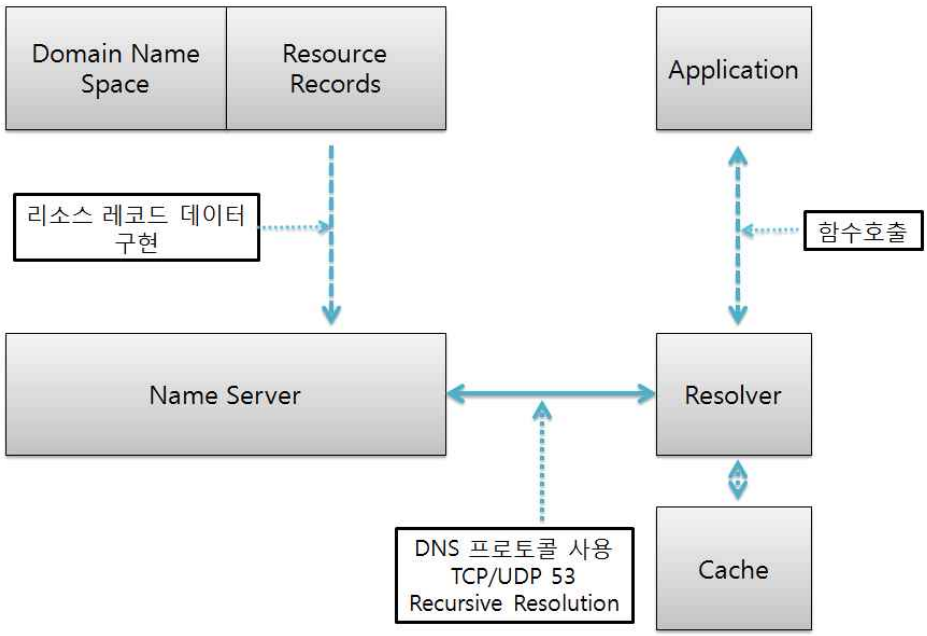

그림 4.1 DNS 구성요소

4.2 IPv6 DNS 작동방식

4.2.1 위임(Delegation)

모든 네임 서버는 루트 서버에 대한 정보를 내부에 저장된 설정 파일에서 얻는다. 루트서버는 차례대로 com, net, kr 등의 최상위 도메인에 대한 정보를 얻는다. 이 과정이 연쇄적으로 진행돼 kr도메인은 re.kr에 대한 정보를 얻고, com 도메인은 admin.com에 대한 정보를 얻는 방식으로 동작한다. 각 존은 하위 도메인에 대한 권한을 다른 서버에 위임할 수 있다.

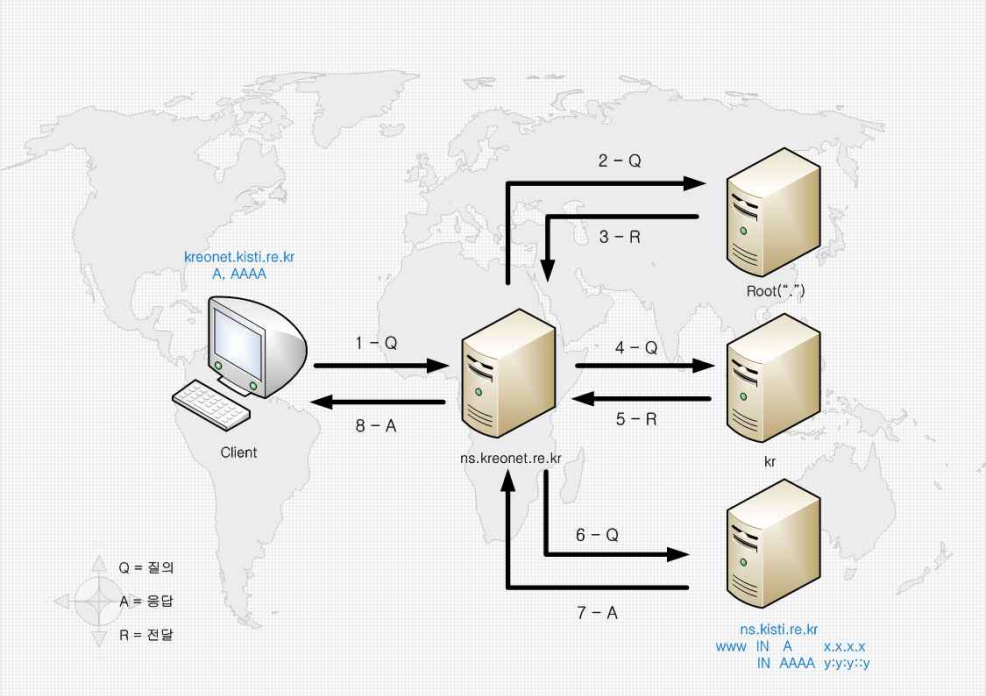

그림 4.2 IPv6 DNS 동작 과정

4.2.2 질의

서버 사이 화살표 위의 숫자는 처리 과정 순서를 나타내며, 글자는 작업 유형을 나타낸다(Q: 질의, R: 전달, A: 응답). 이 예에서는 질의를 보내기 전에 루트 도메인 서버의 IP주소 외에 필요한 정보가 캐시되어 있지 않다고 가정했다.

내부 네임 서버는 kreonet.kisti.re.kr 주소를 모른다. 그러나 루트 도메인의 일부 서버는 알고 있고, DNS 서버는 반복적으로 질의를 보내는 방식으로 처리하므로 kreonet.kisti.re.kr에 대한 요청을 루트 서버로 보내면 kr 도메인을 담당하는 서버의 위임 정보를 받는다. 그러면 내부 네임 서버는 질의를 kr 도메인 서버에 보내고 같은 과정을 반복하여 kisti.re.kr 서버의 위임 정보를 받는다. kisti 도메인 서버에도 정보가 캐시되어 있지 않다면 ns.kisti.re.kr 도메인의 위임

정보를 보낸다. ns.kisti.re.kr 도메인 서버는 해당 도메인을 관리하므로 kreonet의 장비 주소를 알려준다. 모든 과정이 끝나면 ns.kreonet.re.kr 서버는 kreonet의 주소를 캐시 해둔다. 그 뿐만 아니라 re.kr, kisti.re.kr, ns.kisti.re.kr 도메인에 대한 정보도 캐시 해 두는 방식으로 동작한다.

IPv4/IPv6 듀얼스택 호스트의 경우, IPv4 스택과 IPv6 스택을 모두 가지고 있기 때문에 IPv4 호스트와 IPv6 호스트 모두와 직접 통신이 가능하다. IPv4/IPv6 듀얼스택 호스트는 사용자가 입력하는 도메인 네임에 대해 IP 주소를 파악하는 절차에서 기존 IPv4 호스트와는 상이한 동작이 필요하다.

듀얼스택 호스트는 “www.kreonet.net" 호스트로 접속하기 전에 이 도메인 네임에 대한 IP 주소를 먼저 파악해야 한다. 도메인 네임 ”www.kreonet.net"은 IPv4 주소와 IPv6 주소 모두를, 또는 이 중 한 종류의 주소만 가지고 있을 수 있으므로, 듀얼스택 호스트는 “www.kreonet.net"에 대한 A 타입 질의와 AAAA 타입 질의 모두를 수행해 보아야 충분한 주소 정보를 파악할 수 있게 된다. 그림 4.3은 IPv4 호스트와 듀얼스택 호스트의 IP 주소 변환 절차를 비교한 것이다.

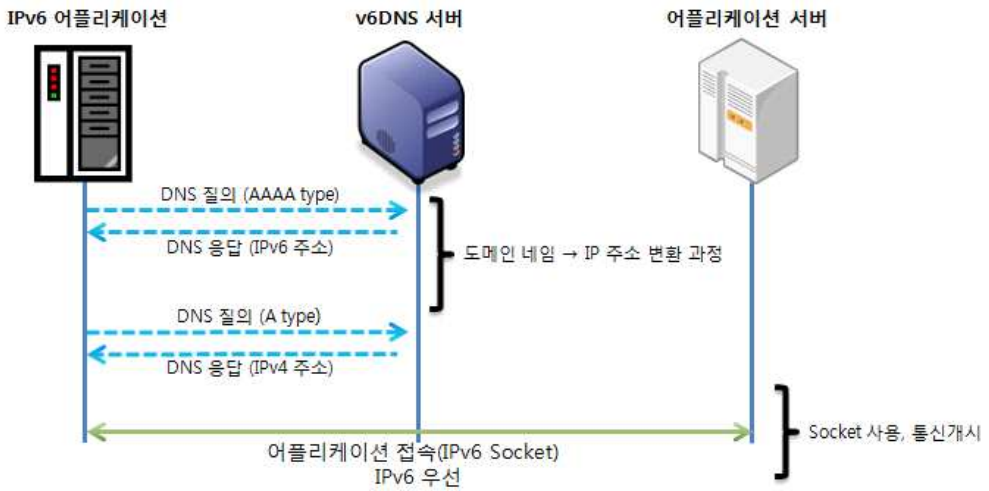

그림 4.3 IPv4/IPv6 주소변환 절차

그림 4.3에서와 같이 듀얼스택 호스트의 경우에는 도메인 네임의 주소 변환을 위한 절차에서 A 타입 DNS 질의와 AAAA 타입 DNS 질의를 각각 수행하여 IPv4 주소 및 IPv6 주소의 모든 정보를 파악하는 절차를 수행한다.

4.3 IPv6 DNS 구축 및 설정방법

IPv6 DNS의 소프트웨어는 IPv4 DNS와 동일한 설치과정을 거치므로 설치 과정을 생략하고 IPv6의 확장 기능 설정 과정을 중심으로 설명하고자 한다.

① BIND 설치 후 IPv6 인터페이스가 활성화 되도록 설정한다.

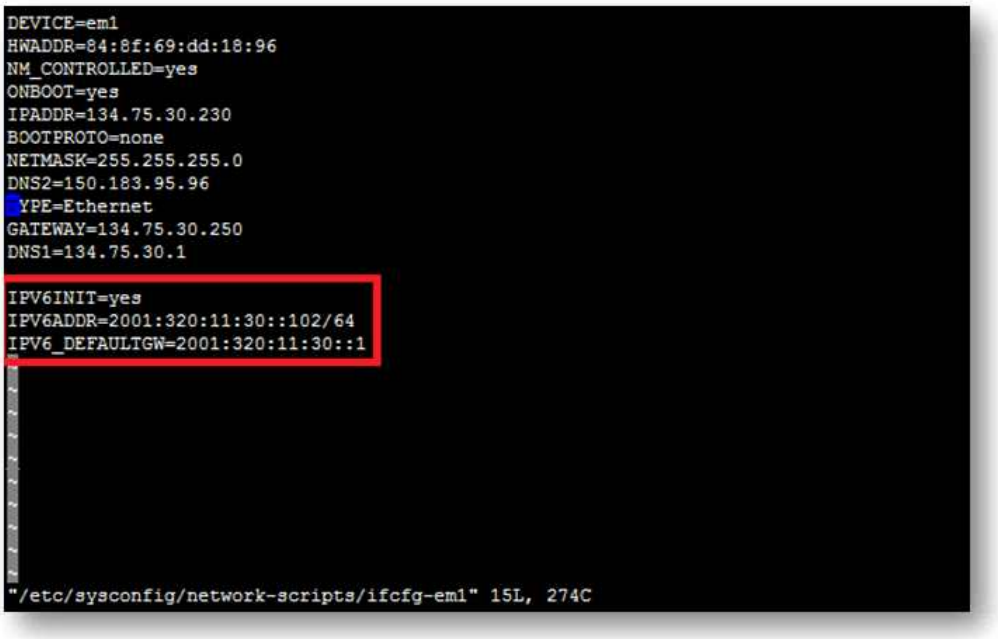

그림 4.4 IPv6 인터페이스 활성화 설정

② IPv6 패킷 처리가 가능하도록 설정 변경한다.

```
NETWORKING=yes
HOSTNAME=IPv6DNS1

NETWORKING_IPV6=yes
IPV6FORWARDING=yes
IPV6_AUTOCONF=no
IPV6_ROUTER=yes
IPV6_AUTOTUNNEL=no
IPV6_TUNNELMODE=IP
```

그림 4.5 IPv6 패킷처리 관련 설정

③ IPv6 역방향 질의를 처리할 수 있도록 설정 변경한다.

```
zone "." {
        type hint;
        file "named.cache";
};

zone "localhost" {
        type master;
        file "named.localhost";
};

zone "0.0.127.in-addr.arpa." {
        type master;
        file "named.ipv4.local";
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" {
        type master;
        file "named.ipv6.local";
};
```

그림 4.6 IPv6 역방향 질의 zone 파일 지정

④ IPv6 루프백 주소 ::1의 역변환 도메인을 처리할 수 있도록 zone file을 생성한다.

```
$ORIGIN 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa.
$TTL    86400
@       IN  SOA  ns.kisti.re.kr.  hostmaster.kreonet.net. (
                                20121011        ; Serial
                                86400           ; Refresh ( 24 Hours )
                                7200            ; Retry   (  2 Hour  )
                                604800          ; Expire  (  7 Days  )
                                3600  )         ; Minimum
                                IN      NS      localhost.
                                IN      A       127.0.0.1
                                IN      AAAA    ::1
```

그림 4.7 IPv6 루프백 주소 ::1의 역변환 도메인 zone file

⑤ 설정 후 AAAA레코드 질의 검증을 한다.

```
; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6 <<>> @134.75.30.230 g.dns.kr AAAA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16348
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 7

;; QUESTION SECTION:
;g.dns.kr.                      IN      AAAA

;; ANSWER SECTION:
g.dns.kr.               85145   IN      AAAA    2001:dc5:a::1

;; AUTHORITY SECTION:
kr.                     171545  IN      NS      f.dns.kr.
kr.                     171545  IN      NS      c.dns.kr.
kr.                     171545  IN      NS      d.dns.kr.
kr.                     171545  IN      NS      e.dns.kr.
kr.                     171545  IN      NS      b.dns.kr.
kr.                     171545  IN      NS      g.dns.kr.

;; ADDITIONAL SECTION:
b.dns.kr.               171545  IN      A       61.74.75.1
c.dns.kr.               171545  IN      A       203.248.246.220
d.dns.kr.               171545  IN      A       203.83.159.1
e.dns.kr.               171545  IN      A       202.30.124.100
e.dns.kr.               171545  IN      AAAA    2001:dcc:5::100
f.dns.kr.               171545  IN      A       218.38.181.90
g.dns.kr.               171545  IN      A       202.31.190.1
```

그림 4.8 AAAA 레코드 질의

⑥ 그림 4.9는 IPv4/IPv6 정·방향 zone file 형식을 나타낸 것이다.

```
$ORIGIN v6kreonet.net.
$TTL 86400

@       IN      SOA     ns1.v6kreonet.net. DNSAdmin.v6kreonet.net. (
                        20111009 ; Serial
                        3600     ; Refresh
                        900      ; Retry
                        604800   ; Expire
                        86400    ; Minimum
                        )

        IN      MX      10      mail.v6kreonet.net.
        IN      MX      100     mail2.v6kreonet.net.
        IN      NS      ns1.v6.kreonet.net.
        IN      NS      ns2.v6.kreonet.net.


ns1     IN      A       134.75.30.230
ns1     IN      AAAA    2001:320:11:30::102
ns2     IN      A       134.75.30.231
ns2     IN      AAAA    2001:320:11:30::103
mail    IN      A       134.75.30.120
mail    IN      AAAA    2001:320:11:30::120
mail2   IN      A       134.75.30.121
mail2   IN      AAAA    2001:320:11:30::121
www     IN      A       134.75.30.125
www     IN      AAAA    2001:320:11:30::125
```

그림 4.9 IPv4/IPv6 zone file

- **IPv6 정방향 레코드 주소형식**

콜론으로 구분된 각 부분은 4자리 16진수이며, 앞부분의 0은 보통 생략한다. 콜론이 연속된 경우는 그 자리에 '128비트 IPv6를 완성하기 위해 충분한 0을 추가'하라는 뜻이다. IPv6 주소에서는 연속된 콜론을 한 번만 쓸 수 있다.

예) ns.v6kreonet.net. IN A 134.75.30.230

IN AAAA 2001:320:11:30::101

• **IPv6 역방향 레코드 주소형식**

이 레코드는 AAAA 레코드의 IPv6 주소를 '니블' 형식으로 변환해 사용한다. 이 형식은 콜론으로 구분된 IPv6 주소 부분을 4자리 16진수로 풀어쓴 후 전체 자리수를 역으로 쓰고, 마지막에 ip6.arpa를 붙여서 만든다. 예를 들면 앞서 예로 든 anchor 장비의 AAAA 레코드에 해당하는 PTR 레코드는 다음과 같다.

예) $ORIGIN 0.3.0.0.1.1.0.0.0.2.3.0.1.0.0.2.ip6.arpa.

1.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR v6kreonet.net.

제 5 장 결론

IPv6가 IPv4의 후속버전으로서 현재 IPv4의 문제점과 향후 예상되는 인터넷 기술들을 수용하기 위해 설계되었지만, IPv6가 어느 시점에서 본격적으로 도입되어 실제 인터넷 기술의 핵심 역할을 하게 될지는 아직 단정할 수 없는 것이 사실이다.

다만 향후 통신기술이 요구하는 성능의 만족을 위해서는 IPv6 이외에는 아직 별다른 대안이 제시되지 못하고 있고 또 IETF를 중심으로 하는 인터넷 관련 기관들이 적극적으로 IPv6의 필요성을 역설하고 있는 상황에서 몇몇 주요 사업자들을 중심으로 IPv6에 대한 공감대가 어느 정도 형성되어 있는 것 또한 사실이다. 따라서 이미 몇몇 사업자들이 전개하고 있는 IPv6관련 사업들이 본격적으로 활성화되고 향후 몇 년 뒤 절실히 부족하게 될 IPv4의 주소를 고려한다면 IPv6의 미래는 밝다고 할 수 있을 것이다.

지금까지 현재 인터넷 프로토콜인 IPv4의 문제점을 해결하면서 동시에 유·무선 복합 망에서 사용 가능한 IPv6의 프로토콜 개요, 네트워크 전환기술 등을 제시하였고 실제 IPv6 DNS 구축 방법을 소개하였다. IPv4의 문제점 중 IP 주소 고갈 문제와 서비스 품질 보장 문제는 기존 IPv4에서 기능을 첨가하면서 일시적으로 해결할 수 있지만 궁극적으로는 IPv6를 채택하여야 한다. 사실 차세대 인터넷의 필요성은 누구나 공감하고 있지만 이에 따른 차세대 인터넷을 어떻게 구축하고 IPv6를 어떻게 활용 할지에 대한 고민은 반드시 필요할 것이다.

따라서 IPv6가 언제 본격적으로 도입되는지에 대한 성급한 예측보다는 실제적으로 IPv6 서비스를 어떻게 안정적으로 제공하느냐에 대한 문제접근 방식으로 향후 차세대 인터넷에서의 기술을 선도해 나가야 할 것이다.

참 고 문 헌

[1] IP : Next Generation (IPng) White Paper Solicitation, RFC 1550, December 1993.

[2] Security Concerns for IPng, RFC 1675, August 1994.

[3] A Large Corporate User's View of IPng, RFC 1687, August 1994.

[4] A Cellular Industry View of IPng, RFC 1674, August 1994.

[5] IPng Requirements : A Cable Television Industry Viewpoint, RFC 1686, August 1994.

[6] S. O. Bradner, A. Mankin, IPng : Internet Protocol Next Generation, Addition-Wesley, 1995.

[7] Special Issue : The Future of the Internet Protocol, IEEE Network Magazine, May 1993.

[8] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017.

[9] 이승민, IPv4/IPv6 프로토콜 및 주소변환 기능의 요소기술 분석 및 설계, KCI, Jun 2008.