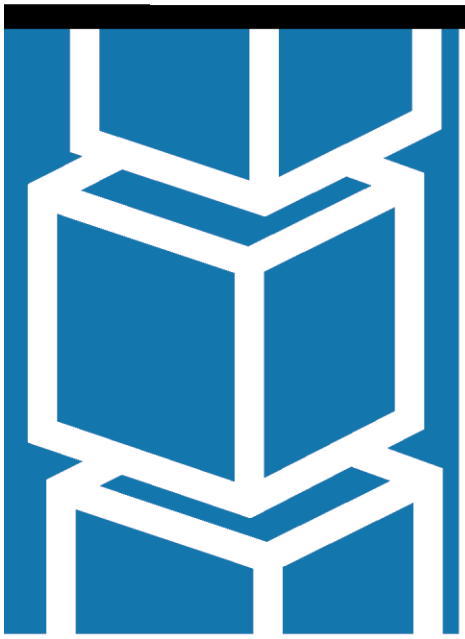
Cisco Systems

CISCO IOS LEARNING SERVICES



The ABCs of IP Version 6

Understanding the Essentials Series

www.cisco.com/go/abc

머리말

본 문서는 IP version4 (IPv4) 네트워킹에 대해 충분한 지식을 가지고 있는 네트워크 전문가를 위해 작성되었습니다. 이 문서는 계정 관리자와 시스템 엔지니어를 포함, IPv6 네트워크 요건을 분석하고 IPv6 네트워크 배치를 위해 전략을 개발해야 하는 모든 사람들에게 가장 큰 도움이 될 것입니다.

이 문서의 기술적 내용은 최대한 일반적인 내용으로만 제한시켰으며, 필요한 경우에는 IPv6에 대한 시스코의 제품 적용을 기반으로 특정 기술 또는 전략에 대해 보다 자세한 내용을 포함하였습니다. 이 문서에서 토폴로지와 설정에 대한 논의 그리고 예는 제외되었습니다.

이 문서를 원래 순서대로 읽는 것을 권장하지만 가장 관심 있는 부분을 먼저 읽어도 상관은 없습니다. 문서 끝의 부록 C에 있는 리뷰용 퀴즈를 이용, 배운 내용을 확인해보실 수 있습니다. 부록에 나열된 자원 외에도 로드맵, 소프트웨어 설정, 향후 방향 등을 포함하는 IPv6 구현에 대한 자세한 정보를 www.cisco.com/ipv6에서 찾아보실 수 있습니다.

보다 심도 있는 IPv6 교육을 원하시면 Learning Locator 또는 www.cisco.com을 참조하거나 abcios@cisco.com으로 메일을 보내주십시오.

본 내용의 기술을 위하여 애써주신 Steve Deering, Patrick Grossetete, Tony Hain, Ole Troan, Florent Parent, Kevin Flood, Neville Fleet, Simon Pollard 그리고 Yatman Lai의 도움과 기술적 검토에 감사를 드립니다.

Casimir Sammanasu
Cisco IOS Learning Services

소개

새로운 버전의 IP가 필요한 이유

IP version 6은 현재 전세계에서 널리 사용되고 있는 인터넷 프로토콜인 IP version 4를 대체하기 위해 설계된 새로운 IP 프로토콜입니다.

현재의 IP 버전은 1981년에 발표된 RFC 791, Internet Protocol DARPA Internet Program Protocol Specification에서 별로 바뀐 것이 없습니다. IPv4는 이미 강력하고, 쉽게 구현 가능하며, 상호 운용성이 뛰어나다는 것이 입증되어 네트워크 간의 연결을 오늘날의 인터넷 규모까지 확장시킬 수 있게 되었습니다.

하지만, 초기의 설계는 다음과 같은 조건들을 예견하지 못했습니다:

- 최근의 기하급수적인 인터넷의 성장과 함께 다가온 IPv4 주소 공간의 소진
- 인터넷의 성장과 인터넷 백본 라우터들의 대규모 라우팅 테이블 유지 능력
- 더욱 간단한 자동 설정 및 리넘버링(renumbering)(renumbering) 에 대한 요구
- IP 수준에서의 보안에 대한 요구
- 보다 나은 실시간 데이터 전송 지원의 필요 – 서비스 품질(QoS)로도 알려져 있음

IP Security(IPSec)와 QoS 같은 기능은 두 가지 IP 버전 모두를 위해 설명되었습니다.

IPv4의 32비트 주소 공간은 약 40억 개의 IP 장치를 지원할 수 있지만 RFC 3194, The Host-Density Ration for Address Assignment Efficiency: An Update on the H Ratio에서 Christian Huitema가 설명한 바와 같이 IPv4의 어드레싱 스키마는 최적의 것이 아닙니다. 초기에 할당된 클래스 A 주소 중 많은 수가 여전히 사용되고 있지 않지만 그것들을 다시 되찾을 수는 없습니다.

Internet Engineering Task Force(IETF)는 1990년경 처음으로 IPv4의 주소가 소진될 수 있다는 문제를 제기했으며 이를 해결하기 위해 약 10년의 기한이 남아 있다고 예측했습니다. 흥미롭게도 이 예측은 1990년대에 일어난 인터넷의 폭발적인 성장 이전에 나온 것입니다. 사실 IP 주소가 부족해지고 있다는 문제가 널리 알려지게 된 것은 최근의 일입니다.

현재의 IP 주소 공간은 인터넷 사용이 가능한 PDA, 홈 네트워크(HAN), 인터넷과 연결된 운송 수단(예를 들면 자동차), 통합된 IP 텔레포니 서비스, IP 무선 서비스 그리고 네트워크 게임 등과 같은 새로운 어플리케이션들의 요구는 고사하고 앞으로의 대대적인 사용자 증가 및 인터넷 확장에 따른 지리적 요구도 만족시킬 수 없습니다. IPv6은 이러한 요구를 만족시키고 네트워크의 어드레싱 규칙이 어플리케이션에게 투명해질 수 있는 글로벌 환경으로 돌아갈 수 있도록 하기 위해 설계되었습니다.

IPv4의 수명은 Network Address Translation(NAT), Classless InterDomain Routing (CIDR) 그리고 일시적인 할당(Dynamic Host Configuration Protocol [DHCP]과 RADIUS/PPP) 등의 주소 재활용 기술을 통해 연장되어 왔습니다. 이러한 기술들은 주소 공간을 늘려주고 전통적인 서버/클라이언트 환경을 만족하는 것 같아 보이지만 peer-to-peer 및 서버 (home)-to-client (인터넷) 어플리케이션의 요구 조건은 만족시키지 못합니다. 지속적인 연결 환경(브로드밴드, 케이블 모뎀 또는 Ethernet-to-the-home 등을 통한 가정용 인터넷)에 대한 필요가 충족되려면 그러한 IP 주소 변환, 풀링(pooling) 및 임시 할당 기술은 고려 대상이 될 수 없으며 소비자용 인터넷 기기들의 "플러그 앤 플레이" 기능은 주소에 대한 요구 사항을 한층 더 크게 만듭니다.

다이얼 업이나 케이블 모뎀/xDSL 같은 임시적인 연결에는 임시 IPv4 주소 또는 사설 주소가 주어져왔습니다. 무선 전화, PDA, 자동차, 가전 기기 같은 수백만 가지의 새로운 기술 장치들은 더 이상 글로벌 IPv4 주소를 받을 수 없게 될 것입니다. IPv4 주소가 완전히 소진되는 경우는 사실상 없다고 볼 수 있지만 IPv4 주소를 얻는 것은 갈수록 어려워지고 있습니다.

IPv4는 곧 새로운 기능과 더욱 큰 네트워크 사이에서 선택을 해야 할 때를 맞이하게 될 것입니다. 그렇다면 우리는 IP 주소 소진 문제를 해결함과 동시에 새롭고 개선된 기능을 갖춘 새로운 프로토콜이 필요합니다.

Network Address Translation (NAT)

개발 도상국들은 유럽이나 미국에 비해 IPv4 주소 부족 문제를 더욱 크게 직면하고 있습니다. NAT를 이용함으로써 IPv4 주소 소진을 지연시키기는 했지만, NAT의 도입은 새로운 IP 프로토콜로만 해결 가능한 문제들을 발생시켰습니다.

IPv4 네트워크에서 NAT는 일반적으로 RFC 1918, Address Allocation for Private Internets에서 설명된 바와 같이 사설 주소 공간을 이용하는 내부 네트워크와 인터넷 사이의 패킷을 변환하여 내부 네트워크를 연결하는데 사용되고 있습니다. NAT는 대규모 내부 네트워크에서도 오직 소수의 글로벌(외부) 주소만을 사용합니다.

NAT의 한계

NAT를 사용하는 것은 IPv4 주소 소진을 지연시킬 뿐, 실제적인 대규모 확장 문제를 해결하지는 못합니다. 왜냐하면 IP는 이제 컴퓨터 이외의 장치들을 위한 어플리케이션의 컨버전스 레이어로 폭넓게 채용되고 있기 때문입니다. 또한 NAT 사용은 RFC 2775, Internet Transparency와 RFC 2993, Architectural Implications of NAT에서 밝힌 바와 같이 많은 부작용을 초래하고 있습니다. 그러한 문제 중의 일부는 IPv6과 같은 새로운 프로토콜만이 해결할 수 있습니다:

- IPv4에서는 오직 종단에서만 연결을 처리할 수 있으며 하위 레이어에서는 어떠한 연결도 처리하지 못합니다. 하지만 NAT를 사용하면 IP의 엔드-투-엔드 연결 모델이 파괴됩니다.
- NAT는 주소와 포트의 변환을 처리해야 하기 때문에 네트워크가 연결 상태를 유지해야 합니다. NAT 장치 또는 NAT 장치 근처의 링크에 장애가 발생하면, 연결을 유지해야 하는 NAT의 특성상 신속한 리라우팅(Rerouting)이 어렵습니다.
- NAT는 또한 엔드-투-엔드 네트워크 보안 구현을 방해합니다. IP 헤더의 무결성은 일종의 암호 기능으로 보호됩니다. 이 헤더는 헤더의 무결성을 보호하는 패킷의 근원지와 수신된 패킷의 무결성을 체크하는 최종 목적지 사이에서 변경될 수 없습니다. 전송 경로 도중 헤더의 일부분이 변환될 경우 무결성 체크가 이뤄지지 않게 됩니다.
- "NAT 친화적이 아닌" 어플리케이션의 경우, 포트와 주소 매핑 만으로는 NAT 장치로 패킷을 포워딩 할 수 없습니다. NAT는 이 목적을 달성하기 위해 모든 어플리케이션에 대한 완전한 정보를 포함시켜야 합니다. 특히 동적으로 할당된 포트와 랑데부 포트, 어플리케이션 프로토콜 내에서의 임베디드(embeded) IP 주소, 보안 결합 등에서는 더욱 그렇습니다. NAT 친화적이 아닌 어플리케이션을 새롭게 설치할 때마다 NAT 장치를 업그레이드해야 합니다.
- 10.0.0.0/8 같이 동일한 사설 주소 공간을 사용하는 여러 네트워크를 연결 또는 결합시켜야 할 경우에는 주소 공간 충돌이 발생하게 됩니다. 리넘버링(renumbering) (renumbering)이나 이중 NAT 같은 기술로 충돌을 피할 수는 있지만 이러한 기술들은 매우 어려우며 NAT를 더욱 복잡하게 만듭니다.
- NAT가 효과적 이려면 내부/도달 가능한 주소와 외부 주소 사이의 매핑 비율이 커야 합니다. 하지만 내부에 여러 개의 서버가 있을 경우, NAT 외부 주소를 사용하는 동일 포트 상에서는 같은 프로토콜이 멀티플렉스 될 수 없습니다. 예를 들어, 동일한 포트(80)를 사용하는 2개의 내부 서버는 포트 주소를 변경하지 않고서는 같은 외부 주소를 사용할 수 없습니다. 외부로부터 도달되어야 하는 서버마다 하나의 외부 주소를 사용하기 시작하게 됩니다. 노드를 서버처럼 취급하고 다수의 외부 주소를 소모하는 프로토콜이 많기 때문에 내부 서버의 수가 클 경우에는 NAT가 그리 유용하지 않게 됩니다.

미래의 네트워크 요건 만족

IPv4 주소 소진이 새로운 프로토콜 개발의 주된 이유이긴 하지만, IPv6를 설계한 사람들은 다른 새로운 기능과 개선점도 추가했습니다.

IPv6은 이용자, 어플리케이션 그리고 서비스 요건을 만족시키기 위해 설계되었으며 네트워크 운영이 어플리케이션에게 투명해지는, 보다 단순한 환경으로의 복귀를 가능케 합니다.

앞으로 예상되는 새로운 무선 데이터 서비스들의 등장은 IPv6 개발의 가장 큰 요인이 되고 있습니다. 3rd Generation Partnership Project(www.3gpp.org), Universal Mobile Telecommunication System(www.umts-forum.org)그리고 Mobile Wireless Internet Forum(www.mwif.org) 같은 무선 업계 표준 단체들은 IPv6을 미래 IP 서비스의 기반으로 삼을 것을 고려하고 있습니다. 현재 IPv6 서비스는 일부 "핫 스팟" 지점에서 IEEE 802.11을 통해 제공되고 있습니다.

IPv6의 전반적인 시장 도입은 아키텍처가 인터넷 성장과 새로운 IP 어플리케이션 및 서비스를 얼마나 잘 수용할 수 있는가에 달려있습니다. 이런 모든 요소들은 IPv6의 등장 원인과 이를 뒷받침하고 있는 시장의 요구를 다시 한번 강조하고 있습니다.

IPv6의 진화

Internet Stream Protocol 또는 ST로 정의된 IPv5는 QoS를 제공하기 위해 시험적으로 만들어진 자원 예약 프로토콜입니다. ST는 IP를 대체하기 위한 것은 아니지만 IPv4와 같은 링크-레이어 프레이밍을 사용하기 때문에 IP 버전 번호(5)가 부여되었습니다. 지금은 자원 예약을 위해 다른 프로토콜(예를 들면 resource reservation protocol; RSVP)을 이용하고 있습니다. IPv5/ST 프로토콜은 RFC 1190, *Experimental Internet Stream Protocol, Version 2 (ST-II)*와 *RFC 1819, Internet Stream Protocol Version 2 (ST2) Protocol Specification – Version ST2+*에 자세히 설명되어 있습니다.

RFC 1752, The Recommendation for the IP Next Generation Protocol에서 원래 제안한 IPv6은 더욱 큰 주소 공간(128 비트)을 가진 Simple Internet Protocol Plus(SIPP)였습니다. SIPP의 주된 제안자는 현재 Cisco Fellow인 Steve Deering이었습니다. 이 제안이 있은 이후, IETF는 워크 그룹을 시작하여 1995년 말 발표된 RFC 1883, Internet Protocol, Version 6(IPv6) Specification을 통해 최초의 스펙을 공개했습니다. *Steve Deering(Cisco)과 Rob Hinden(Nokia)이 발표한 RFC 2460, Internet Protocol, Version 6(IPv6) Specification*은 *RFC 1883*을 대체, 현재의 IPv6 표준이 되었습니다.

IPv6은 네트워크 주소 비트를 IPv4의 32 비트에서 128 비트로 4배 늘렸습니다. 이는 지구 상의 모든 네트워크 장치에 고유의 IP 주소를 제공하고도 남는 용량입니다. 고유한 글로벌 IPv6 주소는 도달 가능성에 사용되는 메커니즘과 네트워크 장치를 위한 엔드-투-엔드 보안을 단순화시켜줍니다. 이는 주소 수요 증가의 원인이 되고 있는 어플리케이션과 서비스를 위해 필수적인 기능입니다.

IPv6 주소 공간의 유연성은 사설 주소에 대한 지원도 제공하지만 글로벌 주소가 폭넓게 제공되기 때문에 NAT의 사용 빈도를 줄이게 될 것입니다. IPv6은 NAT 기반 네트워크에서 손쉽게 얻을 수 없었던 엔드-투-엔드 보안과 서비스 품질(QoS)을 선사하게 될 것입니다.

The ABCs of IP Version 6 문서는 다음 주제들을 자세히 다루게 됩니다:

1. IPv6의 기능과 혜택
2. IPv6 헤더 포맷
3. IPv6 어드레싱 아키텍처
4. IPv6 운영
5. 통합 및 공존 전략
6. IPv6 네트워크 설계 고려 사항

1 장

IPv6의 기능과 혜택

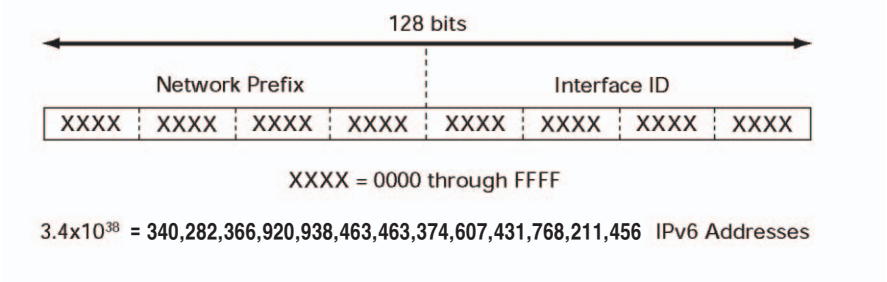
고유한 글로벌 IP 주소에 대한 미래의 수요를 만족시키는 것 외에도 IPv6은 다음과 같은 혜택을 네트워크와 IT 전문가들에게 제공합니다:

- 글로벌한 도달 가능성과 확장성을 위해 더욱 커진 주소 공간
- 효율적인 패킷 처리를 위해 단순해진 헤더 포맷
- 효율적인 라우팅을 위한 계층적 네트워크 아키텍처
- 폭넓게 배치된 기존 라우팅 프로토콜 지원
- 자동 설정 및 플러그 앤 플레이 지원
- 불필요해진 NAT와 ALG(application's layered gateway)
- 필수 IPSec 구현을 통한 임베디드 보안
- 개선된 모바일 IP와 모바일 컴퓨터 장치 지원
- 늘어난 멀티캐스트 주소 수

글로벌한 도달 가능성과 확장성을 위해 더욱 커진 주소 공간

거의 무제한에 달하는 IP 주소의 수는 IPv6 네트워크를 구현함으로써 얻어지는 가장 큰 혜택입니다. IPv4에 비해, IPv6은 주소 비트를 32 비트에서 128 비트로 4배 늘렸습니다. 128 비트는 지구상의 모든 사람마다 약 1030개(다른 교재의 경우 5.4 × 10의 28승으로 나옵니다 확인필요합니다!!) 의 주소를 할당할 수 있는 약 3.4 × 10의 38승개의 주소 노드를 제공합니다. 그림 1은 IPv6 주소의 일반적인 포맷을 보여주고 있습니다.

그림 1: IPv6 주소 포맷



각 네트워크 장치마다 고유한 주소를 부여할 수 있게 되면 엔드-투-엔드 도달 가능성을 실현시켜 줍니다. 이는 특히 가정용 IP 텔레포니에서 중요하게 작용합니다. IPv6은 또한 네트워크 에지에서의 특별한 프로세스 없이도 어플리케이션 프로토콜을 완벽하게 지원할 수 있기 때문에 NAT와 관련된 문제들을 제거해줍니다.

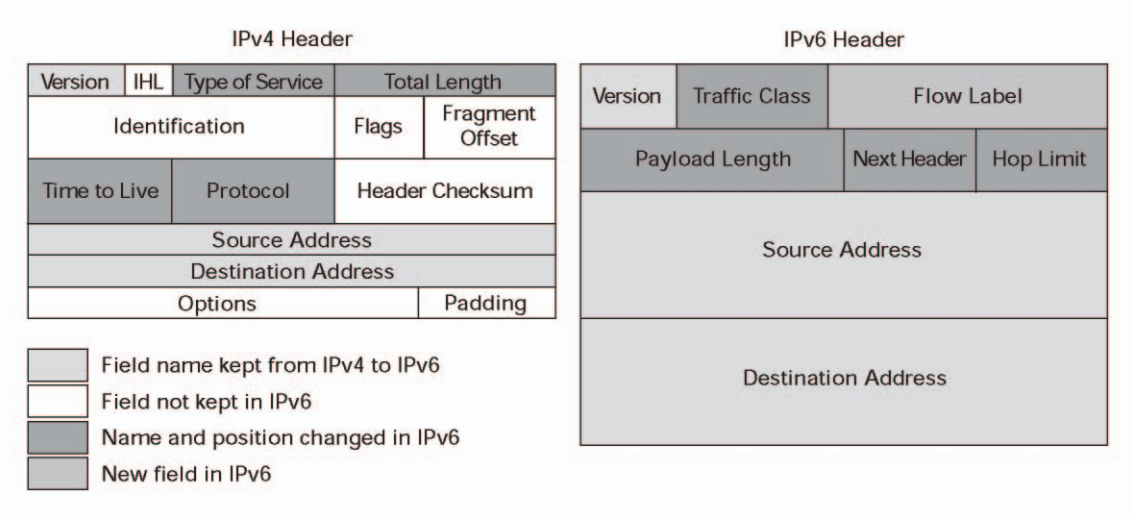
효율적인 패킷 처리를 위해 단순해진 헤더 포맷

IPv6 주소의 증가된 비트 수는 IPv6 헤더 크기를 증가시키게 되지만 IPv6의 헤더 포맷은 IPv4의 헤더에 비해 더 간단합니다. 기본적인 IPv4의 헤더 크기는 20 옥텟에 지나지 않지만 옵션 필드의 변수 길이가 IPv4 패킷의 전체 크기를 증가시키게 됩니다.

IPv6 헤더 크기는 40 옥텟으로 고정되어 있습니다. IPv6에서는 IPv4 헤더 필드 12개 중 6개가 제거되었지만 일부 IPv4 필드들은 바뀐 이름으로 남아있으며, 효율을 증가시키고 새로운 기능을 도입하기 위해 새롭게 추가된 필드도 있습니다. 그림 2에서 볼 수 있듯이 Header Length(IHL), Identification, Flags, Fragment Offset, Header Checksum 그리고 Padding 필드는 IPv6 헤더에서 제거되었습니다.

이러한 필드의 제거는 기본 IPv6 헤더를 보다 빨리 처리할 수 있게 해주지만 라우팅 효율과 전반적인 성능은 옵션 헤더 처리와 해당 장치가 실행해야 하는 검색 알고리즘에 따라 좌우됩니다. 또한 IPv6 헤더의 모든 필드는 64 비트로, 현재의 64 비트 프로세서를 활용할 수 있게 됩니다.

그림 2: IPv4와 IPv6 헤더의 비교



프레그먼트(fragment Offset)는 이제 다른 방법으로 관리되며 기본 IP 헤더 내에 전용 필드를 필요치 않습니다. IPv6에서는 라우터가 더 이상 프레그먼트를 처리하지 않으므로 IPv4에서 발생했던 프래그먼트 처리로 인한 라우터에서의 프로세싱 문제가 없어졌습니다. 체크섬이 제거됨에 따라 IPv6 패킷의 경로에 있는 라우터에서 매번 체크섬을 계산하지 않아도 되기 때문에 라우팅 효율이 향상되었습니다.

IPv6 네트워크에서는 프레그먼트가 경로 MTU(maximum transmission unit) 탐색 프로토콜의 지원하에 소스 장치에서 처리됩니다.

체크섬이 IP 레이어에서 제거된 이유는 대부분의 링크-레이어 기술이 이미 체크섬 및 오류 제어를 하고 있기 때문입니다. 또한 링크 레이어의 상대적인 신뢰성이 매우 좋기 때문에 IP 헤더 체크섬은 불필요하며 그리 유용하지 않은 것으로 여겨졌습니다. 링크 레이어 기술에서 처리하는 오류 탐지 외에도 엔드-투-엔드 연결을 처리하는 트랜스포트 레이어에도 오류 탐지가 가능한 체크섬이 있습니다.

하지만 위에서 제거된 사항들은 User Datagram Protocol(UDP)에서처럼 IPv6에서도 상위 레이어 옵션 체크섬을 필수적으로 수행하도록 만드는데 UDP 트랜스포트 레이어는 IPv4에서 옵션 체크섬을 사용합니다.

IPv4의 Options 필드는 IPv6에서 변경되었으며 이제 확장자 헤더 체인에 의해 관리됩니다. 대부분의 기타 필드들은 변경되지 않았거나 약간만 변경되었습니다. 필드의 수가 적어진 것 외에도 헤더는 현재의 프로세서들이 더욱 빠르게 처리할 수 있도록 64 비트에 맞춰져 있습니다.

효율적인 라우팅을 위한 계층적 네트워크 아키텍처

대용량의 주소공간과 네트워크 프리픽스(prefix)는 유연한 네트워크 아키텍처를 제공합니다. 이러한 유연성은 조직이 전체 네트워크를 위해 오직 하나의 프리픽스(prefix)만을 사용할 수 있게 해줍니다.

더 커진 주소 공간은 인터넷 서비스 공급자(ISP)와 기타 조직에게 대형화된 주소블록을 할당할 수 있게 해줍니다. 그 결과 ISP는 모든 고객들의 프리픽스(prefix)를 하나의 프리픽스(prefix)로 통합할 수 있으며 이 프리픽스(prefix)를 IPv6 인터넷에 알리게 됩니다.

더욱 커진 IPv6 주소 공간은 또한 주소 공간 내에서 여러 레벨의 계층구조를 사용할 수 있게 합니다. 각 레벨은 해당 레벨에 트래픽을 집합시켜 계층적인 포맷으로 주소를 할당할 수 있도록 도와줍니다. 주소 계층구조 내에 여러 개의 레벨을 구현하면 유연성과 유효한 주소사용 범위확인과 같은 새로운 기능이 가능해집니다. IPv6의 계층적 네트워크 아키텍처는 ISP들이 네트워크 프리픽스(prefix)의 집합을 이용하여 효율적이고 확장성 있는 라우팅을 제공합니다.

계층적 주소 할당 구조는 인터넷 라우팅 테이블의 크기를 줄이기 위해 설계되었습니다. 좋은 계층적 주소 스키마가 없다면 라우터들은 큰 규모의 라우팅 테이블을 저장해야 합니다. IPv4는 CIDR(Classless Interdomain routing)을 통한 경로 집합을 이용, 이 문제를 해결하고는 있지만 확장성도 없고 효율적이지도 않습니다.

멀티호밍(Multihoming)

멀티호밍은 하나의 네트워크가 2개 이상의 ISP에 연결될 수 있도록 해주고 높은 신뢰도를 제공하긴 하지만 IPv4에서는 하나의 네트워크를 복수의 서비스 사업자와 연결시키는 것이 쉽지 않습니다. 왜냐하면 그렇게 연결될 경우, 글로벌 라우팅 테이블 내의 모든 집합이 파괴되기 때문입니다. IPv6에서 제공되는 훨씬 큰 주소 공간은 글로벌 라우팅 테이블을 파괴하지 않고도 하나의 네트워크가 여러 개의 프리픽스(prefix)를 동시에 사용할 수게 해줍니다.

하지만 멀티호밍 네트워크를 위한 중복 설계와 로드 분산, 글로벌 라우팅 테이블의 확장성 여부 그리고 간단하고 관리가 용이한 멀티호밍 가이드라인 등은 여전히 정의될 필요가 있습니다. IPv6의 멀티호밍 기능과 어플리케이션이 미치게 될 영향은 IETF Multi6 워킹 그룹에 의해 연구되고 있습니다.

라우팅 프로토콜 지원

확장 가능한 라우팅을 위해 IPv6은 기존의 Interior Gateway Protocol(IGP)과 Exterior Gateway Protocol(EGP)을 지원합니다. IPv6은 IPv4와 마찬가지로 라우팅 알고리즘을 위해 가장 긴 프리픽스(prefix) 매칭을 이용합니다.

Routing Information Protocol

RFC 2080, RIPng for IPv6에서 설명된 바 있는 Routing Information Protocol Next-Generation(RIPng) 프로토콜은 IPv4의 RIP-2(RFC 1721, RIP Version 2 Protocol Analysis)와 같은 기능 및 혜택을 제공합니다. IPv6의 RIPng 개선 사항에는 IPv6 주소와 프리픽스(prefix) 지원이 포함되어 있습니다. RIPng는 RIP 업데이트 메시지를 위한 목적지 주소로 all-RIP 라우터 멀티캐스트 그룹 주소인 FF02::9를 사용합니다. RIPng는 프로토콜 메시지의 전송을 위해 IPv6을 사용합니다.

Open Shortest Path First Protocol Version 3

OSPFv3의 알고리즘은 대부분 OSPFv2와 같지만 OSPFv3는 약간 변경된 부분이 있습니다. 특히 IPv6에서 주소가 늘어났다는 점, 그리고 OSPF가 IP 위에서 직접 실행된다는 점은 그러한 변경을 불가피하게 만들었습니다. OSPFv2는 운영을 위해 IPv4의 주소에 많은 부분을 의존하기 때문에 IPv6을 지원하기 위해서는 RFC 2740, OSPF for IPv6에서 설명된 바와 같이 OSPFv3 프로토콜의 변경이 필요했습니다. 주요 변경 사항에는 플랫폼에 구애 받지 않는 구현, 링크별 프로토콜 프로세싱으로 대체된 노드별 프로세싱, 링크 당 여러 인스턴스 지원 그리고 인증 및 패킷 포맷의 변경 등이 있습니다.

IPv6 OSPF는 이제 IETF에서 제안한 표준입니다. RIPng와 마찬가지로 IPv6 OSPFv3 역시 전달을 위해 IPv6을 사용하며 근원지 주소로 링크-로컬 주소를 이용합니다.

IS-IS 프로토콜

IS-IS 라우팅 프로토콜은 IGP 프로토콜의 일종이며 IPv6 IS-IS는 IETF 표준입니다. 또한 기존의 IS-IS 프로토콜에 새로운 IPv6 기능이 추가되었습니다. Internet Draft draft-ietf-isis-ipv6-02.txt에는 RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*에 설명된 것과 동일한 메커니즘을 사용하는 IS-IS 라우팅 프로토콜을 이용하여 IPv6 라우팅 정보를 교환하는 방법이 명시되어 있습니다. 이는 2 개의 새로운 TLV(type-length-value; "IPv6 Reachability" (128 비트)와 "IPv6 Interface Address" (128 비트))와 새로운 IPv6 프로토콜 식별자를 추가함으로써 가능해졌습니다.

멀티프로토콜 Border Gateway Protocol+

IPv6에서의 멀티프로토콜 BGP는 IPv4의 멀티프로토콜 BGP와 같은 기능 및 혜택을 제공합니다. RFC 2858, Multiprotocol Extensions for BGP-4는 BGP4를 위한 멀티프로토콜 확장자를 새로운 속성으로 정의하고 있습니다. *RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Interdomain Routing*은 멀티프로토콜 BGP의 개선사항에 IPv6 주소군과 Network Layer Reachability Information(NLRI) 그리고 next hop(목적지로의 경로 상에 있는 다음 라우터) 속성에 대한 지원 등이 포함되어 있다고 설명하고 있습니다. 이 속성들은 IPv6 주소와 Scoped 주소를 사용합니다. Next hop 속성은 글로벌 IPv6 주소를 이용하며 로컬 링크에서 피어(peer)에 도달할 수 있을 경우에는 링크-로컬 주소를 이용할 수도 있습니다.

자동 설정 및 "플러그 앤 플레이" 지원

IPv6 프로토콜 내에 내장된 주소 자동 설정 기능은 인트라넷 전체의 주소 관리를 간편하게 함으로써 많은 수의 IP 호스트들이 쉽게 네트워크를 찾고 각각의 위치에 지정된 고유의 글로벌 IPv6 주소를 새롭게 받을 수 있도록 합니다. 자동 설정 기능은 휴대 전화, 무선 장치, 가전 기기 등과 같은 새로운 장치들에 대한 "플러그 앤 플레이" 인터넷 설치가 가능하도록 합니다. 그 결과 네트워크 장치들은 수동 설정이나 DHCP 서버가 없어도 네트워크에 접속할 수 있게 됩니다.

로컬 링크 상의 라우터는 상태를 알릴 때 로컬 링크의 프리픽스(prefix)나 기본 경로 같은 네트워크 타입 정보를 전송합니다. 라우터는 로컬 링크에 있는 모든 노드에 이 정보를 제공합니다. 그 결과 호스트는 라우터가 알린 로컬 링크 프리픽스(prefix)의 64 비트 포맷에 확장된 범용 식별자 EUI-64 비트 포맷으로 된 48 비트 링크 레이어 주소(MAC 주소)를 추가함으로써 스스로를 자동 설정할 수 있습니다.

쉬워진 리넘버링(renumbering)

IPv6 네트워크에서 자동 설정 기능은 기존 네트워크를 리넘버링(renumbering)하는 작업을 비교적 간단하고 쉽게 할 수 있도록 해줍니다. 라우터는 새로운 업스트림 제공자로부터의 새로운 프리픽스(prefix)를 라우터 선언(Router Announcements)과 같이 전송합니다. 네트워크 내의 호스트는 자동으로 새로운 프리픽스(prefix)를 수신, 이를 이용하여 새로운 주소를 만들게 됩니다. 그 결과, 네트워크 운영자들은 제공자 A에서 B로의 변환을 쉽게 할 수 있습니다.

불필요해진 NAT와 ALG(application's layered gateway)

IPv6의 주소 수가 많아짐으로써 모든 IP 장치에 고유한 글로벌 IP 주소를 제공할 수 있게 되자 수백 개의 내부 IP 주소를 소수의 글로벌 IP 주소로 변환할 필요가 없어지게 되었습니다.

네트워크에 NAT 박스를 설치할 필요가 없어지면 NAT 설치와 관련된 다른 문제들도 사라지게 됩니다. 특히 NAT를 제거하면 네트워크 내에서 투명한 엔드-투-엔드 관계가 가능해지며 네트워크의 복잡성이 줄어듭니다. 또한 기업과 ISP의 네트워크 운영 비용도 절감할 수 있게 됩니다.

필수 IPSec 구현을 통한 임베디드 보안

IPv4에서는 IPSec이 옵션이었지만 IPv6에서는 IPSec이 필수일 뿐만 아니라 IPv6 프로토콜 슈트의 일부분 이기도 합니다. 따라서 네트워크를 구현할 때 IPSec을 모든 IPv6 노드에 적용시킬 수 있어 네트워크를 보다 안전하게 해줍니다.

IPv6은 보안 확장자 헤더를 제공하여 암호화, 인증 그리고 가상 사설망(VPN) 구현을 쉽게 해줍니다. IPv6은 고유한 글로벌 주소와 보안을 제공하기 때문에 IPv6은 성능 병목 현상 같은 부수적인 문제를 발생시킬 수 있는 방화벽이 없어도 액세스 제어, 비밀성 그리고 데이터 무결성 등의 엔드-투-엔드 보안 서비스를 제공할 수 있습니다.

개선된 모바일 IP와 모바일 컴퓨터 장치 지원

이동성은 IPv6에 내장되어 있으며 모든 IPv6 노드는 필요에 따라 이동성을 활용할 수 있습니다. 이동성은 네트워크에서 갈수록 더욱 중요한 기능이 되어가고 있습니다. 모바일 IP는 모바일 장치들이 연결을 유지한 상태에서 자유롭게 이동할 수 있게 해주는 IETF 표준입니다. IPv4에서 이동성 기능은 새로운 기능으로 추가되어야 했습니다. IPv6에서의 이동성 지원은 Internet Draft draft-ietf-mobileip-ipv6-17.txt 최신 버전에서 다루고 있습니다.

모바일 노드의 홈 주소로 보내진 IPv6 패킷은 홈 주소와 care-of 주소를 바인딩 한 것을 캐싱함으로써 해당 패킷의 care-of 주소로 투명하게 라우팅 됩니다. 이 바인딩은 모바일 노드로 가는 모든 패킷이 care-of 주소에서 해당 노드로 갈 수 있도록 합니다. Mobile IPv6은 바인딩 업데이트 옵션, 바인딩 승인 옵션, 바인딩 요청 옵션 그리고 홈 주소 옵션 등 4 개의 새로운 IPv6 목적지 옵션을 정의하고 있습니다.

Mobile IPv6은 IPv6의 라우팅 헤더로 인해 Mobile IPv4 보다 엔드 장치들에게 훨씬 더 효율적입니다. IP 캡슐화 대신 Mobile IP에 라우팅 헤더를 이용함으로써 Mobile IP는 삼각 라우팅을 피할 수 있어 IPv6은 IPv4 보다 훨씬 더 효율적입니다.

참고: 모바일 노드와 상대 노드 간의 바인딩 업데이트 인증에 대한 논의는 IETF에서 아직도 계속되고 있습니다.

늘어난 멀티캐스트 주소 수

IPv6의 가장 두드러진 특징 중의 하나는 브로드캐스트를 전혀 사용하지 않는다는 것입니다. IPv4 브로드캐스트가 지원했던 라우터 탐색 (Router Discovery) 및 라우터 요청(Router Solicitation) 같은 기능들은 IPv6 멀티캐스트에 의해 처리됩니다. 멀티캐스트는 비디오 스트림 같은 IP 패킷이 동시에 여러 곳으로 보내질 수 있도록 하여 네트워크 대역폭을 절약시켜 줍니다. 멀티캐스트는 브로드캐스트 요청을 관련된 소수의 노드에만 한정시킴으로써 네트워크의 효율을 높여줍니다. IPv6은 다양한 기능을 위해 특정한 멀티캐스트 그룹 주소를 이용합니다. 따라서 IPv6 멀티캐스트는 IPv4 네트워크의 브로드캐스트 스톰으로 인한 문제를 사전에 방지하고 있습니다.

멀티캐스트 스코프 주소

RFC 2365, *Administratively Scoped IP Multicast*에서 설명된 바와 같이, IPv4 네트워크는 패킷들이 특정한 멀티캐스트 주소 스코프(예를 들면, 239.0.0.0에서 239.255.255.255) 내로 지정될 수 있도록 하기 위해 관리적으로 스코프가 확인된 IP 멀티캐스트 주소를 사용합니다. 멀티캐스트 스코프를 지정해줌으로써, 패킷들은 설정된 관리 스코프 밖으로 벗어날 수 없게 됩니다. IPv4는 특정 스코프 지역 또는 IP 멀티캐스트 스코프를 위해 하나의 브로드캐스트 주소를 이용하며 브로드캐스트는 그 확인된 지역 내의 모든 호스트에서 수신됩니다.

IPv6은 4 비트 Scope ID를 이용, 각 스코프의 멀티캐스트 주소를 위해 예약된 주소 범위를 지정합니다. 따라서 지정된 스코프 주소 내에서 특정 멀티캐스트 주소를 수신하도록 설정된 호스트만이 멀티캐스트를 수신하게 됩니다. 하지만 하나의 호스트는 여러 워크그룹에 속해있을 수 있기 때문에 동시에 여러 개의 멀티캐스트를 수신할 수도 있습니다.

IPv6은 IPv4보다 더 넓은 범위의 멀티캐스트 주소를 제공합니다. 그러므로 멀티캐스트 그룹을 위한 주소 할당은 당분간 제한 받지 않게 될 것입니다.

서비스 품질

IPv6에서의 QoS는 IPv4에서와 같은 방식으로 처리됩니다. 서비스 클래스에 대한 지원은 IETF Differentiated Services (DiffServ) 모델을 따르고 있는 Traffic Class 필드를 통해 제공됩니다.

하지만 IPv6 헤더에는 Flow 레이블이라는 새로운 필드가 있으며 여기에는 비디오 스트림이나 화상 회의 같은 특정 플로우를 식별하는 레이블이 포함되어 있습니다. 이 플로우 레이블은 소스 노드에서 생성됩니다. 플로우 레이블이 있으면 이 레이블에 따라 경로 상에 있는 QoS 장치들이 적절한 행동을 취할 수 있게 해줍니다. 하지만 플로우 레이블의 존재 자체는 QoS 기능의 일부가 아닙니다.

2 장

IPv6 헤더 포맷

IPv6 헤더는 IPv4 헤더보다 더 간단하고 효율적입니다. 간단해진 IPv6 헤더는 프로세싱 비용을 줄여줍니다.

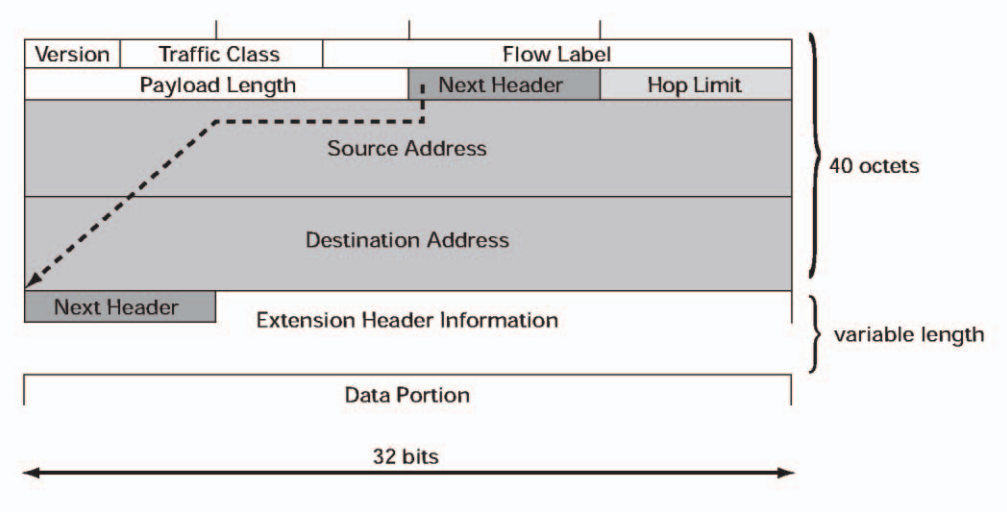
이 장에서는 IPv4와 IPv6 헤더 포맷 사이의 차이점은 무엇인지, IPv6 헤더가 어떻게 간단해졌는지 알아보게 됩니다. 이 장에서는 다음의 주제들을 다루게 됩니다:

- IPv6 헤더 필드
- IPv6 확장자 헤더
- IPv6 프레그먼트 헤더
- IPv6 라우팅 헤더
- IPv6 ICMP 패킷

IPv6 헤더 필드

IPv6 패킷 헤더는 그림 3에서와 같이 기본적으로 8 개의 필드로 이뤄져 있습니다.

그림 3: IPv6 헤더 필드



IPv6 헤더는 다음에서 설명하고 있는 필드들을 포함하고 있습니다:

IPv6 헤더 필드의 설명

Version Number: 버전 번호 필드는 IPv4에서와 같이 4 비트입니다. 이 필드는 IPv4의 숫자 4 대신 숫자 6을 포함하고 있습니다.

Traffic Class: Traffic Class 필드는 IPv4의 ToS(type of service)와 비슷한 8 비트 필드입니다. Traffic Class 필드는 Differentiated Services에서 사용될 수 있는 트래픽 클래스를 패킷에 태깅합니다. 기능은 IPv4에서와 같습니다.

Flow Label: 20 비트의 Flow Label 필드는 IPv6에 새롭게 추가된 것입니다. Flow Label 필드는 네트워크 레이어에서 패킷을 구분할 수 있도록 특정 플로우의 패킷을 태그하는데 사용될 수 있습니다. 따라서 Flow Label 필드는 경로 내에 있는 라우터가 플로우 및 플로우별 프로세스를 식별할 수 있도록 합니다. 이 레이블을 통해 IP 패킷 헤더에서 플로우 정보를 제공하므로 라우터는 플로우를 식별하기 위해 패킷을 깊이 들여다볼 필요가 없습니다. Flow Label은 엔드 시스템에 있는 어플리케이션들이 IP 레이어에서 트래픽을 쉽게 구분할 수 있도록 하여 IPSec에 의해 암호화된 패킷에 QoS를 쉽게 제공할 수 있게 합니다.

플로우 레이블 구현과 관련된 제안에 대해 보다 자세한 정보를 원하시면 Internet *Draft draft-ietf-ipv6-flow-label-01.txt*를 참조하십시오.

Payload Length: IPv4의 Total Length와 비슷한 Payload Length 필드는 패킷의 데이터 부분의 전체 길이를 나타냅니다.

Next Header: IPv4 패킷 헤더의 Protocol 필드와 비슷한 IPv6의 Next Header 필드 값은 기본 IPv6 헤더 다음에 어떤 종류의 정보가 오는지 결정하게 됩니다. 기본 IPv6 헤더 다음에 오는 정보는 그림 4에서 볼 수 있는 것과 같이 TCP 또는 UDP 패킷 같은 전송 레이어 패킷이나 Extension Header가 될 수 있습니다.

IPv6은 헤더의 옵션 정보를 관리하기 위해 다른 접근 방법을 사용합니다. IPv6은 각 확장자 헤더 내에 포함된 Next Header 필드로 서로 연결된 헤더 체인을 구성하는 확장자 체인을 정의합니다. 이 메커니즘은 효율적인 확장자 헤더 프로세싱과 빠른 전달 속도를 가능케 하며 각 패킷에 대한 라우터의 프로세스 작업을 줄여줍니다. 모든 확장자 헤더들은 전송 레이어 데이터까지 계속해서 서로 연결됩니다.

Hop Limit: IPv4 패킷 헤더의 Time to Live 필드와 비슷한 Hop Limit 필드의 값은 패킷이 무효 처리될 때까지 IPv6 패킷이 통과할 수 있는 라우터(hop) 수의 최대치를 나타냅니다. 라우터를 하나 거칠 때마다 값이 하나씩 줄게 됩니다. IPv6 헤더에는 체크섬이 없기 때문에 라우터는 체크섬을 다시 계산할 필요 없이 값을 감소시킬 수 있어 프로세싱 자원을 절약할 수 있습니다.

Source Address: IPv6 Source Address 필드는 IPv4 패킷 헤더의 Source Address와 비슷하지만 IPv4의 32 비트 소스 주소 대신 IPv6의 128 비트 소스 주소를 포함하고 있다는 점이 다릅니다.

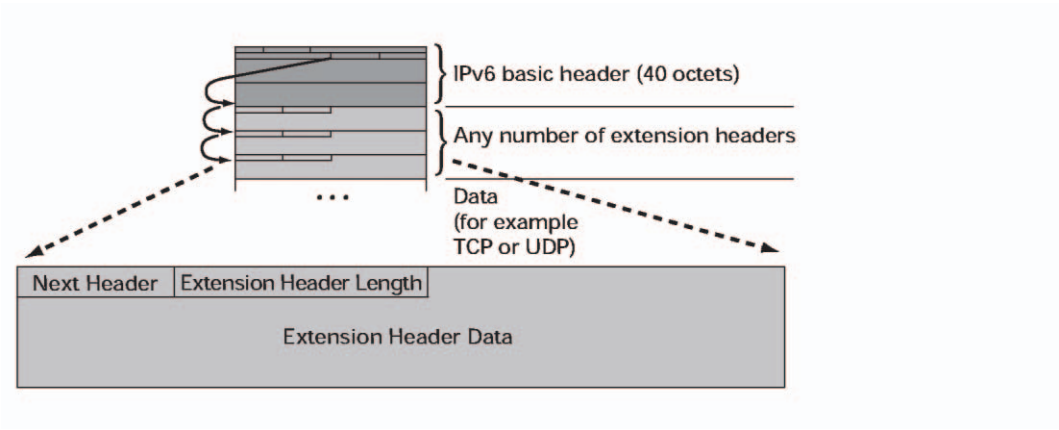
Destination Address: IPv6 Destination Address 필드는 IPv4 패킷 헤더의 Destination Address와 비슷하지만 IPv4의 32 비트 소스 주소 대신 IPv6의 128 비트 소스 주소를 포함하고 있다는 점이 다릅니다.

IPv6 확장자 헤더

기본 IPv6 패킷 헤더의 8 개 필드 다음에는 옵션 확장자 헤더와 패킷의 데이터 부분이 오게 됩니다. 존재할 경우, 확장자 헤더는 64 비트에 맞춰집니다. IPv6 패킷에는 확장자 헤더의 수가 정해져 있지 않습니다. 확장자 헤더는 서로 연결되어 TCP/UDP 포트 같은 정보를 포함할 수 있습니다.

이전 헤더의 Next Header 필드가 확장자 헤더를 식별하게 됩니다. 일반적으로 마지막 확장자 헤더는 TCP 또는 UDP 같은 전송 레이어 프로토콜의 Next Header 필드를 갖게 됩니다. 그림 4는 IPv6 확장자 헤더 포맷을 보여주고 있습니다.

그림 4: IPv6 확장자 헤더



확장자 헤더 순서

확장자 헤더에는 여러 종류가 있습니다. 여러 가지 확장자 헤더가 같은 패킷 안에서 사용될 때는 다음과 같은 순서를 따르게 됩니다:

1. **Hop-by-Hop 옵션 헤더.** Router Alert(RSVP와 MLDv1) 및 Jumbogram이 사용하는 이 헤더(값=0)는 패킷의 경로에 있는 모든 hop에서 프로세싱 됩니다. 포함되어 있을 경우, hop-by-hop 옵션 헤더는 항상 기본 IPv6 패킷 헤더 바로 뒤에 위치하게 됩니다.

2. **목적지 옵션 헤더:** 이 헤더(값=0)는 hop-by-hop 옵션 헤더 뒤에 위치하며 최종 목적지와 라우팅 헤더에서 지정된 주소들에서 프로세싱 됩니다. 이 헤더는 또한 Encapsulating Security Payload(ESP) 헤더 뒤에 위치할 수도 있으며 이 때는 오직 최종 목적지에서만 목적지 옵션 헤더를 프로세싱하게 됩니다. 예를 들면 모바일 IP에서 이 헤더를 사용합니다.

3. **라우팅 헤더:** 이 헤더(값=43)는 소스 라우팅과 Mobile IPv6에서 사용됩니다.

4. **프레그먼트 헤더(Fragment Header):** 이 헤더는 소스가 최대 전송 유닛(MTU) 보다 큰 패킷을 나눠야만 할 때 사용됩니다. 프레그먼트 헤더는 나눠진 모든 패킷에서 사용됩니다.

5. **인증 헤더와 ESP 헤더:** 인증 헤더(값=51)와 ESP 헤더(값=50)는 패킷의 인증, 무결성 그리고 비밀성을 제공하기 위해 IPSec 내에서 사용됩니다. 이 헤더들은 IPv4와 IPv6에서 모두 동일합니다.

6. **상위 레이어 헤더:** 상위 레이어(전송) 헤더는 데이터를 전송하기 위해 패킷 내에서 사용되는 일반적인 헤더입니다. 주된 전송 프로토콜로는 TCP(값=6)와 UDP(값=17)가 있습니다.

참고: 소스 노드는 이 순서를 따라야 하지만 목적지 노드는 순서와 관계없이 이를 받아들일 준비가 되어 있어야 합니다.

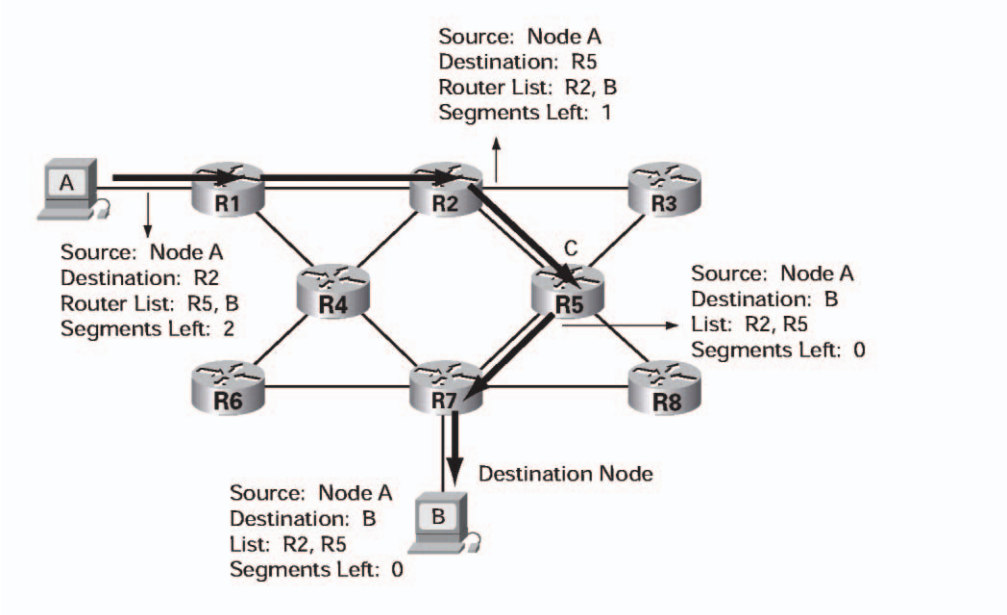
라우팅 헤더

라우팅 헤더는 IPv6 확장자 헤더 중의 하나이며 Next Header 필드 값 43으로 식별됩니다. 라우팅 헤더는 IPv6 기본 헤더 바로 다음 또는 다른 확장자 헤더 다음에 위치할 수 있습니다.

다른 확장자 헤더에서와 마찬가지로, 라우팅 헤더의 첫 번째 필드는 라우팅 헤더 다음의 헤더를 알려주는 Next Header 필드입니다. 두 번째 필드는 라우팅 헤더의 길이를 나타냅니다. "라우팅 종류"는 사용된 라우팅 헤더의 종류를 나타냅니다. "남아 있는 세그먼트"는 라우팅 헤더의 데이터에 포함된 중간 라우터의 수를 나타냅니다. 라우팅 종류가 0인 라우팅 헤더는 강제로 중간 라우터 목록을 통해 라우팅이 이뤄지도록 합니다. 이는 IPv4의 "Loose Source Route" 옵션과 비슷합니다.

그림 5는 라우팅 종류 0인 라우팅 헤더와 중간 라우터 R2 및 R5를 기반으로 하는 라우팅 경로의 활용을 보여주고 있습니다. IPv4의 "Loose Source Route"와 마찬가지로, 경로에 포함된 모든 라우터의 목록은 필요하지 않습니다.

그림 5: IPv6 라우팅 헤더



라우팅 헤더와 IPv6 패킷의 목적지 주소가 상호작용하는 방식은 IPv6에서 새롭게 도입되었습니다. 패킷이 수신되면, 목록에 있는 각 중간 라우터는 목적지 주소를 목록에 있는 다음 라우터와 교체함으로써 라우팅 헤더를 프로세싱 합니다. 남아 있는 세그먼트의 수가 감소하게 되고 패킷은 새로운 목적지로 보내지게 됩니다. 최종 목적지 노드(B)는 남아 있는 세그먼트의 수가 0인 라우팅 헤더를 수신하게 됩니다. B가 최종 목적지이므로 이 노드는 라우팅 헤더 다음에 오는 헤더를 프로세싱하게 됩니다.

프레그먼트 헤더

IPv6은 라우터에 의한 프레그먼트를 지원하지 않습니다. 경로 MTU가 충분하지 않을 경우, 프레그먼트는 소스 노드에서 이뤄집니다. IPv4에서는 경로 MTU가 옵션이었으며 자주 사용되지 않았습니다.

프레그먼트 헤더는 노드가 경로 MTU 보다 큰 패킷을 전송해야 할 때 사용됩니다. 이 상황에서 소스 노드는 패킷을 단편으로 나눈 다음 각 단편을 별도의 패킷으로 전송하며, 패킷의 IP 헤더에 프레그먼트 헤더를 추가하여 단편들을 식별합니다.

프레그먼트 헤더의 필드들은 IPv4 헤더의 프레그먼트 필드와 비슷하며 다음을 포함합니다:

- 오리지널 IP 패킷 내에서의 특정 단편의 위치를 표시하는 단편 오프셋
- 같은 오리지널 패킷에 속한 단편들을 식별하기 위한 식별 번호

목적지 노드는 수신된 단편들을 단편 오프셋의 순서에 따라 조합하여 패킷을 재구성합니다.

ICMPv6 패킷

IPv6의 Internet Control Message Protocol(ICMP)은 IPv4(RFC 792)의 ICMP와 같은 기능을 가지고 있습니다. ICMPv6은 ICMP 목적지 도달 불가 메시지와 같은 오류 메시지와 ICMP 에코 요청 및 응답 메시지 같은 정보 메시지를 생성합니다.

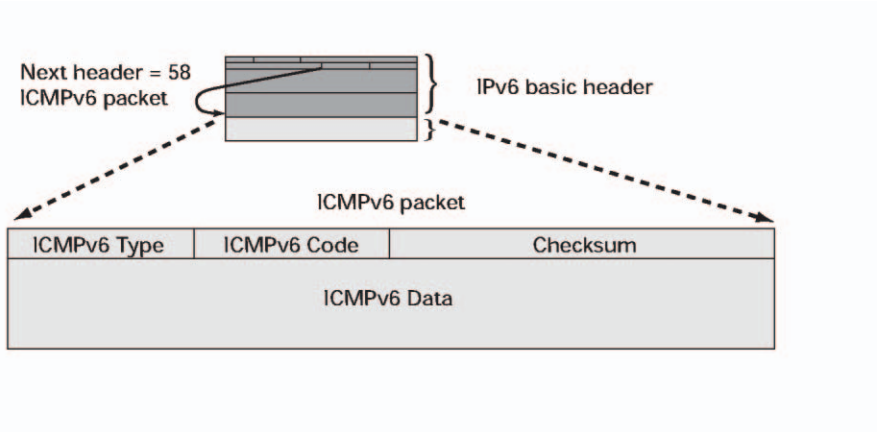
추가적으로 IPv6의 ICMP 패킷은 IPv6 네이버 탐색(Neighbor Discovery) 프로세스, 경로 MTU 탐색 그리고 IPv6을 위한 Multicast Listener Discovery(MLD) 프로토콜에서 사용됩니다. IPv6 라우터들은 MLD를 이용하여 직접 부착된 링크 상의 멀티캐스트 청취자(특정 멀티캐스트 주소로 가는 멀티캐스트 패킷을 수신하고자 하는 노드)를 탐색합니다. MLDv1은 IPv4를 위한 Internet Group Management Protocol(IGMP) 버전 2를 기반으로 하는 RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*에서 설명되어 있습니다. MLDv2(draft)는 IGMPv3과 비슷합니다.

기본 IPv6 패킷 헤더의 Next Header 필드 값이 58이면 IPv6 ICMP 패킷을 의미합니다. IPv6의 ICMP 패킷은 그것이 모든 확장자 헤더 뒤에 위치하며 IPv6 패킷의 마지막 정보라는 점에서 전송 레이어 패킷과 비슷합니다.

IPv6 ICMP 패킷 내에서는 ICMPv6 Type과 ICMPv6 Code 필드가 ICMP 메시지 종류 등과 같은 IPv6 ICMP 패킷의 세부 정보를 나타냅니다. Checksum 필드 값은 IPv6 ICMP 패킷과 IPv6 헤더의 필드에서 얻어집니다. ICMPv6 Data 필드는 IP 패킷 프로세싱과 관련된 오류 또는 진단 정보를 포함합니다.

ICMPv4와 마찬가지로, ICMPv6은 기업의 방화벽에 적용된 보안 정책에 의해 차단되는 경우가 많습니다. 이는 ICMP를 기반으로 하는 공격이 빈번하게 발생하기 때문입니다. 하지만 ICMPv6은 IPSec 인증 및 암호화를 사용할 수 있습니다. 이러한 보안 서비스들은 ICMPv6을 기반으로 하는 공격의 확률을 줄여줍니다. 그림 6은 IPv6 ICMP 패킷 포맷을 보여주고 있습니다.

그림 6: IPv6 ICMP 패킷



3 장

IPv6 주소 아키텍처

IPv6 주소 스키마는 기존 IPv4 네트워크 아키텍처와의 호환성 및 상호운용성을 제공하고 IPv6 네트워크가 기존 IPv4 네트워크와 공존할 수 있도록 하기 위해 설계되었습니다. IPv6은 IPv4의 IP 주소 부족 문제를 해결할 뿐만 아니라 IPv4의 일부 주요 기능들을 향상시켰습니다. IPv6은 라우팅과 주소 할당 기능을 개선함과 동시에 IP 헤더를 단순하게 만들어줍니다. IPv6은 다양한 종류의 IP 주소와 멀티캐스트 라우팅에 사용할 수 있도록 더욱 큰 주소 블록을 지원합니다.

이 장에서는 다음 주제들을 다루게 됩니다:

- IPv6 주소 포맷
- IPv6 주소 종류(유니캐스트, 멀티캐스트 그리고 애니캐스트)
- IPv6 멀티캐스트 주소 스키마
- IPv6 주소 할당

RFC 2373, IP Version 6 Addressing Architecture에서 설명된 IPv6 주소 아키텍처는 프로토콜과 관련된 기능을 기반으로 하는 완전한 주소 공간 활용을 정의합니다.

IPv6 주소 포맷

IPv6은 콜론(:)으로 나뉜 16 비트 16진수 필드를 이용하여 128 비트 주소 포맷을 나타냅니다. 이는 주소 표시를 덜 거추장스럽게 해주며 오류도 줄여줍니다. 16진수는 대소문자 구분을 하지 않습니다.
다음은 유효한 IPv6 주소의 예입니다:
2031:0000:130F:0000:0000:09C0:876A:130B.

또한 IPv6 주소를 단축시키고 주소를 보다 쉽게 표시하기 위해 IPv6은 다음과 같은 규칙을 사용합니다:

- 각 주소 필드의 맨 앞에 오는 0은 생략이 가능합니다. 예를 들어 다음과 같은 16진수는 그 아래의 압축된 포맷으로도 표시될 수 있습니다:

예 1: 2031:0000:130F:0000:0000:09C0:876A:130B =
2031:0:130F:0:0:9C0:876A:130B (압축된 포맷)
예 2: 0000 = 0 (압축된 포맷)

- 연속된 콜론(::)은 값이 0인 필드가 연속됨을 나타냅니다. 하지만 IPv6 주소에서 이러한 표시 방법은 한번 밖에 허용되지 않습니다.

예 1: 2031:0:130F:0:0:9C0:876A:130B =
2031:0:130F::9C0:876A:130B (압축된 포맷)
예 2: FF01:0:0:0:0:0:1 = FF01::1 (압축된 포맷)

주소 구문 해석계를 이용하면 주소를 분석하여 손쉽게 IPv6 주소에서 빠진 0의 수를 알아낼 수 있으며 128 비트 주소가 완성될 때까지 빈 곳을 0으로 채워넣을 수 있습니다. 하지만 만일 2 개의 ::가 같은 주소 안에 있다면 0으로 이뤄진 블록의 크기를 알아낼 방법이 없습니다. ::를 사용함으로써 대부분의 IPv6 주소 길이가 짧아지게 됩니다.

IPv6 주소 프리픽스(prefix)

주소의 일부인 IPv6 프리픽스(prefix)는 가장 왼쪽에 위치한 고정값 비트로 네트워크 식별자를 나타냅니다. IPv6 프리픽스(prefix)는 CIDR(classless interdomain routing) 표기를 따르는 IPv4 주소와 마찬가지로 IPv6-prefix/prefix-length 포맷을 이용하여 표시됩니다. IPv6 프리픽스(prefix) 변수는 RFC 2373을 따라야 합니다.

/prefix-length 변수는 프리픽스(prefix)를 이루고 있는 주소의 고차 연속 비트 수를 나타내는 10진수 값이며 이는 주소의 네트워크 부분입니다. 예를 들면 1080:6809:8086:6502::/64는 유효한 IPv6 프리픽스(prefix) 입니다. 만일 주소가 ::으로 끝날 경우에는 그 뒤의 ::을 생략해도 됩니다. 따라서 앞의 주소는 1080:6809:8086:6502/64로 표시될 수도 있습니다. 어느 경우건 프리픽스(prefix)의 길이는 10진수 64로 표기되며 IPv6 주소의 가장 왼쪽 비트를 나타냅니다.

IPv6 주소 종류

IPv4 노드와 IPv6 노드의 IP 주소 요건 사이에는 커다란 차이가 있습니다. IPv4 노드는 일반적으로 하나의 IP 주소를 사용하지만 IPv6 노드는 하나 이상의 IP 주소를 필요로 합니다.

IPv6 주소의 3가지 종류는 다음과 같습니다:

- **유니캐스트** – 단일 인터페이스를 위한 주소입니다. 유니캐스트 주소로 보내진 패킷은 해당 주소의 인터페이스로 전달됩니다.
- **애니캐스트** – 보통 서로 다른 노드에 속해있는 인터페이스 집합을 위한 주소입니다. 애니캐스트 주소로 보내진 패킷은 애니캐스트 주소에 의해 지정된 가장 가까운 인터페이스로 전달됩니다. 이때 가장 가까운 인터페이스는 사용되고 있는 라우팅 프로토콜의 정의를 따르게 됩니다.
- **멀티캐스트** – 보통 서로 다른 노드에 속해있는 인터페이스 집합(주어진 범위 내에서의)을 위한 주소입니다. 멀티캐스트 주소로 보내진 패킷은 멀티캐스트 주소(주어진 범위 내에서의)에 의해 지정된 모든 인터페이스로 전달됩니다.

IPv6 주소 할당

IPv6 주소는 노드가 아닌 단일 인터페이스에 할당됩니다. 하지만 하나의 인터페이스를 여러 개의 IPv6 주소로 할당할 수 있습니다. 따라서 노드 식별은 해당 노드의 여러 유니캐스트 주소를 통해 쉽게 이뤄질 수 있습니다. 다음은 이러한 일반적인 규칙의 예외 사항들입니다:

- 로드 분산을 위해 여러 개의 물리적 인터페이스 상에서 여러 개의 인터페이스를 사용할 때는 이들 인터페이스에 하나의 유니캐스트 주소를 할당할 수 있습니다.
- 포인트-투-포인트 링크 상의 번호가 없는 인터페이스를 사용하는 라우터에는 IPv6 주소가 할당되지 않습니다. 왜냐하면 인터페이스에 IP 데이터그램을 위한 소스 또는 목적지 기능이 없기 때문입니다.

IPv6 유니캐스트 주소

유니캐스트 주소는 단일 인터페이스를 위한 주소입니다. 유니캐스트 주소로 보내진 패킷은 해당 주소의 인터페이스로 전달됩니다. 구현과 관련된 세부 정보는 벤더에 따라 달라지지만 Cisco IOS 소프트웨어는 다음과 같은 IPv6 유니캐스트 주소 종류를 지원합니다:

- 글로벌 유니캐스트 주소
- 사이트-로컬 유니캐스트 주소
- 링크-로컬 유니캐스트 주소
- IPv4 매핑된 IPv6 주소
- IPv4 호환 IPv6 주소(거의 사용하지 않음)

IPv6은 Unspecified 주소와 루프백 주소 등 특수 주소라 불리는 기타 유니캐스트 주소도 지원합니다.

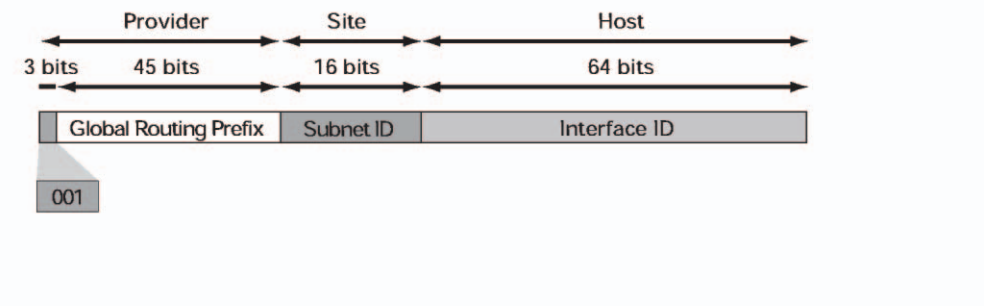
IPv6 글로벌 유니캐스트 주소란?

IPv6 글로벌 유니캐스트 주소는 IPv4 글로벌 유니캐스트 주소와 동등한 것입니다. 글로벌 유니캐스트 주소는 글로벌 유니캐스트 프리픽스(prefix)로부터의 IPv6 주소입니다. 글로벌 유니캐스트 주소의 구조는 글로벌 라우팅 테이블의 라우팅 테이블 항목 수를 제한하는 라우팅 프리픽스(prefix) 집합을 가능케 합니다. 링크에 사용된 글로벌 유니캐스트 주소는 조직 내부를 거쳐 결국 ISP에서 모이게 됩니다.

글로벌 유니캐스트 주소는 글로벌 라우팅 프리픽스(prefix), 서브네트 ID 그리고 인터페이스 ID로 정의됩니다. 이진수 000로 시작하는 주소 외에는 모든 글로벌 유니캐스트 주소에 64비트 인터페이스 ID가 있습니다. 그림 7에서 볼 수 있는 바와 같이 현재의 글로벌 유니캐스트 주소 할당은 이진수 001 (2000::/3)으로 시작되는 주소 범위를 사용합니다.

2000::/3은 글로벌 유니캐스트 주소의 범위이며 전체 IPv6 주소 공간의 1/8을 사용합니다. 이는 할당된 블록 주소 가운데 가장 큰 것입니다.

그림 7: IPv6 글로벌 유니캐스트 주소 포맷



글로벌 유니캐스트 주소의 구조는?

2000::/3(001)으로 고정된 프리픽스(prefix)는 글로벌 IPv6 주소를 나타냅니다. FF00::/8(1111 1111) 멀티캐스트 주소를 제외한 2000::/3(001)에서 E000::/3(111)의 프리픽스(prefix)를 가진 주소들의 64비트 인터페이스 식별자는 EUI(extended universal identifier)-64 포맷을 따라야 합니다. Internet Assigned Numbers Authority(IANA)는 2001::/16 범위 안에 있는 IPv6 주소 공간을 레지스트리에 할당하고 있습니다.

다음 부분은 IETF에서 Internet Draft draft-ietf-ipngwg-addr-arch-v3-07.txt를 통해 권장하고 있는 새로운 주소 스키마를 설명하고 있습니다.

글로벌 유니캐스트 주소는 일반적으로 48비트 글로벌 라우팅 프리픽스(prefix)와 16비트 서브네트 ID로 구성되어 있습니다. *IPv6 aggregatable global unicast address format* 문서(RFC 2374)는 Top-Level Aggregator과 Next-Level Aggregator로 불리는 2개의 추가적인 계층적 구조 필드를 글로벌 라우팅 프리픽스(prefix)에 포함시키고 있습니다. 이들 필드는 정책을 기반으로 하고 있기 때문에 IETF는 RFC에서 이들을 제외하였습니다. 하지만 초기에 설치된 일부 IPv6 네트워크들은 아직도 이전 아키텍처를 기반으로 하는 네트워크를 사용하고 있을 수도 있습니다.

조직들은 독자적인 로컬 주소 계층 구조를 구축하고 서브네트를 식별하기 위해 Subnet ID라 불리는 16비트 서브네트 필드를 사용할 수도 있습니다. 이 필드는 조직에서 최대 65,535개의 개별 서브네트를 사용할 수 있게 해줍니다.

IPv6 주소에서의 EUI-64 포맷 사용

IPv6 주소의 64비트 인터페이스 식별자는 링크 상의 고유 인터페이스를 식별하기 위해 사용됩니다. 링크란 네트워크 노드들이 링크 레이어를 이용해 통신하는 네트워크 매체입니다. 인터페이스 식별자는 더 넓은 범위 상에서도 고유성을 지닐 수 있습니다. 많은 경우, 인터페이스 식별자는 인터페이스의 링크 레이어(MAC) 주소와 같거나 이를 기반으로 하게 됩니다. IPv4에서와 같이 IPv6의 서브네트 프리픽스(prefix)는 하나의 링크와 연결됩니다.

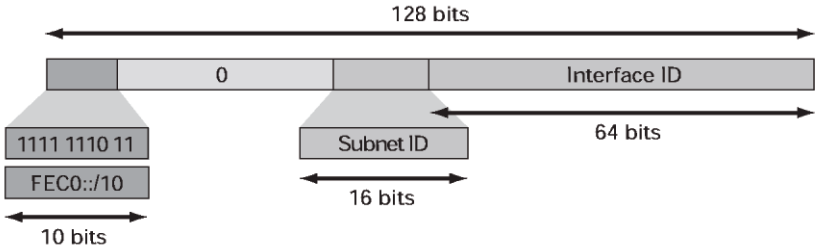
글로벌 유니캐스트 및 기타 IPv6 주소 종류에서 사용되는 인터페이스 식별자는 길이가 반드시 64비트이어야 하며 EUI-64 포맷을 따라야 합니다. EUI-64 포맷 인터페이스 ID는 48비트 링크 레이어(MAC) 주소를 기반으로 링크 레이어 주소의 상위 3 바이트(OUI 필드)와 하위 3 바이트(시리얼 번호) 사이에 16진수 FFFF를 삽입하여 생성됩니다. 선택된 48비트 주소가 유일한 Ethernet MAC 주소임을 확인하기 위해, 상위 바이트의 7번째 비트를 1(IEEE G/L 비트와 동일)로 지정하게 됩니다.

IPv6 사이트-로컬 유니캐스트 주소란?

사이트-로컬 유니캐스트 주소는 IPv4 네트워크에서 사용되는 10.0.0.0/8, 172.16.0.0/12 그리고 192.168.0.0/16 등의 사설 주소와 비슷합니다. 사설 주소는 특정 도메인으로의 통신을 제한하거나 글로벌 인터넷과 연결되지 않은 사이트 내에서 고유한 글로벌 프리픽스(prefix) 없이 주소를 할당하기 위해 사용됩니다. IPv6 라우터들은 경로를 알리거나 사이트 범위 밖에 있는 사이트-로컬 소스 및 목적지 주소를 가진 패킷을 전달해서는 안됩니다. 만일 추후 사이트에 글로벌 연결이 필요해지면 글로벌 유니캐스트 프리픽스(prefix)가 해당 사이트에 할당되어야 합니다. 사이트-로컬 주소를 위해 정의된 사이트-로컬 주소 계획은 글로벌 유니캐스트 프리픽스(prefix)를 이용, 직접적으로 적용될 수 있습니다.

그림 8에서 볼 수 있는 사이트-로컬 유니캐스트 주소는 프리픽스(prefix) 범위 FEC0::/10(1111 1110 11)을 이용하고 서브네트 식별자(16비트 Subnet ID 필드)와 EUI-64 포맷의 인터페이스 ID를 연결시킨 IPv6 유니캐스트 주소입니다. 사이트-로컬 유니캐스트 주소 범위는 전체 주소 공간의 1/1024를 차지합니다.

그림 8: IPv6 사이트-로컬 유니캐스트 주소 포맷



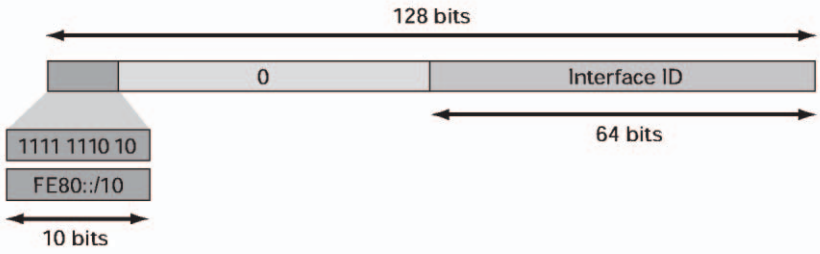
IPv6 링크-로컬 유니캐스트 주소란?

링크-로컬 유니캐스트 주소는 링크-로컬 프리픽스(prefix) FE80::/10(1111 1110 11)와 EUI-64 포맷의 인터페이스 ID를 이용하여 IPv6 노드 인터페이스에서 자동으로 설정되는 IPv6 유니캐스트 주소입니다.

링크-로컬 주소는 4 장에서 다루게 될 네이버 탐색(Neighbor Discovery) 프로토콜과 stateless 자동 설정 프로세스에서 사용됩니다. 링크-로컬 주소는 일반적으로 글로벌 주소를 사용하지 않으면서 같은 로컬 링크 네트워크 상에 있는 장치들을 연결시키기 위해 사용됩니다. 따라서 링크-로컬 주소는 로컬 링크 네트워크 내에서만 유용하게 됩니다.

로컬 링크 상의 노드들은 링크-로컬 주소를 이용하여 라우터가 없이도 서로 통신을 할 수 있습니다. IPv6 노드는 사이트-로컬 또는 고유의 글로벌 주소가 없어도 통신을 할 수 있습니다. IPv6 라우터는 링크-로컬 소스 또는 목적지 주소를 가진 다른 링크 패킷으로 전달해서는 안됩니다. 링크-로컬 유니캐스트 주소 범위는 FE80::/10이며 IPv6 주소 공간의 1/1024를 사용합니다. 그림 9는 링크-로컬 주소의 구조를 보여주고 있습니다.

그림 9: IPv6 링크-로컬 유니캐스트 주소 포맷

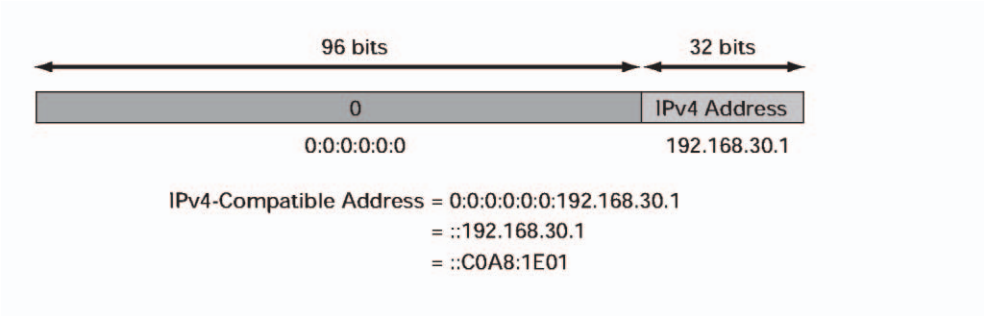


IPv4 호환 IPv6 주소란?

IPv4 호환 IPv6 주소는 IPv4 인프라 상에서 IPv6 패킷을 동적으로 터널링하기 위한 IPv6 변환 메커니즘에서 사용됩니다. IPv4 호환 IPv6 주소는 IPv6 주소의 하위 32비트에 IPv4 주소를 넣고 상위 96비트에 0을 넣은 IPv6 유니캐스트 주소입니다.

IPv4 호환 IPv6 주소의 포맷은 0:0:0:0:0:0:A.B.C.D 또는 ::A.B.C.D입니다. 128비트의 IPv4 호환 IPv6 주소는 노드의 IPv6 주소로 사용되며 하위 32비트에 들어있는 IPv4 주소는 노드의 IPv4 주소로 사용됩니다. IPv4 호환 IPv6 주소는 IPv4 및 IPv6 프로토콜 스택을 모두 지원하고, 5 장에서 다룰 자동 터널에 사용될 노드에 할당됩니다. 그림 10은 IPv4 호환 IPv6 주소의 구조와 주소의 표시 방법을 보여주고 있습니다.

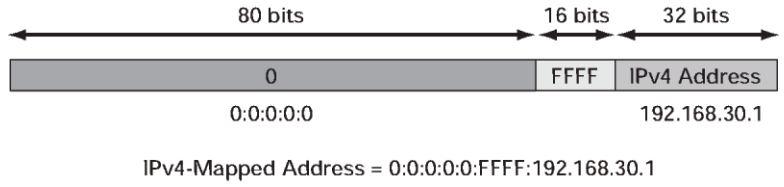
그림 10: IPv4 호환 IPv6 주소 포맷



IPv4 매핑된 IPv6 주소란?

IPv4 매핑된 IPv6 주소는 IPv6 주소의 하위 32비트에 IPv4 주소를, 상위 80비트에 0을 그리고 81에서 96비트에 1을 넣은 IPv6 유니캐스트 주소의 일종입니다. 이 주소는 대부분 IPv4 노드의 주소를 IPv6 주소로 나타내기 위해 사용됩니다. 듀얼 스택 노드의 경우, IPv4 매핑된 IPv6 주소로 표시된 목적지로 트래픽을 보내는 IPv6 어플리케이션은 IPv4 패킷을 해당 목적지로 보내게 됩니다. 그림 11은 IPv4 매핑된 IPv6 주소의 구조를 보여주고 있습니다.

그림 11: IPv4 매핑된 IPv6 주소 포맷



IPv6 애니캐스트 주소

애니캐스트 주소는 보통 서로 다른 노드에 속해있는 인터페이스 집합에 할당되는 글로벌 유니캐스트 주소입니다. 따라서 애니캐스트 주소는 여러 개의 인터페이스를 나타내게 됩니다. 애니캐스트 주소로 보내진 패킷은 애니캐스트 주소에 의해 지정된 가장 가까운 인터페이스로 전달됩니다. 이때 가장 가까운 인터페이스는 사용되고 있는 라우팅 프로토콜의 정의를 따르게 됩니다. 애니캐스트 주소는 구문적으로 글로벌 유니캐스트 주소와 구별할 수 없습니다. 이는 애니캐스트 주소가 글로벌 유니캐스트 주소 공간에서 할당되기 때문입니다.

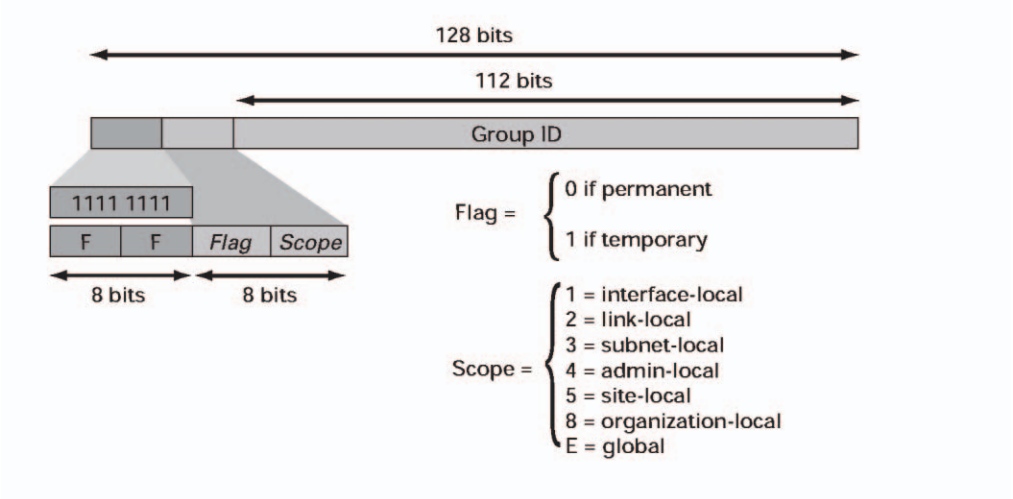
참고: 애니캐스트 주소는 IPv6 패킷의 소스 주소로 사용되어서는 안됩니다.

IPv6 멀티캐스트 주소

IPv6 멀티캐스트 주소(그림 12)는 FF00::/8(1111 1111)을 프리픽스(prefix)로 가지고 있는 IPv6 주소입니다. 멀티캐스트 주소 범위는 전체 IPv6 주소 공간의 1/256을 차지합니다. IPv6 멀티캐스트 주소는 보통 서로 다른 노드에 속해있는 인터페이스 집합을 위한 식별자입니다. 멀티캐스트 주소로 보내진 패킷은 멀티캐스트 주소에 의해 식별된 모든 인터페이스로 전달됩니다.

프리픽스(prefix) 다음에 있는 두 번째 옥텟은 멀티캐스트 주소의 수명과 범위를 정의합니다. 영구적인 멀티캐스트 주소의 수명 매개변수는 0이며 임시 멀티캐스트 주소의 수명 매개변수는 1입니다. 인터페이스, 링크, 서브네트, admin, 사이트, 조직의 범위 또는 글로벌 범위를 가진 멀티캐스트 주소의 범위 매개변수는 각각 1, 2, 3, 4, 5, 8 또는 E 입니다. IPv6 주소 스키마는 수 백만 개의 멀티캐스트 그룹 주소를 지원할 수 있도록 설계되었습니다.

그림 12: IPv6 멀티캐스트 주소 포맷



예약된 멀티캐스트 주소 범위인 FF00::와 FF0F:: 사이에서, 다음과 같은 주소들은 특정 기능을 나타내기 위해 할당됩니다:

FF01::1 – 노드-로컬 범위 내의 모든 노드 (즉, 그 호스트만 해당)

FF02::1 – 로컬 링크 상의 모든 노드 (링크-로컬 범위)

FF01::2 – 노드-로컬 범위 내의 모든 라우터

FF02::2 – 링크-로컬 범위 내의 모든 라우터

FF05::2 – 사이트 내의 모든 라우터 (사이트-로컬 범위)
FF02::1:FFXX:XXXX – Solicited-node 멀티캐스트 주소, XX:XXXX은 노드의 IPv6 주소의 마지막 24비트를 나타냄

TTL(time-to-live) 필드는 IPv6 멀티캐스트에서 사용되지 않는다는 것을 주의하십시오.

IPv6 멀티캐스트 주소와 Ethernet 주소 사이의 상관 관계는 IPv6 멀티캐스트 주소의 마지막 32비트가 멀티캐스트 Ethernet을 위한 33:33: 프리픽스(prefix)에 더해진다는 것입니다. IPv6 멀티캐스트 주소로 패킷을 보내는 호스트는 이 새롭게 만들어진 멀티캐스트 Ethernet 주소를 이용하여 로컬 링크 상의 목적지에 도달하게 됩니다.

IPv6 노드를 위한 멀티캐스트 그룹 멤버쉽 요건

호스트와 라우터의 IPv6 노드 모두 다음의 멀티캐스트 그룹에 합류(그룹으로 향하는 패킷을 수신)해야 합니다:

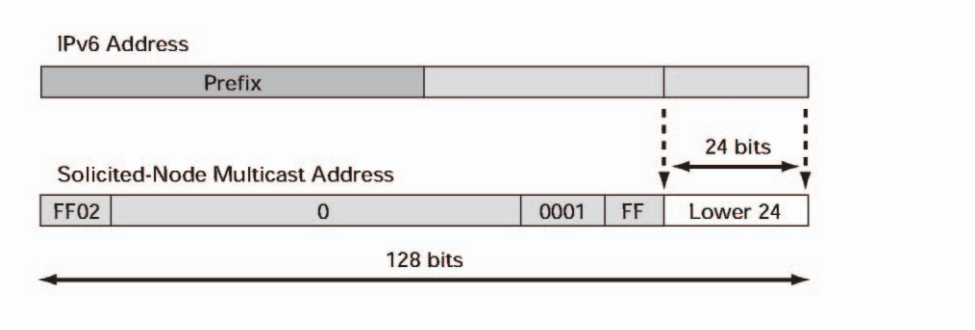
- 전 노드 멀티캐스트 그룹 FF02:0:0:0:0:0:0:1 (범위는 링크-로컬)
- 각각의 지정된 유니캐스트 및 애니캐스트 주소에 대한 Solicited-node 멀티캐스트 그룹 FF02:0:0:0:0:1:FF00:0000/104

추가적으로 IPv6 라우터들은 전 라우터 멀티캐스트 그룹 FF02:0:0:0:0:0:0:2 (범위는 링크-로컬)에도 합류해야 합니다.

IPv6 Solicited-node 멀티캐스트 주소란?

Solicited-node 멀티캐스트 주소는 네이버 탐색(Neighbor Discovery)을 돕기 위해 네이버 요청(Neighbor solicitation) 메시지에서 사용됩니다. 이에 대해서는 4 장에서 다루게 됩니다. Solicited-node 멀티캐스트 주소는 IPv6 유니캐스트 또는 애니캐스트 주소에 해당하는 멀티캐스트 그룹 주소입니다. IPv6 노드는 할당 받은 모든 유니캐스트 및 애니캐스트 주소와 관련된 모든 Solicited-node 멀티캐스트 그룹에 합류해야 합니다. IPv6 solicited-node 멀티캐스트 주소는 그림 13에서와 같이 해당 IPv6 유니캐스트 또는 애니캐스트 주소의 하위 24비트와 연결된 FF02:0:0:0:0:1:FF00:0000/104 프리픽스(prefix)를 가지고 있습니다.

그림 13: IPv6 Solicited-node 멀티캐스트 주소 포맷



예를 들면, IPv6 주소 2037::01:800:200E:8C6C에 해당하는 solicited-node 멀티캐스트 주소는 FF02::1:FF0E:8C6C입니다.

특수 IPv6 주소

이 부분에서 설명된 모든 유니캐스트 주소 외에 IPv6은 비지정 및 루프백 주소도 지원합니다.

IPv6 비지정 주소란?

비지정 IPv6 주소는 주소가 없는 노드가 위치 보유자로 사용하는 특수 주소입니다. 예를 들어, 노드에 할당된 주소가 없어 DHCP 서버에 주소를 요청했을 때, 또는 중복된 주소 탐지 패킷이 전송되었을 때 노드는 비지정 주소를 사용하게 됩니다. 비지정 주소 0:0:0:0:0:0:0:0은 0::0 또는 ::/128로도 표시됩니다.

IPv6 비지정 주소는 아무런 인터페이스에 할당될 수 없으며 IPv6 패킷 또는 IPv6 라우팅 헤더에서 목적지 주소로 사용되어서도 안됩니다.

IPv6 루프백 주소란?

IPv6 루프백 주소는 IP 스택 내의 로컬 인터페이스를 식별합니다. 이는 IPv4의 127.0.0.1 루프백 주소와 비슷합니다. IPv6 루프백 주소는 0:0:0:0:0:0:0:1 또는 ::1로 표시됩니다.

IPv6 루프백 주소는 물리적 인터페이스에 할당될 수 없으며 IPv6 라우터는 IPv6 루프백 주소를 가진 패킷을 소스 또는 목적지 주소로 전달하지 않습니다.

IPv6 주소 할당

Internet Assigned Numbers Authority(IANA)는 전체 주소 공간에서 2001::/16을 레지스트리에 할당합니다. IANA에 따르면, 각 레지스트리는 다음과 같이 2001::/16 공간 내에서 /23 프리픽스(prefix)를 받게 됩니다.

- 2001:0200::/23과 2001:0C00::/23은 아시아 지역에서 사용되기 위해 Asia Pacific Network Information Center(APNIC)에 할당되었습니다.
- 2001:0400::/23은 북남미 지역에서 사용되기 위해 American Registry for Internet Numbers(ARIN)에 할당되었습니다.
- 2001:0600::/23과 2001:0800::/23은 유럽과 중동 지역에서 사용되기 위해 Reseaux IP Europeens – Network Coordination Center(RIPE NCC)에 할당되었습니다.

레지스트리는 IPv6 ISP에게 /32 프리픽스(prefix)를 할당하며 ISP는 /48 프리픽스(prefix)(/32에서 나온)를 각 고객 또는 사이트에 할당합니다. 사이트의 /48 프리픽스(prefix)는 /64 프리픽스(prefix)를 이용하여 각 LAN에 할당될 수 있습니다. 또한 각 LAN에는 최대 64 비트 ID 호스트가 포함될 수 있으며 각 사이트는 최대 65.535 개의 LAN으로 서브네트를 확장시킬 수 있습니다. 사이트에서는 /48 공간 할당을 시작하기 전에 주소 계획을 수립해야 합니다.

ISP가 레지스트리로부터 /32 프리픽스(prefix) 주소 블록을 받으려면 최소 3 개의 다른 ISP와 피어링(peering)하는 외부 라우팅 프로토콜을 가지고 있어야 하며, 고객의 수가 40명 이상 되거나 12개월 내에 IPv6 서비스를 제공하겠다는 의사를 밝혀야 합니다.

IANA에 의한 레지스트리로의 IPv6 주소 공간 할당에 대한 최신 정보는 http://www.iana.org/assignments/ipv6-tls-assignments에서 찾아볼 수 있습니다.

6BONE 네트워크 주소 할당

6BONE은 현재의 인터넷에 있는 IPv4 터널을 이용, WAN 또는 LAN으로 IPv6 트래픽을 전송하는 IPv6 링크를 이용하는 전세계적인 IPv6 네트워크입니다. 6BONE은 새로운 프로토콜, 구현 방법, 변환 메커니즘 및 운영 절차를 시험하기 위한 곳입니다. 6BONE과 관계된 프로젝트는 IETF에서 관할하고 있습니다.

현재의 6BONE 주소 할당은 모든 pTLA(pseudo Top-Level Aggregator)가 /28 프리픽스(prefix)를 받는 3ffe:0000::/16에서 시작됩니다. 이 프리픽스(prefix)는 3ffe:0800:/28 범위 내에 있으며 최대 2048개의 pTLA를 허용합니다. 엔드 사이트는 업스트림 제공자로부터 /48을 받게 되며 사이트 내의 LAN은 해당 사이트 프리픽스(prefix)로부터 /64 프리픽스(prefix)를 할당받게 됩니다.

6BONE 구조도는 제공자 네트워크의 계층 구조입니다. IANA 및 6BONE 정책에 의한 6BONE 주소 할당은 RFC 2921, *6BONE pTLA and pNLA Formats (pTLA)*에 정의되어 있습니다.

IPv6 주소는 URL에서 어떻게 표시되나?

콜론(:)은 다음의 URL 예에서 볼 수 있는 것과 같이 이미 URL에서 옵션 포트 번호를 나타내기 위해 사용되고 있습니다: http://www.abc.test:8080/index.html. 따라서 URL에서는 IPv6 주소를 나타내기 위해 콜론을 사용할 수 없습니다. 만일 URL에 두 개의 콜론이 있다면, URL 구문 해석기는 포트 번호의 콜론과 IPv6 주소 내의 콜론을 구분할 수 있어야 합니다. 하지만 압축 기술의 사용은 이를 불가능하게 합니다.

콜론을 유지하면서 IPv6 주소를 나타내려면, 주소가 다음과 같이 [] 안에 들어가 있어야 합니다:

http://[2001:1:4F3A::206:AE14]:8080/index.html

URL 내에서 IPv6 주소를 사용하는 것은 거추장스럽기 때문에 진단 용도로, 또는 네이밍 서비스가 없을 때만 사용할 것을 권장합니다. 그 외의 경우에는 정식 도메인 이름만을 사용할 것을 권장합니다.

IPv6 호스트에서 요구하는 IP 주소의 수는?

IPv6 노드는 올바른 운영을 위해 다음의 IPv6 주소를 요구합니다:

- 각 인터페이스를 위한 링크-로컬 주소
- 할당된 유니캐스트 주소
- 루프백 주소
- 전 노드 멀티캐스트 주소
- 할당된 유니캐스트 및 애니캐스트 주소를 위한 Solicited-node 멀티캐스트 주소
- 호스트가 속해있는 다른 모든 그룹의 멀티캐스트 주소
- 사이트-로컬 주소(사용될 경우)

IPv6 라우터에서 요구하는 IP 주소의 수는?

IPv6 라우터는 올바른 운영을 위해 다음의 IPv6 주소를 요구합니다:

- 모든 필요한 노드 주소
- 전 라우터 멀티캐스트 주소
- 전달 인터페이스 역할을 하도록 설정된 인터페이스를 위한 서브네트-라우터 애니캐스트 주소
- 기타 애니캐스트 설정 주소
- 라우팅 프로토콜을 위한 특정 멀티캐스트 주소

4 장

IPv6 운영

IPv6 네이버 탐색(Neighbor Discovery)프로토콜과 ICMP(Internet Message Control Protocol)는 IPv6 운영에 매우 중요합니다.

이 장에서는 다음 주제들을 다루게 됩니다:

- 네이버 탐색(Neighbor Discovery)
- 라우터 탐색 (Router Discovery)
- Stateless autoconfiguration
- 경로 최대 전송 유닛(MTU) 검색
- Dynamic Host Configuration Protocol Version 6(DHCPv6)
- Domain Name Server(DNS) 운영

네이버 탐색(Neighbor Discovery)

네이버 탐색(Neighbor Discovery) 프로토콜은 IPv6 노드와 라우터가 다음과 같은 일을 할 수 있게 해줍니다:

- 같은 링크에 있는 네이버의 링크-레이어 주소 결정
- 네이버 라우터 찾기
- 네이버 추적

IPv6 네이버 탐색(Neighbor Discovery) 프로세스는 같은 네트워크(로컬 링크)에 있는 네이버의 링크-레이어 주소를 결정하고, 네이버로의 도달 가능성을 확인하고, 네이버 라우터를 추적하기 위해 IPv6 ICMP(ICMPv6) 메시지와 solicited-node 멀티캐스트를 이용합니다. 모든 IPv6 노드는 각각의 유니캐스트 및 애니캐스트 주소에 해당하는 멀티캐스트 그룹에 합류해야 합니다.

IPv6 네이버 검색 프로세스는 운영을 위해 다음과 같은 메커니즘을 사용합니다:

- 네이버 요청(Neighbor solicitation)
- 네이버 선언(Neighbor advertisement)

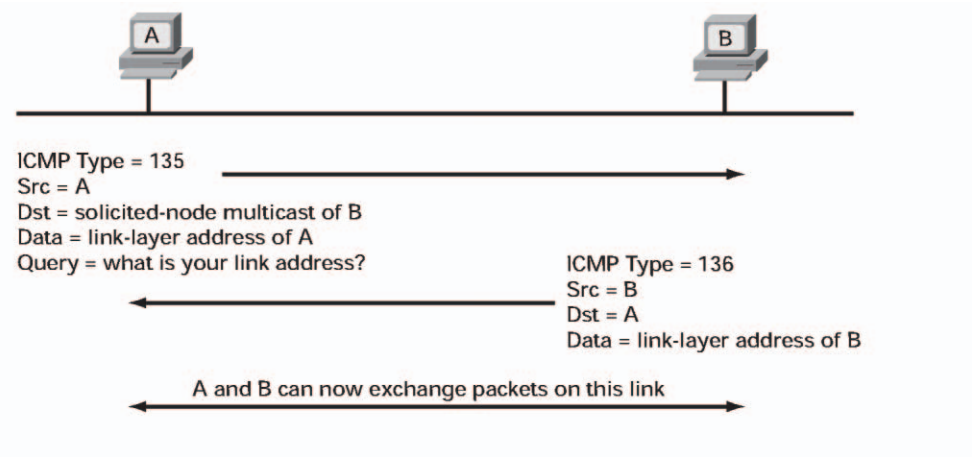
IPv6 네이버 요청(Neighbor solicitation)이란?

네이버 요청(Neighbor solicitation) 메시지는 노드가 동일한 로컬 링크 상에 있는 다른 노드의 링크-레이어 주소를 결정하고자 할 때 로컬 링크로 보내어집니다. 이 기능은 IPv4의 ARP와 비슷하지만 IPv4 ARP 메시지에서 사용되는 브로드캐스트를 사용하지 않아 모든 노드가 관련 없는, 불필요한 브로드캐스트 요청을 받게 되는 일이 없습니다.

소스 노드는 목적지 노드의 IPv6 주소에서 가장 오른쪽 24비트를 받은 후, 로컬 링크의 solicited-node 멀티캐스트 그룹 주소로 ICMP 패킷 헤더의 Type 필드 값이 135인 네이버 요청(Neighbor solicitation) 메시지를 보냅니다. 목적지 노드는 해당 노드의 링크-레이어 주소로 응답합니다. 네이버 요청(Neighbor solicitation) 메시지를 보내기 위해, 소스 노드는 먼저 DNS 같은 네이밍 서비스 메커니즘을 이용, 목적지 노드의 IPv6 유니캐스트 주소를 알아내야 합니다.

네이버 요청(Neighbor solicitation) 메시지는 네이버의 링크-레이어 주소를 알아낸 다음 네이버로의 도달 가능성을 확인하기 위해서도 사용될 수 있습니다. 그림 14는 네이버 요청(Neighbor solicitation) 메시지가 네이버의 링크-레이어 주소를 결정하기 위해 어떻게 사용되는지 보여주고 있습니다.

그림 14: 네이버 요청(Neighbor solicitation) 메시지



IPv6 네이버 선언(Neighbor advertisement)이란?

IPv6 네이버 선언(Neighbor advertisement) 메시지는 IPv6 네이버 요청(Neighbor solicitation) 메시지에 대한 응답입니다. 네이버 요청(Neighbor solicitation) 메시지를 수신한 다음, 목적지 노드는 ICMP 패킷 헤더의 Type 필드 값을 136으로 하여 네이버 선언(Neighbor advertisement) 메시지를 로컬 링크에 전송합니다. 네이버 선언(Neighbor advertisement)을 수신한 다음, 소스 노드와 목적지 노드는 통신을 할 수 있게 됩니다.

네이버 선언(Neighbor advertisement) 메시지는 로컬 링크에 있는 노드의 링크-레이어 주소가 변경되었을 때도 전송됩니다.

IPv6 라우터 탐색 (Router Discovery)

IPv6 라우터 탐색 (Router Discovery)은 IPv6 노드가 로컬 링크에 있는 라우터를 탐색하기 위해 사용합니다. IPv6 라우터 탐색 (Router Discovery) 프로세스는 나중에 설명할 하나의 커다란 차이점을 빼고는 IPv4의 ICMP 라우터 탐색 (Router Discovery)과 비슷합니다.

IPv6 라우터 발견 프로세스는 다음과 같은 이용합니다:

- 라우터 선언(Router Announcements)
- 라우터 요청(Router Solicitation)

IPv6 라우터 선언(Router Announcements)이란?

라우터 선언(Router Announcements) 메시지는 IPv6 라우터에 설정된 모든 인터페이스에서 정기적으로 보내집니다. 라우터 선언(Router Announcements)은 링크에 있는 IPv6 노드로부터의 라우터 요청(Router Solicitation) 메시지에 대한 응답으로도 보내집니다. 라우터 선언(Router Announcements)은 라우터 요청(Router Solicitation) 메시지를 보낸 노드의 전 노드 링크-로컬 멀티캐스트 주소(FF02::1) 또는 유니캐스트 IPv6 주소로 전송됩니다.

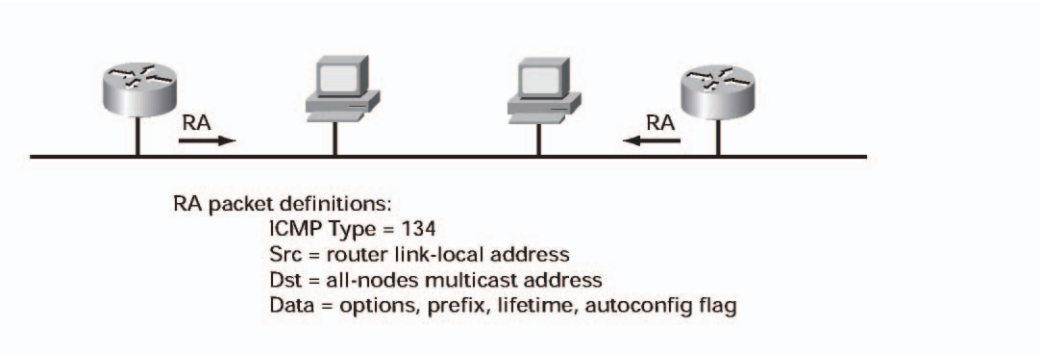
라우터 선언(Router Announcements)은 ICMP 패킷 헤더의 Type 필드 값이 134이며 메시지에 다음과 같은 정보를 포함합니다:

- 노드가 주소 자동 설정을 사용할 수 있는지 여부
- 완료될 수 있는 자동 설정의 종류(stateless 또는 stateful)를 나타내는 플래그
- 로컬 링크의 노드가 IPv6 주소를 자동 설정하기 위해 사용할 수 있는 하나 이상의 온링크 IPv6 프리픽스(prefix)

- 선언에 포함된 각 프리픽스(prefix)의 수명 정보
- 선언을 보내는 라우터가 기본 라우터로 사용될 것인지에 대한 여부와 그럴 경우 라우터가 기본 라우터로 사용되는 시간(초 단위)
- 호스트가 시작하는 패킷에 사용될 hop 제한, MTU 등과 같은 호스트를 위한 추가 정보

로컬 링크의 IPv6 노드는 라우터 선언(Router Announcements) 메시지를 수신한 다음 그 정보를 이용하여 기본 라우터, 프리픽스(prefix) 목록 그리고 기타 업데이트된 설정 매개변수에 대한 정보를 유지합니다. 그림 15는 라우터 선언(Router Announcements)의 예를 보여주고 있습니다.

그림 15: 라우터 선언(Router Announcements)



IPv6 라우터 요청(Router Solicitation)이란?

시스템 시동 때와 같이 호스트에 설정된 유니캐스트 주소가 없을 때, 호스트는 라우터 요청(Router Solicitation) 메시지를 보냅니다. 라우터 요청(Router Solicitation)은 호스트가 다음 예약된 라우터 선언(Router Announcements) 메시지를 기다리지 않고도 빠르게 스스로를 자동 설정할 수 있게 해주므로 유용합니다. 라우터 요청(Router Solicitation) 메시지는 ICMP 패킷 헤더의 Type 필드 값이 133입니다.

라우터 요청(Router Solicitation) 메시지에 사용되는 소스 주소는 대부분 비지정 IPv6 주소 (0:0:0:0:0:0:0:0)입니다. 만일 호스트가 설정된 유니캐스트 주소를 가지고 있으면, 라우터 요청(Router Solicitation) 메시지를 보내는 인터페이스의 유니캐스트 주소가 메시지의 소스 주소로 사용됩니다.

라우터 요청(Router Solicitation) 메시지의 목적지 주소는 링크-로컬 범위의 전 라우터 멀티캐스트 주소 (FF02::2)입니다. 라우터 요청(Router Solicitation)에 대한 응답으로 라우터 선언(Router Announcements)을 보낼 때, 라우터 선언(Router Announcements) 메시지에 사용되는 목적지 주소는 라우터 요청(Router Solicitation) 메시지 소스의 유니캐스트 주소가 됩니다.

참고: 라우터 요청(Router Solicitation)은 부팅 시 그리고 그 후 3회만 전송됩니다. 이는 네트워크에 라우터가 없을 때 라우터 요청(Router Solicitation) 패킷이 넘치는 것을 막기 위해서 입니다.

IPv6 리다이렉트 메시지

IPv4에서와 마찬가지로 IPv6 리다이렉트 메시지 역시 패킷을 더 나은 라우터로 재라우팅하는 것을 돕기 위해서만 사용됩니다. 리다이렉트 메시지를 수신하는 노드는 패킷을 더 나은 라우터로 재전송하게 됩니다. 라우터는 유니캐스트 트래픽을 위해서만 시작 노드로 리다이렉트 메시지를 보내서 노드들이 이를 처리할 수 있도록 합니다.

Stateless 자동 설정

Stateless 자동 설정은 IPv6의 주요 기능입니다. 이 기능은 IPv6 노드의 서버가 없는 기본 구성과 쉬운 리넘버링(renumbering)을 가능케 합니다. Stateless 자동 설정은 라우터 선언(Router Announcements) 메시지 내의 정보를 이용하여 노드를 설정합니다. 라우터 선언(Router Announcements)에 포함된 프리픽스(prefix)는 노드 주소를 위한 /64 프리픽스(prefix)처럼 사용됩니다. Ethernet에서는 나머지 64비트를 EUI-64 포맷의 인터페이스 ID로부터 얻어냅니다. 따라서 IPv6 노드는 자신의 링크-레이어 주소(EUI-64 포맷)를 로컬 링크 프리픽스(prefix)(64비트)에 첨부함으로써 고유한 글로벌 IPv6 주소를 자동 설정할 수 있습니다.

IPv6 노드의 리넘버링(renumbering)

IPv6 노드의 리넘버링(renumbering)은 라우터 선언(Router Announcements)의 도움으로 가능합니다. 라우터 선언(Router Announcements) 메시지는 이전 프리픽스(prefix)와 새로운 프리픽스(prefix)를 모두 포함하고 있습니다. 이전 프리픽스(prefix)의 수명 값이 감소하면 이전 프리픽스(prefix)를 통한 현재의 연결을 유지시키면서 동시에 노드가 새로운 프리픽스(prefix)를 사용하도록 알려줍니다. 이 기간 동안 노드는 2개의 유니캐스트 주소를 사용하게 됩니다. 이전 프리픽스(prefix)를 더 이상 사용할 수 없게 되면, 라우터 선언(Router Announcements)에 새로운 프리픽스(prefix)만이 포함되게 됩니다.

만일 리넘버링(renumbering)에 stateless 자동 설정을 사용하지 않으면 다른 리넘버링(renumbering) 방법을 사용해야 합니다. 자동 설정은 리넘버링(renumbering) 프로세스에 커다란 도움이 됩니다. 리넘버링(renumbering)은 DNS 항목 변경과 새로운 IPv6 DNS 기록의 도입을 필요로 합니다. 사이트 전체를 리넘버링(renumbering)하기 위해서는 모든 라우터를 리넘버링(renumbering)해야 합니다. 라우터 리넘버링(renumbering) 프로토콜은 IETF에서 제안되었습니다.

Stateless 자동 설정은 DNS 해석을 위해 DNS 서버를 찾는 문제나 DNS 공간에 컴퓨터를 등록하는 문제는 처리하지 않습니다. 이 문제들은 IETF에서 논의되고 있습니다.

중복 주소 탐지는 어떻게 이뤄지나?

IPv6은 네트워크 내의 중복된 주소를 탐지하기 위한 보호 메커니즘도 제공하여 주소 충돌을 예방합니다. IPv6은 네이버 요청(Neighbor solicitation)을 이용하여 링크 상의 다른 노드가 같은 IPv6 주소를 가지고 있는지 탐지합니다.

중복 주소 탐지는 자동 설정 프로세스 동안 다른 노드가 자동 설정된 주소를 이용하지 않도록 하기 위해 사용됩니다.

경로 최대 전송 유닛(MTU) 탐색

IPv6 라우터들은 프레그먼트를 처리하지 않기 때문에 프레그먼트는 필요에 따라 시작 노드 또는 패킷의 소스 노드에서 처리됩니다. 경로 MTU 탐색 프로세스는 IPv6 네트워크 내의 호스트들이 프레그먼트를 처리하기 위해 매우 중요합니다. IPv6은 경로 MTU 탐색을 이용하여 소스와 목적지 사이의 경로의 최대 MTU를 알아냅니다. 소스 노드는 패킷을 실제로 보내기 전에 경로 MTU 탐색 프로세스를 시작합니다. IPv6 네트워크 내의 주어진 데이터 경로에 있는 모든 링크의 경로 MTU가 패킷을 수용할 만큼 크지 않을 경우에는 소스 노드가 패킷을 프레그먼트한 다음 이를 재전송합니다.

IPv4에서처럼 IPv6의 경로 MTU 탐색은 노드가 주어진 데이터 경로에 있는 모든 링크의 MTU 크기 차이를 동적으로 탐색하고 여기에 적응할 수 있도록 합니다. IPv4에서는 최소 링크 MTU 크기가 68 옥텟이었으며 권장 최소 크기는 576 옥텟이었습니다. 이는 재구성 버퍼의 최소 크기입니다. 따라서 모든 IPv4 패킷의 길이는 68 옥텟 이상이어야 합니다.

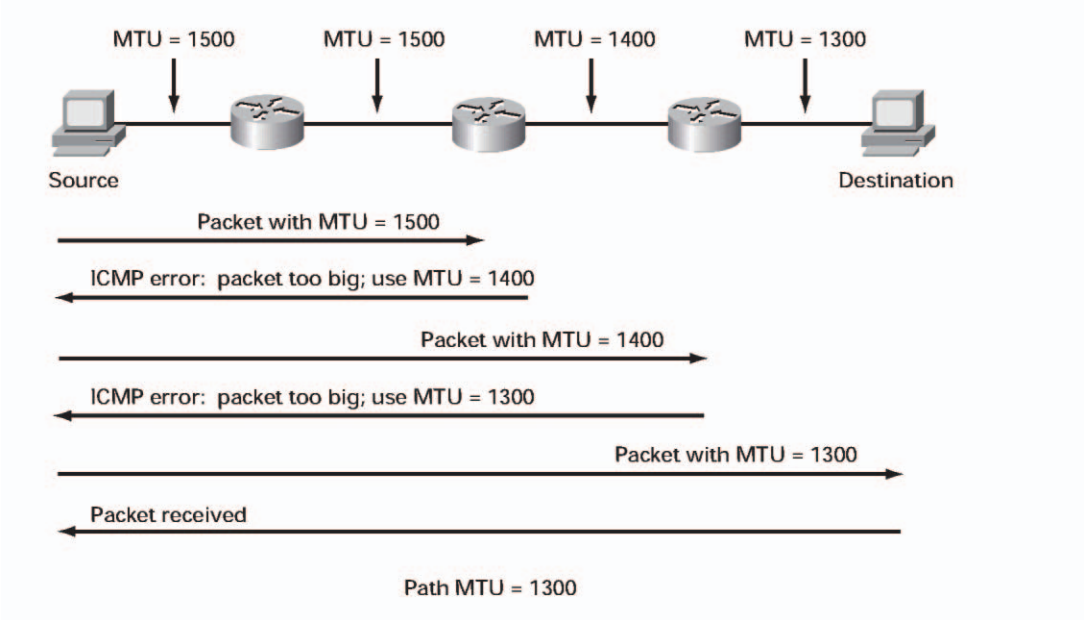
IPv6의 최소 링크 MTU는 1280 옥텟이지만 IPv6 링크의 권장 MTU 값은 1500 옥텟입니다. 기본 IPv6 헤더가 지원하는 최대 패킷 크기는 64,000 옥텟입니다. 점보그램이라 불리는 더 큰 패킷들은 hop-by-hop 확장자 헤더 옵션을 이용해 처리될 수 있습니다.

IPv6 경로 MTU 탐색은 어떻게 이뤄지나?

IPv6 소스 노드는 링크 레이어의 최소 MTU와 같은 크기의 패킷을 전송합니다. 그림 16의 예를 보면, 크기가 1500인 MTU가 사용되고 있습니다. 패킷은 경로 내에서 더 작은 MTU를 만나기 전까지 네트워크를 거쳐 목적지로 전달됩니다. 패킷이 더 작은 MTU를 가진 링크를 만나면, 라우터가 소스 노드로 "packet too big"이라는 이름의 ICMP 오류 메시지를 보냅니다. ICMP 패킷 내용에는 다음 링크의 MTU 크기가 포함되며 이는 패킷의 크기보다 작습니다(예를 들면 그림 16의 마지막 두 링크에 있는 1400과 1300).

소스 IPv6 노드는 수신된 최대 MTU와 같은 크기의 패킷을 재전송합니다. 이 프로세스는 패킷이 목적지에 도달할 때까지 반복됩니다. 이 예에서 마지막 링크의 경로 MTU는 1300이 됩니다.

그림 16: 경로 MTU 탐색



DHCP(Dynamic Host Configuration Protocol) Version 6

클라이언트를 위한 설정 데이터를 얻는 과정은 IPv4와 비슷합니다. 하지만 DHCPv6은 많은 메시지에 멀티캐스트를 사용합니다. 초기에 클라이언트는 우선 네이버 탐색(Neighbor Discovery) 메시지를 이용하여 링크 상의 라우터 존재를 탐색해야 합니다. 만일 라우터가 발견되면, 클라이언트가 라우터 선언(Router Announcements)을 검토하여 DHCP를 사용할지 결정합니다. 만일 라우터 선언(Router Announcements)이 해당 링크에 DHCP를 사용하도록 허용하거나 라우터가 발견되지 않았다면, 클라이언트는 DHCP 서버를 찾기 위해 DHCP 요청 단계를 시작합니다.

다음은 DHCPv6의 혜택들입니다:

- serverless/stateless 자동 설정보다 통제가 용이
- 라우터가 없이 서버만 사용하는 환경에서 활용
- stateless 자동 설정과 동시에 사용
- 리넘버링(renumbering)을 위해 사용

- 동적 DNS를 이용한 호스트의 자동 도메인 이름 등록에 사용
- IPv6 프리픽스(prefix)를 하단의(leaf) CPE(customer-premise equipment) 라우터에 내려 보내 줄 때 사용.

IPv6 DNS(Domain Name System) 운영

IPv6은 IPv6 주소에 DNS name-to-address 및 address-to-name 검색 프로세스에서 지원되는 새로운 DNS 레코드 종류를 도입했습니다. DNS 쿼리는 IPv4와 IPv6 트랜스포트에서 모두 가능합니다. 하지만 DNS 루트 서버는 아직 IPv6 트랜스포트를 통해 도달할 수 없습니다. 레코드 종류는 다음과 같습니다:

AAAA 레코드 – "quad A" 레코드라고도 불리는 이 레코드는 IPv6 주소에 호스트 이름을 매핑합니다. 이 레코드는 IPv4의 A 레코드와 같으며 다음 포맷을 사용합니다: www.abc.test AAAA 3FFE:B00:C18:1::2. IETF는 이 레코드를 host name-to-IP address resolution에 사용하기로 했습니다.

A6 레코드 – IETF에 의해 시험용으로 지정된 A6 레코드는 상용 네트워크에서는 사용되지 않을 예정입니다. AAAA 레코드와 같지만 네트워크 리넘버링(renumbering)을 단순화하기 위해 IPv6 주소를 계층 방식으로 저장할 수 있게 해줍니다.

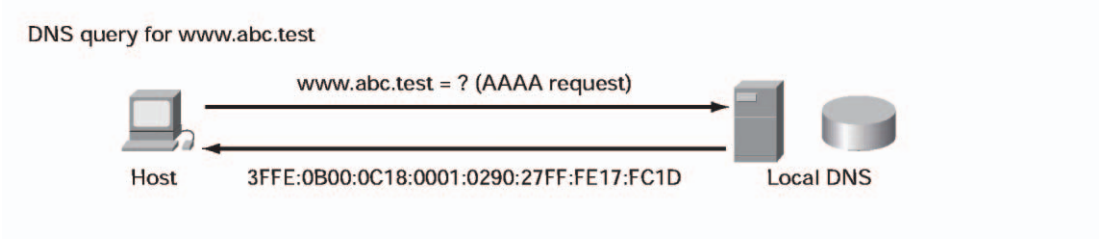
PRT 레코드 – IPv4에서 address-to-host 이름 매핑을 지정해주는 포인터(PTR) 레코드와 같습니다. IP address-to-host name 탐색에 이용되는 역 매핑에 PTR 레코드가 사용됩니다. IPv6 주소의 최상위 도메인은 ip6.arpa입니다. 처음에는 IPv6 DNS를 위한 최상위 도메인이 ip6.int였습니다. PTR 레코드는 다음 포맷을 사용합니다: 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.0.0.b.0.e.f.f.3.ip6.arpa PTR www.abc.test.

DNAME 및 Binary Labels 레코드 – 이 새로운 레코드들은 역 매핑을 위한 리넘버링(renumbering)을 쉽게 해줍니다(IP address-to-host name)

DNS Resolution을 위한 AAAA 레코드 활용

노드가 다른 노드(www.abc.test)의 IPv6 주소를 필요로 하면, www.abc.test에 대한 AAAA 요청을 DNS로 전송합니다. Abc.test 도메인에 대한 권한을 가진 DNS는 요청된 IPv6 주소(이 경우에는 3FFE:0B00:0C18:0001:0290:27FF:FE17:FC1D)로 응답하게 됩니다. AAAA 레코드는 하나의 IPv6 주소를 저장합니다. 하나 이상의 주소를 가진 노드는 DNS 데이터베이스에 하나 이상의 레코드를 가지고 있어야 합니다. 그림 17은 host name-to-IP address 쿼리를 해결하기 위한 AAAA 레코드 종류의 활용을 보여주고 있습니다.

그림 17: AAAA 레코드를 통한 DNS 해결



만일 네트워크 리넘버링(renumbering)에 DNS가 사용되었다면, 모든 노드의 IPv6 주소 프리픽스(prefix) 부분이 변경되어야 합니다. DNS에 포함된 노드의 경우에는 DNS 데이터베이스 내에서 이 새 주소가 변경되어야 합니다.

5 장

통합 및 공존 전략

모든 새로운 기술의 성공적인 시장 도입은 심각한 서비스 장애 없이 기존 인프라와 얼마나 쉽게 통합될 수 있는가에 달려있습니다. 인터넷은 수 십만 개의 IPv4 네트워크와 수 백만 개의 IPv4 노드로 구성되어 있습니다. 통합 및 변환을 최대한 투명하게 하는 것이야말로 가장 큰 과제입니다.

여러 분야에서 IPv6을 도입하는데 걸릴 것으로 예상되는 기간은 다음과 같습니다:

- 1996-2002: 모든 새로운 기술과 마찬가지로, 기술 전문가와 학술 기관에서 가장 먼저 IPv6 네트워크를 도입했습니다. 얼리어댑터들을 지원하기 위해 Cisco IOS 소프트웨어를 위한 IPv6가 1996년부터 초기 필드 시험(EFT)을 위해 제공되었습니다.
- 2001-2005: IPv6 도입을 위한 필수조건인 IPv6로의 기존 어플리케이션 포팅은 2001년 후반부터 시작되었습니다. 이 과정은 3년 이상 걸릴 것으로 예상되고 있습니다.
- 2001-2005: 2001년 후반부터 인터넷 서비스 공급자들이 IPv6 서비스를 고객에게 제공하기 위해 이를 도입하기 시작했습니다. ISP 도입 단계는 3년 이상 걸릴 것을 예상되고 있습니다.
- 2003-2010: 온라인 게임 및 피어-투-피어 컴퓨팅 같은 어플리케이션의 공급이 소비자들의 IPv6 서비스 도입을 좌우하게 될 것이며 이 과정은 2003년부터 시작되어 5년 이상 걸릴 것으로 예상되고 있습니다.
- 2003-2010: 소비자들의 IPv6 서비스 도입과 비슷하게, 기업들 역시 어플리케이션 공급을 기다리고 있으며 2003년부터 IPv6 도입을 시작할 것으로 예상하고 있습니다.

IETF IPv6 워킹 그룹은 IPv6 도입을 위해 여러 가지 전략을 구상했습니다. 이 장에서는 다음과 같은 변환 전략을 다루게 됩니다:

- 듀얼 스택 백본 상에서의 IPv6 배치
- IPv4 터널 상에서의 IPv6 배치
- 전용 데이터 링크 상에서의 IPv6 배치
- MPLS 백본 상에서의 IPv6 배치
- 프로토콜 변환 메커니즘을 이용한 IPv6 배치

변환 메커니즘

네트워크 설계자들은 통합으로 인한 비용과 운영에 미치는 영향을 줄이기 위해 IPv6 배치를 네트워크 에지에서 시작하여 네트워크 코어로 이동할 것을 권장합니다. IPv6을 네트워크 에지에 배치하는데 사용되는 핵심 전략에는 IPv4 네트워크로 IPv6 트래픽을 진입시키는 것, 네이티브 IPv6 백본으로의 완전한 변환이 이뤄지기 전에 고립된 IPv6 도메인끼리 서로 통신하도록 하는 것 등이 포함됩니다. 또한 에지에서 코어에 이르는 네트워크 전반에 걸쳐 IPv4와 IPv6을 같이 실행하거나 서로 다른 프로토콜로 구동되는 호스트들이 서로 통신을 할 수 있도록 IPv4와 IPv6 간의 통역을 제공하는 것도 가능합니다. 이런 기법들은 IPv4 서비스에 지장을 주지 않으면서 네트워크를 업그레이드하고 IPv6을 점진적으로 배치할 수 있도록 해줍니다.

IPv6을 배치하기 위한 4가지 핵심 전략은 다음과 같습니다:

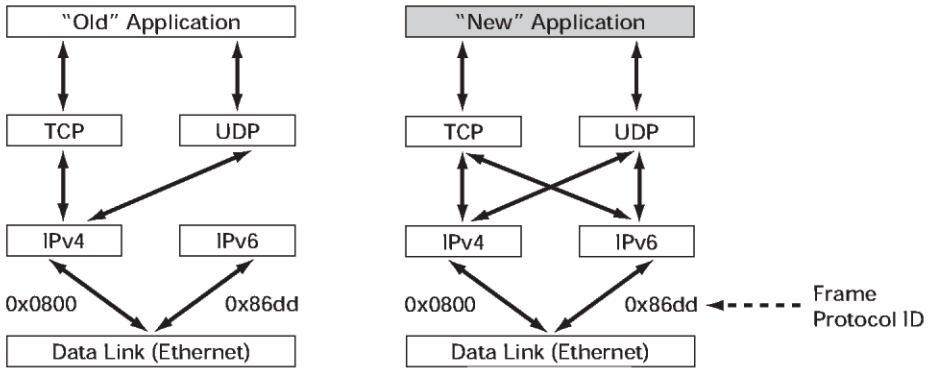
- **듀얼 스택 백본 상에서의 IPv6 배치** – 이 기법은 IPv4와 IPv6 어플리케이션이 듀얼 IP 레이어 라우팅 백본에서 공존할 수 있도록 합니다. 네트워크 내의 라우터 전체 또는 일부(예를 들면 액세스 CPE 라우터와 집합 라우터들은 듀얼 스택으로 하고 코어 라우터는 그대로 두는)를 듀얼 스택으로 업그레이드 하여 IPv4 통신은 IPv4 프로토콜 스택을 이용하고 IPv6 통신은 IPv6 스택을 이용하도록 합니다.
- **IPv4 터널 상에서의 IPv6 배치** – 이 터널들은 IPv4 패킷 내에서 IPv6 트래픽을 캡슐화하며 고립된 IPv6 사이트 간의 통신이나 IPv4 백본을 통한 원격 IPv6 네트워크로의 연결을 위해 사용됩니다. 이 기법은 수동 설정 터널, 일반 라우팅 캡슐화(GRE) 터널, 터널 브로커 서비스 같은 반자동 터널 메커니즘 그리고 WAN용 6to4과 캠퍼스 환경용 ISATAP(intra-site automatic tunnel addressing protocol) 같은 완전한 자동 터널 메커니즘을 포함합니다.
- **전용 데이터 링크 상에서의 IPv6 배치** – 이 기법은 IPv6 도메인이 IPv4에서 사용되는 것과 동일한 Layer 2 인프라를 이용하여 통신할 수 있도록 하지만 IPv6은 별도의 Frame Relay나 ATM PVC(permanent virtual circuit), 옵티컬 링크 또는 DWDM(dense wave division multiplexing)을 사용하게 됩니다.
- **MPLS 백본 상에서의 IPv6 배치** – 이 기법은 코어 인프라를 변경하지 않고 MPLS IPv4 백본을 통해 고립된 IPv6 도메인들이 서로 통신할 수 있게 합니다. 네트워크의 여러 지점마다 서로 다른 기법을 사용할 수 있지만 그럴 때마다 백본 인프라를 조금씩 수정하거나 코어 라우터를 재설정해야 합니다. 왜냐하면 IP 헤더 자체가 아닌 레이블을 기반으로 전달이 이뤄지기 때문입니다.

IPv4-IPv6 프로토콜 듀얼 스택 장치 사용

듀얼 스택 백본은 IPv4와 IPv6을 동시에 라우팅하기 위한 기본적인 전략이며 이를 위해서는 라우터나 엔드 시스템 같은 네트워크 장치들이 IPv4와 IPv6 프로토콜 스택을 모두 실행해야 합니다. 듀얼 스택 엔드 시스템은 어플리케이션들이 한번에 하나씩 IPv4에서 IPv6 트랜스포트로 이전할 수 있도록 합니다. IPv6 스택을 지원하도록 업그레이드되지 않은 어플리케이션들은 동일한 엔드 시스템 상에서 업그레이드된 어플리케이션과 공존할 수 있습니다.

그림 18에서 볼 수 있듯, 새롭게 업그레이드된 어플리케이션은 IPv4와 IPv6 프로토콜 스택을 모두 사용합니다. IPv4와 IPv6 주소 및 DNS 요청을 지원하기 위해 새로운 API(application programming interface)가 정의되었습니다. 새로운 API로 업그레이드된 어플리케이션이라도 IPv4 프로토콜 스택만을 사용할 수 있습니다.

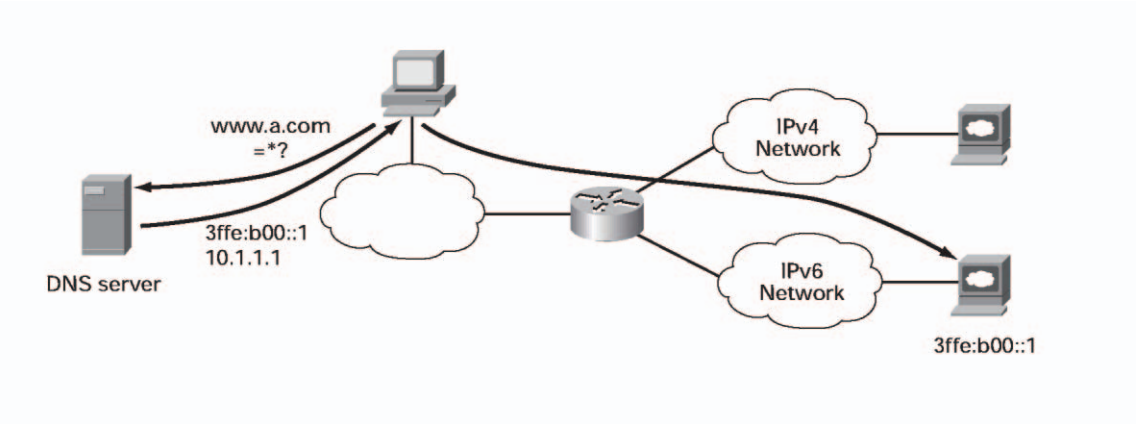
그림 18: IPv4-IPv6 듀얼 스택



어플리케이션은 이름 검색을 기반으로 IPv4와 IPv6 프로토콜 가운데 어떤 것을 사용할 것인지 선택하게 됩니다. 이 때 DNS는 IPv4와 IPv6 주소를 모두 보낼 수 있으며 어플리케이션(IETF 문서 Default Address Selection for IPv6에 정의된 규칙에 따르면 시스템이 될 수도 있음)은 IP 트래픽의 종류와 통신의 특정 요건에 따라 올바른 주소를 선택하게 됩니다.

듀얼 IPv4와 IPv6 프로토콜 스택을 지원하는 어플리케이션은 목적지 호스트 이름(예를 들면 www.a.com)을 위해 DNS 서버로부터 모든 가능한 주소를 요청하게 됩니다. DNS 서버는 www.a.com을 위한 모든 가능한 주소(IPv4와 IPv6 주소)로 응답하게 됩니다. 어플리케이션은 주소를 하나 선택(대부분의 경우 IPv6 주소가 기본 선택)한 다음 IPv6 프로토콜 스택을 이용하여 소스 노드와 목적지 노드를 연결합니다. 그림 19는 IPv4와 IPv6 듀얼 스택 운영을 보여주고 있습니다.

그림 19: IPv4-IPv6 듀얼 스택 운영



듀얼 스택 백본을 이용한 IPv6 배치

듀얼 스택 백본 배치에서는 네트워크 내의 모든 라우터가 듀얼 스택으로 업그레이드 되어야 합니다. IPv4 통신은 IPv4 프로토콜 스택을 이용, IPv4 전용 라우팅 프로토콜을 통해 얻은 경로를 기반으로 IPv4 패킷을 전송하며 IPv6 통신은 IPv6 전용 라우팅 프로토콜을 통해 얻은 경로와 IPv6 스택을 이용합니다.

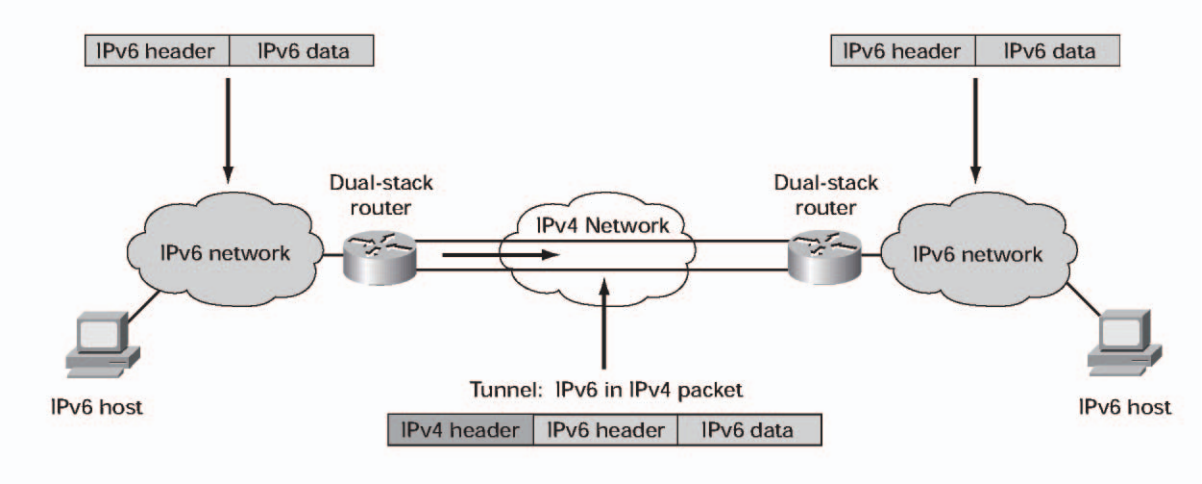
어플리케이션은 DNS 해결 라이브러리로부터의 응답에 따라 IPv4를 사용할 것인지 IPv6을 사용할 것인지 선택하며 IP 트래픽의 종류와 통신의 특정 요건에 따라 올바른 주소를 선택하게 됩니다.

듀얼 스택 라우팅은 IPv4와 IPv6 어플리케이션이 혼합되어 있어 두 가지 프로토콜을 모두 설정해야 할 필요가 있는 특정 네트워크 인프라에서 유효한 배치 전략입니다. 하지만 네트워크 내의 모든 라우터를 업그레이드해야 한다는 점과 라우터에 듀얼 주소 스키마가 정의되어야 한다는 것, IPv4와 IPv6 라우팅 프로토콜을 모두 관리해야 하고 IPv4와 IPv6 라우팅 테이블을 모두 수용할 수 있도록 충분한 메모리를 제공해야 한다는 점은 이 접근 방식의 한계입니다.

IPv4 터널 상에서의 IPv6 배치

터널링은 IPv4 패킷 내에 IPv6을 캡슐화하여 이를 IPv4 백본 상으로 전송할 수 있게 하므로 IPv4 인프라를 업그레이드하지 않아도 고립된 IPv6 엔드 시스템과 라우터가 서로 통신할 수 있게 해줍니다. 터널링은 IPv4와 IPv6 공존 기간 동안 서비스 공급자와 기업이 사용할 수 있는 주요 배치 전략입니다. 그림 20은 IPv4 터널 상에서의 IPv6 활용을 보여주고 있습니다.

그림 20: 터널 상에서의 IPv6



예를 들면, 터널링은 서비스 공급자들이 대대적인 인프라 업그레이드나 IPv4 서비스 장애 없이 엔드-투-엔드 IPv6 서비스를 제공할 수 있게 해주며 기업들이 기존 IPv4 인프라를 통해 고립된 IPv6 도메인을 연결하거나 6BONE 같은 원격 IPv6 네트워크를 연결할 수 있게 해줍니다.

IPv6 배치를 위해 다양한 터널링 메커니즘이 제공되고 있습니다. 그런 메커니즘에는 IPv6 수동 설정 터널(RFC 2893)이나 IPv4 GRE 터널 상에서의 IPv6 같은 수동 생성 터널, 반자동 터널 메커니즘 그리고 IPv4 호환 및 6to4 터널 같은 완전 자동 터널 메커니즘이 포함됩니다. 캠퍼스 내의 ISATAP, 6over4 그리고 터널 브로커 서비스(서비스 공급자가 제공) 같은 기타 터널 기법도 제공되고 있습니다.

터널링 요건

모든 터널링 메커니즘은 터널의 엔드포인트에서 IPv4 및 IPv6 프로토콜 스택을 실행할 것을 요구하고 있습니다. 즉, 엔드포인트들이 듀얼 스택 모드에서 실행되어야 한다는 것입니다. 듀얼 스택 라우터들은 IPv4와 IPv6 프로토콜을 동시에 실행하므로 IPv4 및 IPv6 엔드 시스템 또는 라우터와 직접 상호운용될 수 있습니다.

듀얼 스택 접근 방식은 동일 라우터에서 IP와 IPX, DECnet 또는 AppleTalk를 같이 실행하는 것과 비슷하며 이는 Cisco IOS Software에서 옛날부터 해오던 것입니다.

터널링과 보안

IPv4 IPSec을 이용, 터널 인터페이스와 물리적 인터페이스에 암호 맵을 적용하여 송신 및 수신되는 트래픽을 암호화하면 IPv4 터널 상의 IPv6 트래픽을 보호하는 것이 가능합니다.

이 방법으로 터널을 보호하면 성능에 악영향을 미칠 수 있으므로 조심스러운 네트워크 설정을 통해 성능과 보안 사이의 균형을 잘 맞춰야 합니다.

참고: 만일 터널의 두 엔드 포인트 사이에 있는 중간 장치가 IPv4 캡슐화에서의 IPv6 트래픽인 IPv4 프로토콜 41을 필터링할 경우에는 터널이 작동하지 않게 됩니다.

IPv6 터널 메커니즘

모든 상황 및 네트워크에 모든 변환 전략을 적용할 수 있는 것은 아닙니다. 적어도 초기에는 고객들이 기존의 IPv4 네트워크 상에서 IPv6을 터널링하는 것에 관심을 보일 것이기 때문에 이 부분에서는 다음과 같은 IPv4 네트워크에서의 IPv6 터널링 기법에 대해 자세히 알아보도록 하겠습니다.

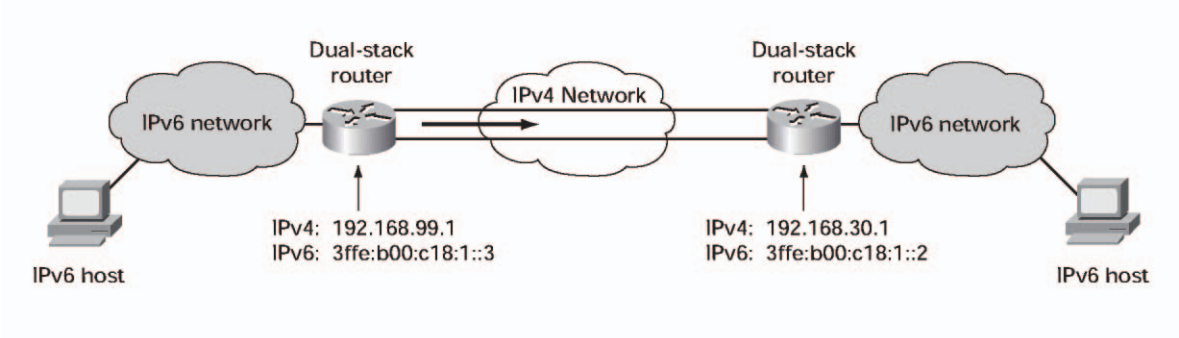
- IPv6 수동 설정 터널
- IPv4 GRE 터널 상의 IPv6
- 자동 IPv4 호환 터널
- 자동 6to4 터널
- ISATAP 터널
- Teredo 터널

IPv6 수동 설정 터널

설정 터널의 주된 용도는 두 개의 에지 라우터, 또는 엔드 시스템과 에지 라우터 사이의 일반적인 통신이나 6BONE 같은 원격 IPv6 네트워크로의 연결을 위해 안정적이고 안전한 연결을 제공하는 것입니다. 터널의 엔드포인트로 사용되는 에지 라우터와 엔드 시스템은 듀얼 스택 시스템이어야 합니다. 두 지점 사이에서는 수동 터널이 사용되며 터널의 소스 및 목적지 주소를 모두 설정해줘야 합니다. 자동 터널 메커니즘은 그렇게 할 필요가 없습니다.

각 터널은 독자적으로 관리되므로 터널 엔드 포인트가 많을수록 더 많은 터널이 필요하게 되며 관리 부담도 커지게 됩니다. 다른 터널 메커니즘과 마찬가지로 터널의 경로에서는 NAT가 허용되지 않습니다. 그림 21은 수동 설정 터널의 구성을 보여주고 있습니다.

그림 21: 수동 설정 터널



IPv6 수동 설정 터널에 대한 추가 정보는 RFC 2893, Transition Mechanisms for IPv6 Hosts and Routers를 참조하십시오.

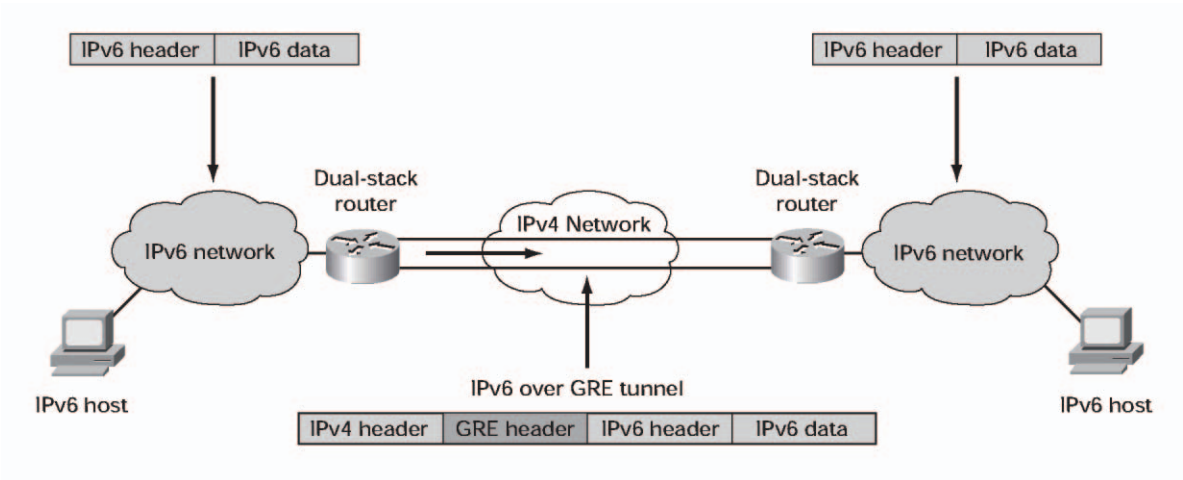
IPv4 GRE 터널 상의 IPv6

IPv4 GRE 터널 상의 IPv6은 표준 포인트-투-포인트 캡슐화 스키마를 구현하는데 필요한 서비스를 제공하기 위해 설계된 표준 GRE 터널링 기법을 사용합니다. 수동 설정 터널에서처럼 이 터널들은 두 포인트 사이의 링크가 되며 각 링크마다 별도의 터널을 사용합니다. GRE 터널은 특정한 패신저(passenger) 또는 트랜스포트 프로토콜에 국한되지는 않지만 이 경우에는 IPv6 트래픽이 패신저 프로토콜이 되며 GRE는 캐리어 프로토콜이 됩니다.

수동 터널에서처럼 GRE 터널은 두 포인트 사이에서 사용되며 터널의 소스 및 목적지 주소를 모두 설정해줘야 합니다. 터널 엔드 포인트로 사용되는 에지 라우터와 엔드 시스템은 듀얼 스택 장치여야 합니다.

Layer 2 데이터 링크에는 통합 IS-IS 라우팅 프로토콜이 실행되므로 GRE 이외의 터널링 기법은 사용될 수 없습니다. IPv4 GRE 터널 상에서의 IPv6은 표준 포인트-투-포인트 캡슐화 스키마를 구현하는데 필요한 서비스를 제공하기 위해 설계된 표준 GRE 터널링 기법을 사용합니다. 그림 22는 IPv6 패킷이 GRE 터널 상에서 어떻게 전송되는지 보여주고 있습니다.

그림 22: GRE 터널 상에서의 IPv6



수동 설정 터널에서처럼 듀얼 스택 라우터의 IPv4 및 IPv6 주소는 GRE 터널 인터페이스에서 설정하며, IPv4 주소를 이용하여 터널의 입구 및 출구 지점(또는 소스 및 목적지)을 식별합니다.

각 GRE 터널은 독자적으로 관리되므로 터널 엔드 포인트가 많을수록 더 많은 터널이 필요하게 되며 관리 부담도 커지게 됩니다. 다른 터널 메커니즘과 마찬가지로 터널의 경로에서는 NAT가 허용되지 않습니다.

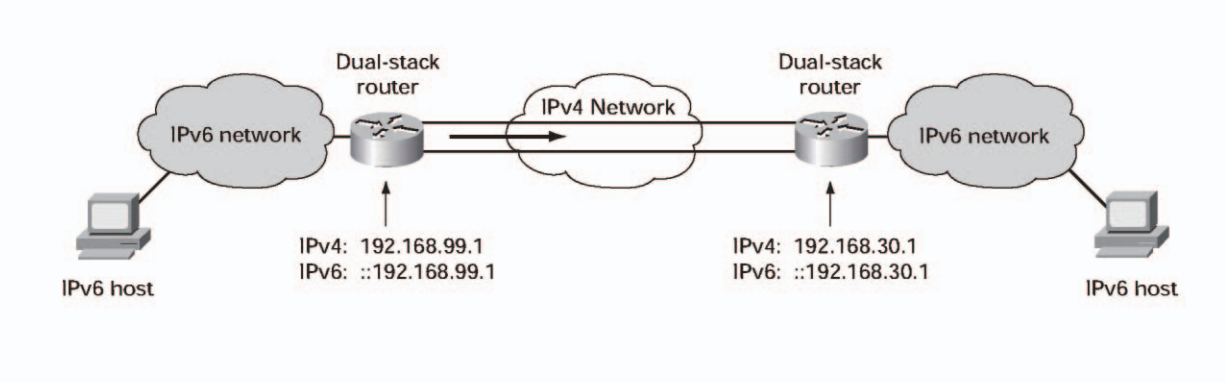
자동 IPv4 호환 터널

자동 IPv4 호환 터널은 IPv4와 호환되는 IPv6 주소를 사용하는 IPv4 터널 상의 IPv6 메커니즘입니다. IPv4와 호환되는 IPv6 주소는 앞의 96비트에 0을 넣고 그 다음 32비트에 IPv4를 붙인 것입니다. 예를 들면, ::192.168.99.1은 IPv4와 호환되는 IPv6 주소입니다.

엔드 시스템과 에지 라우터 사이에 자동 터널을 설정할 수도 있지만, 자동 IPv4 호환 터널은 주로 라우터 간의 연결을 위해 사용되어 왔습니다.

수동 설정 터널과 달리, 자동 IPv4 호환 터널 기법은 원격 노드를 이용하여 즉흥적으로 터널을 구축합니다. 터널 소스와 터널 목적지가 IPv4 주소에 의해 자동으로 결정되므로 터널의 엔드 포인트를 수동 설정할 필요는 없습니다. 자동 터널은 요청에 따라 생겨났다가 사라지게 되며 통신이 지속되는 동안에만 존재하게 됩니다. 그림 23은 자동 IPv4 호환 터널의 구성을 보여주고 있습니다.

그림 23: 자동 IPv4 호환 터널



터널을 쉽게 만들 수 있는 방법이긴 하지만 IPv4 호환 터널 메커니즘은 IPv6 배치를 위한 확장성이 떨어집니다. 그 이유는 각 호스트마다 IPv4 주소를 필요로 하므로 IPv6의 커다란 주소 공간이 주는 혜택이 사라지게 되기 때문입니다. IPv4 호환 터널은 6to4(RFC 3056, *Connection of IPv6 Domain via IPv4 Clouds*) 자동 터널 메커니즘에 의해 대부분 교체되었습니다. 따라서 IPv4 호환 터널을 변환 메커니즘으로 사용하는 것은 거의 의미가 없어졌습니다.

IPv4 호환 터널에 대한 추가 정보는 RFC 2893, *Transition Mechanism for IPv6 Hosts and Routers*를 참조하십시오.

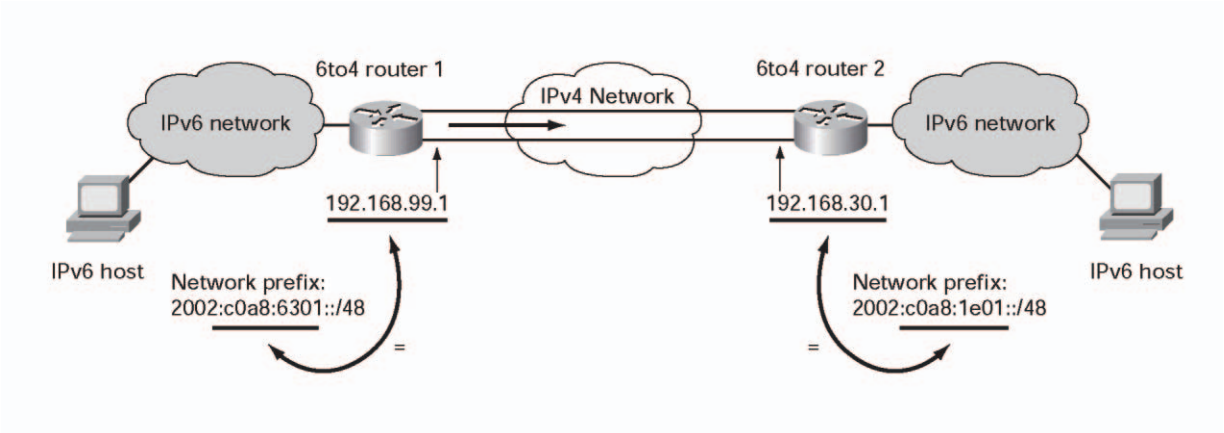
자동 6to4 터널

자동 6to4 터널은 고립된 IPv4 도메인들이 IPv4 네트워크를 통해 서로 연결될 수 있게 해주며 6BONE 같은 원격 IPv6 네트워크로의 연결도 가능케 합니다.

6to4 터널을 위한 가장 간단한 배치 시나리오는 공유된 IPv4 네트워크로 적어도 하나 이상의 연결을 가지고 있는 여러 개의 IPv6 사이트를 서로 연결하는 것입니다. 이 IPv4 네트워크는 글로벌 인터넷이나 기업의 백본이 될 수도 있습니다.

6to4 터널은 IPv4 인프라를 IPv6 주소에 매입된 IPv4 주소를 이용하여 터널의 반대쪽 끝을 찾아내는 가상 non-브로드캐스트 링크로 취급합니다. 각 IPv6 도메인은 자동적으로 IPv4 터널을 구축하는 듀얼 스택 라우터를 필요로 합니다. IPv4 터널 구축에는 고유의 라우팅 프리픽스(prefix) 2002::/16와 터널 목적지의 IPv4 주소를 연결한 IPv6 주소가 사용됩니다. 핵심 요건은 각 사이트가 6to4 주소를 가지고 있어야 한다는 것입니다. IPv6에서 각 사이트에는 고유의 라우팅 프리픽스(prefix)가 있으며 IPv4 주소는 공통으로 사용될 수도 있습니다. 그림 24는 6to4 도메인을 서로 연결하는 6to4 터널 구성을 보여주고 있습니다.

그림 24: 자동 6to4 터널



각 사이트마다 라우터의 외부 인터페이스에 오직 하나의 6to4 주소를 할당할 것을 권장합니다. 사이트 내에서 IPv6을 라우팅하려면 RIPng(routing information protocol next generation) 같은 IPv6 내부 라우팅 프로토콜이 모든 사이트에서 실행되어야 합니다. 외부 라우팅은 관련 IPv4 외부 라우팅 프로토콜이 처리하게 됩니다.

6to4 터널에 대한 추가 정보는 RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds*를 참조하십시오.

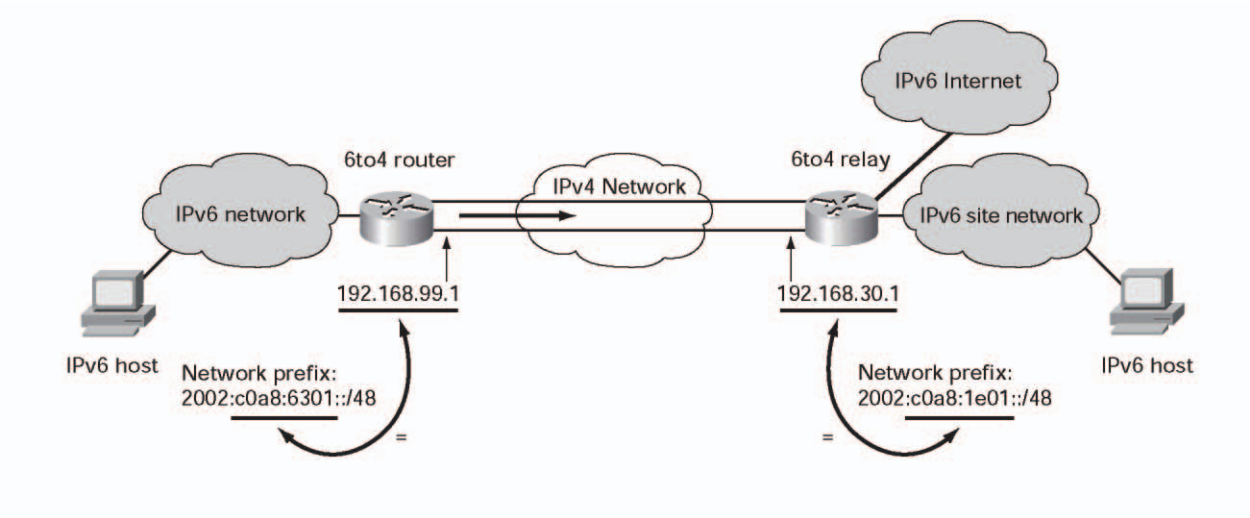
6to4 릴레이 라우터

네이티브 IPv6 사용이 점차 확산되면 다음 단계는 6to4 릴레이 라우터가 됩니다. 이 릴레이 라우터들은 일반적인 라우터이지만 6to4 IPv6 주소와 일반 IPv6 주소를 모두 가지고 있으며 라우팅 프로토콜이 실행되고 있는 네이티브 IPv6 도메인과 라우팅 프로토콜이 실행되고 있지 않은 6to4 도메인 간의 라우팅 서비스를 제공합니다. 6to4 사이트와 네이티브 IPv6 도메인 사이의 통신은 최소한 하나 이상의 릴레이 라우터를 필요로 합니다.

6to4는 에지 라우터가 2002::/16 프리픽스(prefix)를 가진 모든 목적지로 패킷을 전달할 수 있게 합니다. 하지만 6to4 릴레이로 지정된 6to4 에지 라우터가 IPv6 인터넷으로의 트래픽 전달을 제공하지 않으면 다른 IPv6 목적지에는 도달할 수 없습니다.

6to4 라우터들은 사이트 내에서 IPv6 라우팅을 위한 IPv6 내부 라우팅 프로토콜을 실행하지만 IPv6 도메인 간의 라우팅에는 특정 릴레이 라우터를 가리키는 기본 IPv6 경로를 이용합니다. 그림 25는 6to4와 네이티브 IPv6 도메인을 서로 연결시키기 위한 6to4 릴레이 라우터의 활용을 보여주고 있습니다.

그림 25: 6to4 릴레이 라우터



참고: 그림 27에 나오는 IPv4 주소는 사설 주소이며 실제 인터넷 연결에서는 6to4 릴레이에 의해 사용될 수 없습니다. 인터넷으로 패킷을 전달할 때는 글로벌 유니캐스트 주소를 사용해야 합니다.

ISATAP 터널

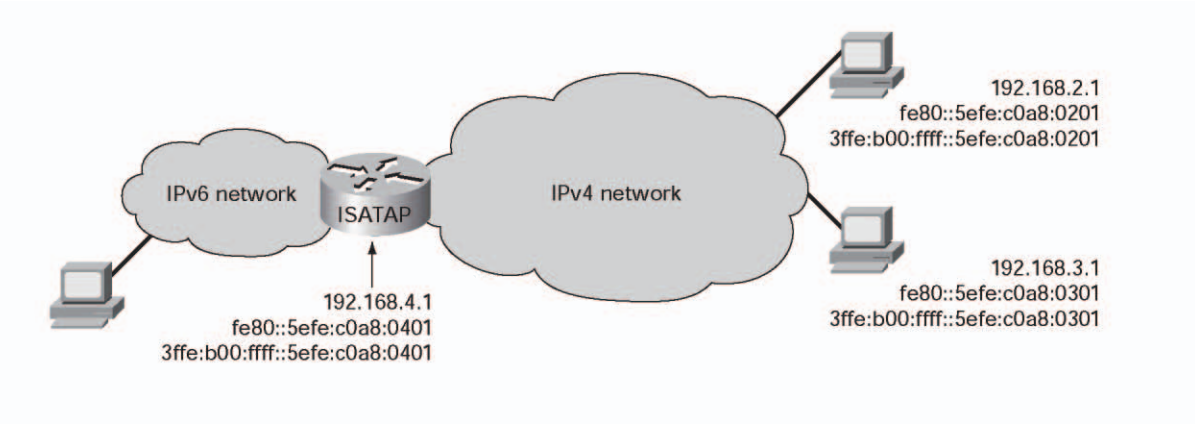
ISATAP은 6to4 터널과 비슷한 IPv6 변환 메커니즘으로 사이트의 IPv4 인프라를 NBMA(non-broadcast multi-access) 링크 레이어처럼 취급하여 점진적인 IPv6 배치를 가능케 합니다.

ISATAP 변환 메커니즘은 사이트의 기존 IPv4 네트워크 내에서 간단하고 확장성 있는 대규모 IPv6 배치를 점진적으로 진행할 수 있게 해줍니다. 또한 집합 확장 문제를 발생시키지도 않고 멀티캐스트 같은 특별한 IPv4 서비스를 사이트 전체에 배치할 필요도 없습니다.

ISATAP 터널은 캠퍼스 네트워크 상에서 또는 로컬 사이트 변환를 위해 사용될 수 있습니다. ISATAP는 사이트-로컬과 글로벌 IPv6 라우팅 도메인 내에서 IPv6 라우팅을 지원하며 네이티브 IPv6 지원 없이도 사이트의 IPv4 네트워크 일부분에 걸쳐 자동 IPv6 터널링을 지원합니다. ISATAP는 글로벌하지 않은 고유의 IPv4 주소 할당과 NAT를 같이 사용하는 사이트 내에서의 자동 터널링도 지원합니다. 모든 ISATAP 노드는 듀얼 스택입니다.

ISATAP는 64비트 네트워크 프리픽스(prefix)를 이용하며 여기에서 ISATAP 주소가 생성됩니다. 64비트 인터페이스 식별자는 0000:5EFE와 듀얼 스택 노드의 IPv4 주소(192.168.99.1)를 연결하여 만들어집니다. 3FFE:0B00:0C18:0001:0:5EFE.192.169.99.1은 ISATAP 주소의 한 예입니다. ISATAP 터널링은 대부분 사이트 경계 내에서만 이뤄지므로 ISATAP에 포함된 IPv4 주소는 고유한 글로벌 주소일 필요가 없습니다. 그림 26은 ISATAP 터널링 메커니즘의 한 예를 보여주고 있습니다.

그림 26: ISATAP 터널



6to4와 ISATAP 변환 메커니즘은 다음과 같은 세가지 일반적인 시나리오에서 노드를 위한 IPv6 연결을 제공합니다: ISP 또는 기업 네트워크에서 IPv6 연결 제공, 하나 이상의 글로벌 IPv4 주소 액세스를 가진 노드 그리고 ISATAP 라우터를 배치한 기업 네트워크. 하지만 노드가 6to4의 일부가 아닌 NAT 장치 뒤에 위치한 사설 네트워크의 일부라면 이러한 터널링 메커니즘은 사용될 수 없습니다.

ISATAP 터널에 대한 추가 정보는 *Intra-Site Automatic Tunnel Addressing Protocol* (draft-ietf-ngtrans-isatap-04.txt) 문서를 참조하십시오.

Teredo 터널

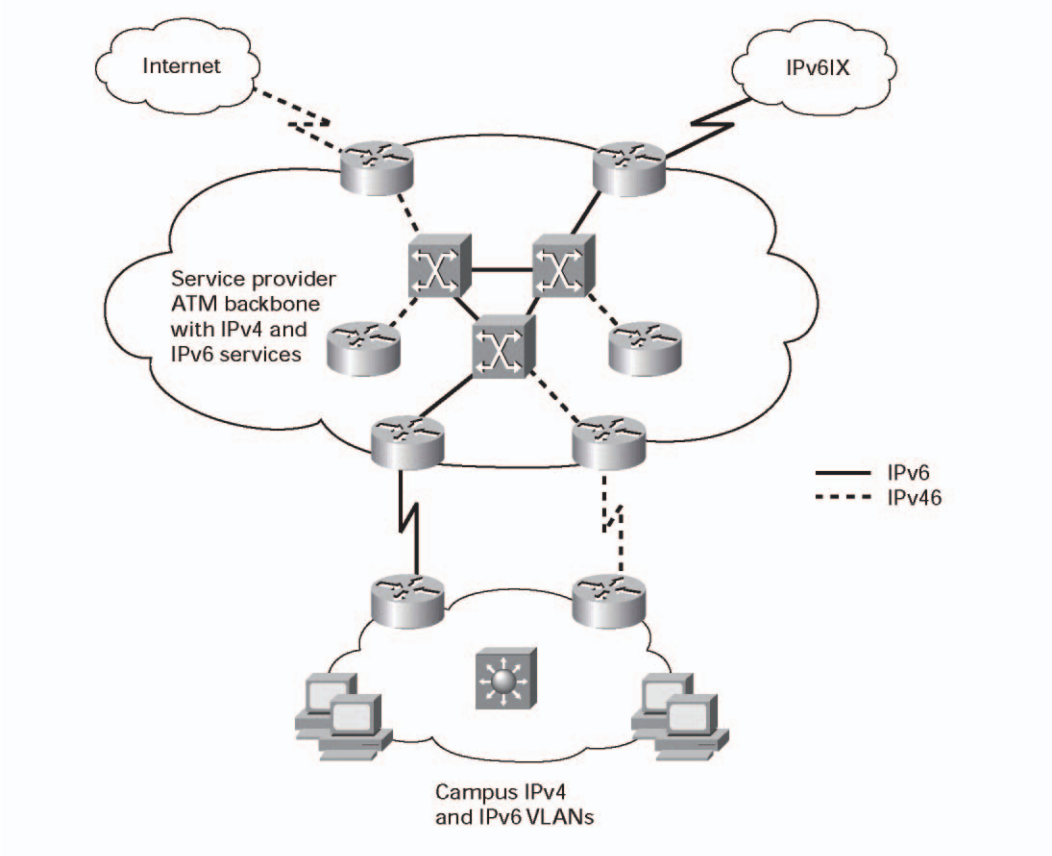
Teredo(또는 Shipworm)서비스는 NAT 장치를 통해 UDP 상에서 IPv6 패킷을 터널링하여 하나 이상의 IPv4 NAT 뒤에 위치한 노드에 IPv6 연결을 제공하는 터널 메커니즘입니다. Teredo 서비스는 NAT 장치가 네이티브 IPv6 라우팅을 제공하거나 6to4 라우터처럼 행동하도록 업그레이드될 수 없는 경우를 위해 정의되었습니다.

Teredo 터널은 Teredo 서비스와 Teredo 릴레이를 사용합니다. Teredo 서비스는 stateless이며 Teredo 클라이언트 간의 트래픽 일부를 관리합니다. 동시에, Teredo 릴레이는 Teredo 서비스와 네이티브 IPv6 인터넷 사이에서 IPv6 라우터 역할을 합니다. Teredo 네트워크는 Teredo 클라이언트, 서버 그리고 릴레이로 구성되어 있습니다. Teredo 네트워크에서는 Teredo 클라이언트를 설정할 필요가 없습니다. 클라이언트에는 특별히 만들어진 IPv6 주소 프리픽스(prefix)가 할당되며 Teredo 서버와 릴레이들은 고유한 글로벌 IPv4 주소를 사용합니다.

전용 데이터 링크 상에서의 IPv6 배치

많은 WAN 및 MAN(metropolitan-area network)은 Frame Relay, ATM 또는 옵티컬 등의 Layer 2 기술을 통해 구현되었으며 그 중 일부는 DWDM을 사용하기 시작했습니다. 그림 27은 전용 데이터 링크 상에서의 IPv6 구성 예를 보여주고 있습니다.

그림 27: 전용 데이터 링크 상에서의 IPv6 배치



ISP WAN 또는 MAN에 부착된 라우터들은 서로 다른 ATM, Frame Relay PVC 또는 옵티컬 람다(lambda) 상에서 IPv6을 실행하도록 IPv4와 같은 Layer 2 인프라를 사용하도록 설정될 수 있습니다. 이 설정은 서비스 공급자가 IPv4 트래픽의 서비스 장애 및 수익 손실을 피할 수 있는 추가 혜택도 선사합니다.

MPLS 백본 상에서의 IPv6 배치

MPLS 백본 상에서의 IPv6은 고립된 IPv6 도메인들이 MPLS IPv4 코어 네트워크를 통해 서로 통신할 수 있도록 합니다. 이 구현은 IP 헤더 자체가 아닌 레이블을 기반으로 전달이 이뤄지기 때문에 훨씬 적은 수의 백본 인프라 업그레이드와 코어 라우터 재설정을 필요로 하여 매우 효율적인 비용의 IPv6 배치 전략을 제공합니다.

또한, MPLS 환경에 내재된 VPN 및 트래픽 엔지니어링 서비스는 IPv6 네트워크가 IPv4 VPN 및 MPLS-TE를 지원하는 인프라 상에서 VPN 또는 익스트라넷으로 결합될 수 있게 합니다.

다음과 같은 다양한 배치 전략이 제공되거나 개발되고 있습니다:

- 고객 에지(CE) 라우터 상에서 터널을 이용한 IPv6 배치
- MPLS의 서킷 트랜스포트 상에서의 IPv6 배치
- 공급자 에지(PE) 라우터 상에서의 IPv6 배치(6PE)

이들 중 가장 첫 번째 전략은 IPv4 터널을 이용하여 IPv6 트래픽을 캡슐화하기 때문에 네트워크 안에서는 IPv4 트래픽처럼 보이므로 MPLS 공급자(P) 또는 PE 라우터에 아무런 영향도 미치지 않으며 변경도 필요 없습니다. 두 번째 전략은 Cisco 12000 및 7600 인터넷 라우터 같은 특정 시스코 라우터에만 적용가능하며 이 역시 코어 라우팅 메커니즘을 변경하지 않아도 됩니다. 마지막 전략은 듀얼 스택 구현을 지원하기 위해 PE 라우터를 변경해야 하지만 모든 코어 기능은 IPv4로 남아있게 됩니다. 또 다른 전략으로는 네이티브 IPv6 MPLS 코어를 실행시키는 것이지만 이 전략은 모든 P 및 PE 라우터를 완전히 업그레이드해야 하며 IPv4와 IPv6을 위해 듀얼 제어 평면을 갖춰야 합니다.

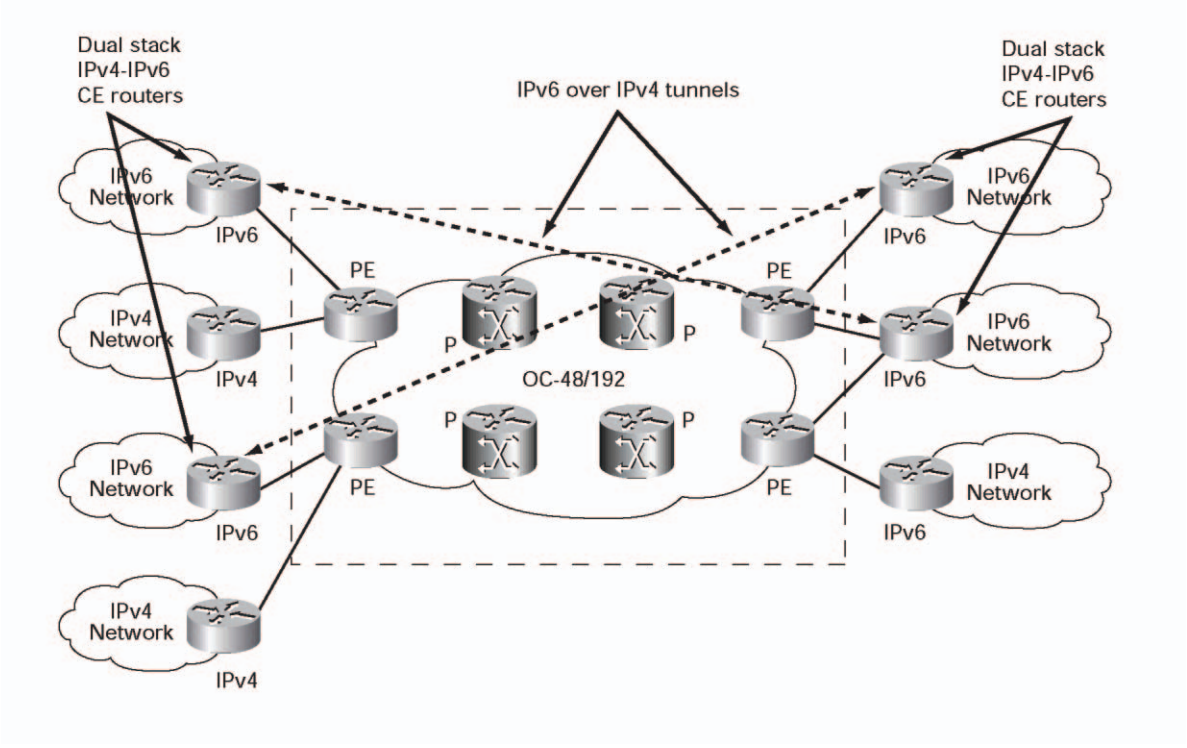
다음 부분에서는 각 메커니즘을 더 자세히 살펴보게 됩니다.

고객 에지 라우터의 터널을 이용한 IPv6 배치

CE 라우터에 터널을 사용하는 것은 MPLS 네트워크 상에서 IPv6을 배치하는 가장 간단한 방법입니다. 이 방법은 MPLS의 운영이나 인프라에 아무런 영향을 미치지 않으며 코어의 P 라우터나 고객과 연결된 PE 라우터에 대한 변경도 필요로 하지 않습니다.

원격 IPv6 도메인 간의 통신은 표준 터널링 메커니즘을 사용, MPLS VPN이 네이티브 IPv4 터널을 지원하는 것과 비슷한 방법으로 IPv4 터널 상에서 IPv6을 실행합니다. CE 라우터는 듀얼 스택으로 업그레이드해야 하며 수동 수정 터널이나 6to4 터널을 이용, 설정되어야 합니다. 하지만 PE 라우터와의 통신은 IPv4이며 MPLS 도메인은 트래픽을 IPv4로 인식합니다. 듀얼 스택 라우터는 서비스 공급자가 제공하는 IPv6 주소 대신 6to4 주소 또는 원격 공급자가 할당한 IPv6 프리픽스(prefix)를 사용합니다. 그림 28은 CE 라우터의 터널을 이용한 IPv6 배치 예를 보여주고 있습니다.

그림 28: 고객 에지 라우터에 터널을 이용한 IPv6 배치

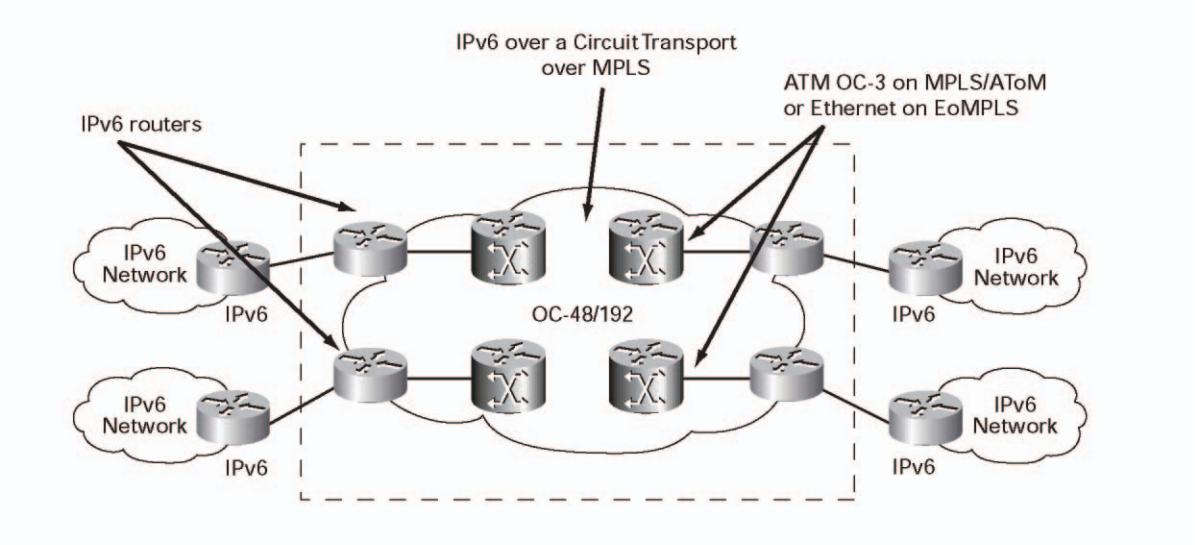


MPLS의 서킷 트랜스포트 상에서의 IPv6 배치

MPLS 네트워크 상에서 IPv6을 배치하기 위해 서킷 트랜스포트를 사용하는 것은 MPLS의 운영이나 인프라에 아무런 영향을 주지 않습니다. 코어의 P 라우터나 고객과 연결된 PE 라우터를 변경해야 할 필요도 없습니다.

원격 IPv6 도메인 간의 통신은 전용 링크 상에서의 IPv6 프로토콜을 실행하며 모든 기본 메커니즘은 IPv6에게 투명하게 제공됩니다. IPv6 트래픽은 Any Transport over MPLS(MPLS/AToM) 또는 Ethernet over MPLS(EoMPLS)를 이용하여 터널링되며 IPv6 라우터는 각각 ATM OC-3 또는 Ethernet 인터페이스를 통해 연결됩니다. 그림 29는 MPLS의 서킷 트랜스포트 상에서의 IPv6 배치 예를 보여주고 있습니다.

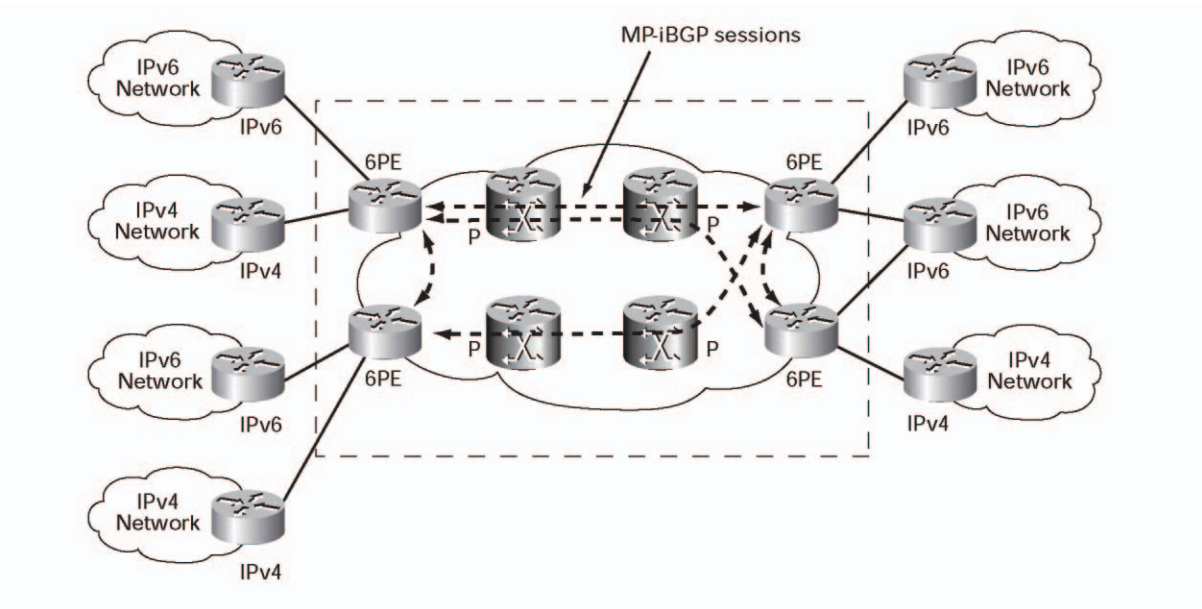
그림 29: MPLS의 서킷 트랜스포트 상에서의 IPv6 배치



공급자 에지 라우터 상에서의 IPv6 배치

또 다른 배치 전략은 MPLS PE 라우터 상의 IPv6을 설정하는 것입니다. 이 전략은 서비스 공급자들에게 크게 유리합니다. 왜냐하면 코어 네트워크의 하드웨어 및 소프트웨어를 업그레이드하지 않아도 되기 때문에 운영에 지장을 주거나 기존 IPv4 트래픽을 통한 수익 창출에도 영향을 주지 않기 때문입니다. 이 전략은 현재의 MPLS 기능(예를 들면, IPv4를 위한 MPLS 또는 VPN 서비스)의 혜택을 유지하면서 기업 고객들에게 네이티브 IPv6 서비스를 제공하는 것처럼 보이게 합니다(ISP에서 공급하는 IPv6 프리픽스(prefix) 사용). 6PE 아키텍처는 IPv6 VPN도 지원합니다. 그림 30은 PE 라우터 상에서의 IPv6 배치 예를 보여주고 있습니다.

그림 30: 공급자 에지 라우터 상에서의 IPv6 배치



IPv6 전달은 레이블 스위칭을 통해 이뤄지므로 IPv4 상의 IPv6이나 추가적인 Layer 2 캡슐화가 필요치 않습니다. 따라서 네트워크 전반에 걸쳐 네이티브 IPv6 서비스가 제공되고 있는 것처럼 보이게 됩니다.

IPv6 연결을 지원해야 하는 각 PE 라우터는 듀얼 스택으로 업그레이드(6PE 라우터로)해야 하며 코어와 연결된 인터페이스에서 MPLS를 실행하도록 설정되어야 합니다. 사이트의 요구 조건에 따라, 각 라우터는 IPv6 및 IPv4 트래픽을 CE 라우터로 가는 인터페이스로 전달하도록 설정될 수 있어 네이티브 IPv6 및 IPv4 서비스 제공이 가능합니다. 6PE 라우터는 연결의 종류에 따라 지원되는 모든 라우팅 프로토콜을 통해 IPv4 또는 IPv6 라우팅 정보를 교환하며 MPLS를 실행하지 않는 IPv4 및 IPv6 인터페이스로 IPv4 및 IPv6 트래픽을 전환합니다.

6PE 라우터는 멀티프로토콜 BGP를 이용하여 MPLS 도메인 내의 다른 6PE 라우터와 도달 가능성 정보를 교환하며 도메인 내의 다른 P 및 PE 장치와 공통의 IPv4 라우팅 프로토콜(OSPF 또는 통합 IS-IS)을 공유합니다.

6PE 라우터는 두 레벨의 MPLS 레이블을 이용하여 IPv6 트래픽을 캡슐화합니다. 상위 레이블은 IPv4 라우팅 정보를 이용, 목적지 6PE로 패킷을 보내기 위해 장치들이 코어에서 사용하는 LDP(label distribution protocol) 또는 TDP(tag distribution protocol)을 통해 배포됩니다. 두 번째 또는 하위 레이블은 멀티프로토콜 BGP4를 통해 목적지의 IPv6 프리픽스(prefix)와 연관됩니다.

6PE 라우터에 대한 자세한 정보는 *Internet-Draft draft-ietf-ngtrans-bgp-tunnel-04.txt*를 참조하십시오.

프로토콜 통역 메커니즘

이러한 통합 전략들은 모두 엔드-투-엔드 IPv6을 제공합니다. 하지만 일부 조직이나 개인들은 위와 같은 IPv6 전환 전략을 구현하고 싶지 않을 수도 있습니다. 또한 일부 조직이나 개인은 그들의 노드나 네트워크에 IPv6만 설치하고 듀얼 스택은 설치하고 싶지 않을 수도 있습니다. 일부 노드 또는 네트워크에 듀얼 스택을 설치한다 해도 이들 노드는 듀얼 스택 노드에 사용될 IPv4 주소가 없을 수도 있습니다.

이러한 상황에서 IPv6 전용 호스트와 IPv4 전용 호스트 간의 통신을 가능케 하려면 호스트, 라우터 또는 듀얼 스택 호스트 상에서 어떤 프로토콜을 사용할 것인지에 대한 어플리케이션 레벨의 이해를 바탕으로 IPv6과 IPv4 프로토콜 사이의 통역이 어느 정도 이뤄져야 합니다. 예를 들면, IPv6 전용 네트워크가 IPv4 전용 웹 서버 같은 IPv4 전용 자원을 액세스해야 할 필요가 있을 수도 있기 때문입니다.

IETF NGTrans Working Group은 다음과 같은 다양한 IPv6-to-IPv4 통역 메커니즘을 고려하고 있습니다:

- 네트워크 주소 통역-프로토콜 통역(NAT-PT)
- TCP-UDP 릴레이
- Bump-in-the-stack (BIS)
- 듀얼 스택 변환 메커니즘(DSTM)
- SOCKS 기반 게이트웨이

위와 같은 프로토콜 통역 메커니즘은 IPv6이 보다 폭넓게 사용되어감에 따라 더욱 중요해지고 있으며 IPv6이 프로토콜의 주류를 이룬다 해도 레거시 IPv4 시스템이 전체 IPv6 네트워크의 일부가 될 수 있도록 하려면 통역 메커니즘이 필요하게 됩니다.

통역 메커니즘은 IPv4 또는 IPv6 호스트를 변경할 필요가 없는 종류와 변경이 필요한 종류의 두 가지로 분류할 수 있습니다. 전자의 예로는 전용 서버에서 실행되면서, 트랜스포트 레벨에서 IPv4 및 IPv6 호스트와 각각 연결한 다음 정보를 교환하는 TCP-UDP 릴레이 메커니즘을 들 수 있습니다. 후자의 예로는 IPv4 프로토콜 스택에 별도의 프로토콜 레이어를 추가해야 하는 BIS 메커니즘을 들 수 있습니다.

Stateless IP/ICMP 통역기

NAT-PT 또는 BIS 같이 IPv6 전용 호스트와 IPv4 전용 호스트 간의 통신을 가능케 하는 통역 메커니즘들은 Stateless IP/ICMP Translator(SIIT)라는 알고리즘을 사용합니다. 이 알고리즘은 패킷별로 IPv4와 IPv6 사이의 IP 패킷 헤더를 통역하고 IPv4와 IPv4로 통역 또는 매핑된 IPv6 주소 간의 헤더 안에 있는 주소를 통역합니다. 이 알고리즘은 IPv6 호스트가 IPv4 주소 또는 해당 주소로 오가는 경로 패킷을 획득할 수 있게 해주는 메커니즘을 포함하지는 않지만 각 IPv6 호스트에 임시 IPv4 주소가 할당된 것으로 가정합니다.

SIIT에 대한 추가 정보는 RFC 2765, Stateless *IP/ICMP Translation Algorithm (SIIT)*를 참조하십시오.

다음 부분에서는 각 프로토콜 통역 메커니즘에 대해 더 자세히 다루게 됩니다.

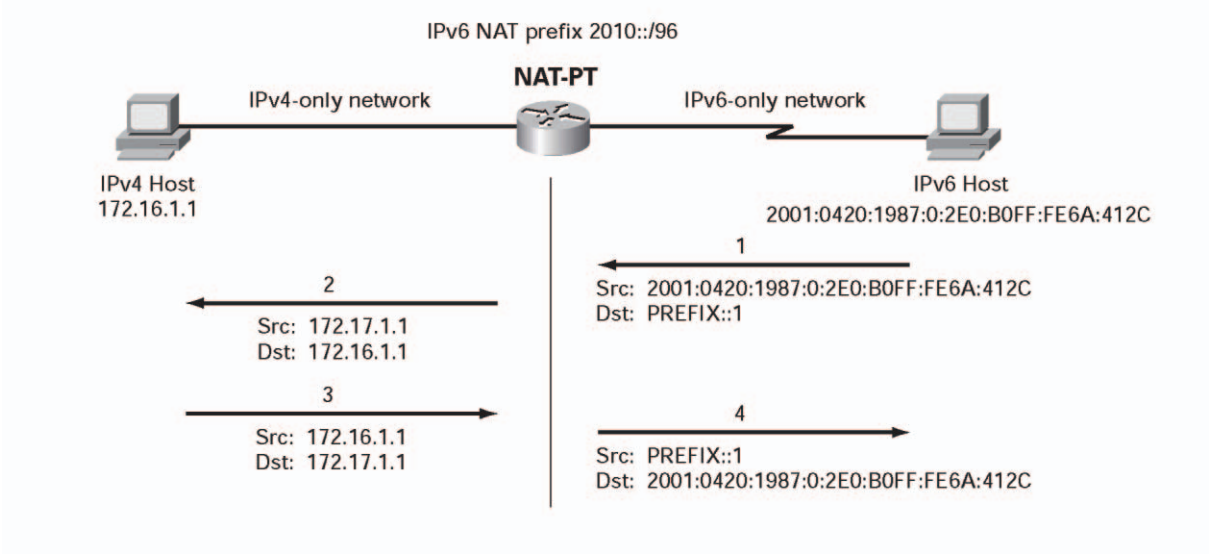
네트워크 주소 변환-프로토콜 변환(NAT-PT)

NAT-PT는 IPv6 전용 ISP가 IPv4 호스트 및 어플리케이션과 서로 연결될 수 있도록 합니다. NAT-PT는 인터넷의 대부분이 IPv6 네트워크 도메인으로 구성되고 나면 매우 중요해질 것입니다.

NAT-PT 변환 메커니즘(RFC 2766)은 IPv4와 IPv6 주소 사이의 네트워크 레이어에서 변환을 하게 되며 네이티브 IPv6 호스트와 어플리케이션들이 네이티브 IPv4 호스트 및 어플리케이션과 통신할 수 있도록 합니다.

IPv4와 IPv6 DNA 요청 및 응답 사이의 변환은 Application Level Gateway(AGL)가 하게 됩니다. 그림 31은 IPv6을 배치하기 위한 NAT-PT의 사용 예를 보여주고 있습니다.

그림 31: NAT-PT를 이용한 IPv6 배치



NAT 구현에 대해 잘 아는 사람들은 프로토콜 변환 메커니즘으로 NAT-PT를 고려할 수도 있지만 NAT-PT는 IPv4 NAT와 같은 한계를 지니고 있습니다. 단일 장애 지점과 ALG의 낮은 성능 그리고 사용할 수 있는 어플리케이션의 제한 등은 네트워크의 전반적인 가치와 유용성을 떨어뜨립니다. NAT-PT는 또한 IP 레이어에서의 보안 구현에도 장애가 됩니다.

NAT-PT에 대한 추가 정보는 RFC 2766, *Network Address Translation - Protocol Transition(NAT-PT)*를 참조하십시오.

TCP-UDP 릴레이

TCP-UDP 릴레이 변환 메커니즘은 전용 서버와 DNS를 필요로 한다는 점에서 NAT-PT와 비슷합니다. 이 방식은 네트워크 레이어가 아닌 트랜스포트 레이어에서 변환을 하며 DNS가 IPv4와 IPv6 주소 간의 매핑을 제공합니다.

이 메커니즘은 IPv6 또는 IPv4에 대한 업그레이드 비용을 들이지 않으면서 IPv4 웹 서버 같은 IPv4 전용 호스트를 액세스하고자 하는 네이티브 IPv6 네트워크에 가장 효과적입니다. TCP-UDP 릴레이 구현은 다양한 여러 곳에서 제공되고 있습니다.

TCP-UDP 릴레이에 대한 추가 정보는 RFC 3142, *An IPv6-to-IPv4 Transport Relay Translator*를 참조하십시오.

Bump-in-the-Stack

BIS 메커니즘은 IPv4 전용 호스트 상의 IPv4 어플리케이션과 IPv6 전용 호스트 간의 통신을 위해 사용됩니다.

이름 해결 확장자, 주소 매퍼, 변환기 등 3개의 추가 레이어가 어플리케이션과 네트워크 레이어 사이의 IPv4 프로토콜 스택에 추가되었습니다.

어플리케이션이 IPv6 전용 호스트와 통신할 필요가 있을 때마다, 추가된 레이어들이 IPv6 주소를 IPv4 호스트의 IPv4 주소로 매핑시켜 줍니다. 변환 메커니즘은 SIIT의 일부로 정의됩니다.

이 메커니즘은 엔드 시스템에만 구현될 수 있습니다. BIS 메커니즘의 확장된 버전은 듀얼 스택 호스트가 이 기법을 이용할 수 있게 해줍니다. 추가 정보는 RFC 2767, *Dual Stack Hosts using the "Bump-in-the-Stack" Technique (BIS)*을 참조하십시오.

듀얼 스택 변환 메커니즘(DSTM)

DSTM 변환 메커니즘은 아직 IPv4 쪽에 IPv4 주소를 할당하지 않은 상태로 IPv4 시스템과 통신을 하거나 IPv6 프로토콜 스택 상에서 IPv4 어플리케이션을 실행시켜야 하는 IPv6 도메인의 듀얼 스택 호스트를 위해 사용합니다. 이 메커니즘은 통신 기간 동안 임시 글로벌 IPv4 주소를 동적으로 제공(DHCPv6 사용)하는 전용 서버를 필요로 하며 동적 터널을 이용, IPv6 도메인에서 IPv6 패킷 내의 IPv4 트래픽을 통과시킵니다.

DSTM은 IPv6이 보편화되고 IPv4 주소는 부족해져서 호스트끼리 이를 공유해야 될 때, IPv6 상에서 IPv4 트래픽을 전송해야 할 때, 그리고 IPv6 도메인 내의 IPv6 호스트와 소수의 원격 레거시 IPv4 시스템 간의 통신이 필요할 때가 되면 훨씬 중요해지게 됩니다.

DSTM에 대한 추가 정보는 Internet Draft *draft-ietf-ngtrans-dstm-07.txt*를 참조하십시오.

SOCKS 기반 IPv6/IPv4 게이트웨이

SOCKS 기반 IPv6/IPv4 게이트웨이 메커니즘은 IPv4 전용 호스트와 IPv6 전용 호스트 간의 통신을 위해 사용됩니다. 이 메커니즘은 양쪽 엔드 시스템(클라이언트)과 듀얼 스택 라우터(게이트웨이)에 기능을 추가하여 두 개의 IPv4 및 IPv6 연결이 어플리케이션 레이어에서 통신할 수 있는 환경을 허용합니다.

이들 자원의 게이트웨이와 위치에 대한 추가 정보는 RFC 3089, *A SOCKS-based IPv6/IPv4 Gateway Mechanism*을 참조하십시오.

변환 메커니즘 배치

IPv4를 이용하는 어플리케이션과 IPv6을 사용하는 어플리케이션 사이의 통신(예를 들면, IPv6 전용 웹 브라우저가 IPv4 전용 웹 서버와 통신하게 하려면)을 가능케 하려면 IPv4 환경 내에서 IPv6을 배치하기 위한 전략 외에도, 프로토콜 변환 메커니즘(예를 들면 NAT-PT 또는 어플리케이션 레벨 게이트웨이)이 필요합니다.

이들 메커니즘은 IPv6 배치가 시험 단계에서 실용 단계로 넘어가게 될 때 유용하며 어플리케이션 개발자들이 IPv4를 계속 지원하는 것이 비용적으로 효과적이지 못하다는 결정을 내리게 되면 더욱 중요해집니다. 결국 IPv6이 프로토콜의 주류를 이루게 되면 이러한 메커니즘들은 레거시 IPv4 시스템들이 전체 IPv6 네트워크의 일부가 될 수 있도록 해주게 될 것입니다. 이러한 메커니즘들은 IPv6 네트워크 내의 엔드 시스템, 전용 서버, 라우터 상에서 IPv4와 IPv6 프로토콜 간의 변환 기능을 제공하며 듀얼 스택 호스트와 함께 IPv4 트래픽에 지장을 주지 않으면서 점진적으로 IPv6을 배치할 수 있게 합니다.

IPv6 호스트 및 라우터에 대한 전반적인 정보는 RFC 2893, Transition Mechanisms for IPv6 Hosts and Routers를 참조하고, IPv6 변환의 라우팅 관련 정보는 RFC 2185, Routing Aspects of IPv6 Transition을 참조하십시오.

6 장

IPv6 네트워크 설계 고려 사항

IPv6 배치를 위해 시스코는 네트워크의 에지에서 시작하여 코어로 진행하는 변환 전략을 권장합니다. 이 전략은 여러분이 배치 비용을 조절할 수 있게 해주며 지금 단계에서 네이티브 IPv6 네트워크로 완전히 업그레이드하는 것 보다는 어플리케이션에 집중할 수 있도록 합니다. 시스코 IPv6 라우터 제품들은 그러한 통합 전략을 위한 기능을 제공하고 있습니다. 다양한 배치 전략들은 여러분이 구상하고 있는 IPv6로의 첫 번째 변환 단계가 IPv6 기능을 테스트하기 위한 것이 되었건, 대대적인 IPv6 네트워크 구현을 위한 초기 단계가 되었건, 지금 바로 이뤄질 수 있도록 해드립니다.

서비스 공급자 네트워크 환경에서의 IPv6 배치

서비스 공급자를 위한 네트워크 관리자로써, 여러분은 지금 IPv6을 평가하고 파악해보는 것이 좋습니다. 왜냐하면, 현재의 IP 주소 공간은 폭발적인 사용자의 증가나 고객들의 새로운 기술에 대한 요구를 만족시키지 못할 수 있기 때문입니다. 고유한 글로벌 IPv6 주소를 이용하면 도달 가능성과 네트워크 장치의 엔드-투-엔드 보안을 위해 사용되는 메커니즘을 간단하게 만들어주며 이런 기능은 인터넷 기반 PDA, HAN(home-area network), 인터넷으로 연결된 자동차, 통합 텔레포니 서비스 그리고 네트워크 게임 등 새롭게 등장하는 어플리케이션을 위해 필수적입니다.

시스코는 세 단계에 걸친 IPv6 배치를 검토할 것을 권장합니다:

- 고객 액세스 레벨에서 IPv6 서비스 제공: 고객 액세스 레벨에서 IPv6 배치를 시작하는 것은 코어 인프라에 대한 대대적인 업그레이드나 현재의 IPv4 서비스에 대한 악영향 없이 지금 당장 IPv6 서비스를 제공할 수 있게 합니다. 이 접근 방식은 IPv6 제품 및 서비스가 네트워크에 완전히 구현되기 전에 평가받을 수 있도록 합니다. 또한 초기 단계부터 많은 투자를 하지 않고도 IPv6에 대한 미래의 수요를 평가해볼 수 있습니다.
- 코어 인프라 자체 내에서 IPv6 실행: 초기 평가 및 분석 단계가 끝난 다음, 라우터 내에서의 IPv6 지원이 개선되고 (특히 IPv6 고속 포워딩) 네트워크 관리 시스템이 IPv6을 완전히 포용하게 되면 IPv6을 지원하도록 네트워크 인프라를 업그레이드할 수 있습니다. 이런 업그레이드 방식은 듀얼 스택 라우터(IPv4와 IPv6 프로토콜을 하나의 라우터에서 동시에 실행하기 위한 기법)의 사용이 필요할 수 있으며 IPv6 트래픽이 점차 주류를 이루게 되면 결국 IPv6 전용 라우터를 사용하게 됩니다.
- 다른 IPv6 서비스 공급자와 서로 연결: 다른 IPv6 서비스 공급자 또는 6BONE과의 연결은 IPv6에 대한 추가적인 검토 및 평가를 가능케 하여 IPv6의 요구 조건들을 보다 잘 이해할 수 있게 됩니다.

엔터프라이즈 네트워크 환경에서의 IPv6 배치

기업의 네트워크 관리자 또는 운영자로써, 여러분은 가까운 미래에 IPv6 어플리케이션을 네트워크로 도입하기 위해 지금 당장 IPv6을 검토 및 평가해야 할 수도 있습니다. 처음부터 많은 수의 IPv6 전용 어플리케이션들이 등장하지는 않겠지만, 지금 시장에 나오고 있는 일부 모바일 IP 제품들은 IPv6 인프라에서 제공하는 직접 경로 기능을 통해 훨씬 뛰어난 성능과 확장성을 보여줍니다.

새로운 휴대 전화 환경에서 요구하는 엔드-투-엔드 어드레싱, 통합 자동 설정, QoS 및 보안이 IPv6를 검토 및 평가하는 이유가 될 수도 있습니다. 또는 IP 기반 전화 시스템 같은 새로운 서비스를 위해 사용 가능한 주소 공간을 확장시키고 싶을 수도 있습니다.

여러분은 네트워크의 주소 규칙이 어플리케이션에게 보다 투명해지는 글로벌 환경으로의 회귀 또는 주소 변환, 풀링, 임시 할당을 위해 NAT를 비롯한 기타 기법을 사용하는 IPv4 네트워크에서는 구현이 어려운 엔드-투-엔드 보안 및 QoS를 위해 IPv6를 검토할 수도 있습니다.

다음은 IPv6 제품 및 서비스를 검토 및 분석하기 위한 두 가지 방법입니다:

- IPv6 도메인을 구성한 후 6BONE 같은 기존 원격 IPv6 네트워크로 연결
- 2개 이상의 IPv6 도메인을 구성한 후 기존 IPv4 인프라 상에서 이들을 서로 연결

현재 Cisco IOS Software에서 지원하고 있는 IPv6 변환 기법들은 현재의 업무에 지장을 주지 않는 독립적인 방법으로 위에서 설명한 환경 안에서 IPv6 제품 및 어플리케이션을 평가 및 테스트 할 수 있게 해드립니다.

시스코의 IPv6 지원

시스코 시스템즈는 IPv6 포럼(www.ipv6forum.com)의 창단 멤버 중 하나입니다. 시스코는 IETF 내에서 IPv6 아키텍처를 정의 및 구현하는데 앞장서 왔으며 앞으로도 표준화를 위해 업계를 선도해나갈 것입니다. 시스코의 직원인 Steve Deering과 Tony Hain은 각각 IETF IPv6 워킹 그룹과 차세대 변환 (Ngtrans) 워킹 그룹의 공동 회장입니다. 이미 다수의 IPv6 표준이 IETF에 의해 공개되었지만 계속해서 개선되고 있습니다.

시스코는 3 단계에 걸쳐 Cisco IOS Software 및 제품에서 IPv6 기능을 구현하기로 결정했습니다. 여러분은 **www.cisco.com/ipv6**에서 IPv6을 위한 시스코의 로드맵과 Statement of Direction 같은 IPv6 구현 정보를 찾아보실 수 있습니다.

Cisco IOS Software를 위한 IPv6 초기 필드 테스트 버전은 이미 3년 전부터 무료로 제공되어 왔습니다. Cisco IOS IPv6 소프트웨어는 테스트를 위해 지난 수년간 6BONE 네트워크(www.6bone.net)에 대대적으로 배치되어 왔습니다. 또한 Cisco 6BONE 라우터는 5년 이상 6BONE 허브 역할을 해오며 다른 회사들에게 70개 이상의 터널을 제공해왔습니다.

Cisco IOS Software를 위한 IPv6는 Cisco 800 Series 같은 로우엔드급에서 Cisco 12000 인터넷 라우터 같은 하이엔드급 플랫폼에 이르는 모든 시스코 라우터 플랫폼에서 제공됩니다. Cisco IOS Software Release 12.2(2)T 이후부터 시스코는 공식적으로 전세계적인 지원을 제공하고 있습니다. Cisco IOS IPv6에 대한 추가 정보는 www.cisco.com/ipv6에서 찾아보실 수 있습니다.

시스코는 IPv6 배치에 대한 솔루션 문서를 발표할 계획입니다. 이 부분은 문서가 발표된 이후 업데이트될 예정입니다. 또한 시스코 장비에 사용하기 위해 Cisco IOS Software를 위한 IPv6 설정 정보가 필요하시면 cisco.com의 문서를 참조하십시오.

부록 A

관련 서적 및 참고 자원

이 부분은 이 문서를 작성하는데 이용되었던 문서, 서적 및 RFC에 대한 정보와 IPv6에 대한 추가적인 정보 자원을 제공합니다. 여기에는 시스코에서 작성한 기술 문서와 IPv6에 대한 시스코의 웹 페이지가 포함됩니다. 또한 관련 RFC 및 draft에 대한 정보도 포함되어 있습니다.

IPv6에 대한 시스코의 공식 발표

http://www.cisco.com/warp/public/732/tech/ipv6/

시스코 기술 문서

IPv6 for Cisco IOS Software feature documentation (Cisco.com) for IPv6 overview, configuration, and command reference information:
http://www.cisco.com/univercd/cc/td/doc/product/software/

IPv6 integrated solutions documents (ISDs) for detailed information about the various IPv6 transition mechanisms:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6_sol/index.htm

서적

Marcus Gonglaves and Kitty Niles, IPv6 Networks, McGraw Hill, New York, NY 1998

Microsoft Windows 2000 Server, Introduction to IP Version 6, white paper

Cisco Training Guide: Implementing IPv6 Networks

백서 및 기타 문서

Alcatel Technical Paper: The Move to IPv6

Cisco: Engineering Training for IPv6

Cisco: The Internet Protocol Journal

Glocom Platform Tech Reviews: Nobuo Ikeda and Hajime Yamada, Is IPv6 Necessary?

Hirahara.ourfamily.com: Technical – IPv6 and Subnetting IPv4

IP Infusion White Paper: IPv6 Network Processing

IPv6 Forum IPv6 Tutorial: Jordi Palet, ICMPv6 & Neighbor Discovery

Nortel Networks White Paper: *Building the Foundation of the Multimedia Wireless Internet _The migration to IPv6 and MPLS for UMTS*

The O'Relly Network: *Introduction to IPv6*

RFC와 draft

IPv6의 존재 이유

The Recommendation for the IP Next-Generation Protocol: RFC 1752

The Case for IPv6: draft-iab-case-for-ipv6-06.txt

Classless interdomain routing (CIDR): RFC 1519

The H Ratio for Address Assignment Efficiency: RFC 1715

Architectural Implications of NAT: RFC 2993

Internet Transparency: RFC 2775

프로토콜

Internet Protocol Version 6 (IPv6) Specification: RFC 2460

Path MTU Discovery for IP Version 6: RFC 1981

IP Version 6 Management Information Base for TCP: RFC 2452

Internet Control Message Protocol (ICMPv6) for the IPv6 Specification: RFC 2463

IPv6 주소 종류

IP Version 6 Addressing Architecture: RFC 2373

An IPv6 Aggregatable Global Unicast Address Format: RFC 2374

Format for Literal IPv6 Addresses in URL's: RFC 2732

IPv6 Multicast Address Assignments: RFC 2375

IPv6 자동 설정 및 리넘버링(renumbering)

Neighbor Discovery for IP Version 6 (IPv6): RFC 2461

IPv6 Stateless Address Autoconfiguration: RFC 2462

Router Renumbering for IPv6: RFC 2894

IPv6 링크 레이어

Transmission of IPv6 Packets over Ethernet Networks: RFC 2464

Transmission of IPv6 Packets over FDDI Networks: RFC 2467

Transmission of IPv6 Packets over Token Ring Networks: RFC 2470

Transmission of IPv6 over IPv4 Domains without Explicit Tunnels: RFC 2529

Transmission of IPv6 Packets over ARCnet Networks: RFC 2497

IP Version 6 over PPP: RFC 2472

IPv6 over Non-broadcast Multiple Access (NBMA) Networks: RFC 2491

IPv6 over ATM Networks: RFC 2492

Transmission of IPv6 Packets over Frame Relay Networks Specification: RFC 2590

IPv6 라우팅 프로토콜 지원

RIPng for IPv6: RFC 2080

OSPF for IPv6: RFC 2740

Routing IPv6 with IS-IS: draft-ietf-isis-ipv6-02.txt

Multiprotocol Extensions for BGP-4: RFC 2858

Use of BGP-4 Multiprotocol Extensions for IPv6 Interdomain Routing: RFC 2545

IPv6 통합 및 변환 메커니즘

Transmission of IPv6 over IPv4 Domains Without Explicit Tunnels (6over4): RFC 2529

Connection of IPv6 Domains via IPv4 Clouds (6to4): draft-ietf-ngtrans-6to4-07.txt

Network Address Translation-Protocol Translation (NAT-PT): RFC 2766

Transition Mechanisms for IPv6 Hosts and Routers: RFC 2893

Generic Packet Tunneling in IPv6: RFC 2473

Connection of IPv6 Domains via IPv4 Clouds: RFC 3056

On overview of the introduction of IPv6 in the Internet: draft-ietf-ngtrans-introduction-to-ipv6-transition-04.txt

IPv6 Tunnel Broker: draft-ietf-ngtrans-broker-04.txt

IPv6 배치

6BONE pTLA and pNLA Formats (pTLA): RFC 2921

6BONE Backbone Routing Guidelines: RFC 2772

기타 웹 참고 자료

IETF: http://www.ietf.org/html.charters/ipv6-charter.html

6BONE: http://www.6bone.net

6TAP exchange: http://www.6tap.net

Freenet6: http://www.freenet6.net

IPv6 Forum: http://www.ipv6forum.com

http://playground.sun.com/ipv6

http://www.hs247.com

IPv6 호스트 설정

Solaris IPv6

Solaris IPv6: http://www.sun.com/software/solaris/ipv6/

Microsoft IPv6

www.microsoft.com/ipv6

FreeBSD IPv6

Kame: http://www.kame.net

IPv6 주소 할당

Proposed TLA and NLA Assignment Rules: RFC 2450

IPv6 Address Allocation and Assignment Global Policy:

http://www.ripe.net/ripencc/mem-services/registration/ipv6/global-ipv6-assign-2002-04-25.html

Efficient method for address plan: draft-ietf-ipngwg-ipaddressalloc-01.txt

Allocation policy: *ftp://ftp.ripe.net/ripe/docs/ripe-196.txt*

IPv6 주소 등록

RIPE NCC (Europe and Middle East): http://www.ripe.net

ARIN (Americas): http://www.arin.net

APNIC (Asia): http://www.apnic.net

현재의 Sub-TLA 할당

http://www.ripe.net/ripencc/mem-services/registration/ipv6/ipv6allocs.html

부록 B

용어 해설

6BONE – IPv6 네트워크로 구성된 IPv6 테스트 장소. 6BONE은 비공식적으로 진행되는 전세계 공동 프로젝트로 IETF의 IPv6 워킹 그룹에 의해 운영되고 있습니다. IPv4 네트워크 상에서의 IPv6 터널이나 캡슐화를 이용하는 가상 네트워크로 시작되었지만 서서히 IPv6을 트랜스포트를 위한 네이티브 링크로 옮겨가고 있습니다.

6to4 터널 – 터널 엔드 포인트가 6to4 주소에 매입된 고유한 글로벌 IPv4 주소에 의해 결정되는 IPv6 자동 터널링 기법. 6to4 주소는 프리픽스(prefix) 2002::/16과 고유한 글로벌 32비트 IPv4 주소의 조합입니다.(IPv4 호환 주소는 6to4 터널링에서 사용되지 않습니다.)

6to4 릴레이 – 다른 6to4 경계 라우터를 위해 IPv6 인터넷으로의 트래픽 포워딩을 제공하는 6to4 경계 라우터. 6to4 릴레이는 202::/16 프리픽스(prefix)를 가진 목적지로 패킷을 포워딩합니다.

A6 레코드 – 128비트 IPv6 주소를 표시하기 위해 사용된 IPv6 번호를 저장하는 DNS 레코드. IPv6을 인지하는 어플리케이션이 IPv6 서버의 이름을 찾아보고자 할 때는 DNS 서버로부터 A6 레코드를 요청할 수 있습니다. A6 레코드는 시험용으로 사용되는 것이기 때문에 IPv6에서의 이름 해결을 위한 최선의 방법은 아닙니다.

AAAA – 128비트 IPv6 주소를 표시하기 위해 사용된 IPv6 번호를 저장하는 DNS 레코드. AAAA 레코드는 호스트 이름을 해결하기 위해 사용됩니다. 이 작업은 IPv4에서 어플리케이션이 A 레코드를 요청하는 프로세스와 비슷합니다. AAAA 레코드는 IPv6에서의 이름 해결을 위해 가장 선호되는 방법입니다.

애니캐스트 주소 – 대개 서로 다른 노드에 속해있는 인터페이스 집합을 위한 식별자. 애니캐스트 주소로 보내진 패킷은 애니캐스트 주소에 의해 지정된 가장 가까운 인터페이스로 전달됩니다. 이때 가장 가까운 인터페이스는 사용되고 있는 라우팅 프로토콜의 정의를 따르게 됩니다. 글로벌 유니캐스트 주소, IPv6 멀티캐스트 주소, 링크-로컬 주소, 사이트-로컬 주소 및 solicited-node 멀티캐스트 주소도 참조하십시오.

APNIC – Asia Pacific Network Information Center. 아시아 태평양 지역의 국가에 IP 주소를 할당하는 임무를 맡고 있는 지역 인터넷 레지스트리(RIR)입니다.

ARIN – The American Registry for Internet Numbers. 북남미 지역의 국가에 IP 주소를 할당하는 임무를 맡고 있는 지역 인터넷 레지스트리(RIR)입니다.

자동 IPv6 터널 – 특별히 할당된 6to4 IPv6 프리픽스(prefix) 2002::/16을 사용하는 IPv6 주소의 하위 32비트에 포함된 IPv4 주소를 이용하여 터널 소스와 터널 목적지를 자동으로 결정하는 IPv6 터널링 기법. 각 IPv6 자동 터널의 양 끝에 위치한 호스트 및 라우터는 IPv4와 IPv6 프로토콜 스택을 모두 지원해야 합니다. 자동 터널은 경계 라우터 사이에서, 또는 경계 라우터와 호스트 사이에서 설정될 수 있습니다. IPv4 호환 IPv6 주소와 수동 설정 IPv6 터널을 참조하십시오.

BIS – Bump-in-the-Stack. IPv4 전용 호스트 상의 IPv4 어플리케이션과 IPv6 전용 호스트 간의 통신을 위해 사용되는 변환 메커니즘입니다. 스누핑 모듈과 풀에서 자동 할당되는 IPv4 주소를 사용하며 자가 변환기처럼 작동합니다.

CE 라우터 – 고객 에지(customer edge) 라우터는 고객 MPLS 네트워크의 일부인 라우터로 공급자 에지(PE) 라우터와 인터페이스됩니다.

DSTM – Dual-Stack Transition Mechanism. IPv4 쪽에 IPv4 주소를 할당하지 않은 상태로 IPv4 시스템과 통신을 하거나 IPv6 프로토콜 스택 상에서 IPv4 어플리케이션을 실행시켜야 하는 IPv6 도메인의 듀얼 스택 호스트를 위해 사용되는 변환 메커니즘 입니다. DSTM 운영은 IPv4-over-IPv6 터널 그리고 통신을 요청하는 호스트로의 글로벌 IPv4 주소 할당을 기반으로 하고 있습니다.

글로벌 유니캐스트 주소 – 일반적인 IPv4 주소와 비슷한 IPv6 유니캐스트 주소. 글로벌 유니캐스트 주소의 구조는 글로벌 라우팅 테이블의 라우팅 테이블 항목 수를 제한하는 라우팅 프리픽스(prefix) 집합을 가능케 합니다. 애니캐스트 주소, IPv6 멀티캐스트 주소, 링크-로컬 주소 그리고 사이트-로컬 주소도 참조하십시오.

GRE 터널 – IS-IS 프로토콜에 특히 적합한 수동 설정 터널. GRE 터널은 특정 패신저 또는 트랜스포트 프로토콜에 국한되지 않지만, 이 경우에는 IPv6 트래픽이 패신저 프로토콜이 되며 GRE는 캐리어 프로토콜이 됩니다.

IANA – Internet Assigned Number Authority. 인터넷 프로토콜에 고유한 매개 변수 값을 할당하는 책임을 맡고 있습니다.

IETF – Internet Engineering Task Force. 네트워크 연구자, 설계자, 운영자 및 벤더들의 국제적인 모임으로 TCP/IP 및 글로벌 인터넷을 설계 및 엔지니어링하는 책임을 맡고 있습니다.

IPv4 호환 IPv6 주소 – 주소의 상위 96비트에는 0이 들어있고 주소의 하위 32비트에는 IPv4 주소가 들어있는 IPv6 유니캐스트 주소. IPv4 호환 IPv6 주소의 포맷은 0:0:0:0:0:0:A.B.C.D 또는 ::A.B.C.D입니다. 128비트의 IPv4 호환 IPv6 주소는 노드의 IPv6 주소로 사용되며 하위 32비트에 들어있는 IPv4 주소는 노드의 IPv4 주소로 사용됩니다. IPv4 호환 IPv6 주소는 IPv4 및 IPv6 프로토콜 스택을 모두 지원하며, 자동 터널에 사용될 노드에 할당됩니다. 애니캐스트 주소, 자동 IPv6 터널, IPv6 멀티캐스트 주소, 링크-로컬 주소 및 사이트-로컬 주소 등을 참조하십시오.

IPv6 멀티캐스트 주소 – FF00::/8을 프리픽스(prefix)로 가지고 있는 IPv6 주소. IPv6 멀티캐스트 주소는 보통 서로 다른 노드에 속해있는 인터페이스 집합을 위한 식별자입니다. 멀티캐스트 주소로 보내진 패킷은 멀티캐스트 주소에 의해 식별된 모든 인터페이스로 전달됩니다. 글로벌 유니캐스트 주소, 애니캐스트 주소, 링크-로컬 주소, 사이트-로컬 주소 및 solicited-node 멀티캐스트 주소 등을 참조하십시오.

ISATAP – 특히 캠퍼스 네트워크 환경 같은 곳에서 IPv6을 배치하기 위해 사용되는 변환 메커니즘. ISATAP은 사이트의 IPv4 인프라를 NBMA(non-broadcast multi-access) 링크 레이어처럼 취급하여 점진적인 IPv6 배치를 가능케 합니다.

링크 – 링크는 부수적인 네트워크로 인한 복잡함으로부터 서브 네트워크를 보호하면서 멀티 레벨, 계층적 라우팅 구조를 제공하기 위해 네트워크 관리자가 임의로 분할한 네트워크. IPv4의 서브 네트워크와 비슷합니다. 링크와 서브 네트워크 프리픽스(prefix)는 일대일로 지정되지만 여러 개의 서브 네트워크 프리픽스(prefix)를 동일한 링크로 지정할 수도 있습니다.

링크-로컬 주소 – 로컬 링크(로컬 네트워크)로 범위가 제한된 IPv6 유니캐스트 주소. 링크-로컬 주소는 링크-로컬 주소를 위한 특정 프리픽스(prefix) (FE80::/10)에 수정된 EUI-64 포맷의 인터페이스 ID를 추가하여 자동으로 설정됩니다. 링크-로컬 주소는 네이버 탐색(Neighbor Discovery) 프로토콜과 라우터 탐색 (Router Discovery) 프로토콜에 의해 사용됩니다. 또한 많은 라우팅 프로토콜에서도 사용하고 있습니다. 링크-로컬 주소는 글로벌 주소를 사용하지 않으면서, 같은 로컬 네트워크 상의 장치들을 연결하기 위한 방법으로 사용됩니다. 글로벌 유니캐스트 주소, 애니캐스트 주소, IPv6 멀티캐스트 주소, 사이트-로컬 주소 및 solicited-node 멀티캐스트 주소 등을 참조하십시오.

수동 설정 IPv6 터널 – 수동으로 설정된 IPv6 주소가 터널 인터페이스로 설정되고 수동 설정된 IPv4 주소가 터널 소스 및 목적지로 설정되는 IPv6 터널링 기법. 터널의 엔드포인트로 사용되는 에지 라우터와 엔드 시스템은 듀얼 스택 시스템이어야 합니다. 수동 설정 터널은 경계 라우터 사이 또는 경계 라우터와 호스트 사이에 설정 될 수 있습니다. 자동 IPv6 터널을 참조하십시오.

MPLS – Multiprotocol Label Switching. 레이블을 이용하여 IP 트래픽을 포워딩하는 스위칭 기법입니다. 이 레이블은 미리 정해진 IP 라우팅 정보를 토대로 네트워크 내의 라우터와 스위치에게 패킷을 어디로 포워딩할지 알려주게 됩니다.

NAT-PT – Network address translation-protocol translation. IPv4와 IPv6 주소 사이의 네트워크 레이어에서 변환을 하는 변환 메커니즘으로 네이티브 IPv6 호스트와 어플리케이션들이 네이티브 IPv4 호스트 및 어플리케이션과 통신할 수 있도록 합니다. IPv4와 IPv6 DNA 요청 및 응답 사이의 변환은 Application Level Gateway(AGL)가 하게 됩니다.

NLA – IPv6 네트워크 계층에서 설명된 Next Level Aggregator. Top Level Aggregator 서비스 공급자 아래에 위치한 IPv6 서비스 공급자입니다. 24비트의 NLA 필드는 최대 1,600만개의 Site Level Aggregator를 지원할 수 있습니다. NLA는 더 이상 IPv6 RFC의 일부가 아닙니다. TLA와 SLA를 참조하십시오.

pTLA – pseudo Top Level Aggregator. IPv6 네트워크 계층에서 설명된 바와 같이 6BONE 네트워크와 사용됩니다. TLA를 참조하십시오.

SIIT – Stateless IP/ICMP Translator. 패킷별로 IPv4와 IPv6 사이의 IP 패킷 헤더를 변환하고 IPv4와 IPv4로 변환 또는 매핑된 IPv6 주소 간의 헤더 안에 있는 주소를 변환하는 알고리즘입니다.

RIPE NCC – Reseaux IP Europeens_Network Coodination Center (RIPE NCC). 유럽 및 중동 지역의 국가에 IP 주소를 할당하는 임무를 맡고 있는 지역 인터넷 레지스트리(RIR)입니다.

사이트-로컬 주소 – 사이트 내에서만 유용한 주소로 IPv4 네트워크에서 사용되는 사설 주소와 유사합니다. 사이트-로컬 주소는 프리픽스(prefix) 범위 FEC0::/10(1111 1110 11)을 이용하고 서브네트 식별자(16비트 Subnet ID 필드)와 EUI-64 포맷의 인터페이스 ID를 연결시킨 IPv6 유니캐스트 주소 입니다. 애니캐스트 주소, 글로벌 유니캐스트 주소, IPv6 멀티캐스트 주소, 링크-로컬 주소 및 solicited-node 멀티캐스트 등을 참조하십시오.

SLA – Site Level Aggregator. IPv6 네트워크 계층에서 설명된 바와 같이 Next Level Aggregator 서비스 공급자 아래에 위치한 IPv6 서비스 공급자입니다. 16비트의 SLA 필드는 사이트 내에서 최대 65,535 개의 서브네트를 지원합니다. NLA와 TLA를 참조하십시오.

Solicited-node 멀티캐스트 주소 – 해당 IPv6 유니캐스트 또는 애니캐스트 주소의 하위 24비트와 연결된 FF02:0:0:0:0:1:FF00:0000/104 프리픽스(prefix)를 가지고 있는 IPv6 주소. Solicited-node 멀티캐스트 주소는 IPv6 유니캐스트 또는 애니캐스트 주소에 해당하는 멀티캐스트 그룹 주소입니다. IPv6 노드는 할당 받은 모든 유니캐스트 및 애니캐스트 주소와 관련된 모든 Solicited-node 멀티캐스트 그룹에 합류해야 합니다. 애니캐스트 주소, 글로벌 유니캐스트 주소, IPv6 멀티캐스트 주소, 링크-로컬 주소 및 사이트-로컬 주소를 참조하십시오.

TCP-UDP 릴레이 – NAT-PT와 비슷한 변환 메커니즘. 전용 서버와 DNS를 필요로 합니다. 이 방식은 네트워크 레이어가 아닌 트랜스포트 레이어에서 변환을 하며 DNS가 IPv4와 IPv6 주소 간의 매핑을 제공합니다.

Teredo 터널 – Teredo(또는 Shipworm)서비스는 NAT 장치를 통해 UDP 상에서 IPv6 패킷을 터널링하여 하나 이상의 IPv4 NAT 뒤에 위치한 노드에 IPv6 연결을 제공하는 터널 메커니즘입니다.

TLA – Top Level Aggregator. IPv6 네트워크 계층에서 설명된 바와 같이 IPv6 네트워크 계층 구조에서 가장 위쪽에 위치한 서비스 공급자입니다. TLA는 IPv6 네트워크 라우팅 계층의 상위 레벨을 유지하는 책임을 맡고 있습니다. 13비트의 TLA 필드는 최대 8192 개의 TLA를 지원합니다. TLA는 더 이상 IPv6 RFC의 일부가 아닙니다.

부록 C

리뷰 문제

다음 리뷰 문제들은 ABCs of IP Version 6 문서를 통해 여러분이 기술 정보를 얼마나 잘 배웠는지 평가할 수 있도록 도와드립니다. 이 문서의 부록 D에는 다음 리뷰 문제들에 대한 해답이 있습니다.

1. NAT가 IP 주소 고갈 문제를 해결하기 위한 이상적인 솔루션이 아닌 이유는 무엇입니까?

   a. NAT는 IP의 엔드-투-엔드 보안 모델을 파괴한다.

   b. NAT는 네트워크 장치와 데이터를 외부 침입자로부터 보호한다.

   c. NAT는 네트워크 내에서 사설 주소 공간을 이용하여 글로벌 IP 주소를 보존한다.

   d. NAT는 인터넷과의 통신을 위해 내부 네트워크 장치에 글로벌 주소를 동적으로 할당한다.

2. IPv6 주소 스키마는 몇 비트를 지원합니까?

   a. 32비트

   b. 64비트

   c. 96비트

   d. 128비트

3. IPv6 헤더에서 삭제된 IPv4 헤더 필드는 무엇입니까?

   a. 버전, 프레그먼트 필드, 헤더 체크섬, 패딩

   b. 버전, 헤더 길이, 프레그먼트 필드, 헤더 체크섬

   c. 헤더 길이, 프레그먼트 필드, 헤더 체크섬, 플로우 레이블

   d. 헤더 길이, 프레그먼트 필드, 헤더 체크섬, 패딩

4. IPv6 라우팅 프로토콜에 대해 다음 중 옳은 것은 무엇입니까?

   a. IPv6 RIP 프로토콜의 이름은 RIP-2 이다.

   b. IPv6 IS-IS 프로토콜은 현재 IETF 표준이다.

   c. IPv6 OSPF 프로토콜은 IETF에서 제안된 표준이다.

   d. IPv6 OSPF 프로토콜은 현재 IETF 표준이 아니다.

5. IPv6에서의 라우팅에 대해 다음 중 옳지 않은 것은 무엇입니까?

   a. IPv4와 IPv6 모두 같은 라우팅 프로토콜을 지원한다.

   b. IPv6 RIP 업데이트는 all-rip-router 멀티캐스트 그룹 주소 FF02::9로 전송된다.

   c. IPv6은 라우팅 알고리즘을 위해 longest-prefix 매칭을 사용하지 않는다.

   d. BGP-4+ NEXT_HOP와 NLRI는 IPv6 주소 및 프리픽스(prefix)로 표시되어 있다.

6. IPv6 자동 설정에 대해 다음 중 옳은 것은 무엇입니까?

   a. IPv6은 모든 IPv6 네트워크에서의 DHCP 서버 사용을 의무화하고 있다.

   b. IPv6 네트워크에서는 충돌이 없기 때문에 자동 설정이 가능하다.

   c. 대규모의 주소 공간은 IPv6 호스트들이 스스로를 자동 설정할 수 있게 한다.

   d. IPv6 장치들은 미리 정해진 IPv6 주소를 가지고 있어 설정이 필요없다.

7. IPv6의 브로드캐스트와 멀티캐스트에 대해 다음 중 옳은 것은 무엇입니까?

   a. IPv6에서는 브로드캐스트가 사용되지 않는다.

   b. 브로드캐스트는 IPv6 네트워크를 완전히 마비시킬 수 있다.

   c. 브로드캐스트는 IPv6의 다양한 기능을 수행하기 위한 기본 메커니즘이다.

   d. 브로드캐스트는 LAN 네트워크의 모든 노드를 방해할 수 있다.

8. IPv6의 기능이 아닌 것은 무엇입니까?

   a. 자동 설정

   b. 자동 QoS 지원

   c. 쉬운 리넘버링(renumbering)

   d. 대규모 주소 공간

9. IPv6 헤더에 새롭게 추가된 필드는 무엇입니까?

   a. 목적지 주소

   b. 소스 주소

   c. 플로우 레이블

   d. 버전

10. IPv6 기능에 대해 옳지 않은 것은 무엇입니까?

    a. IPv6에서는 UDP 체크섬이 필수이다.

    b. 모든 IPv6 노드가 이동성 기능을 사용할 수 있다.

    c. 내장된 IPSec 지원을 통해 IPv6은 엔드-투-엔드 보안을 지원한다.

    d. IPv6의 멀티호밍 구현은 IPv4보다 어렵다.

11. IPv6 링크-로컬 주소 프리픽스(prefix)로 옳은 것은 무엇입니까?

    a. 2001:1

    b. 2002:1

    c. FE80::/10

    d. FEC0::/10

12. IPv6 링크-로컬 주소는:

    a. 주소의 가장 왼쪽 필드에 96 개의 0이 있다.

    b. 링크-로컬 프리픽스(prefix), 16비트 서브네트 ID 필드, EUI-64 포맷의 인터페이스 ID로 구성되어 있다.

    c. 글로벌 주소 없이 두 네트워크의 장치들을 연결하는 방법으로 쓰인다.

    d. 링크-로컬 프리픽스(prefix)와 EUI-64 포맷의 인터페이스 ID를 이용하여 모든 인터페이스 상에 자동 설정된다.

13. IPv6 헤더 필드에 대해 옳지 않은 것은 무엇입니까?

    a. IPv6 Next Header 필드는 IPv4 헤더의 Protocol 필드와 비슷하다.

    b. IPv6 Traffic Class 필드는 IOPv4 헤더의 Type of Service 필드와 비슷하다.

    c. IPv6 Hop Limit 필드는 매우 효율적인 체크섬 계산을 가능케 한다.

    d. Next Header 필드 값은 기본 IPv6 헤더 다음에 오는 정보의 종류를 결정한다.

14. IPv6이 확장자 헤더를 보다 효율적으로 처리하는 방법은 무엇입니까?

    a. 정확한 프로세싱을 위해 모든 개별 헤더 필드를 검토

    b. 빠른 프로세싱을 위해 확장자 헤더 필드를 서로 연결

    c. 빠른 프로세싱을 위해 라우팅 헤더 필드를 서로 연결

    d. Routing Header가 없을 경우 확장자 헤더 필드를 무시

15. 다음 중 유효한 IPv6 주소는 무엇입니까?

    a. 2001:1:0:4F3A:206:AE14

    b. 2001:1:0:4F3A:0:206:AE14

    c. 2001:1:0:4F3A::206:AE14

    d. 2001:1::4F3A:206::AE14

16. IPv6 노드에서 필요로 하는 주소가 아닌 것은 무엇입니까?

    a. All-nodes 멀티캐스트 주소

    b. 각 인터페이스의 링크-로컬 주소

    c. 라우팅 프로토콜을 위한 특정 멀티캐스트 주소

    d. 각 지정된 유니캐스트 및 애니캐스트 주소를 위한 Solicited-node 멀티캐스트 주소

17. 6BONE 네트워크에 대해 옳지 않은 것은 무엇입니까?

    a. 6BONE은 IPv6 네트워크를 테스트하기 위한 네트워크이다.

    b. 6BONE은 공급자들로 이뤄진 계층 구조이다.

    c. 6BONE 네트워크 pTLA 프리픽스(prefix)는 2001::/16 범위 내에 있다.

    d. 6BONE은 레지스트리에서 할당된 주소와 6BONE 주소만을 허용한다.

18. 네이버 탐색(Neighbor Discovery) 프로세스가 도와주는 결정은?

    a. 같은 링크에 있는 네이버의 링크-레이어 주소

    b. 다른 링크에 있는 네이버의 멀티캐스트 주소

    c. 다른 링크에 있는 가장 가까운 라우터의 IPv6 주소

    d. 같은 링크에 있는 네이버의 IPv6 주소

19. IPv6 네이버 요청(Neighbor solicitation)은:

    a. 네이버의 도달 가능성을 확인하기 위해 사용될 수 있다.

    b. 부팅시 전송되어 라우터 선언(Router Announcements)을 즉시 수신할 수 있도록 한다.

    c. IPv4에서 사용되는 Reverse Address Resolution Protocol(RARP)과 비슷하다.

    d. 정기적인 선언의 형태로 All-node 멀티캐스트 주소를 향해 전송된다.

20. IPv6에서 지원하는 최소 MTU는 무엇입니까?

    a. 68 octets

    b. 576 octets

    c. 1280 octets

    d. 1500 octets

21. 올바른 IPv6 운영을 설명하고 있는 것은 무엇입니까?

    a. 프레그먼트는 시작 호스트에서만 할 수 있다.

    b. 프레그먼트는 시작 라우터에서만 할 수 있다.

    c. 프레그먼트는 IPv4와 똑같이 처리된다.

    d. ICMPv6 메시지는 프레그먼트 프로세스에서 사용되지 않는다.

22. DHCPv6을 가장 잘 설명한 것은 무엇입니까?

    a. DHCPv6은 stateful 자동 설정에서만 사용될 수 있다.

    b. DHCPv6은 stateless/serverless 자동 설정에서만 사용될 수 있다.

    c. DHCPv6은 자동 도메인 이름 등록에 사용될 수 없다.

    d. DHCPv6은 stateless 자동 설정과 함께 사용될 수 있다.

23. DNS를 위한 hostname-to-IP 주소 변환을 위해 권장되는 IPv6 DNS 레코드는 무엇입니까?

    a. A

    b. AAAA

    c. A6

    d. PTR

24. IPv6을 위한 설정 터널의 터널 엔드 포인트에 대해 옳지 않은 것은 무엇입니까?

    a. 터널 엔드 포인트는 듀얼 스택이어야 한다.

    b. 터널 엔드 포인트에 IPv4 및 IPv6 주소가 모두 설정되어야 한다.

    c. 터널 엔드 포인트의 설정은 동적으로 변경된다.

    d. 터널 엔드 포인트는 에지 라우터 및 엔드 시스템이 될 수 있다.

25. 수동 설정 터널과 IPv4 호환 터널의 가장 큰 차이를 설명하고 있는 것은 무엇입니까?

    a. 수동 설정 터널은 정적인 터널이지만 IPv4 호환 터널은 자동 터널이다.

    b. 수동 설정 터널은 전혀 확장될 수 없지만 IPv4 호환 터널은 상당히 확장될 수 있다.

    c. 수동 설정 터널은 IPv6 주소를 절약할 수 있지만 IPv4 호환 터널은 IPv4 주소를 절약할 수 있도록 도와준다.

    d. 수동 터널은 IPv4 주소도 사용하지만 IPv4 호환 터널은 IPv6 주소만을 사용한다.

26. IPv4 호환 터널과 6to4 터널의 가장 큰 차이를 설명하고 있는 것은 무엇입니까?

    a. IPv4 호환 터널은 정적인 터널이지만 6to4 터널은 자동 터널이다.

    b. IPv4 호환 터널은 보통 2 개의 IPv6 도메인 사이에서만 사용되지만 6to4 터널은 여러 개의 IPv6 도메인을 연결하기 위해 사용된다.

    c. IPv4 호환 터널을 배치하려면 에지 라우터에 특별한 코드가 있어야 하지만 6to4 터널은 그런 특별한 코드를 필요로 하지 않는다.

    d. IPv4 호환 터널에는 ISP가 각 도메인에 IPv4 주소만을 할당하지만, 6to4 터널에는 각 도메인에 IPv6 주소만을 할당한다.

27. 6to4 릴레이 운영을 가장 잘 설명한 것은 무엇입니까?

    a. 6to4 릴레이는 라우터가 아니며 IPv6 인터넷으로의 게이트웨이이다.

    b. 6to4 릴레이는 다른 6to4 라우터로만 패킷을 포워딩하기 위해 사용된다.

    c. 6to4 릴레이는 IPv6 인터넷으로만 패킷을 포워딩하기 위해 사용된다.

    d. 6to4 릴레이는 다른 6to4 라우터 및 IPv6 인터넷으로 패킷을 포워딩하기 위해 사용된다.

부록 D

리뷰 문제 해답

1a, 2d, 3d, 4c, 5c, 6c, 7a, 8b, 9c, 10d, 11c, 12d, 13c, 14b, 15c, 16c, 17c, 18a, 19a, 20c, 21a, 22d, 23b, 24c, 25a, 26b, 27d

Please direct comments to abcios@cisco.com

www.cisco.com/kr

2004-11-15

■ Gold SI파트너	• (주)데이타크레프트코리아	02-6256-7000	• (주)인네트	02-3451-5300	• (주)인성정보	02-3400-7000
	• 한국아이비엠(주)	02-3781-7800	• (주)콤텍시스템	02-3289-0114	• 쌍용정보통신(주)	02-2262-8114
	• 에스넷시스템(주)	02-3469-2400	• (주)링네트	02-6675-1216	• 한국후지쯔(주)	02-3787-6000
	• 한국휴렛팩커드(주)	02-2199-0114	• (주)LG씨엔에스	02-6363-5000		
■ Silver SI파트너	• 한국NCR	02-3279-4423	• (주)시스폴	02-6009-6009	• 포스데이타주식회사	031-779-2114
	• SK씨앤씨(주)	02-2196-7114/8114				
■ Local 디스트리뷰터	• (주)소프트뱅크커머스코리아	02-2187-0176	• (주)아이넷뱅크	02-3400-7490	• (주)SK 네트웍스	02-3788-3673
■ IPT 전문파트너	• 에스넷시스템(주)	02-3469-2900	• (주)인성정보	02-3400-7000	• 크리스넷	1566-3827
	• LG기공	02-2630-5280	• (주)컴웨어	02-2631-4300		
■ IP/VC(Video Conferencing)	• (주)텔레트론	031-340-7102	• (주)컴웨어	02-2631-4300		
■ IPCC전문파트너	• 한국IBM	02-3781-7114	• 한국HP	02-2199-4272	• LG기공	02-2630-5280
	• (주)인성정보	02-3400-7000	• 삼성네트웍스주식회사	02-3415-6754		
■ WLAN 전문 파트너	• (주)에어키	02-584-3717	• (주)텔레트론	02-6245-7600		
■ Security 전문 파트너	• 코코넛	02-6007-0133	• (주)토탈인터넷시큐리티시스템	051-743-5940	• 나래시스템	02-2190-5533
	• UNNET Systems	02-565-7034				
■ Optical 전문 파트너	• (주)LG씨엔에스	02-6363-5000	• 에스넷시스템(주)	02-3469-2900	• 미리넷주식회사	02-2142-2800
■ CN 전문 파트너	• 메버릭시스템	02-6283-7425				
■ Storage 전문 파트너	• (주)패킷시스템즈코리아	02-558-7170	• 메크로임팩트	02-3446-3508		