《主 題》

인터네트 프로토콜

김형기[1], 송관호[2]
1. 한국전산원 표준본부 연구원
2. 한국전산원 표준본부 본부장(공학박사)

□차 례□

Ⅰ. 서 론

전세계에 걸친 거대 네트워크를 구성하고 있는 인터네트는 인포메이션 슈퍼하이웨이라는 차세대 정보통신망이 그 하부구조로 떠오르면서 일반 사용자의 관심이 더욱 증가되고 있으며 각 기업의 상용서비스가 연결되면서 발전의 기반이 더욱 튼튼히 다져지고 있다.

인터네트 프로토콜(IP : Internet Protocol)은 그림 1의 TCP/IP 프로토콜 구조에서 보는 바와 같이 4계층 구조의 2번째 계층에 위치하여 있다. 이 인터네트 프로토콜은 RFC 791에 기술되어 있으며 TCP/IP 프로토콜 스위트에서 핵심이 되는 계층이며 인터네트 계층에서 가장 중요한 프로토콜이다. 인터네트 프로토콜은 TCP/IP 망에서 기본 패킷 전달 서비스를 제공한다. 인터네트 프로토콜의 상위 계층 및 하위 계층의 모든 프로토콜은 데이터를 전송하기 위해 들어오는 데이터이든 나가는 데이터이든 그 목적지에 관계없이 인터네트 프로토콜을 사용한다.

인터네트 프로토콜은 신뢰성 없는 비연결형 서비스(Connectionless Services)를 제공한다[1-4]. 즉, 종단대종단(end-to-end) 혹은 홉간(hop-to-hop)의 acknowledgements도 없으며, 데이터에 대한 오류제어 기능도 제공하지 않는다. 또한 재전송이나 흐름 제어 기능도 없다. 단지 IP 데이터그램의 헤더에 대한 검사합(header checksum)만을 제공할 뿐이다.

1	응용 계층 : 네트워크를 사용하는 응용 및 프로세스로 이루어짐
2	수송 계층 : 호스트와 호스트간의 종단 대종단간의 데이터 전송 서비스를 제공
3	**인터네트 계층 : 데이터그램을 정의하고 데이터의 경로 설정을 다룸**
4	네트워크 접속 계층 : 물리적인 네트워크를 접속하기 위한 루틴으로 이루어짐

(그림 1) TCP/IP 프로토콜 구조

인터네트 프로토콜의 주요 기능은 다음과 같다:
- 데이터그램의 정의
- 인터네트 주소 지정 방법의 정의
- 네트워크 접속 계층과 수송 계층 사이의 데이터 전송
- 경로 지정
- 데이터그램을 분할(fragmentation) 및 재결합(reassembly)

본 고에서는 인터네트 프로토콜에서 목적지가 어디 있는지를 식별하는 인터네트 주소 체계를 소개한다. 그리고 TCP/IP 프로토콜 스위트에서 비연결형의 신뢰성 없는 기본 패킷 전달 서비스를 하는 인터네트 프로토콜의 현재 버전인 IPv4를 기술하고 IPv4의 문제점을 개선한 차세대 인터네트 프로토콜인 IPv6를 기술한다.

Ⅱ. 인터네트의 IP 주소 체계

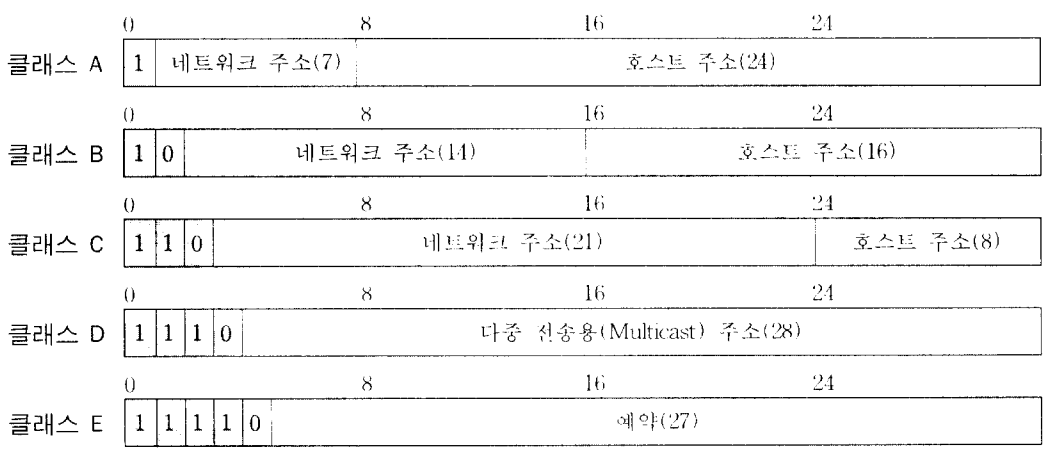
2.1 IP v4의 주소 체계

두 인터네트 호스트 사이에 데이터를 전달하기 위해서는 네트워크 상의 올바른 호스트를 식별하여 원하는 프로세스에게 데이터를 전달하는 방법이 필요하다. TCP/IP에서는 이를 위해 다음의 세 가지 방법을 사용한다[2]:

- 주소지정(Addressing) : 네트워크 상에서 호스트를 유일하게 식별할 수 있는 정보인 IP 주소는 올바른 호스트에 데이터를 전달하는데 사용된다.
- 경로지정(Routing) : 라우터 혹은 게이트웨이가 올바른 네트워크로 데이터를 전달하는데 사용된다.
- 멀티플렉싱(Multiplexing) : 프로토콜과 포트 번호는 호스트 내에서 올바른 소프트웨어 모듈에 데이터를 전송하는데 사용된다

즉, 주소지정은 호스트 사이에, 경로 지정은 네트워크 사이에, 그리고 멀티플렉싱(다중화)은 계층 사이에서 인터네트를 통해 협력하는 응용 사이에 데이터를 전달하기 위해 사용된다. 인터네트 프로토콜은 데이터그램의 형태로 호스트 사이에 데이터를 전송한다. 각 데이터그램은 데이터그램 헤더의 목적지 IP 주소로 전달된다. 이 IP 주소는 32비트 길이로 인터네트 상의 네트워크 및 특정 호스트를 유일하게 식별할 수 있는 충분한 정보를 가지고 있다.

32 비트의 IP 주소는 (네트워크 주소, 호스트 주소)의 쌍으로 이루어진다. IP 주소의 네트워크 주소는 네트워크 사이에 데이터그램의 경로를 설정하는데 사용되며 호스트 주소는 특정한 호스트로 데이터그램을 전송하는데 사용되며 클래스에 따라 네트워크 주소의 길이와 호스트 주소의 길이가 다르다. 그림 2는 다섯 개의 IP 주소 클래스를 보여준다. 32비트의 주소는 202.30.67.159와 같이 각각 1바이트(8비트)씩 4개의 10진수로 각 숫자 사이는 '.'으로 분리하여 표현한다. 각각의 주소 클래스는 주소의 첫 번째 몇 비트로 구별된다. A 클래스는 '0'으로 시작되며, B 클래스는 '10', C 클래스는 '110', D 클래스는 '1110', E 클래스는 '11110'으로 시작된다.



(그림 2) 인터네트 주소

클래스 A 주소의 첫 번째 비트는 '0'이며 7비트는 네트워크 주소로 24비트는 호스트 주소로 사용된다. 그러므로 클래스 A는 128개의 네트워크와 네트워크당 16,777,216개의 호스트를 가질 수 있다. 이 주소는 호스트의 수가 많은 네트워크에 사용된다.

클래스 B 주소의 첫 번째 두 비트는 '10'으로 시작되며 14 비트는 네트워크 주소로 16 비트는 호스트 주소로 사용된다. 그러므로 클래스 B에서는 16,384개의 네트워크와 네트워크마다 65,536개의 호스트를 가

질 수 있다. 이 주소는 호스트의 수가 중간 정도의 네트워크에 사용된다.

클래스 C 주소의 첫 번째 3비트는 '110'으로 시작되며 21비트는 네트워크 주소로 8비트는 호스트 주소로 사용된다. 그러므로 클래스 C에서는 2,097,152개의 네트워크와 네트워크마다 256개의 호스트를 수용할 수 있다. 이 주소는 호스트의 수가 작은 네트워크를 위해 사용된다.

클래스 D 주소의 첫 번째 4비트는 '1110'으로 시작되며 이 주소는 다중 전송용(Multicast) 주소로 사용된다. 그리고 첫 번째 5비트가 '11110'으로 시작되는 클래스 E 주소는 장래에 특별한 용도로 사용하기 위해 예약되어 있는 상태이다. 이들 각 클래스 별 네트워크 수, 호스트 수, 그리고 주소 범위는 그림 3을 참조하라.

클래스	네트워크 수	호스트 수 (네트워크 당)	주소 범위
A	2^{7} = 128	2^{24} = 16,777,216	**0**.0.0.0 - **127**.255.255.255
B	2^{14} = 16,384	2^{16} = 65,536	**128**.0.0.0 - **191**.255.255.255
C	2^{21} = 2,097,152	2^{8} = 256	**192**.0.0.0 - **223**.255.255.255
D		2^{28} = 268,435,456	**224**.0.0.0 - **239**.255.255.255
E		2^{27} = 134,217,728	**240**.0.0.0 - **247**.255.255.255

(그림 3) 클래스 별 IP 주소 통계

그러나 모든 네트워크 주소 혹은 호스트 주소가 사용되지는 않는다. 클래스 D와 E는 각각 다중 전송용 주소 및 미래에 사용하기 위해 예약되어 있다. 그리고 두 클래스 A 주소 0과 127은 각각 디폴트 경로(default route) 및 루프백 주소(Loopback Address)로 사용된다. 디폴트 경로는 경로 설정 정보를 단순하게 하기 위해 사용되며, 루프백 주소는 로컬 호스트가 원격지의 호스트와 같은 방식으로 주소 지정될 수 있도록 함으로써 로컬 호스트 상에서 프로세스 사이의 통신을 시험할 목적으로 설계되었다. 호스트 상의 프로그램이 루프백 주소로 데이터그램을 전송하면 프로토콜 소프트웨어는 이 데이터그램을 네트워크로 전송하지 않고 다시 그 호스트로 되돌린다.

모든 네트워크 클래스의 주소에서 호스트 주소 0과 255는 특별한 용도를 위해 예약되어 있다. IP 주소에서 호스트 주소가 모두 0으로 설정되면 네트워크 자신을 표시하기 위해 사용된다. 예를 들어 26.0.0.0은 A 클래스 네트워크 26을 나타내며, 128.66.0.0은 클래스 B 네트워크인 128.66을 표시한다. 그리고 192.30.65.0은 클래스 C 네트워크인 192.30.65를 나타낸다. 호스트 주소의 모든 비트가 '1'로 설정된 IP 주소는 방송용 주소(broadcast address)로 사용된다. 방송 주소는 다중 전송용 주소와는 달리 네트워크의 모든 호스트에 동시에 데이터그램을 전송하는데 사용된다. 예로 192.30.65 네트워크의 방송용 주소는 192.30.65.255이다. 이 주소로 보내진 데이터그램은 192.30.65 상의 모든 호스트로 전송된다.

TCP/IP가 설계될 당시에 TCP/IP 설계자들은 오늘날의 데스크탑으로 된 네트워크가 등장하리라고 예상하지 못했다. 그 당시에는 커다란 기관만이 컴퓨터 시스템을 보유하고 있었으며 이들만이 네트워크에 연결되었으므로 32비트의 주소로는 충분했으며 라우터의 부하를 줄이기 위해 클래스를 나누었다. 예를 들어 6개의 C 클래스 대신에 하나의 커다란 B 클래스로 네트워크를 할당함으로써 전체 하나의 기관에 라우터를 유지할 수 있도록 하여 라우터의 부하를 줄였다. 또한 B 클래스의 주소를 할당받은 기관이 65,636개의 호스트 컴퓨터를 가지고 있지 않기 때문에 많은 호스트 주소가 낭비되는 결과를 초래했다.

인터네트의 모든 네트워크로 주소 지정할 수 있는 IP 주소는 TCP/IP 프로토콜의 커다란 강점이었다. 그러나 32비트 길이의 IP 주소는 인터네트에 접속하는 호스트의 수가 폭발적으로 증가함에 따라 고갈될 위기에 놓여 있다. 이를 지연시키기 위해 임시방편으로 C 클래스의 주소만을 할당하며 CIDR(Classless

Inter-Domain Routing)를 사용하여 주소의 고갈을 지연시키고 있다.

위와 같은 주소의 고갈, 라우팅의 어려움 및 보안 등의 문제점들로 인해 현재 인터네트에서 사용되고 있는 IPv4를 개선한 IPv6의 연구가 진행되어 이제는 실용화의 단계에 와 있다.

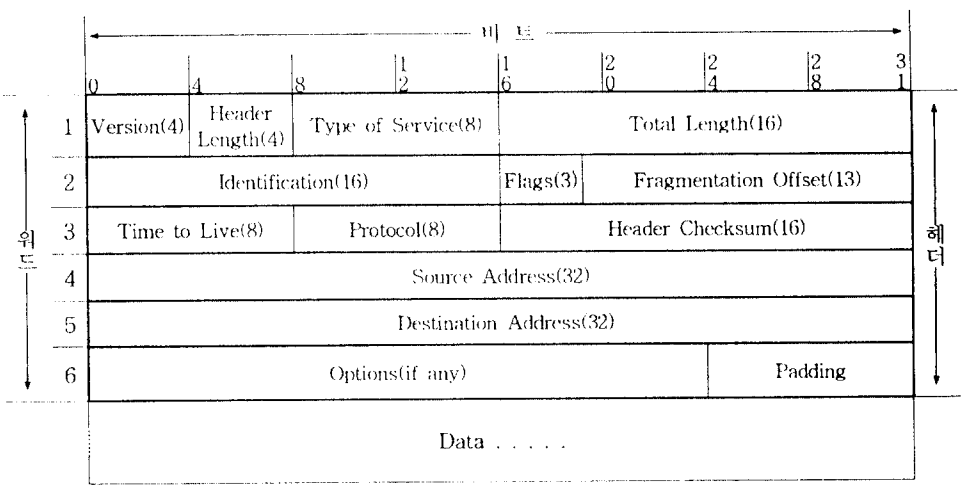
2.2 IP v6의 주소 체계

2.1 절에서 언급한 IPv4의 주소 체계의 문제점을 해결하기 위해 IPv6 주소는 IPv4 주소의 4배인 128 비트의 주소를 사용한다. IPv6의 주소 공간은 IPv4의 296배의 주소 공간을 더 갖는다. 즉 엄청나게 커다란 340,282,366,920,938,463,463,374,607,431,768,211,456개의 주소 공간을 갖으며, 이것은 이론적으로 지구의 표면적을 약 511,263,971,197,990㎡라고 하면 지구 표면 1㎡ 당 665,570,793,348,866,943,898,599개의 주소를 갖게 되는 것이다. IPv6의 주소 체계는 4.4절을 참조하라.

Ⅲ. 인터네트 프로토콜 버전 4 (IPv4 : Internet Protocol version 4)

3.1 IP 헤더(Header)

그림 4는 IP 데이터그램의 구조를 보여준다. 정상적인 IP 헤더의 길이는 선택 사항 필드가 없으면 20 바이트이다. 그림 4에서 최상위 비트(most significant bit)는 0으로 표시되어 있으며 최하위 비트(least significant bit)는 31로 표시되어 있다. 32비트로 된 4 바이트는 비트 0-7, 비트 8-15, 비트 16-23의 순서로 전송되며 마지막으로 비트 24-31이 전송된다. 이것을 Big endian 바이트 순서라고 하며 데이터그램이 네트워크를 통해 전송될 때 TCP/IP 헤더의 모든 이진 정보는 이 순서로 전달되기 때문에 네트워크 바이트 순



(그림 4) IP 데이터그램 구조

서(Network Byte Order)라고도 부른다.

3.1.1 버전 (VER)

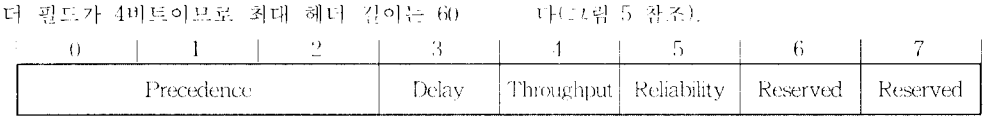
4비트의 길이로 인터네트 프로토콜의 버전을 표시한다. 현재의 인터네트 프로토콜의 버전은 4이다.

3.1.2 헤더 길이 (IHL)

선택 사항 필드를 포함한 32비트 워드 단위의 헤더의 길이로 4비트를 사용한다. 헤더의 최소 길이는 5이며 헤더 필드가 4비트이므로 최대 헤더 길이는 60 바이트(IHL = 15)를 넘지 못한다.

3.1.3 서비스의 유형(TOS)

데이터그램에 대한 원하는 서비스의 품질을 표시한다. 이 TOS 필드는 8비트의 길이로 상위 3비트는 우선 순위를 나타내고 그 다음 3비트는 TOS를, 그리고 하위 2비트는 장래 사용을 위해 예약되어 있다. 3 비트의 TOS는 각각 지연, 처리율 및 신뢰도를 나타낸다(그림 5 참조).



(그림 5) 서비스 필드

3.1.4 전체 길이(TL)

바이트 단위로 IP 데이터그램 헤더부와 데이터부를 포함한 데이터그램의 전체 길이를 나타낸다. 이 필드와 헤더 길이 필드(IHL)를 이용하여 IP 데이터그램에서 데이터의 시작 부분을 알 수 있으며 16비트 필드이므로 IP 데이터그램의 길이는 최대 65,535 바이트이다.

3.1.5 식별(ID)

16비트의 길이로 호스트가 전송한 데이터그램을 유일하게 식별하는데 사용된다. 송신자에 의해 할당된 이 ID 값을 이용하여 수신 측에서 데이터그램의 조각(fragment)을 재 결합한다. 일반적으로 이 필드의 값은 데이터그램이 전송될 때마다 1씩 증가한다.

3.1.6 플래그

3비트의 길이로 조각화(fragmentation)와 관련된 플래그를 설정한다(그림 6 참조).

0	1	2
0	DF	MF
예약, 반드시 0	DF=0 May Fragment DF=1 Don't Fragment	MF=0 Last Fragment MF=1 More Fragment

(그림 6) 플래그 필드

3.1.7 조각 오프셋(FO)

16비트의 길이로 이 필드는 데이터그램에서 조각이 속해 있는 위치를 표시한다. 이 조각 오프셋(Fragment Offset)은 8 옥텟의 단위로 측정되며 첫 번째 조각은 0으로 설정된다.

3.1.8 생존시간(TTL)

16비트 길이로 데이터그램이 경유하는 라우터의 최대 개수이다. 이 필드는 데이터그램이 인터네트에 남아 있을 수 있는 최대의 시간을 나타낸다. 이 필드의 값이 0으로 되면 데이터그램을 파괴되며 ICMP (Internet Control Message Protocol) 메시지가 파괴된 데이터그램의 송신자에게 전송된다. 이 필드는 데이터그램이 라우팅 루프(routing loops)에 빠지는 것을 막기 위한 것이다.

3.1.9 프로토콜(PROT)

어떤 프로토콜이 인터네트 프로토콜에게 데이터의 전송을 의뢰했는지를 식별한다. 이 필드는 8비트의 길이로 정확한 값은 RFC 1700 Assigned Numbers에 기술되어 있다.

3.1.10 헤더 검사합

IP 헤더에 대한 검사합으로 헤더 내의 모든 16비트 워드에 대한 1의 보수 합의 16비트 1의 보수를 취하여 검사합으로 사용한다.

3.1.11 발신지 주소(SOURCE)

32비트 길이의 발신지 주소

3.1.12 목적지 주소(DEST)

32비트 길이의 목적지 주소

3.1.13 선택 사항

이 필드는 가변 길이로 데이터그램에 포함되지 않을 수도 있다. 현재 정의된 선택 사항은 보안, 레코드 라우트, 시각 소인(Time Stamp), 여유 있는 발신지 경로 설정, 엄격한 발신지 경로 설정 등이 있다.

3.1.14 패딩

IP 헤더가 32비트 단위로 끝나도록 하기 위해 추가하는 가변 길이의 필드로 '0'의 값이 추가된다.

3.2 IPv4 라우팅

패킷 교환 시스템에서 라우팅은 패킷을 전송할 경로를 설정하는 과정이며 라우터는 이러한 기능을 하는 컴퓨터를 말한다. 개념적으로 IP 라우팅은 단순하다. 목적지가 PPP(point-to-point) 링크와 같이 직접 호스트에 연결되어 있거나 이더넷 혹은 토큰 링과 같이 매체를 공유하는 경우에는 IP 데이터그램을 직접 목적지로 전송한다. 그렇지 않으면 호스트는 데이터그램을 기본 라우터(default router)로 보내서 라우터가 데이터그램을 목적지로 보내도록 한다.

일반적으로 IP는 TCP, UDP, ICMP, 혹은 IGMP로부터 전송할 데이터그램을 받거나 혹은 네트워크 접속 계층으로부터 들어오는 데이터그램을 받는다. IP 계층은 메모리에 라우팅 표를 가지고 있어 전송할 데이터그램을 받을 때마다 이 표를 검색한다. 데이터그램이 네트워크 접속 계층으로부터 들어올 경우에는, IP는 먼저 목적지 주소가 자신의 IP 주소를 가리키는지를 검사한다. 만일 목적지 주소가 자신을 가리키면 IP 헤더의 프로토콜 필드에 지정된 프로토콜 모듈로 데이터그램을 전달한다. 만일 데이터그램의 목적지가 자신의 IP 주소가 아닌 경우에는 다음 두 가지 중의 한 가지로 동작한다: (1) 호스트가 라우터로 동작하도록 설정되었으면, 데이터그램을 다른 호스트나 라

우터로 전송하고, (2) 그렇지 않으면 데이터그램을 파괴한다.

라우팅 표는 다음과 같은 정보를 포함하고 있다:

- 목적지 IP 주소
- 다음 홉으로 연결된 라우터(next-hop router)의 주소 혹은 직접 연결된 네트워크의 주소
- 플래그 두개의 플래그가 있다. 하나의 플래그는 목적지 IP 주소가 네트워크의 주소인지 호스트의 주소인지를 식별하며, 다른 하나의 플래그는 다음 홉 연결 라우터 필드가 진짜 다음 홉으로 연결된 라우터인지 혹은 직접 연결된 인터페이스인지를 식별한다.
- 데이터그램을 전송할 네트워크 인터페이스의 종류

IP 라우팅은 hop-by-hop으로 이루어진다. 라우팅 표의 정보에서 보는 바와 같이 IP는 전송하는 호스트에 직접 연결된 경우를 제외하고는 목적지에 대한 완벽한 경로는 알지 못한다. IP 라우팅이 제공하는 것은 데이터그램이 전송 될 다음 홉 라우터의 주소가 전부이다.

IP 라우팅은 다음과 같은 동작을 수행한다[2]:

1. 목적지 주소와 정확하게 일치하는 항목을 라우팅 표에서 찾는다. 만일 일치하는 주소가 발견되면 패킷을 그 주소의 다음 홉 라우터 혹은 직접 연결된 인터페이스로 보낸다.
2. 목적지의 네트워크 ID와 일치하는 항목을 라우팅 표에서 찾는다. 만일 일치하는 항목이 발견되면 패킷을 그 주소의 다음 홉 라우터 혹은 직접 연결된 인터페이스로 보낸다.
3. 라우팅 표에서 "default"라는 표시가 붙은 항목을 찾는다. 만일 발견되면 그 항목이 지시하는 다음 라우터로 패킷을 전송한다.

만일 위의 단계에 해당하는 것이 없으면 해당 패킷을 전달할 수 없다. 전달 불가능한 데이터그램이 생성되면 "host unreachable" 혹은 "network unreachable"과 같은 오류 메시지를 데이터그램을 생성한 응용에 반환한다. 네트워크에 대한 라우트를 지정하는 기능 즉, 모든 호스트에 대한 라우트를 지정하지 않는 기능은 IP 라우팅의 중요한 특징이다. 이렇게 함으로써 라우팅 표에는 모든 호스트에 대하여 라우트를 등록하지 않아도 된다.

Ⅳ. 인터네트 프로토콜 버전 6 (Internet Protocol version 6: IPv6)

4.1 IPv6의 개요

인터네트 프로토콜 버전 6 (IPv6)는 인터네트 프로토콜 버전 4를 잇는 새로운 인터네트 프로토콜이다[6]. IPv6의 또 다른 이름은 IPng(Internet Protocol Next Generation)이며 여기에서도 IPv6와 동일한 의미로 사용한다.

IPv6는 IPv4를 자연스럽게 개선하는 방식을 취하고 있으며 간편한 소프트웨어 업그레이드로 설치될 수 있으며 현재 사용되고 있는 인터네트 프로토콜인 IPv4와 상호운용성이 있다. IPv6는 ATM과 같은 고속망에 적합하도록 설계되었으며, 동시에 무선망과 같은 대역폭이 작은 망에서도 효율적이도록 설계되었다. IPv6와 기존의 IPv4와의 주된 차이점은 다음과 같다[6]:

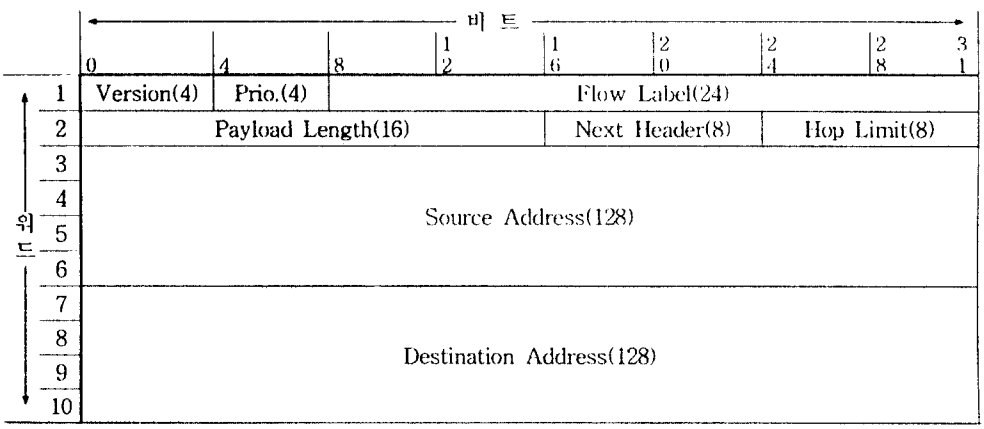
- 확장된 주소 지정 능력
  IPv6는 IP 주소를 IPv4의 32비트 길이에서 128비트로 늘려 다단계의 주소 계층화와 훨씬 많은 수의 노드의 지원, 간단한 주소 자동 설정을 지원하도록 하였다. 다중 전송 주소에 "scope"필드를 포함하여 다중 전송 라우팅의 확장성을 개선하였다. 또한 "Anycast address"라는 새로운 형태의 주소는 노드의 그룹에 속해 있는 어느 하나에게 패킷을 전송할 때 사용되도록 하였다. IPv6의 소스 라우트에서 이 Anycast 주소를 사용함으로써 노드는 트래픽이 흐르는 패스를 제어할 수 있다.
- 단순화된 헤더 구조
  IPv4의 헤더 필드 중 일부를 삭제하거나 선택 영역으로 변경하여 패킷 처리에 있어 공통적인 부분 처리를 간단히 하여 일반적인 패킷의 처리를 효율적으로 하며, 헤더가 차지하는 대역폭 비용을 줄일 수 있도록 하였다.
- 개선된 선택 사항과 확장 기능의 지원
  변경된 IP 헤더 선택 사항 처리 방법은 보다 효율적인 패킷의 포워딩을 가능하게 하며, 선택 사항 길이에 대한 한정을 완화하였으며, 새로운 선택 사항의 추가가 쉽게 이루어질 수 있는 구조로 만들어졌다.
- 흐름 표시(Flow Labelling) 기능
  기본이 아닌(non-default) 서비스 품질이나 혹은 실시간 서비스와 같이 송신자가 특별한 처리를 요구하는 특정한 트래픽 '흐름'에 속하는 패킷을 표시하는(labelling) 기능이 추가되었다.
- 인증 및 프라이버시 기능
  인증, 데이터 무결성 및 데이터 기밀성(선택 사

항)을 지원하는 기능이 IPv6에 추가되었다.

4.2 IPv6 헤더 구조

IPv6의 헤더는 40바이트의 길이로 그림 6과 같다. IPv6의 헤더는 IPv4에서와는 달리 헤더 구조를 단순화시킨 것이 특징이다.

- Version : 4 비트의 인터네트 프로토콜 버전 번호 = 6
- Prio. : 4 비트의 우선 순위 값
- Flow Label : 24 비트의 흐름 표시
- Payload Length : 16 비트의 음이 아닌 정수. 헤더에 실려 가는 데이터의 길이로 IPv6 헤더 다음의 패킷의 길이(옥텟 단위).
- Next Header : 8 비트의 선택자(selector). IPv6 헤더 바로 다음에 오는 헤더의 형태를 나타낸다. 사용되는 값은 IPv4 헤더의 프로토콜 필드의 값과 동일하다.
- Hop Limit : 8 비트의 음이 아닌 정수. 패킷을 포워딩하는 노드에 의해 1씩 줄어든다. 이 값이 0으로 줄어들면 패킷은 삭제된다.
- Source Address : 128 비트의 패킷을 처음 보낸 노드의 주소
- Destination Address : 128 비트의 패킷을 받도록 지정된 수신자의 주소(라우팅 헤더가 있으면 최종의 수신자가 아닐 수 있다.).



(그림 7) IPv6 헤더 구조

4.3 IPv6 확장 헤더의 구조

IPv6에서는 선택 사항인 인터네트 계층 정보가 IPv6 헤더와 상위 계층 헤더 사이에 올 수 있는 분리된 확장 헤더에 포함되어 전송된다. IPv6 패킷은 0 또는 그 이상의 확장 헤더를 가질 수 있으며 IPv6 헤더의 Next Header 필드에 표시된다. 한가지 예외를 제외하고 확장 헤더는 IPv6 헤더의 목적지 주소 필드에 표시된 노드에 도착하기 전에는 패킷의 전송 경로에 있는 노드가 검사하거나 처리하지 않는다. IPv6 헤더의 Next Header 필드에 대해 정상적인 디멀티플렉싱을하여 첫 번째 확장 헤더를 처리할 모듈을 호출하거나 확장 헤더가 없는 경우에는 상위 계층 헤더를 처리하는 모듈을 호출한다. 각 확장 헤더의 내용과 의미에 따라 다음 헤더를 처리할지의 여부가 결정된다. 그러므로 확장 헤더는 패킷에 나온 순서대로 반드시 처리되어야 한다.

Hop-by-hop 선택 사항 헤더는 최초 송신 노드 및 최종 수신 노드를 포함하여 패킷의 전송 경로 상에 있는 각 노드가 검사하여 처리해야 한다. Hop-by-hop 선택 사항 헤더가 있는 경우에는 반드시 IPv6 헤더 다음에 와야 한다. 각 확장 헤더는 연속된 헤더들의 8 옥텟 정렬을 하기 위해 8 옥텟의 정수 배수이다. 각 확장 헤더의 다중 옥텟 필드 또한 이를 감안하여 구성되어야 한다. IPv6의 완전히 구현은 다음과 같은 확장 헤더의 구현을 포함한다:

- Hop-by-hop Options 헤더
  hop by hop 처리를 위해 필요한 특별한 선택 사항
- Routing 헤더
  확장 라우팅을 위한 정보
- Fragment 헤더

조각화 및 재결합을 위한 정보
- Destination Options 헤더
  목적지 노드에서 검사될 선택적인 정보
- Authentication 헤더
  무결성, 인증, 및 보안에 관련 정보
- Encapsulating Security Payload 헤더
  기밀성에 관한 정보

동일한 패킷에 하나 이상의 확장 헤더가 사용되면 확장 헤더는 다음의 순서를 따르도록 권고된다[6]:
- IPv6 헤더
- Hop-by-hop Options 헤더
- Destination Options 헤더
  IPv6 목적지 주소 필드에 나타난 첫 번째 목적지 및 라우팅 헤더에 기록된 중간 목적지에서 처리될 선택 사항
- Routing 헤더
- Fragment 헤더
- Authentication 헤더
- Encapsulating Security Payload 헤더
- Destination Options 헤더
  패킷의 최종 목적지에서만 처리되어야 할 선택 사항
- Upper-Layer 헤더

각 확장 헤더는 Destination Options 헤더를 제외하고는 많아야 한 번 나와야 한다. Destination Options 헤더는 한 번은 Routing 헤더 앞에 한 번은 Upper-Layer 헤더 앞에 많아야 두번 나올 수 있다.

4.4 IPv6 주소

IPv6의 주소는 인터페이스 또는 인터페이스의 집합을 위한 128 비트 길이의 식별자이다. IPv6에는 Unicast, Anycast, 그리고 Multicast 등 세 종류의 주소가 있다[7].

- Unicast : 하나의 인터페이스를 위한 식별자. Unicast 주소로 전송된 패킷은 그 주소로 식별되는 인터페이스로 전달된다.
- Anycast : 인터페이스의 집합(일반적으로 인터페이스들은 각기 다른 노드들에 속함)을 위한 식별자. Anycast 주소로 전송된 패킷은 그 주소로 식별되는 여러 인터페이스 중 (라우팅 프로토콜에 따른 가장 가까운) 한 인터페이스로 전달된다.
- Multicast : 인터페이스의 집합(일반적으로 인터페이스들은 각기 다른 노드들에 속함)을 위한 식별자. Multicast 주소로 전송된 패킷은 그 주소로 식별되는 모든 인터페이스로 전달된다.

IPv6에는 방송용 주소가 없으며, 이 기능은 Multicast 주소로 대체되었다.

4.4.1 주소 지정 모델

IPv6의 모든 주소는 노드가 아니라 인터페이스에 할당된다. 각각의 인터페이스는 하나의 노드에 속하므로, 노드의 인터페이스의 Unicast 주소는 그 노드의 식별자로 사용될 수 있을 것이다. IPv6의 Unicast 주소는 하나의 인터페이스를 의미한다. 하나의 인터페이스에는 여러 개의 IPv6 주소(Unicast, Anycast, Multicast)가 할당될 수 있다. 이 모델에는 두 가지 예외가 있다[7].

- 구현이 여러 개의 물리 인터페이스를 인터네트 계층을 대표하는 하나의 인터페이스로 취급하는 경우에 하나의 주소가 여러 개의 물리 인터페이스에 할당될 수 있다. 이것은 여러 개의 물리 인터페이스에 대해 부하 분산을 위해 유용하다.
- 수동으로 주소를 설정하고 선전하지 않도록 하기 위해 종단대종단 링크상에서 라우터는 IPv6 주소가 할당되지 않은 인터페이스를 가질 수 있다. IPv6 데이터그램의 최초 송신자나 최종 목적지로 사용되지 않으면 라우터상의 종단대종단 링크에 대한 주소는 필요가 없다.

IPv6는 부속망(subnet)이 하나의 링크와 연계되어 있는 IPv4 모델을 계속 따르고 있으며, 여러개의 부속망이 동일한 링크에 할당될 수도 있다.

4.4.2 주소의 문자 표현

IPv6 주소를 문자열로 표시하는 3가지 방법이 있다[7].

- X:X:X:X:X:X:X:X -- 가장 선호되는 형태로 X는 16진수로 된 8개의 16비트 값.
  예)FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
  1080:0:0:0:0:8:800:200C:417C
- 연속된 0을 표시하는 "::" -- "::"는 0 값을 가지는 연속된 16비트를 표시.
  "::"는 주소에서 단 한 번만 나온다.
  예)1080:0:0:0:8:800:200C:417A --)1080::8:800:200C:417A
  0:0:0:0:0:0:0:1 --) ::1
- X:X:X:X:X:X:D.D.D.D -- "X"는 16진수로 된 상위 6개의 16진수 값.
  "D"는 10진수로 된 하위 4개의 8비트 값
  예) 0:0:0:0:0:0:13.1.1.68.3 --) ::13.1.1.68.3
  0:0:0:0:0:FFFF:129.144.52.38 --) ::FFFF:129.144.52.38

4.4.3 주소 형식 표현

IPv6 주소의 특정 형식은 주소의 몇 개의 앞 머리 비트(leading bits) 값으로 결정된다. 이 앞 머리 비트를 구성하는 가변 길이의 필드를 FP(Format Prefix)라고 하며 현재 이 FP의 할당은 그림8과 같다.

Allocation	Prefix (이진수)	Fraction of Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider-Based Unicast Address	010	1/8
Unassigned	011	1/8
Reserved for Geographic-Based Unicast Addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

(그림 8) IPv6의 주소 종류별 주소 공간 할당 내용

그림 8의 주소 할당은 서비스 제공자를 위한 주소, 국부 사용 주소 및 다중 전송 주소의 직접 할당을 지원하기 위한 것이다. NSAP 주소, IPX 주소 및 지리 주소를 위한 주소 공간이 미리 할당되었다. 현재는 전체 주소 공간 중 15%만이 할당되었고 장래에 사용하기 위해 85%는 예약되어있다.

Unicast 주소는 상위 옥텟의 값으로 FF(11111111)를 갖는 Multicast 주소와 구별된다. 상위 옥텟의 값으로 FF이외의 값을 갖는 주소는 Unicast 주소이며, Anycast 주소는 Unicast 주소 공간의 일부를 사용하며 구문적으로 구분되지는 않는다.

4.4.4 Unicast 주소

IPv6에서는 여러 형태의 Unicast 주소 할당 영역이 존재한다. 여기에는 서비스 제공자 기반 Unicast 주소, 지리 기반 Unicast 주소, NSAP 주소, IPX 계층 주소, 사이트 지역 사용 주소, 링크 지역 사용 주소, 그리고 IPv4 지원 호스트 주소 등이 있다. 물론 앞으로도 새로운 형태의 주소를 추가할 수 있다.

- Unspecified 주소
  주소 0:0:0:0:0:0:0:0을 말하며 어느 노드에도 할당되지 않는다.
- Loopback 주소
  0:0:0:0:0:0:0:1을 루프백 주소라고 부르며 노드가 자신에게 IPv6 데이터그램을 전송할 때 사용될 수 있다.
- IPv4가 주소가 내장된 IPv6 주소
  - IPv4-compatible IPv6 주소 : 하위 32비트에 IPv4 주소를 갖는 IPv6 주소로 터널링에 사용된다.
  - IPv4-mapped IPv6 주소 : IPv6를 지원하지 않는 IPv4 노드만을 위한 주소
- NSAP 주소 : NSAP 주소를 IPv6 주소로 매핑
- IPX 주소 : IPX 주소를 IPv6 주소로 매핑

- 서비스 제공자 기반 Unicast 주소 : 글로벌 서비스 제공자를 위한 주소
- Local-Use IPv6 Unicast 주소
  - Link-Local : 단 하나의 링크를 위한 주소. 자동 주소 설정, 이웃 노드 발견 및 라우터가 없을 경우에 사용된다.
  - Site-Local : 단 하나의 사이트를 위한 주소. 글로벌 인터네트에 연결되지 않는 사이트나 조직에서 사용된다.

4.4.5 Anycast 주소

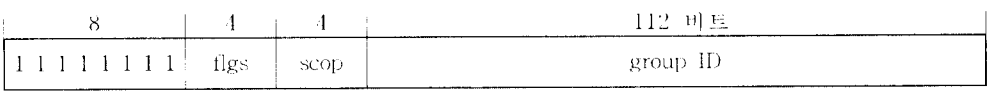
인터페이스의 집합(일반적으로 인터페이스들은 각기 다른 노드들에 속함)을 위한 식별자. Anycast 주소로 전송된 패킷은 그 주소로 식별되는 여러 인터페이스 중 (라우팅 프로토콜에 따른 가장 가까운) 한 인터페이스로 전달된다.

Anycast 주소는 Unicast 주소 공간의 일부를 사용하며 구분적으로 Unicast 주소와 구분되지는 않는다. Unicast 주소가 하나 이상의 인터페이스에 할당되면, 이 주소는 Anycast 주소로 된다. IPv6 Anycast 주소에는 다음과 같은 제약이 가해진다:

- Anycast 주소는 IPv6 패킷의 최초 송신지(Source) 주소로 사용되어서는 안된다.
- Anycast 주소는 IPv6 호스트 주소로 할당되어서는 안된다. 즉 IPv6 라우터에만 할당될 수 있다.

4.4.6 Multicast 주소

다중 전송(Multicast) 주소는 노드의 그룹에 대한 식별자이다. 한 노드는 여러 개의 다중 전송 그룹에 속할 수 있다. 다중 전송 주소의 상위 8비트는 반드시 '11111111'로 시작된다(그림 9).



- 11111111 : 다중 전송 주소임을 표시
- flgs : flags
- scop : 4 비트의 다중 전송 범위 값

(그림 9) 다중 전송 주소 구조

4.5 IPv6 라우팅

IPv6의 라우팅은 32비트 IPv4 주소 대신 128비트 IPv6 주소를 사용하는 점을 제외하고는 CIDR(Classless Inter-Domain Routing)하의 IPv4 라우팅과 거의 동일하다. IPv4의 라우팅 알고리즘(OSPF, RIP, IDRP, ISID 등)을 약간 확장하여 IPv6 라우팅에 사용할 수 있다. IPv6 라우팅은 또한 강력한 새로운 라우팅 기능, 즉 주소 순서(address sequence)를 지원하는 라우팅 확장을 포함한다. 이 확장된 기능은 다음과 같다:

- 서비스 제공자 선정(정책, 성능, 비용 등을 바탕으로)
- 호스트의 이동성 지원(플러그엔 플레이)
- 자동 재 주소 설정(리버스 주소 순서)

새로운 라우팅 기능은 IPv4 라우팅 선택 사항을 사용하여 IPv6 주소 순서(sequences)를 만들어 가능하게 된다. 라우팅 선택 사항은 IPv4 소스가 패킷의 최종 목적지로 가는 도중에 거칠 하나 이상의 중간 노드를 나열하기 위해 사용된다. 이 기능은 IPv4의 Loose Source and Record Route 선택 사항의 기능과 매우 유사하다.

주소 순서를 일반적인 기능이 되도록 하기 위해, 대부분의 경우에 IPv6 호스트는 수신하는 패킷의 전송자에게 패킷을 반환하기 위해 필요한 주소 순서를 포함하는 리버스 라우트를 필요로 한다. 이 방법은 IPv6 호스트 구현이 처음부터 소스 라우트의 처리와 반환을 지원하게 했다. 이 것은 서비스 제공자 선정 혹은 확장 주소와 같은 새로운 기능을 구현하는 호스트가 동작하도록 하는 핵심 기능이다.

4.6 IPv6 보안

오늘날의 IPv4는 한 두 가지의 보안 문제를 가지고 있다. 기본적으로 응용 계층 아래에서는 프라이버시 및 인증 기능이 없다. 이 문제를 해결하기 위해 IPv6는 2개의 보안 관련 선택 사항을 제공한다.

- IPv6 인증 헤더

  이 헤더는 인증(authentication) 및 무결성(integrity)은 제공하나 기밀성(confidentiality)은 제공하지 않는다. 이 헤더는 알고리즘에 따라 다르며 나양한 인증 기법을 지원할 것이다. 전 세계의 인터네트와 상호 운용이 될 수 있도록 MD5

를 사용하도록 제안되었다.

- IPv6 캡슐화 보안 헤더
  이 헤더는 IPv6 인증 헤더에는 없는 무결성 및 기밀성을 제공한다. 이 헤더 또한 알고리즘에 따라 달라질 수 있다. 전 세계의 인터네트와 상호 운용이 될 수 있도록 DES-CBC가 표준 알고리즘으로 사용되고 있다.

Ⅴ. IPv4에서 IPv6로의 전이 방안

IPv4에서 IPv6로 전이하는 데 있어서 가장 큰 문제는 기존의 IPv4 네트워크의 운영에 영향을 미치지 않고 전체 인터네트가 IPv6를 사용하게 하는 것이다. 수립된 전이방안은 2단계로 첫 단계에서는 IPv4 및 IPv6의 호스트 및 라우터가 혼재하는 단계이며, 두 번째 단계는 IPv6 의 호스트와 라우터만이 사용되는 것이다. 단순 IPv6 전이(Simple IPv6 Transition : SIT)는 적어도 다음과 같은 점을 지원하여야 한다:

- IPv6와 IPv4 호스트는 상호운용이 가능하다.
- IPv6 라우터와 호스트는 인터네트에 상호 의존적으로 배치된다.
- 최종 사용자, 시스템 관리자 및 네트워크 운영자가 전이를 이해하고 실행하기에 가능한한 쉬워야 한다.

IPv6 전이는 다음과 같은 특징을 제공한다:

- Incremental upgrade
  IPv4가 설치된 기존의 호스트나 라우터는 다른 호스트 및 라우터의 전이와는 관계없이 언제든지 IPv6로 전이할 수 있어야 한다.
- Incremental Deployment
  새로운 IPv6는 언제든지 전제조건 없이 설치 가능해야 한다.
- 쉬운 주소 지정
  IPv4가 설치된 기존의 호스트나 라우터가 IPv6으로 전이될 때 기존의 주소를 그대로 사용할 수 있어야 한다.
- 최소의 전이 의존성
  IPv6로 호스트를 전이할 때의 유일한 전제조건은 DNS 서버가 IPv6 주소 레코드를 처리할 수 있도록 먼저 전이하는 것뿐이다.
- 적은 시작 비용
  기존의 IPv4 시스템을 IPv6로 전이하거나 새로 설치하기 위해 필요한 준비 작업은 거의 없어야 한다.

위와 같은 전이의 특징을 실현하기 위해 다음과 같은 전이 기법이 사용된다:

- 이중 IP 계층(IPv4 와 IPv6)의 사용
- IPv6 주소에 IPv4 주소를 내장하는 두 개의 IPv6 주소 지정 구조
- IPv4 라우팅 하부 구조 상에 IPv6 패킷의 터널링 기법
- IPv4 패킷 헤더를 IPv6 패킷 헤더로 IPv6 패킷 헤더를 IPv4 패킷 헤더로 번역하는 기법

Ⅵ. 결 론

본 고에서는 TCP/IP 프로토콜 스위트에서 인터네트 계층을 차지하고 있는 인터네트 프로토콜과 주소 체계를 다루었다. 현재 사용되고 있는 인터네트 프로토콜은 버전 4로 32비트 주소 체계를 사용하고 있다. 그러나 인터네트의 사용자의 폭발적인 증가로 인하여 주소 공간의 부족과 라우팅 테이블의 항목이 증가하여 라우팅이 어려워지는 문제점이 대두되었다. 또한 멀티미디어와 영상 회의와 같은 새로운 응용이 대두됨에 따라 새로운 기능의 인터네트 프로토콜이 필요하게 되었다.

이 문제를 해결하기 위해 IETF의 IPng Working Group에서는 차세대 인터네트 프로토콜인 버전6을 개발하기에 이르렀다. IPv6는 128비트의 주소를 사용하며, IP 헤더 구조를 단순화시켰으며, 흐름 제어 기능, 그리고 인증 및 프라이버시 기능을 추가하였다. 현재 IPv6와 관련된 기본 명세는 확정되어 제안 표준(proposed standard)의 상태에 있으나, 보안 기술 라우팅 문제 및 IPv4에서 IPv6로의 전환 문제 등은 계속 연구되고 있다.

충분한 주소 공간의 확보, 효율적인 라우팅, 영상 회의 및 멀티미디어 응용에 필수적인 다중 전송 및 실시간 서비스의 지원, 호스트의 이동성 지원, 그리고 인증 및 보안을 지원하는 차세대 인터네트 프로토콜인 IPv6는 초고속정보통신망의 구축 시점에서 중요한 핵심 기술이다. 초고속정보통신망의 성공적인 구축과 초고속정보통신망에 필요한 고속의 멀티미디어 응용 기술을 확보하기 위해서는 국내의 연구 개발자도 IETF의 활동에 적극적으로 참여하여야 할 것이다.

참 고 문 헌

1. Craig Hunt, TCP/IP Network Administration, O'Reilly & Associates, 1992
2. W. Richard Stevens, TCP/IP Illustrated Vol.1 : The Protocols, Addison-Wesley, 1994
3. Douglas E. Comer, Internetworking with TCP/IP Vol. 1 : Principles, Protocols, and Architecture, Prentice Hall, 1991
4. RFC 791, J. Postel, "Internet Protocol", 09/01/1981
5. RFC 1752, S. Bradner, A. Mankin, "The Recommendation for the IP Next Generation Protocol", 01/18/1995
6. RFC 1883, S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", 01/04/1996
7. RFC 1884, R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", 01/04/1996
8. RFC 1885, A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)", 01/04/1996
9. RFC 1886, S. Thomson, C. Huitema, "DNS Extensions to support IP version 6", 01/04/1996
10. RFC 1887, Y. Rekhter, T. Li, "An Architecture for IPv6 Unicast Address Allocation", 01/04/1996
11. 최문실, 신현상, 송관호, "국내 Internet의 현황과 전망," 정보처리 제2권 제2호(1995. 6), 한국정보처리학회
12. 한국전산원, 초고속정보통신망을 위한 인터넷 프로토콜 연구, NCA V-RER-95119, 1995. 12
13. KIS 12, 인터네트 규약(IP) 표준, 정보통신부, 1993

김 형 기

- 1993년 2월 : 한양대학교 대학원 전자계산학과(석사)
- 1993년 1월 - 현재 : 한국전산원 표준본부 연구원

관심분야 : Internet, 망 관리, 네트워크 보안, 고속 통신 프로토콜

송 관 호

- 서울대학교 전자공학과(학사)
- 한양대학교 대학원 전자공학과(석사)
- 광운대학교 대학원 전자공학과(박사)
- 1979년 - 1984년 금성전선(주) 정보시스템 과장
- 1984년 - 1987년 대이콤 미래연구실장
- 1987년 - 1992년 한국전산원 정보통신표준부장
- 1992년 - 1994년 한국전산원 시스템기술부장
- 1995년 1월 - 1995년 12월 한국전산원 초고속사업단 국가망구축실장
- 1996년 1월 - 현재 한국전산원 표준본부 본부장
- 1987년 - 1993년 공진청 JTC1 표준화 위원
- 1987년 - 1994년 체신부 전기통신 형식승인 위원
- 1994년 - 현재 공보처 해외정보망 자문위원
- 1995년 - 현재 서울시방범촬영 정보범죄센터 자문위원
- 1987년 - 현재 개방형컴퓨터통신연구회 홍보이사
- 1995년 - 현재 한국정보과학회 이사

관심분야 : 초고속통신망, 멀티미디어, 통신프로토콜, 분산시스템 등