컴퓨터 네트워크

김 화 종

1. 인터넷

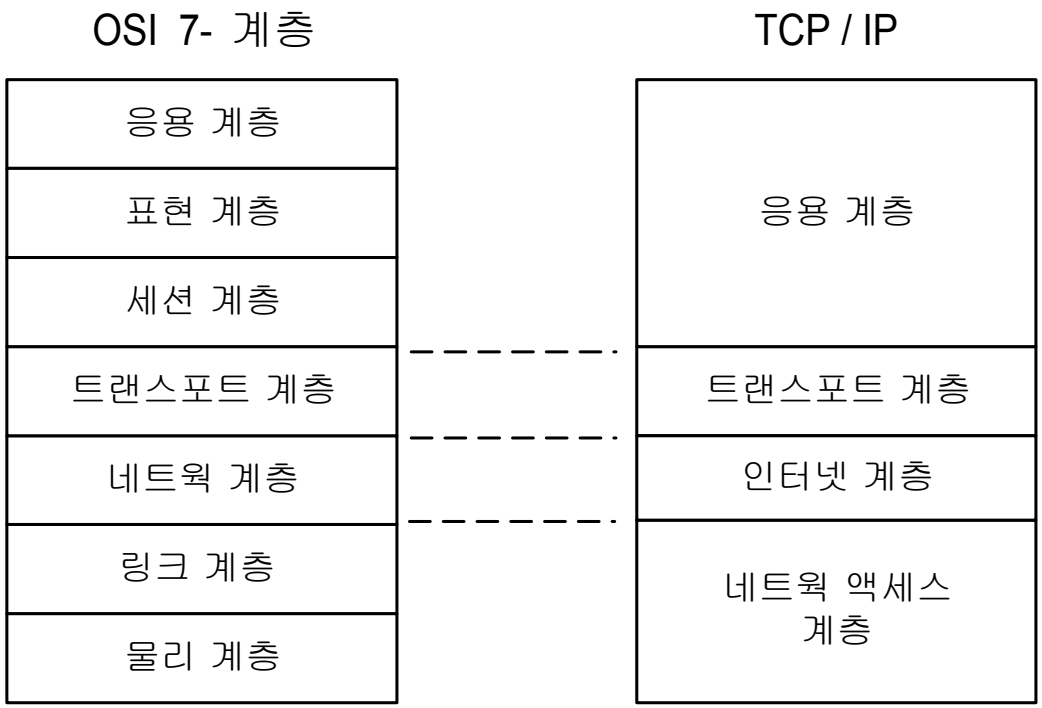
- 인터넷 동작의 기본이 되는 TCP/IP 프로토콜의 주요 기능을 설명한다.

TCP/IP

- 인터넷은 전 세계 컴퓨터들을 연결하고 있으며 통신 프로토콜로 TCP/IP를 사용한다.
- TCP/IP와 관련된 표준은 RFC(Request For Comments) 라는 이름의 문서로 제공되는데 자세한 내용은 아래의 주소에서 얻을 수 있다.
- http://www.ietf.org/

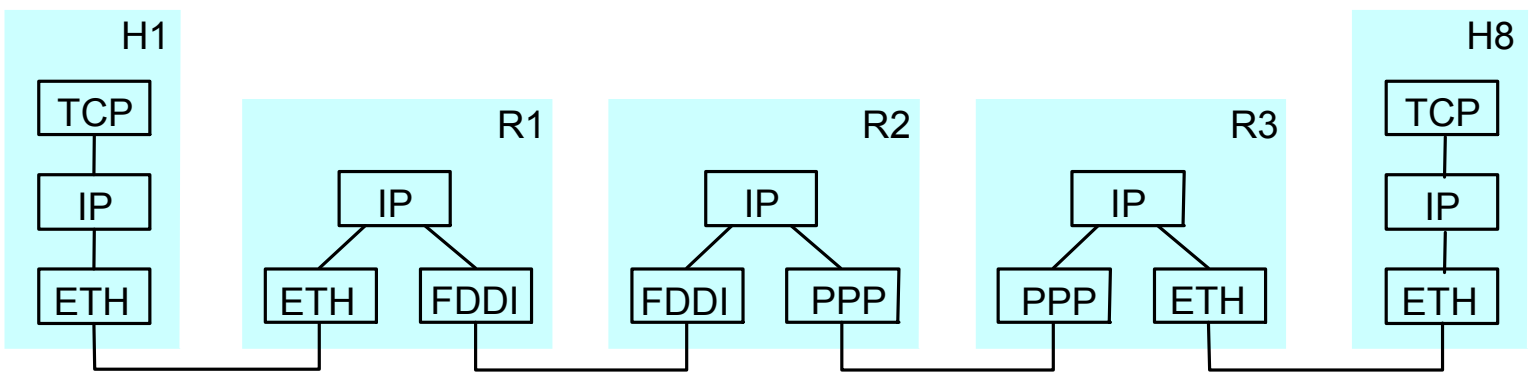
TCP/IP 프로토콜 개요

- 미국 국방성에서 1968년에 컴퓨터들간의 통신이 가능하도록 컴퓨터 통신 프로토콜을 만들었으며 이 때 TCP/IP가 만들어졌다.
- TCP/IP의 기본 프로토콜은 TCP(Transmission Control Protocol)와 IP(Internet Protocol)이며 이들은 각각 OSI 계층 4와 계층 3의 기능을 수행한다.
- 인터넷은 TCP와 IP 뿐 아니라, 네트워크 액세스 계층, 응용 계층 등 4개의 계층으로 구성되어 있으며 이를 OSI 7 계층과 비교하면 다음 그림과 같다.

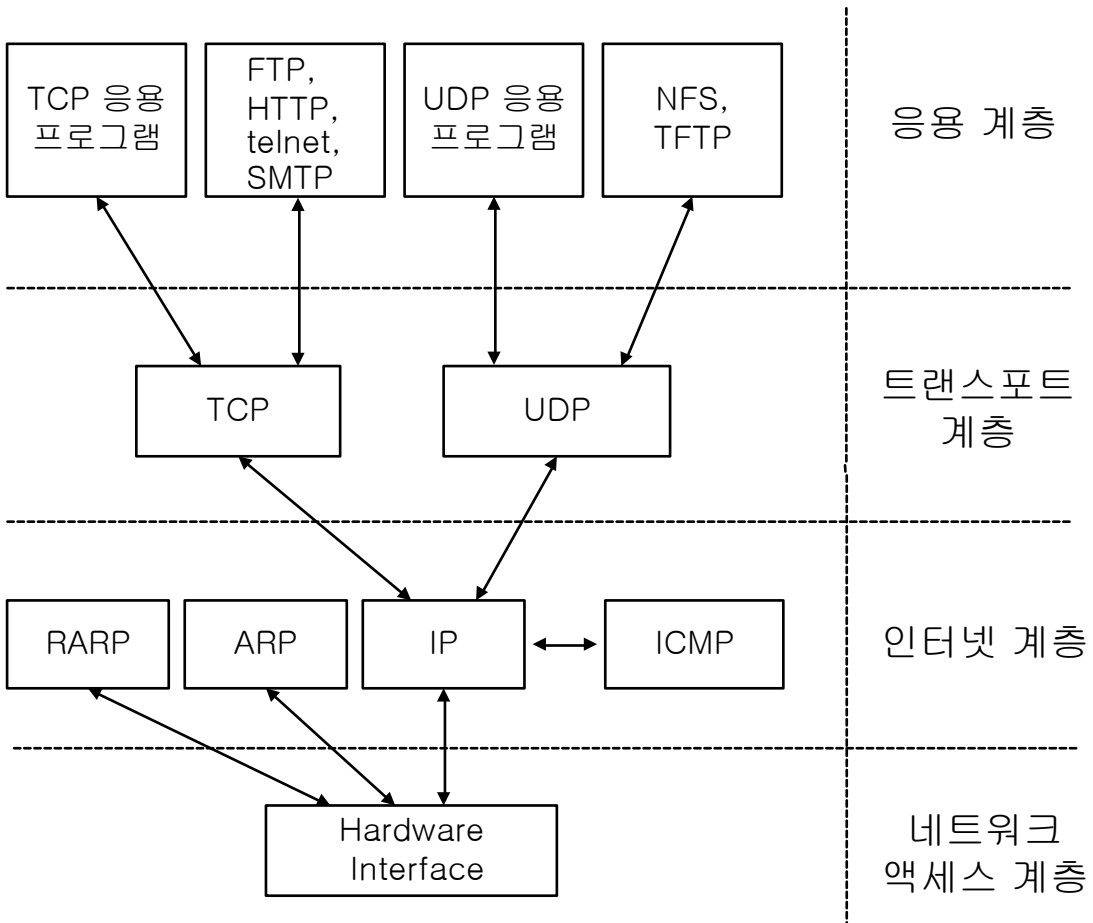


TCP/IP와 OSI 7-계층 프로토콜 구조의 비교

- TCP/IP의 동작을 아래에 나타냈는데 호스트 H1이 호스트 H8로 패킷을 전달하기 위해서 세 개의 라우터 R1, R2, R3를 경유하는 경우를 나타냈다.
- IP 패킷은 이더넷, PPP, FDDI 등의 랜이나 서브네트워크를 경유하여 목적지로 전달되며 각 네트워크의 경계에 있는 라우터에서는 모두 IP 프로토콜을 구현하고 있어야 한다.



TCP/IP 프로토콜 스택



- TCP/IP 프로토콜 모음(suite)에는 TCP와 IP 외에도 UDP(User Datagram Protocol), ICMP(Internet Control Message Protocol), IGMP(Internet Group Message Protocol), ARP(Address Resolution Protocol), RARP(Reverse ARP) 등 관련된 프로토콜이 포함된다.
- 네트워크 액세스 계층은 IP 패킷의 물리적인 전달을 담당하는데 전용선(PPP), LAN 등이 이 계층에 해당된다
- 네트워크 액세스 계층의 구체적인 내용이 TCP/IP 표준에 포함되어 있지는 않다.
- 인터넷 계층의 핵심 기능은 호스트 사이에 IP 패킷을 전달하는 기능과 라우팅 등을 수행하며 이를 위해서 4바이트의 IP 주소를 사용한다.

- 트랜스포트 계층은 호스트 사이의 종점간 연결관리와 흐름제어 등을 처리한다.
- 트랜스포트 계층 프로토콜에는 TCP와 UDP 두 개의 프로토콜이 있다.‘
- TCP는 신뢰성 있는, 즉 재전송에 의한 오류제어와 흐름제어를 하는 스트림(stream) 형태의 연결형 서비스를 제공하며, UDP는 재전송이나 흐름제어가 없는 비연결형 서비스를 제공한다.
- 응용 계층은 TCP/IP 프로토콜을 이용하는 응용 프로그램으로, TCP 또는 UDP를 사용하는 응용으로 각각 구분할 수 있다.

- 아래에 TCP, UDP, 그리고 TCP와 UDP가 동시에 지원하는 대표적인 응용 계층 서비스를 나타냈다(유닉스의 경우 /etc/services 파일 참조).

트랜스포트 프로토콜	응용 계층 서비스
TCP	- File Transfer Protocol(FTP), Telnet - Simple Mail Transfer Protocol(SMTP) - HyperText Transport protocol(HTTP)
TCP, UDP	- Network File System(NFS) - Domain Name System(DNS)
UDP	- Trivial FTP(TFTP)

2. IP 프로토콜

인터넷 계층

- 인터넷 계층은 인터넷 프로토콜(IP)을 수행하는 계층으로 하위(sub) 네트워크에 무관하게 IP 패킷을 호스트(컴퓨터) 사이에 전달하는 기능을 수행한다.
- OSI 7 계층 관점에서 보면 인터넷 계층은 주소(addressing)와 교환(switching) 그리고 라우팅을 담당한다.
- IP는 비연결형 서비스로 동작한다. 따라서 IP에서는 각 패킷이 개별적으로 목적지를 찾아갈 수 있어야 하므로 IP 패킷은 송신지와 수신지의 주소로서 각각 32비트의 IP 주소를 항상 포함하고 있어야 한다.

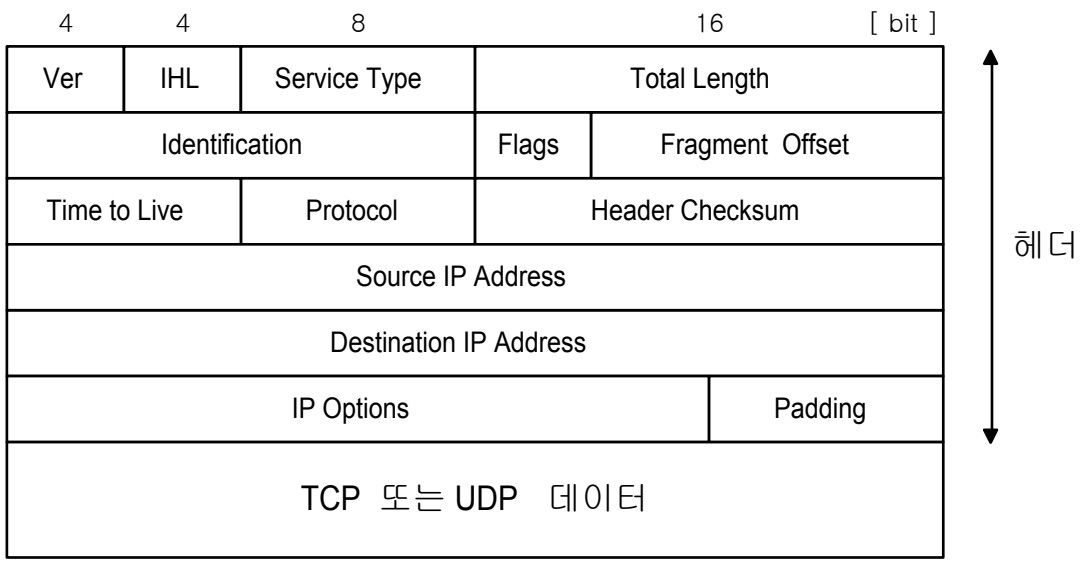
- 비연결형(connectless) 서비스란 연결설정과 종료과정이 따로 없이, 바로 데이터를 송수시하는 통신 방법을 말한다.
- 연결설정과 종료과정이 항상 필요한 통신 방식은 연결형(connection-oriented) 서비스라고 한다.
- IP 프로토콜의 핵심은 바로 이 32비트의 IP 주소(이를 인터넷 주소라고도 한다)의 사용인데, IP 주소는 인터넷에 접속된 모든 호스트에 대하여 전세계적으로 유일하게 배정되는 주소이다.

best effort

- IP는 “best effort로 패킷을 전달” 하는데 이것의 의미는 IP는 비연결형으로 패킷을 전달하며 패킷의 분실, 중복 패킷 전달, 패킷 전달 순서의 바뀜, 비트 오류 등이 발생하더라도 IP에서 패킷 재전송이나 오류 확인 등의 기능을 제공하지 않는다는 것을 뜻한다.
- 즉, IP 계층은 최대한 잘 전달하려고 노력만 할 뿐 전송 결과를 패킷 단위로 확인해주지 않는다.
- 두 호스트 사이에 패킷이 잘 전달되는지의 확인은 상위 계층인 트랜스포트 계층(TCP 또는 UDP)에서 처리된다.

IP 패킷 구조

- IP 계층에서 다루는 프로토콜 데이터 단위(PDU)인 IP 패킷의 구조는 다음과 같다.



- 앞의 그림에서 한 줄(row)은 4바이트(32비트) 크기이며 네트워크로 전송될 때에는 상위의 좌측 바이트부터 전송된다.
- 송신지와 수신지를 나타내는 IP 주소는 각각 네 번째와 다섯 번째 줄에 들어가며 상위 계층의 사용자 메시지는 헤더 뒤에 전송된다.
- Ver(Version)은 IP 프로토콜의 버전을 표시하는데 현재는 4이다(따라서 현재 사용중인 인터넷 버전을 IPv4라고도 표현한다.).
- IHL(Internet Header Length)은 헤더 길이를 4바이트 단위로 표시하는데 디폴트 값은 5이다(즉, 헤더의 기본 크기는 20바이트가 된다).
- 서비스 타입은 응용에 따라 이 IP 패킷이 각각 다르게 처리되기를 지정하는 필드이다.

- Total Length는 헤더를 포함한 IP 패킷의 전체 크기를 바이트 단위로 나타내는데 Total Length가 16비트 크기이므로 IP 패킷의 최대길이는 65535 바이트까지 표현할 수 있다.
- Identification은 수신측에서 패킷을 재조립할 때 사용하는 고유 번호이다.
- Flags는 세 비트로 구성되는데, 첫 비트는 사용하지 않으며 항상 0이어야 한다. 두 번째 비트는 세분화 금지 플래그 DF이고 세 번째 비트는 More 비트인데 이들의 사용은 뒤에서 설명하겠다.

필 드 명		길이(비트)	기 능
Ver(Version)		4	IP 버전 값을표시(현재는 4임)
IHL		4	4바이트 단위로 헤더길이를 표시(최소값은 5)
Service Type		8	서비스 클래스 지정(보통 0으로 지정)
Total Length		16	IP 패킷 크기(바이트 단위이며 최대값은 65535)
Identification		16	패킷을 유일하게 구분할 필요가 있을 때 사용하는 번호
Flags	미사용	1	미사용(항상0)
	DF	1	세분화 금지 플래그(0: 허용, 1: 금지)
	More	1	More 비트(0: 마지막 패킷, 1: 연속되는 패킷)
Fragment Offset		13	전체 메시지 중 이 패킷의 위치를 표시(8바이트 단위)
TTL(Time To Live)		8	패킷이 통신망 내에서 계속 돌아다니는 것을 방지하기 위하여 사용되며 보통 hop counter 값을 사용한다
Protocol		8	데이터를 전달할 상위 계층 프로토콜을 지정 (1: ICMP, 6: TCP, 17:UDP)
Header Checksum		16	헤더 부분의 오류 검출
Source IP Address		32	송신지 IP 주소
Destination IP Address		32	수신지 IP 주소
IP Options		가변	옵션 선택(보통 사용하지 않는다)
Padding		가변	32비트 단위로 헤더의 길이를 맞춤(보통 사용하지 않는다)

- TTL(Time To Live)은 패킷이 어떤 오류에 의해서 제대로 목적지에 전달되지 못하고 인터넷 내에서 계속 돌아다니는 것을 방지하기 위해서 패킷이 일정시간 동안만 인터넷상에서 전달되도록 제한하려고 정의한 것이다.
- 즉, 중간의 라우터들은 이 TTL 시간 동안만 이 패킷의 전달을 처리해주며 TTL 값은 시간이 지나면서 값이 감소하다가 0이 되면 전달을 중지한다.
- 그러나 인터넷 전체를 통해 동일한 시계를 운영하는 것이 불편하므로 TTL은 실제로는 시간 대신 hop counter 값으로 사용되고 있다(hop이란 패킷이 링크를 통해 노드를 하나 지나가는 것을 말한다).
- 즉, TTL 값은 패킷이 한 노드를 지나갈 때마다 1씩 감소하고 TTL이 0이 되는 노드에서 이 패킷을 제거함으로써 이 패킷이 더 이상 인터넷상에서

돌아다니지 않도록 한다.

- TTL의 초기 값을 어떻게 정해줄지를 정해야 하는데 이것은 목적지까지 패킷이 전달될 동안 거치게 될 총 라우터의 수보다 조금 크게 잡아주면 된다.

- TTL 값이 너무 크면 오류가 발생한 경우에 패킷이 네트워크 내에 오래 남아 있게 되어 트래픽이 증가할 수 있고, TTL 값이 너무 적으면 라우팅이 달라져서 패킷이 먼 거리를 돌아가게 되었을 때 목적지에 도착하지 못할 수가 있다.

- 실제로는 TTL 값을 매 IP 패킷마다 별도로 정해주는 것은 불편하므로 보통 디폴트로 64 값을 사용한다.

- Protocol은 이 IP 패킷을 전달할 상위 계층 프로토콜을 구분하는데 사용된다. 상위계층 프로토콜이 TCP이면 6, UDP이면 17, ICMP이면 1로 지정된다.
- Header Checksum은 헤더의 오류 검출을 위해 사용되며 헤더를 16비트 단위로 나누어 각각을 숫자로 보고 이를 차례로 더한 값이 된다.
- 덧셈은 one's complement로 계산하며 수신측에서도 같은 계산을 하여 결과를 비교하여 결과가 다르면 헤더에서 오류가 발생한 것이므로 이 패킷을 버린다.
- 목적지 주소는 패킷을 전달하기 위해서 필요하며 송신지 주소는 이 패킷을 목적지에서 수신할지를 판단할 때 사용되면 답장을 하기 위해서도 필요하다.
- IP Options은 IP 프로토콜의 기본 기능 외에 추가로 세부적인 옵션을

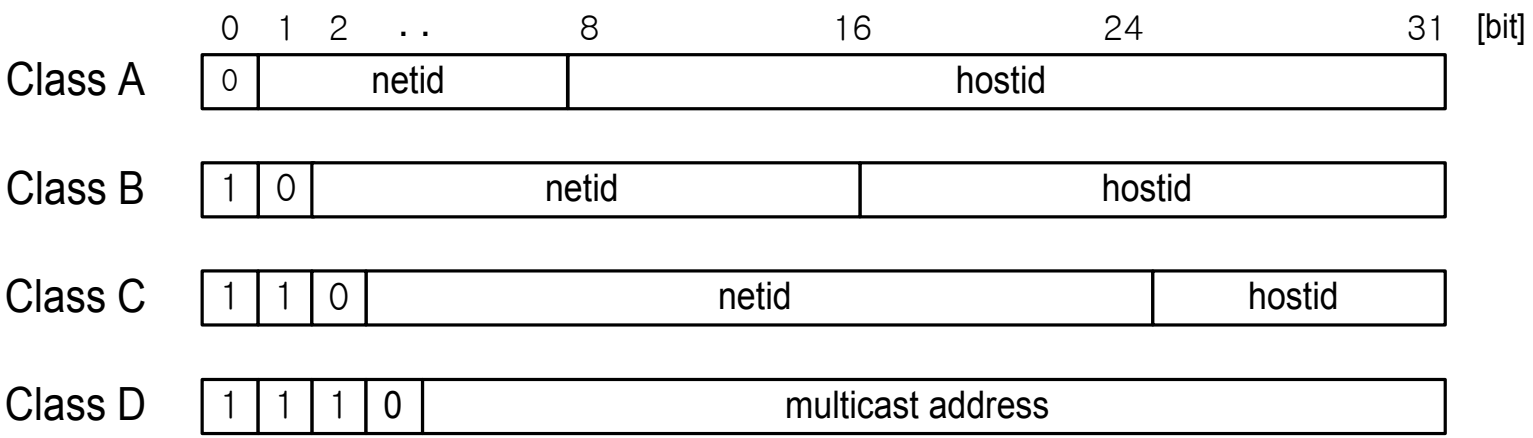
지정할 때 사용되는데 실제로는 거의 사용하지 않는다.

- IP 패킷에 옵션이 들어 있는지는 Length 필드의 값을 보고 판단할 수 있다(즉, Length가 5이면 옵션이 없는 것임을 알 수 있다).

IP 주소

- 호스트, 라우터 등 인터넷 장비를 구분하기 위해서 4 바이트의 IP 주소를 사용한다.
- 4바이트의 IP 주소를 보기 쉽게 표시하기 위하여 IP 주소를 네 개의 바이트 단위로 나누고 각 바이트의 값을 10진수로 표시하는 dotted decimal 표현 방식이 널리 사용되고 있다.
- 예를 들어 IP 주소 10000001 00001010 0000110 0000111을 dotted decimal IP 주소로 표현하면 129.10.6.7이 된다.
- IP 주소는 네트워크를 구분하기 위한 netid 필드와 한 네트워크 내에서 호스트를 구분하기 위한 hostid 필드 두 부분으로 구성된다.

- netid와 hostid에서 각각 사용하는 비트 수의 크기에 따라 여러 가지 클래스의 주소 체계를 가지고 있다.



- 클래스 A 주소는 IP 주소 첫번째 바이트의 첫 비트가 0이고 나머지 7비트가 netid이다. 뒤의 세 바이트가 hostid이므로 하나의 클래스 A 주소의 netid는 (2**24 - 2) 대의 호스트를 수용할 수 있다.

- 클래스 A 네트워크 개수는 126개가 있다.(netid 부분이 모두 0과 모두 1인 주소는 사용할 수 없어므로 2개를 제외해야 한다).
- 클래스 B 주소는 IP 주소 첫번째 바이트의 처음 두 비트가 10이고 나머지 6비트와 두번째 바이트가 netid이다. 뒤의 두 바이트가 hostid이므로 하나의 클래스 B 주소는 (2**16 - 2) 대의 호스트를 수용할 수 있다.
- 클래스 C 주소는 IP 주소 첫번째 바이트의 처음 세 비트가 110이고 나머지 5비트와 2, 3번째 바이트가 netid이다. 마지막 한 바이트가 hostid이므로 하나의 클래스 C 주소는 254대의 호스트를 수용한다.
- 클래스 D 주소는 IP 주소 첫번째 바이트의 처음 네 비트가 1110이다. 이것은 멀티캐스트 주소로 사용된다(뒤에서 설명함).

- IP 주소 체계의 가장 특징은 IP 주소가 netid와 hostid 두 부분으로 구성되어 있다는 것이다.
- IP 주소 체계의 또 다른 특징은 어떤 호스트가 둘 이상의 네트워크에 연결되어 있는 경우 이 호스트는 접속된 네트워크 수만큼 IP 주소를 각각 가지고 있어야 한다는 것이다.
- 왜냐하면 IP 주소에는 netid 부분이 있으므로 접속된 네트워크 별로 각각 netid가 다르기 때문이다.
- 이와 같이 둘 이상의 네트워크에 연결되어 다수의 IP 주소를 가지고 있는 호스트를 멀티홈(multi-homed) 호스트라고 한다.
- 멀티홈 호스트가 되려면 둘 이상의 LAN 또는 전용선을 통하여 각기 다른

네트워크로 연결되어 있어야 한다.

- 라우터도 일종의 multi-homed 호스트이므로 라우터는 접속된 각 네트워크의 netid와 같은 netid를 가지는 IP 주소들을 각각 가지고 있어야 한다.

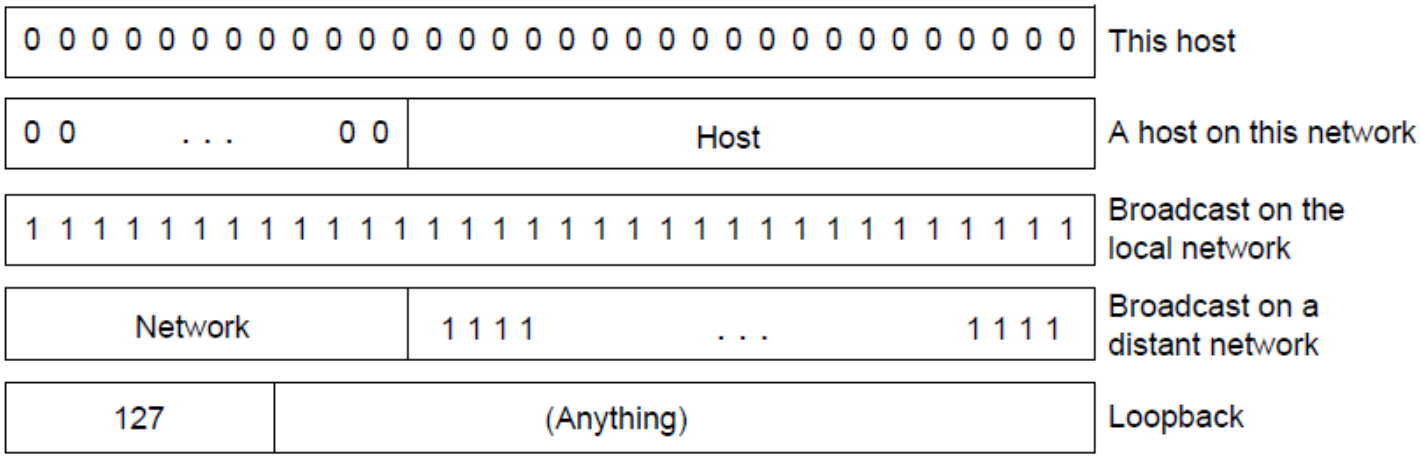
IPv6

- 4바이트로 구성된 IP 주소를 사용해서는 전세계의 모든 통신장비에게 고유한 주소를 배정할 수 없다. 이를 해결하기 위해서 주소가 16바이트(128비트)로 구성된 IPv6을 제정하였다.

- 그러나 IPv6는 실제로 도입되지 않았으며 부족한 주소는 다른 방법으로 해결하였다. (뒤에서 설명함)

특수 주소

- 0.0.0.0 주소는 현재 네트워크 또는 이 장비를 나타내며 boot시에 사용한다
- 255.255.255.255 주소는 현재 네트워크에 접속된 모든 장비를 나타낸다. LAN의 경우 방송을 할 때 사용된다.
- 127.....로 시작하는 주소는 loopback 테스트 즉, 자체 컴퓨터에게 IP 패킷을 전송할 때 사용한다. 이 주소를 가진 패킷은 외부로 나가지 않고 자신의 상위 계층으로 전달된다.


0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
This host
0 0 . . . 0 0
Host
A host on this network
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Broadcast on the local network
Network
1 1 1 1 . . . 1 1 1 1
Broadcast on a distant network
127
(Anything)
Loopback

메시지 분할 전송

- 인터넷이 여러 네트워크들로 구성되어 있을 때 각 네트워크마다 처리할 수 있는 최대 패킷의 크기가 다를 수 있으므로 인터넷을 통해 IP 패킷을 전송하기 위해서 다음과 같은 IP 패킷의 분할/재조립 기능이 필요하다.

- 어떤 네트워크에서 한 번에 전달할 수 있는 패킷의 최대 크기를 MTU(Maximum Transmission Unit)라고 하는데 예를 들어 이더넷이 한 프레임에 실어 전달할 수 있는 최대 메시지 크기는 1500바이트이다.

- 예를 들어 1200 바이트 크기의 메시지를 MTU가 500 바이트인 하위 네트워크로 전송하면 다음과 같이 세 개의 패킷으로 세분화되어 전송된다.

  ID=x, M=1, offset = 0 (데이터 크기= 480 바이트)
  ID=x, M=1, offset = 480 (데이터 크기= 480 바이트)
  ID=x, M=0, offset = 960 (데이터 크기= 240 바이트)

- 첫 패킷의 데이터 크기가 480 바이트인 이유는 IP 헤더 20 바이트를 포함하여 총 패킷의 크기가 500 바이트로 제한되어야 하기 때문이다.

- offset=0의 의미는 이 패킷이 전체 메시지의 첫 부분인 것을 알린다. 두 번째 패킷에서 offset=480의 의미는 이 패킷이 전체 메시지의 481번째 바이트 이후의 데이터를 포함하고 있는 것을 알린다.