Chapter 01

네트워크 개요

1. 인터넷

- 인터넷 (Internet) 이란, '여러 개의 네트워크를 묶었다'는 의미를 가지고 있다.

- 인터넷의 특징
  - 하나의 프로토콜(TCP/IP)만을 사용한다.
  - 웹 브라우저를 이용해서 인터넷을 탐험한다.
  - 인터넷에는 없는 정보가 없다.

2. 인트라넷

- 사내 업무도 이렇게 웹 브라우저만을 가지고 쓸 수 없을까 해서 만든 게 바로 인트라넷!!
- 인트라넷 역시 TCP/IP란 프로토콜을 사용하고, 또 웹 브라우저를 이용해서 마치 우리가 인터넷을 사용하듯이 사내 업무를 처리할 수 있다.
- 인트라넷과 인터넷의 차이는 그 회사사림 말고 다른 사람은 인터넷을 통해서 접속이 불가능하다는 것이다.

3. 엑스트라넷

- 내용은 인트라넷과 거의 유사하지만, 기업의 인트라넷을 그 기업의 종업원 이외에도 협력 회사나 고객에게 사용할 수 있도록 한 것이 바로 엑스트라넷의 가장 큰 차이점이다.

4. LAN(Local Area Network)이란?

- LAN이란, 'Local Area Network'의 약자로 Local, 즉 '어느 한정된 공간에서 네트워크를 구성한다'는 것이다.

- LAN과 비교되는 말로 WAN이 있다.
- WAN은 'Wide Area Network'의 약자로서 '멀리 떨어진 지역을 서로 연결하는 경우'에 사용한다.

5. 이더넷(Ethernet)이란?

- 그럼 이더넷 (Ethernet)은 또 뭘까?
- 이더넷은 네트워킹의 한 방식이다.
- 즉 네트워크를 만드는 방법 중 하나라고 생각하면 된다.
- 이러한 이더넷 방식의 가장 큰 특징은 CSMA/CD라는 프로토콜을 사용해서 통신을 한다는 것이다.

- 네트워킹 방식은 얼마 전까지만 해도 우리가 말한 이더넷 방식 말고도 토큰링 방식도 있었고, FDDI 방식도 있었으며. 또 ATM 방식도 있었다.
- 어떤 네트워킹 방식을 사용하느냐에 따라 랜카드를 비롯하여 구입해야 하는 네트워크 장비들이 다르다.

5. 이더넷(Ethernet)이란?

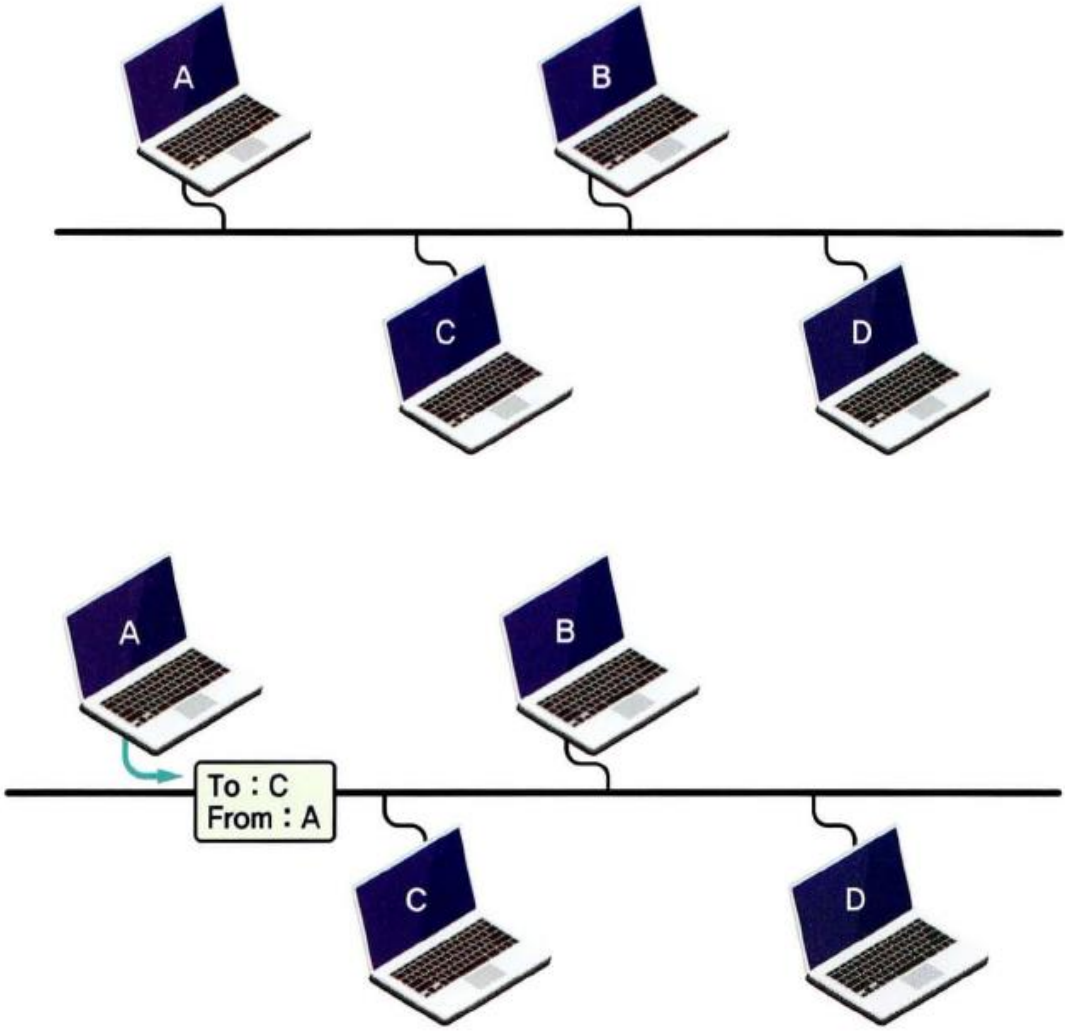
- 이더넷 환경에서 통신을 하고 싶은 PC나 서버는 먼저 지금 네트워크상에 통신이 일어나고 있는지를 확인한다.
- 이것을 바로 'Carrier Sense'라고 한다.
- 이때 만약 캐리어가 감지되면, 다시 말해서 누군가가 네트워크상에서 통신을 하고 있으면 자기가 보낼 정보가 있어도 못 보내고 기다린다.
- 그러다가 네트워크에서 통신이 없어지면 눈치를 보다가 무조건 자기 데이터를 네트워크상에 실어서 보낸다.
- 그런데 만약 네트워크상에서 두 PC나 서버가 보낼 데이터를 가지고 눈치를 살피고 있었다고 가정해보자.
- 이더넷에서는 이렇게 2개 이상의 PC나 서버가 동시에 네트워크상에 데이터를 실어 보내는 경우가 발생할 수 있다.
- 이 경우를 바로 'Multiple Access(다중 접근)'라고 한다.

5. 이더넷(Ethernet)이란?

- 통신에서 이렇게 2개의 장비들이 데이터를 동시에 보내려다 부딪치는 경우를 충돌(Collision)이 발생했다고 한다.
- 따라서 이더넷에서는 데이터를 네트워크에 실어서 보내고 나서도 혹시 다른 PC 때문에 충돌이 발생하지 않았는지를 잘 점검해야 한다.
- 그것이 바로 'Collision Detection(충돌 감지)'라고 한다.
- 그러다 만약 충돌이 발생하게 되면 데이터를 전송했던 PC들은 랜덤(Random)한 시간 동안 기다린 후 다시 데이터를 전송한다.

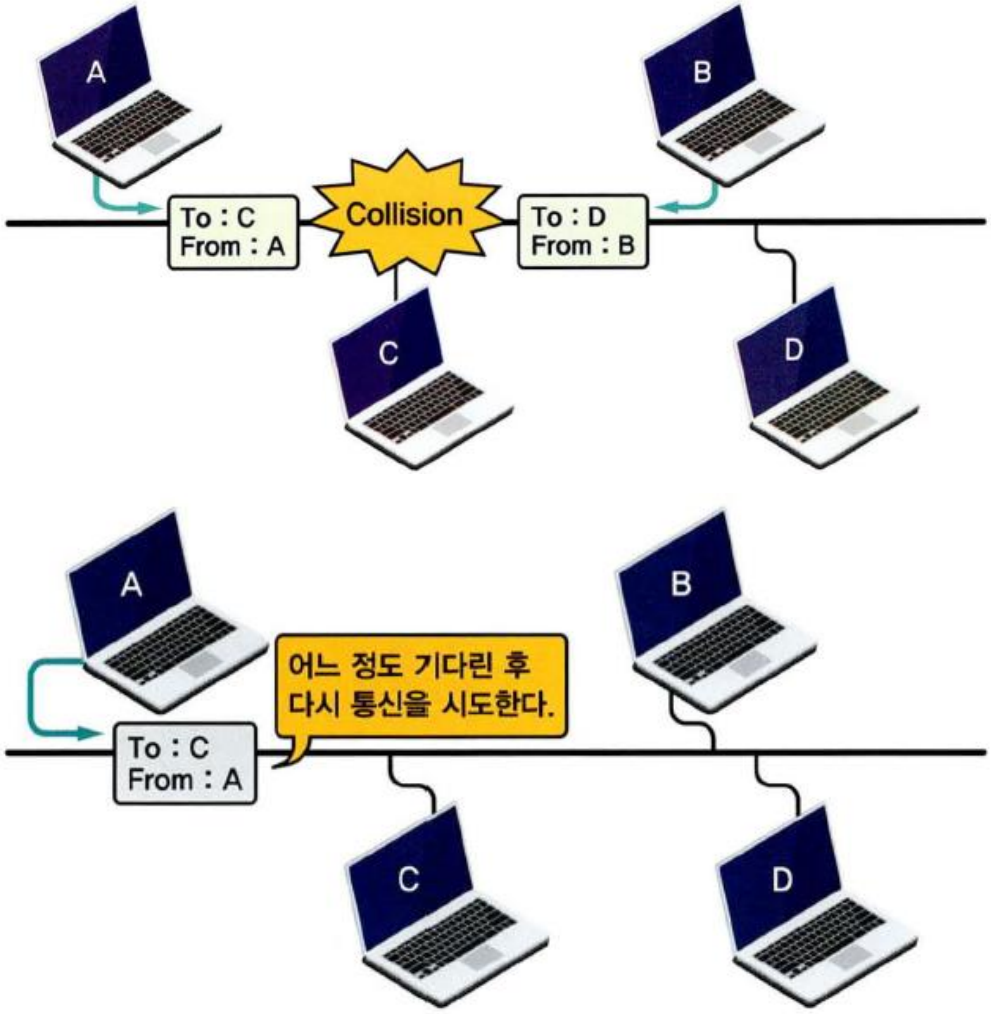
5. 이더넷(Ethernet)이란?

- CSMA/CD의 동작



5. 이더넷(Ethernet)이란?

- CSMA/CD의 동작

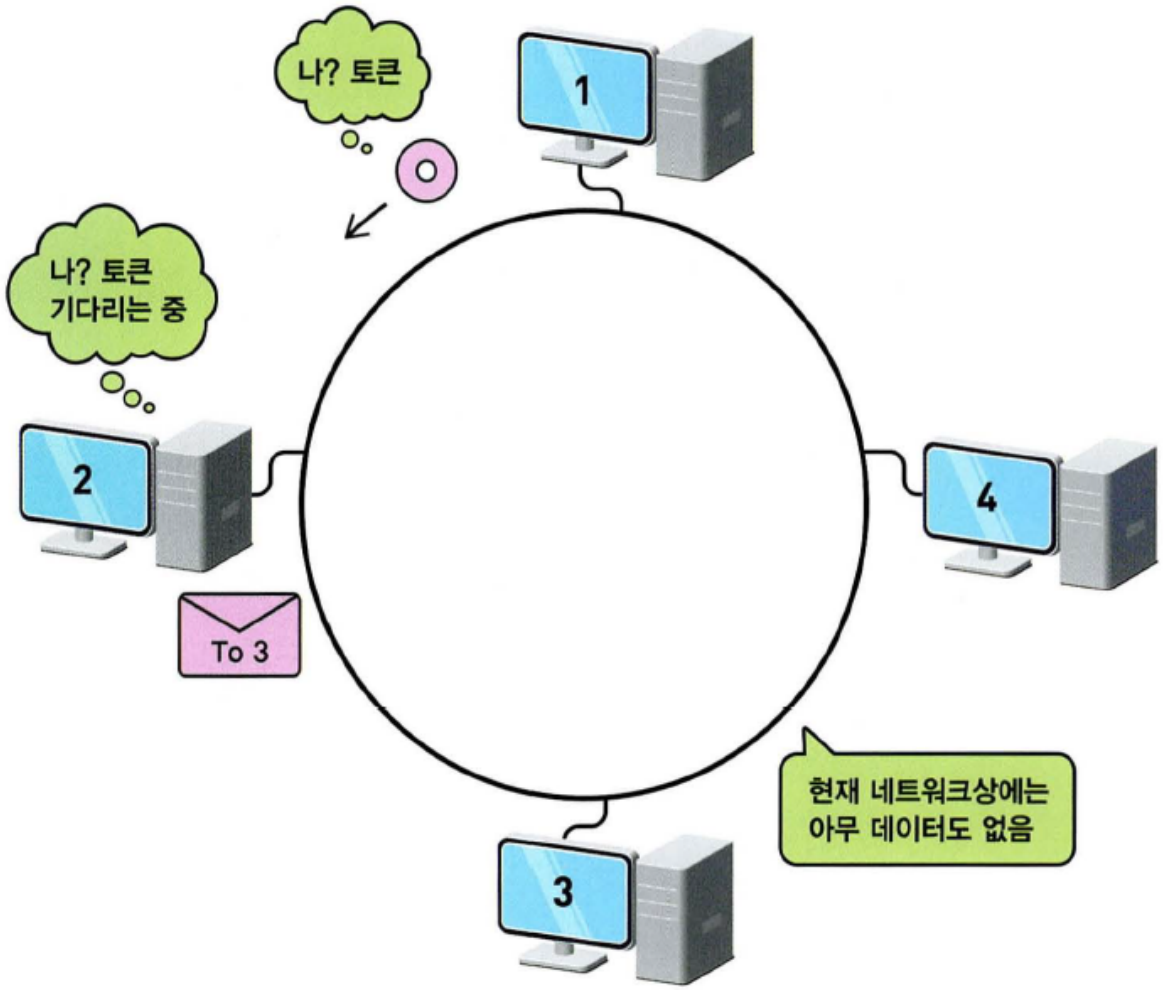


6. 토큰링(TokenRing)이란?

- 토큰링 방식의 네트워크에서 오직 한 PC, 즉 토큰을 가진 PC만이 네트워크에 데이터를 실어 보낼 수 있다.
- 데이터를 다 보내고 나면 바로 옆 PC에 토큰을 건네주게 된다.
- 만약 전송할 데이터가 없다면 토큰을 다시 옆 PC에 전달한다.
- 이렇게 옆으로 전달하는 방식으로 통신이 이루어진다.
- 따라서 토큰링에서는 당연히 충돌(Collision)이 발생하지 않는다.
- 또한 네트워크에 대한 성능을 미리 예측하기도 쉽다.
- 그 대신 단점도 있다.
- 내가 지금 바로 보내야 할 데이터가 있고, 다른 PC들은 보낼 데이터가 하나도 없다고 하더라도 차례가 올 때까지 계속 기다려야 된다.

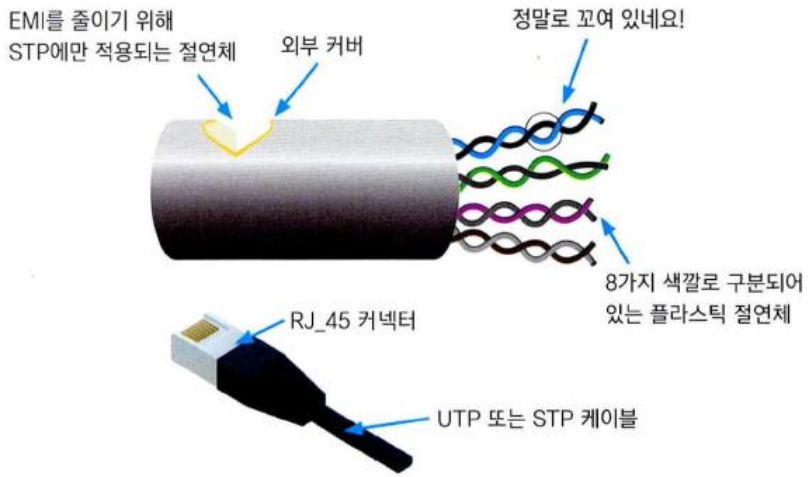
6. 토큰링(TokenRing)이란?

토큰링 방식



7. UTP 케이블

- PC에서 허브나 스위치까지의 연결, 스위치와 스위치의 연결, 스위치와 라우터의 연결, 라우터와 라우터의 연결 등 아무튼 네트워크 장비와 네트워크 장비를 연결하기 위해서는 어떤 종류의 케이블이든 반드시 케이블이 들어가게 된다.
- 이렇게 들어가는 케이블은 광케이블, UTP 케이블, 동축 케이블 등 종류도 가지가지이다.
- UTP 케이블의 의미는 무엇일까?
- 일단 TP 케이블이란 (twisted – pair), 즉 '꼬인 케이블'이다.
- 그림처럼 페어가 서로 꼬여있는 것을 말한다.



7. UTP 케이블

- TP에는 UTP와 STP가 있다.
- UTP는 Unshielded TP를 말한다.
- 주로 우리가 사용하는 케이블이 바로 이 UTP이다.
- STP는 Shielded로 케이블의 주위를 어떤 절연체로 감싸서 만든 것을 말한다.
- STP가 좀 더 비싸고 성능이 좋다.
- 암튼 그래도 기존에 워낙 UTP로 구성된 네트워크가 많았기 때문에 결국은 UTP가 중심을 이루게 되었고, STP는 주로 토큰링쪽에 많이 쓰이고 있는 추세이다.
- 자, 그러면 우리가 보통 말하는 카테고리 5나 카테고리 3이니 하는 것은 무엇을 의미하는 것일까?

7. UTP 케이블

- 카테고리 1
  - 주로 전화망에 사용하는 용도로 만들어진 케이블이다.
  - 따라서 데이터 전송용으로는 적합하지 않다.
- 카테고리 2
  - 데이터를 최대 4Mbps의 속도로 전송할 수 있는 능력을 가지고 있는 케이블이라고 한다.
- 카테고리 3
  - 10 BaseT 네트워크에 사용되는 케이블이다.
  - 전에는 UTP 케이블이라고 하면 바로 이 케이블을 이야기 할 정도로 일반적인 케이블이었다.
  - 최대 10Mbps 속도까지 데이터 전송을 할 수 있다.
  - 잘만 구성하면 100Mbps 속도에도 적용이 가능한 케이블이지만, 실제로 이 케이블을 가지고 100Mbps를 구성하는 것은 매우 드물다.
- 카테고리 4
  - 토큰링 네트워크에서 사용되는 케이블이다.
  - 최대 16Mbps의 데이터 전송 능력을 가지고 있다.

7. UTP 케이블

카테고리 5

- 지금까지는 최대 전송 속도 100Mbps를 지원하는 Fast Ethernet용으로 사용되었다.
- 그런데 얼마 전에 기가비트 표준이 완성되면서 이제 이 케이블로도 기가비트 속도의 데이터 전송이 가능해졌다. (이 경우에는 8가닥을 모두 사용해야 가능하다)

카테고리 6

- 기가비트 이상의 속도에 적합한 케이블이다.
- 최근 사용하는 케이블 중 가장 많은 종류가 바로 카테고리 6 케이블이다.
- 카테고리 6 케이블은 Cat6와 Cat6a로 구분되는데, 뒤에 나온 Cat6a 케이블이 좀 더 성능이 개선된 케이블이고, 최대 10Gbps를 지원한다.

카테고리 7

- 주로 10Gbps 속도 이상을 지원하기 위한 케이블로, 아직까지 많이 사용되고 있진 않지만 앞으로 점점 더 많이 사용될 케이블이다.
- 이제 곧 10Gbps가 일반화되고 나면 좀 더 자주 보게 될 케이블이기도 하다.

8. 케이블의 종류

- 일단 우리가 케이블 종류를 말할 때는 약간의 법칙이 있다.
- 10 Base T에서 일단 맨 앞에 나오는 10이란 숫자는 속도를 나타낸다.
- 즉 여기에서 10이란, 10Mbps의 속도를 지원하는 케이블을 의미한다.
- 그 다음에 나오는 Base란 말은 이 케이블이 Baseband용 케이블이라는 것을 알려주고 있다.
- 원래 케이블 종류에는 베이스밴드(Baseband)와 브로드밴드(Broadband)가 있는데, 쉽게 생각해서 베이스밴드는 디지털 방식이고, 브로드밴드는 아날로그 방식이라고 생각하면 된다.
- 그 다음은 T라고 되어 있는데, 원래 이 자리에는 케이블의 종류 또는 이 케이블이 전송할 수 있는 최대 거리가 나오게 되어 있다.
- 위의 예, 즉 10 Base T에서 T란, TP(Twisted Pair) 케이블이라는 것을 나타낸다.
- 이것이 바로 우리가 보통 사용하는 UTP 케이블을 나타낸다.

8. 케이블의 종류

- 만약 맨 뒷자리에 위에서처럼 글자(여기선 T였다.)가 나오지 않고 숫자가 나오면, 예를 들어 '10 Base 5'일 때 맨 뒤에 나오는 숫지는 최대 통신 거리이다.
- 따라서 최대 500미터까지 통신이 가능하다는 것을 뜻한다.

- **10 Base T**
  - 10Mbps로 통신하고, 최대 전송 거리 100미터인 UTP 케이블로, 카테고리 3, 4, 5를 사용할 수 있다.
  - 이 케이블에는 RJ45 잭을 사용해서 연결해 준다.

- **10 Base FL**
  - 10Mbps로 통신하는 케이블인데, 광케이블이다.
  - 즉 뒤에 나오는 FL(Fiber- optic)이 광케이블이란 것을 알려주고 있다.
  - 이 케이블은 ST 커넥터라는 것을 사용해서 연결하고 광케이블은 싱글 모드 또는 멀티 모드 케이블을 사용한다.

8. 케이블의 종류

10 Base 2

- 10Mbps로 통신이 가능하고 최대 200 미터까지 전송이 가능한 케이블이다.
- 몇 년 전까지만 해도 이 케이블을 사무실에서 가장 많이 사용했다.
- 그런데 요즘은 UTP 케이블에 밀려서 완전히 자취를 감추고 말았다.
- 이 케이블은 그냥 'Thin 케이블'이라고도 불렸고 BNC 커넥터를 사용했다.

10 Base 5

- 10Mbps 통신을 지원하는 케이블이고 최대 거리는 500 미터로 두껍게 생겼다고 해서 'Thick 케이블'이라고 부르거나 색이 노랗다고 해서 '옐로우(Yellow) 케이블'이라고 부른다.
- 주로 백본 케이블, 즉 중앙망용으로 천장 위에 설치하고 트랜시버 케이블을 이용해서 천장에서 하나씩 뽑아 내린 다음에 PC의 랜카드와 연결했다.
- 랜카드 중에 AUI 인터페이스(15핀으로 생긴 사다리꼴 인터페이스)를 가진 것이 바로 이 케이블과 연결하기 위한 인터페이스가 된다.

8. 케이블의 종류

100 Base TX

- Category 5 UTP 케이블을 사용하는 케이블이고 최대 거리는 100미터, 전송 속도는 100Mbps짜리 케이블이다.

100 Base T2

- 원래 100Mbps 속도를 내려면 위에서처럼 Category 5 케이블을 사용하는데, 100 Base T2 방식을 쓰면 Category 3, 4, 5를 전부 사용해서 100M를 구현할 수 있다고 한다.

100 Base T4

- Category 3 케이블을 가지고 100Mbps용으로 사용할 때 만드는 케이블입니다.
- 그 대신 다른 케이블은 2페어(4가닥)를 사용하지만 이것은 4페어(8가닥)를 전부 사용한다는 차이점이 있다.

8. 케이블의 종류

100 Base FX

- 이 케이블은 100Mbps 광케이블을 이용해서 구현하는 건데, 전송 거리가 보통 2km에서 10km까지 가능하고 SC라는 네모난 접속 커넥터를 이용해서 접속한다.
- 물론 ST(동그렇게 생겨서 돌려서 끼우는 방식)도 사용하지만 일반적이지는 않다.

1000 Base SX

- 이것은 기가비트, 즉 1,000Mbps의 속도가 나는 케이블이다.
- Short Wavelength라는 광케이블을 사용하는데, 최대 전송 거리는 약 270 미터 (62.5micro meter = 1/1,000,000m)에서 550미터 (50micro meter) 정도이다.

1000 Base T

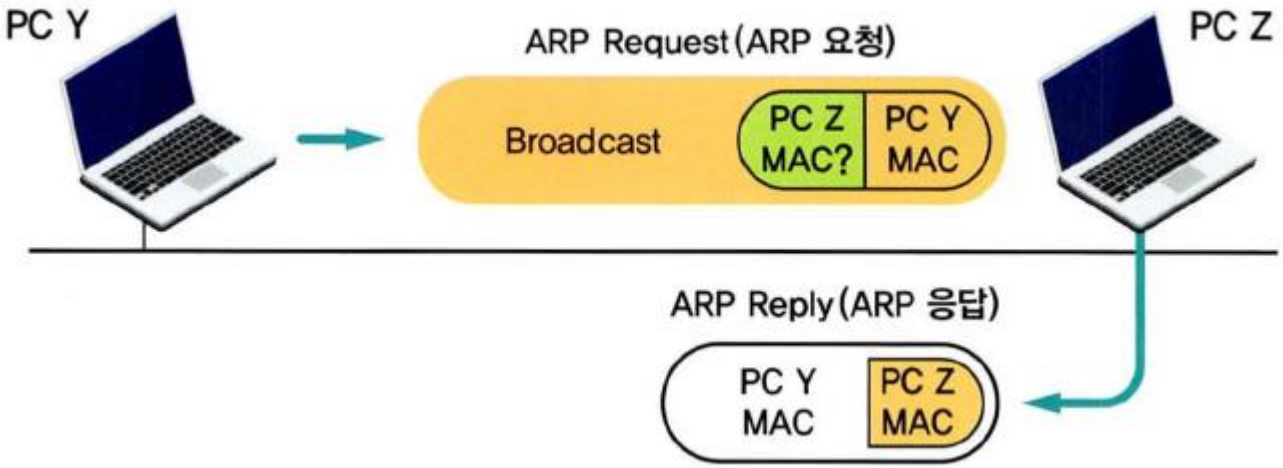
- 1,000Mbps로 UTP 케이블을 통해 전송하고 최대 거리는 100미터인 케이블 스펙이다.
- Category 5 케이블을 사용하면 된다.

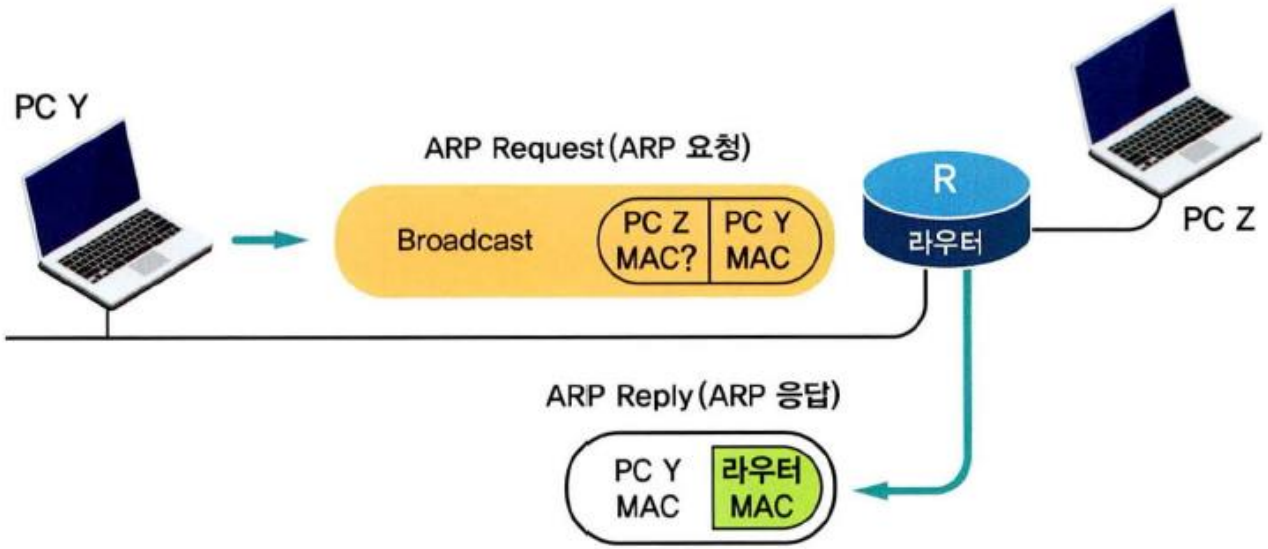
9. 맥 주소(MAC Address)

- 컴퓨터는 네트워크상에서 어떻게 서로를 구분해서 인식할까?
- 즉 통신을 위해서는 서로를 구분할 일종의 주소가 필요하다.
- 이 역할을 담당하는 주소가 바로 MAC 주소이다.
- 인터넷은 TCP/IP로 통신을 하고 따라서 통신을 위해서 IP 주소를 사용한다.
- 그럼 이 경우에 맥 주소는 사용하지 않는 걸까?
- 일단 답은 '이 경우에도 맥 주소를 사용한다' 이다.
- 우리가 IP 주소를 사용하니까 IP 주소만 있으면 모든 통신이 일어날 것 같지만, 사실은 IP 주소를 다시 MAC으로 바꾸는 절차(이 과정을 ARP; Address Resolution Protocol이라고 한다.)를 밟고 있는 것이다.

9. 맥 주소(MAC Address)

- ARP 요청과 응답





9. 맥 주소(MAC Address)

- 네트워크(여기서는 이더넷- Ethernet이다)에 붙는 각장비들은 48bit (6octet)의 주소를 갖게 되는데, 이 주소는 랜카드 또는 네트워크 장비에 이미 고정되어 있는 주소이고 유일한(즉 전 세계에서 유일한) 주소이다.
- 이 주소를 바로 '맥 주소' 또는 '하드웨어 주소'라고 한다.
- 모든 랜(LAN)의 디바이스(device)들은 반드시 유일한 맥 주소를 가져야 한다.
- 따라서 랜카드 하나하나마다 서로 다른 맥 주소가 있고 또 라우터나 스위치에도 맥 주소가 들어있다.
- 물론 서버에도 들어있다.
- 서버에도 랜카드가 설치될 거니까.

9. 맥 주소(MAC Address)

- 맥 어드레스는 8자리마다 하이픈(-)이나 콜론(:), 점 (.)으로 구분되기도 한다.
- 예를 들어 다음과 같이 나타낸다.

```
00-60-97-8F-4F-86
00:60:97:8F:4F:86
0060.978F.4F86
```

- 이 주소에서 앞쪽 6개의 16진수(여기서는 00-60-97)가 벤더, 즉 생산자를 나타내는 코드로, 이 코드를 'OUI(Organizational Unique Identifier)'라고 한다.
- 즉 이 코드는 메이커에 따라 다르기 때문에 우리가 MAC 주소의 앞부분을 보면 어느 회사에서 만든 제품인지를 알 수 있는 것이다.
- 그리고 뒤에 오는 나머지 6자리의 수가 메이커에서 각 장비에 분배하는 Host Identifier이다.
- 한마디로 시리얼 넘버인 셈이다.

9. 맥 주소(MAC Address)

- 맥 주소 중에서 앞쪽의 절반은 미리 약속된 규정에 따라 각 네트워크 장비를 만드는 회사에 분배해주고, 그 회사에서는 나머지 절반을 일련번호로 만들어 각 장비에 부여하는 것이다.

10. 유니캐스트, 멀티캐스트, 브로드캐스트

유니캐스트

- 유니캐스트란, 우리가 랜에서 통신을 한다고 할 때 데이터를 보내고자 하는 PC의 맥 주소가 (00-60-80-AA-BB-CC이라고 가정하고 받는 PC의 맥 주소가 (00-60-80-DD-EE-FF) 라고 가정한 경우이다.
- 즉 정확하게 받는 PC의 주소를 프레임 안에 써넣는데, 이때 PC가 하나이어야 한다는 것이다.
- 이런 방식으로 어떤 PC가 유니캐스트 프레임을 뿌리게 되면, 어차피 로컬 이더넷의 기본 성격이 붙어있는 모든 PC들에게 정보를 뿌리는 Shared 방식이기 때문에 그 로컬 네트워크상에 있는 모든 PC들은 일단 이 프레임을 받아들여서 랜카드에서 자신의 맥 어드레스와 비교하게 된다.
- 그 다음 자신의 랜카드 맥 어드레스와 목적지 맥 어드레스가 서로 다른 경우는 바로 그 프레임을 버리게 된다.
- 이렇게 되면 그 PC의 CPU까지는 영향을 주지 않기 때문에 PC의 성능이 저하되는 일은 발생하지 않는다.
- 이때 만약 목적지 주소를 자신의 맥 주소와 비교했더니 같으면 랜카드는 이 프레임을 CPU로 올려보낸다.

10. 유니캐스트, 멀티캐스트, 브로드캐스트

유니캐스트

- 현재 네트워크상에서 가장 많이 사용되는 통신 방식이 바로 이 유니캐스트 방식이다.
- 유니캐스트는 특정 목적지의 주소 하나만을 가지고 통신하는 방식이다.
- 그리고 이런 유니캐스트 통신 방식은 그 목적지 주소가 아닌 다른 PC들의 CPU 성능을 저하시키지는 않는다.
- 그 이유는 자신의 맥 어드레스가 아니라고 판단되면 랜카드가 이 프레임을 버리기 때문이다.

10. 유니캐스트, 멀티캐스트, 브로드캐스트

브로드캐스트

- 브로드캐스트는 한마디로 로컬 랜에 붙어 있는 모든 네트워크 장비들에게 보내는 통신이다.
- 여기서 로컬 랜이란, 라우터에 의해서 구분된 공간, 즉 브로드캐스트 도메인이라고 하는 공간을 뜻한다.
- 브로드캐스트는 자기가 받기 싫다고 해서 받지 않는 것이 아니라 무조건 받는 것이다.
- 브로드캐스트의 주소는 미리 정해져 있는데, 바로 FFFF.FFFF.FFFF(맥 어드레스로 했을 때)이다.
- 이 주소가 오면 랜카드는 비록 자신의 맥 어드레스와 같지는 않지만 이 브로드캐스트 패킷을 CPU에 보내게 된다.
- 그 다음은 CPU가 이 패킷을 알아서 처리하게 된다.
- 브로드캐스트는 네트워크상의 전체 노드로 전송되기 때문에 전체적인 트래픽도 증가하지만, 이 패킷을 받은 모든 랜카드가 이 패킷을 CPU로 전송하기 때문에 CPU는 하던 일을 멈추고 또 다른 일을 해야 하고 이에 따라 전체 PC의 성능도 떨어지게 되는 것이다.
- 따라서 과도한 브로드캐스트는 전체 네트워크의 성능뿐만 아니라 PC 자체의 성능 역시 떨어뜨리는 결과를 가져오는 것이다.

10. 유니캐스트, 멀티캐스트, 브로드캐스트

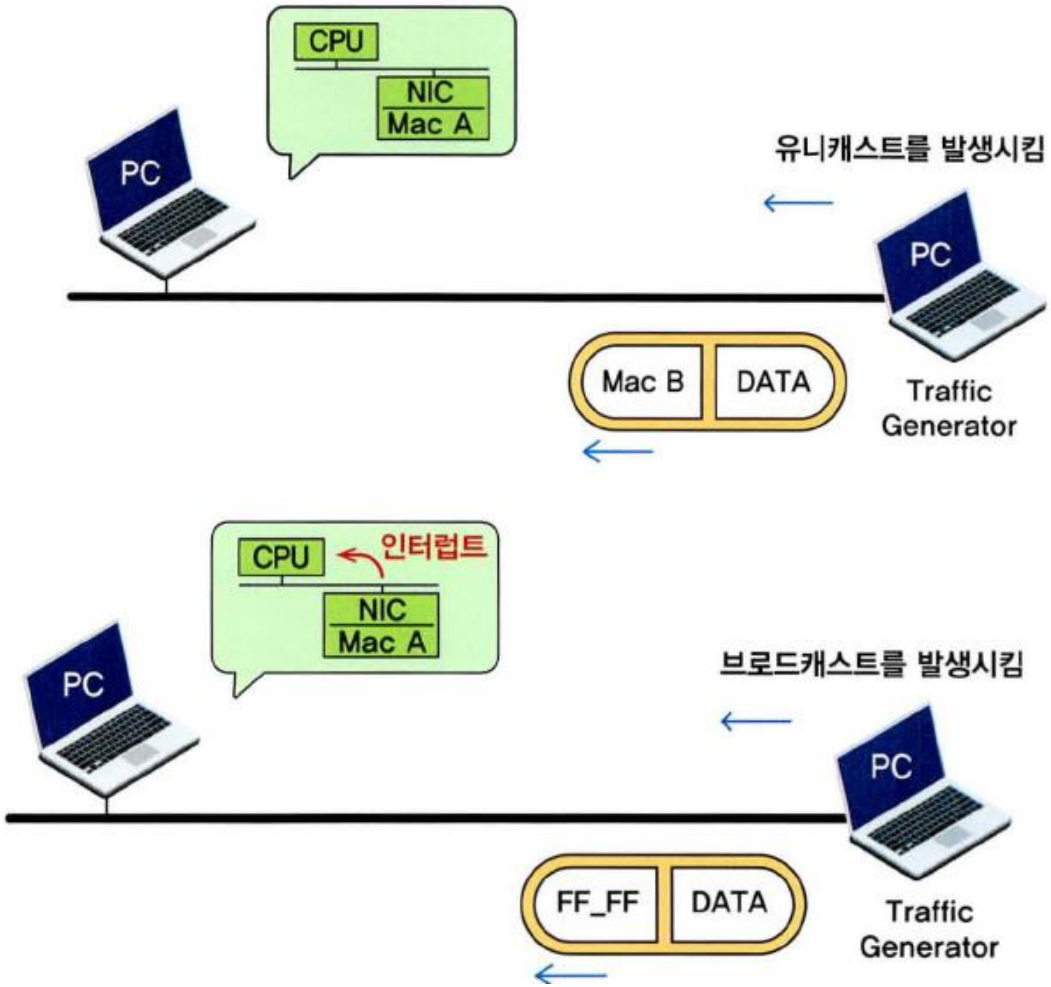
브로드캐스트

- 그럼 브로드캐스트는 어떤 경우에 발생할까?
- 예를 들어 처음 두 PC 간에 통신을 하는 경우에는 상대편의 맥 어드레스를 모를 것이다.
- 상대편의 IP 주소는 알 수 있어도 말이다.
- 이 경우에 상대의 맥 어드레스를 알아내기 위해서 하는 동작이 바로 ARP(Address Resolution Protocol)이다.
- 이 ARP가 바로 브로드캐스트이다.
- 그 외에도 라우터끼리 정보를 교환한다거나 다른 라우터를 찾을 때, 또 서버들이 자신이 어떤 서비스를 제공한다는 것을 모든 클라이언트들에게 알릴 때 등 여러 경우에 사용된다.

10. 유니캐스트, 멀티캐스트, 브로드캐스트

브로드캐스트

- 유니캐스트와 브로드캐스트에 대한 비교



10. 유니캐스트, 멀티캐스트, 브로드캐스트

멀티캐스트

- 200명의 사용자가 있는 네트워크에서 150명에게만 같은 정보를 동시에 보내야 하는 상황이라고 가정해 보자.
- 그렇다면 서버는 어떻게 해야 이 정보를 동시에 150명의 사용자에게 뿌려줄 수 있을까?
- 첫 번째, 우리가 이미 배운 유니캐스트라는 걸 사용하는 경우이다. 즉 150명의 주소로 하나씩 전부 보내주는 것이다.
- 또 하나의 방법은 브로드캐스트를 이용하는 방법이다.
- 브로드캐스트로 한 번에 모든 사용자에게 보내는 것이다.
- 마지막은 멀티캐스트를 이용하는 방법이다.
- 멀티캐스트는 보내고자 하는 그룹 멤버들에게만 한 번에 보낼 수 있기 때문에 유니캐스트처럼 여러 번 보낼 필요도 없고 브로드캐스트처럼 받기 싫어하는 사람에게까지 보낼 필요도 없다.
- 그 그룹에 속해있는 사람들에게만 선택적으로, 그것도 한 번에 보낼 수 있는 것이다.
- 멀티캐스트는 라우터나 스위치에서 이 기능을 지원해 주어야만 쓸 수 있다.

11. OSI 7계층

- 통신에 관한 국제적인 표준기구인 International Organization for Standardization(ISO) 라는 곳에서 만든 OSI7 레이어는 통신이 일어나는 과정을 7개의 단계로 나누었다.
- 이는 통신을 7개의 단계별로 표준화하여 그 효율성을 높이기 위해서 사용되었다.
  - Application Layer(애플리케이션 계층)
  - Presentation Layer(프레젠테이션 계층)
  - Session Layer(세션 계층)
  - Transport Layer(트랜스포트 계층)
  - Network Layer(네트워크 계층)
  - Data Link Layer(데이터 링크 계층)
  - Physical Layer(물리 계층)

11. OSI 7계층

물리계층

- 이 계층은 통신의 맨 아래 단계로, 여기서는 주로 전기적, 기계적, 기능적인 특성을 이용해서 통신 케이블로 데이터를 전송하게 된다.
- 이 계층에서 사용되는 통신 단위는 비트이며, 이것은 1과 0으로 나타내는, 즉 전기적으로 On, Off 상태라고 생각하면 된다.
- 이 계층에서는 단지 데이터를 전달할 뿐 이 데이터가 무엇인지, 어떤 에러가 있는지, 어떻게 보내는 것이 더 효과적인지 하는 것은 전혀 관여하지 않는다.
- 이 계층에 속하는 대표적인 장비는 통신 케이블, 리피터, 허브 등이 있다.

데이터 링크 계층(Data Link Layer)

- 피지컬 레이어를 통하여 송 수신되는 정보의 오류와 흐름을 관리하여 안전한 정보의 전달을 수행할 수 있도록 도와주는 역할을 한다.
- 따라서 통신에서의 오류도 찾아주고 재전송도 하는 기능을 가지고 있을 뿐만 아니라 전에 배운 맥 어드레스를 가지고 통신할 수 있게 해준다.
- 이 계층에서 전송되는 단위를 우리는 '프레임 '이라고 부른다.
- 이 계층에 속하는 대표적인 장비에는 브리지, 스위치 등이 있다.

11. OSI 7계층

네트워크 계층(Network Layer)

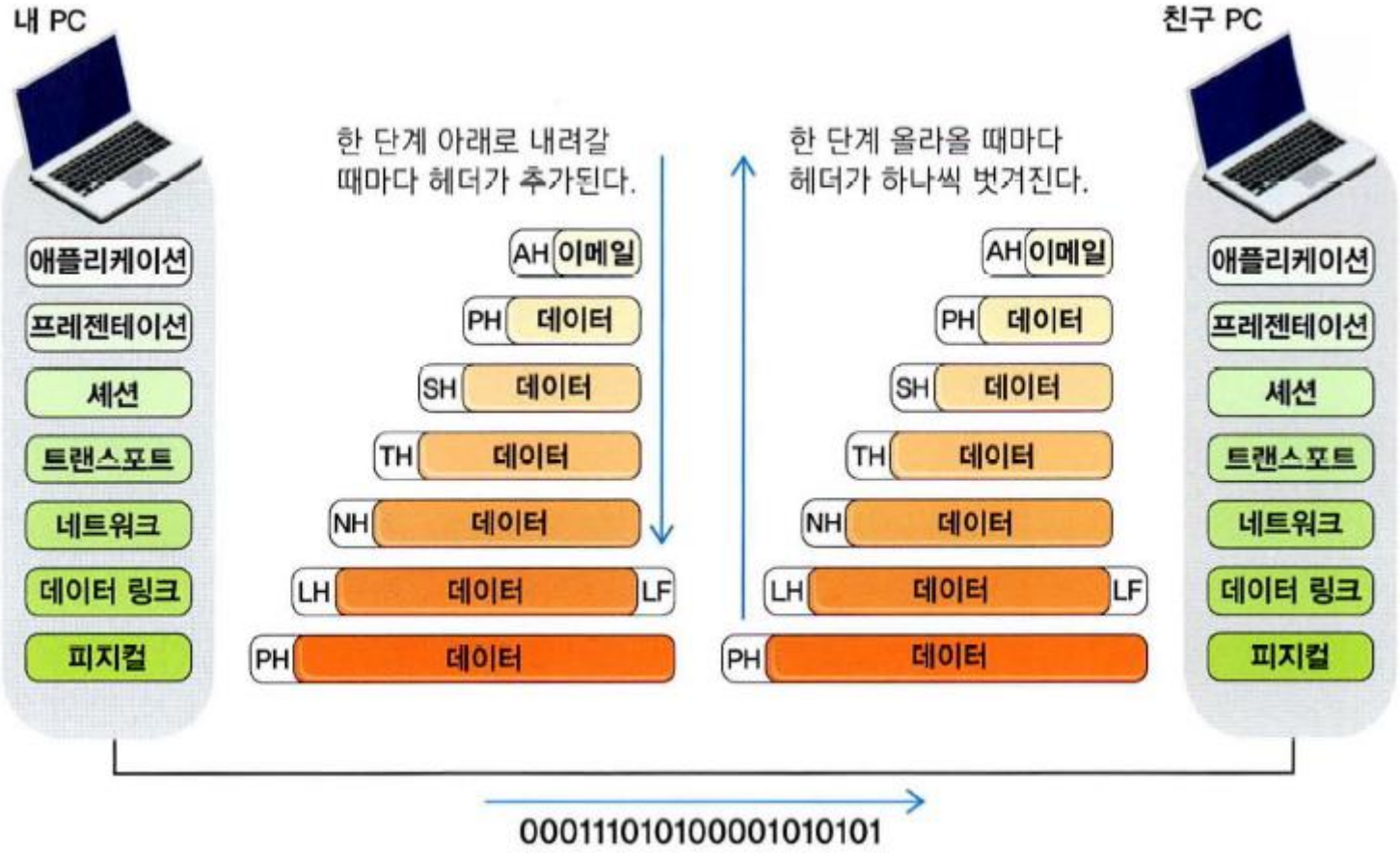
- 네트워크를 하시는 여러분이 가장 많이 다루어야 하는 계층이다.
- 여기서 하는 가장 중요한 기능은 데이터를 목적지까지 가장 안전하고 빠르게 전달하는 것이다.
- 보통 이것을 '라우팅'이라고 한다.
- 따라서 경로를 선택하고 주소를 정하며, 경로에 따라 패킷을 전달해주는 것이 이 계층의 역할이다.
- 라우터가 바로 이 계층에 속하는 장비이며, 요즘은 스위치 중에서도 라우팅 기능을 수행하는 스위치가 나오고 있는데 이들 스위치를 보통 'Layer 3 스위치'라고 하는 이유도 여기에 있다.

트랜스포트 계층(Transport Layer)

- 트랜스포트 계층에서 하는 중요한 일은 주로 흐름제어와 에러 복구 기능이다.
- 즉 에러 복구를 위해 패킷을 재전송하거나 흐름을 조절해서 데이터가 정상적으로 전송될 수 있도록 하는 역할을 한다.
- 우리가 나중에 배우게 될 TCP나 UDP가 이 계층에 해당된다.

11. OSI 7계층

■ 7계층을 이용한 이메일 전송



12. 프로토콜

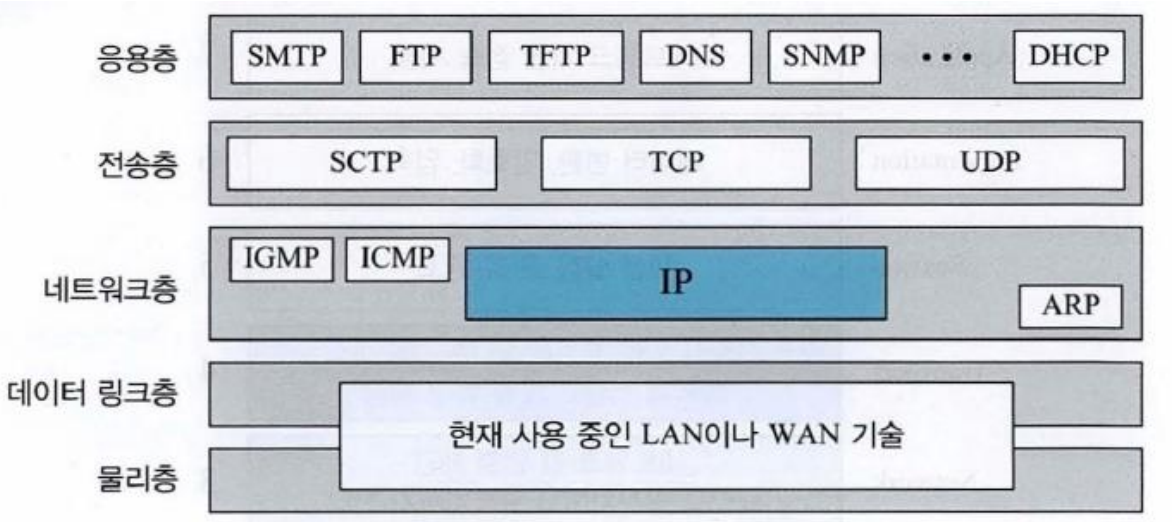
- 프로토콜(Protocol)이란, 우리말로 하면 규약, 협약과 비슷한 뜻인데, 컴퓨터끼리는 프로토콜이 서로 같은 것끼리만 통신이 가능하다.
- 그렇다면 인터넷을 사용하고 있는 모든 PC는 같은 언어를 사용하고 있는 걸까?
- 답은 '그렇다.'이다.
- 인터넷을 사용하기 위해서는 모든 PC가 TCP/IP라는 프로토콜을 사용해야 한다.
- 인터넷을 사용하는 모든 PC는 바로 이 프로토콜을 사용하기 때문에 인터넷을 접속할 수 있는 것이다.

12. 프로토콜

- 그런데 프로토콜에도 여러 종류가 있다.
- TCP/IP는 인터넷에서 사용하는 프로토콜이다.
- IPX(Internetwork Packet eXchange) 라는 프로토콜이다.
- 스타크래프트를 배틀넷에 접속해서 하는 경우, 즉 인터넷에 접속한 게이머들과 게임을 하는 경우에는 TCP/IP를 사용하지만, 같은 게임방에서 친구들끼리 편을 나누어 게임을 하는 경우에는 IPX라는 프로토콜을 사용한다.
- IPX도 컴퓨터가 통신하는 방법 중 하나이고, 또 서로 게임을 할 수 있는 건 바로 이 프로토콜을 사용하기 때문이다.

12. TCP/IP

- Transmission Control Protocol/Internet Protocol의 약자인 TCP/IP는 ARPATET에 의해서 처음 개발되었다.
- 각각의 네트워크에 접속되는 호스트들은 고유의 주소를 가지고 있어서 자신이 속해 있는 네트워크뿐만 아니라 다른 네트워크에 연결되어 있는 호스트까지도 서로 데이터를 주고받을 수 있도록 만들어져 있는 것이 특징이라고 할 수 있다.
- 이때 사용하는 호스트들의 고유 주소는 Internet Network Information Center(InterNIC)란 단체에서 관리 분배되고 있다.



Thank You