

## LAN(Local Area Network)과 WAN(Wide Area Network)

Lan이란, 'Local Area Network'의 약자로 Local, 즉 '어느 한정된 공간에서 네트워크를 구성하는 것이다.

예를 들어 한 사무실에 컴퓨터가 30대 있는데, 이것들을 네트워크로 구성한다면 '사무실에 LAN을 구축한다'라고 말한다. 또 PC방에서 각 PC를 네트워킹하는 것을 LAN을 구축한다고 하는 것이 맞다.

LAN과 비교되는 말로 WAN이 있다. WAN은 'Wide Area Network'의 약자로서 '멀리 떨어진 지역을 서로 연결하는 경우'에 사용한다. 요즘은 모두 인터넷을 쓰는 세상이니 인터넷에 접속하는 것은 WAN이라고 봐야 한다.

즉, LAN은 한정된 지역 안에서의 네트워크 구축이고, WAN은 서로 멀리 떨어진 곳을 네트워크로 연결하는 것이다.

### 1. 이더넷(Ethernet)

이더넷은 네트워킹의 한 방식이다. 즉 네트워크를 만드는 방법의 하나라고 생각하면 된다. 이러한 이더넷 방식의 가장 큰 특징은 CSMA/CD라는 프로토콜을 사용해서 통신한다는 것이다. 지금 우리나라에서 사용하고 있는 네트워킹 방식의 대부분이 바로 이런 이더넷 방식이기 때문에 이더넷에 대해 어느 정도 알아야 한다.

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 사야 하는 네트워크 장비들이 다르다.

CSMA/CD는 'Carrier Sense Multiple Access/collision Detection'을 줄여서 부르는 방식이다. 이더넷 환경에서 통신하고 싶은 PC나 서버는 먼저 지금 네트워크상에 통신이 일어나고 있는지를 확인한다. 우리 네트워크 자원을 쓰고 있는 PC나 서버가 있는지를 확인해보는 것이다. 즉 캐리어(네트워크상에 나타나는 신호)가 있는지를 감지하는 것이다. 이때 만약 캐리어가 감지되면, 자기가 보낼 정보가 있어도 못 보내고 기다린다. 그러다가 네트워크에서 통신이 없어지면 자기 데이터를 네트워크상에 실어서 보내게 된다.

그런데 만약 네트워크상에서 두 PC나 서버가 보낼 데이터를 가지고 눈치를 살피고 있었다고 가정하자. 그러다가 네트워크상에서 통신이 일어나지 않고 있다는 것을 알아내고 바로 자신의 데이터를 네트워크상에 동시에 실어서 보냈다고 생각해보자. 이더넷에서는 이렇게 2개 이상의 PC나 서버가 동시에 네트워크상에 데이터를 실어 보내는 경우가 발생할 수 있는데 이 경우를 바로 'Multiple Access(다중 접근)'라고 한다.

통신에서 이렇게 2개의 장비가 데이터를 동시에 보내려다 부딪치는 경우를 충돌(콜리전, Collision)이 발생했다고 한다. 따라서 이더넷에서는 데이터를 네트워크에 실어서 보내고 나서도 혹시 다른 PC 때문에 콜리전이 발생하지 않았는지를 잘 점검해야 한다. 그것이 바로 'Collision Detection(충돌감지)'이라는 것이다. 만약 콜리전이 발생하게 되면 데이터를 전송했던 PC들은 랜덤(Random)한 시간 동안 기다린 후 다시 데이터를 전송하게 된다. 15번을 했는데도 계속 충돌이 나게 되면 그냥 포기하게 된다.

따라서 이더넷에서 충돌, 즉 콜리전이 발생하는 것은 이더넷의 CSMA/CD라는 특성상 자연스러운 일이지만, 너무 많은 충돌이 발생하게 되면 통신 자체가 불가능해지는 경우도 생길 수 있습니다.

## 2. 토큰링(TokenRing)

토큰링 방식의 네트워크에서 데이터를 전송하고자 하는 PC는 이더넷처럼 자기 맘대로 보내고 싶을 때 남들이 전송만 하지 않고 있으면 막 보내는 게 아니다. 그 네트워크에서 오직 한 PC, 즉 토큰을 가진 PC만이 네트워크에 데이터를 실어 보낼 수 있다(한 네트워크에 토큰은 대부분 하나이지만 몇 개씩 가질 수도 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. 그러므로 토큰링에서는 당연히 충돌(Collision)이 발생하지 않는다. 또한, 네트워크에 대한 성능을 예측하기도 쉽다.

단점도 있다. 내가 지금 바로 보내야 할 데이터가 있고, 다른 PC들은 보낼 데이터가 하나도 없다고 하더라도 차례가 올 때까지 계속 기다려야 된다. 비록 다른 PC들은 보낼 데이터가 없더라도 토큰은 계속 옆으로만 전달되기 때문이다. 참고로 토큰링 프로토콜은 IBM이 처음 개발을 하였다.

## 3. UTP(Unshielded Twisted-pair)

네트워크를 설치하다 보면 자주 문제가 생기는 부분은 장비보다는 케이블인 경우가 많다. 따라서 케이블에 대한 이해는 꼭 필요한 부분이다. 여기에서 케이블이란, 전화 케이블이나 전원 케이블이 아니고 통신 케이블을 말한다.

통신 케이블들은 장비와 장비의 연결에는 어디에나 들어간다. 즉 PC에서 허브나 스위치까지의 연결, 스위치와 스위치의 연결, 스위치와 라우터의 연결, 라우터와 라우터의 연결 등 네트워크 장비와 네트워크 장비를 연결하기 위해서는 어떤 종류의 케이블이든 반드시 케이블이 들어가게 된다. 이렇게 들어가는 케이블은 광케이블, UTP 케이블, 동축 케이블 등 종류도 여러 가지이다.

UTP 케이블은 우리가 가장 많이 사용하는데 거의 모든 사무실과 게임방이 사용하고 있다. 일단 TP 케이블이란 Twisted-pair, 즉 ‘꼬인 쌍’이라는 것이다. 페어(페어는 한 쌍, 즉 두 가닥을 의미)가 서로 꼬여 있는 것을 말한다. 그래서 ‘TP’라고 하는 것이다. TP에는 UTP와 STP가 있다. UTP는 Unshielded(언세드, 즉 감싸지 않음) TP를 말한다. 주로 우리가 사용하는 케이블이 바로 UTP이다. STP는 Shielded로 케이블 주위를 어떤 절연체로 감싸서 만든 것을 말한다. STP가 좀 더 비싸고 성능이 좋다. EMI를 줄였다고 한다.

기존에 워낙 UTP로 구성된 네트워크가 많았기 때문에 결국은 UTP가 중심을 이루게 되었고, STP는 주로 토큰링 쪽에 많이 쓰이고 있다. 그렇다면 우리가 보통 말하는 카테고리라고 하는 것은 무엇을 의미하는 것일까?

- **카테고리 1** : 주로 전화망에 사용하는 용도로 만들어진 케이블이다. 따라서 데이터 전송용으로는 맞지 않는다.
- **카테고리 2** : 데이터를 최대 4Mbps의 속도로 전송할 수 있는 능력을 갖추고 있는 케이블이다.
- **카테고리 3** : 10 Base T 네트워크에 사용되는 케이블이다. 전에는 UTP 케이블이라고 하면 바로 이 케이블을 이야기할 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 갖추고 있다.
- **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, 아직 많이 사용되고 있진 않지만 앞으로 점점 더 많이 사용될 케이블이다. 이제 곧 10Gbps가 일반화되고 나면 좀 더 자주 보게 될 케이블이기도 하다.

#### 4. 케이블 종류

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. 그다음에 나오는 Base란 말은 이 케이블이 Baseband용 케이블이라는 것을 알려준다. 원래 케이블 종류에는 베이스밴드(Baseband)와 브로드밴드(Broadband)가 있는데, 쉽게 생각해서 베이스밴드는 디지털 방식이고, 브로드밴드는 아날로그 방식이라고 생각하면 된다.

그다음 T자리는 원래 케이블의 종류 또는 이 케이블이 전송할 수 있는 최대 거리가 나오게 되어 있다. 즉 10 Base T에서는 케이블의 종류가 나온 것이다. 그래서 T란, TP(Twisted Pair) 케이블이라는 것을 나타낸다. 이것이 바로 우리가 보통 사용하는 UTP 케이블을 나타낸다. 만약 맨 뒷자리에 위에서처럼 글자가 나오지 않고 숫자가 나오면, 예를 들어 '10 Base 5' 일 때 맨 뒤에 나오는 숫자는 최대 통신 거리이다. 따라서 최대 500m까지 통신할 수 있다는 것을 뜻한다. 즉 10 Base 5 케이블은 10M의 속도로 최대 500m까지 전송이 가능한 케이블을 말한다. 그런데 이 케이블은 전에는 많이 썼지만, 요즘에는 쓰지 않고 있다. 너무 두껍고, 전송 거리도 짧고, 게다가 10Mbps 속도밖에 지원하지 않기 때문이다.

다음은 요즘 우리가 많이 쓰는 케이블이다.

- **10 Base T** : 10Mbps로 통신하고, 최대 전송 거리 100m인 UTP 케이블로, 카테고리 3, 4, 5를 사용할 수 있다. 이 케이블에는 RJ45잭을 사용해서 연결해 준다.
- **10 Base FL** : 10Mbps로 통신하는 케이블인데, 광케이블이다. 즉 뒤에 나오는 FL(Fiber-optic)이 광케이블이란 것을 알려준다. 이 케이블은 ST 커넥터라는 것을 사용해서 연결하고 광케이블은 싱글 모드 또는 멀티 모드 케이블을 사용한다.
- **10 Base 2** : 몇 년 전까지만 해도 이 케이블을 사무실에서 가장 많이 사용하였다. 그런데 요즘은 UTP 케이블에 밀려서 완전히 자취를 감추고 말았다. 이 케이블은 그냥 'Thin 케이블' 이라고도 불렀고 BNC 커넥터를 사용했다.
- **10 Base 5** : 10Mbps 통신을 지원하는 케이블이고 최대 거리는 500m로 두껍게 생겼다고 해서 'Thick 케이블' 이라고 부르거나 색이 노랗다고 해서 '옐로우 케이블' 이라고 부른다. 주로 백본 케이블, 즉 중앙망용으로 천장 위에 설치하고 트랜시버 케이블을 이용

해서 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.

- **10 Base TX** : Category 5 UTP 케이블을 사용하는 케이블이고 최대 거리는 100m, 전송 속도는 100Mbps짜리 케이블이다.
- **100 Base T4** : Category 3 케이블을 가지고 100Mbps용으로 사용할 때 만드는 케이블이다. 그 대신 다른 케이블은 2 페어를 사용하지만, 이것은 4 페어를 전부 사용하는 차이점이 있다.
- **100 Base FX** : 이 케이블은 100Mbps 광케이블을 이용해서 구현하는 건데, 전송 거리가 보통 2km에서 10km까지 가능하고 SC라는 네모난 접속 커넥터를 이용해서 접속한다.
- **1000 Base SX** : 이것은 기가비트, 즉 1,000Mbps의 속도가 나는 케이블이다. Short Wavelength이라는 광케이블을 사용하는데, 최대 전송 거리는 약 270m에서 550m 정도이다.
- **1000 Base T** : 1,000Mbps로 UTP 케이블을 통해 전송하고, 최대 거리는 100m인 케이블 스펙이다. Category 5 케이블을 사용하면 된다. 4 페어를 사용한다.

케이블의 경우 속도가 빨라지면 빨라질수록 전송 거리는 점점 짧아진다.

광케이블은 얇게 생긴 광섬유를 타고 전송이 이루어진다. 여기서 광케이블의 한 가닥을 ‘코어’라고 부르는데, 통신을 위해서는 최소 2코어의 광케이블이 필요하다(수신과 송신에 각각 하나씩 필요하다). 따라서 우리는 광케이블을 이야기할 때 “이게 몇 코어짜리 광케이블이다”라고 말한다.

UTP 케이블은 좀 꼬여 있다. 4가닥으로 보일 수 있지만, 사실은 8가닥으로 2가닥이 하나로 꼬여 있다. 그래서 UTP의 T가 바로 Twist, 즉 꼬였다는 뜻이라고 한다.

## 5. 맥 어드레스(Media Access Control Address)

컴퓨터는 네트워크상에서 어떻게 서로를 구분해서 인식할까? 즉 통신을 위해서는 서로를 구분할 일종의 주소가 필요하다. 이 역할을 담당하는 주소가 바로 MAC 주소이다.

우리는 IP 주소를 사용하니까 IP 주소만 있으면 모든 통신이 일어날 것 같지만, 사실은 IP 주소를 다시 MAC으로 바꾸는 절차(이 과정을 ARP: Address Resolution Protocol이라고 함)를 밟고 있다.

먼저, 단독 네트워크, 즉 라우터를 거치지 않는 하나의 네트워크 안에서의 통신을 생각해 보자. PC Y가 Z와 통신을 하려고 한다. 이때 PC Y는 PC Z의 IP 주소를 알고 있다. 그럼 PC Y는 자기가 속한 네트워크에 있는 모든 PC에 메시지를 보낸다(브로드캐스트).

“우리 네트워크에 혹시 Z라는 녀석이 있으면 내가 통신하고 싶으니까 맥 어드레스 좀 알려주라.” 이렇게 보낸다. 이때 Z는 Y와 같은 네트워크에 있으므로 Y가 보낸 브로드캐스트를 받았을 것이다. 그럼 Z는 Y에게 자신의 맥 어드레스를 알려주게 되고 Y는 Z의 맥 어드레스를 안 다음에 비로소 통신을 시작하게 되는 것이다.

호스트 Z가 라우터를 넘어서 다른 네트워크에서 사는 예도 있다. 이 경우 호스트 Y가 브로드캐스트를 보내도 호스트 Z는 그 메시지를 받아볼 수 없다. 이 경우 앞의 경우처럼 메시지를 보내게 되면 Y와 연결된 라우터는 PC Z의 IP 주소를 보고 이 PC가 우리 네트워크에 살고 있지 않고 따라서 아무도 이 질문에 대답하지 않을 것을 알게 된다. 이것을 알

게 된 라우터는 Y에게 라우터 자신의 맥 어드레스를 보내준다. 따라서 PC Y는 PC Z에게 정보를 보낼 때 받는 맥 어드레스를 라우터의 맥 어드레스로 해서 보내게 된다. 그럼 그 정보를 라우터가 받은 후 Z가 사는 해당 네트워크로 넘겨주는 것이다. 그곳에 사는 라우터에 전달을 해주고 그곳에 사는 라우터는 다시 자기 네트워크 안에 있는 PC Z의 맥 어드레스를 찾게 된다. 그리고 PC Z의 맥 어드레스를 알아낸 후 Z의 맥 어드레스를 이용해서 전달하게 된다.

네트워크(여기서는 이더넷)에 붙는 장비들은 48bit(6octet, 여기서 옥텟이란 8개의 비트를 묶은 것을 말한다.)의 주소를 갖게 되는데, 이 주소는 랜카드 또는 네트워크 장비에 이미 고정되어 있는 주소이고 유일한 주소이다. 이 주소를 바로 ‘맥 어드레스’ 또는 ‘하드웨어 주소’라고 한다. 모든 랜의 디바이스들은 반드시 유일한 맥 어드레스를 가져야 한다. 따라서 랜카드 하나하나마다 서로 다른 맥 어드레스가 있고 또 라우터나 스위치에도 맥 어드레스가 들어있다. 물론 서버에도 들어있다.

맥 어드레스는 8자리마다 하이픈(-)이나 콜론(:), 점(.)으로 구분되기도 한다. 예를 들어 00-60-97-8F-4F-86, 00:60:97:8F:4F:86, 0060, 978F, 4F86 과 같이 나타낸다. 이진수로 표시하면 너무 길고 복잡해서 관리하고 기억하기가 불편하므로 보통은 16진수로 표시하게 된다.

이때 이 주소에서 앞쪽 6개의 16진수가 벤더, 즉 생산자를 나타내는 코드로, 이 코드를 ‘OUI(Organizational Unique Identifier)’라고 한다. 즉 이 코드는 메이커에 따라 다르므로 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. 이렇게 만들어진 어드레스는 통신하는데 가장 중요한 요소로 사용된다.

## 6. 유니캐스트, 브로드캐스트, 멀티캐스트

유니캐스트, 멀티캐스트, 브로드캐스트 등, 이 캐스트 3형제는 한마디로 네트워크에서 통신하는 방식에 따른 구분이라고 생각하면 된다. 즉 1대 1로 하는 통신 방식이나, 어떤 그룹을 대상으로 하는 통신 방식이나, 아니면 전부를 대상으로 하는 통신 방식이나 하는 것이다.

### ▶ 유니캐스트(Unicast)

네트워크를 분석해보면 이 3가지의 통신이 모두 사용되고 있는데, 그중에서도 현재 우리가 네트워크상에서 가장 많이 사용되는 트래픽이 무엇인가 하면 바로 유니캐스트이다.

유니캐스트란, 우리가 랜에서 통신한다고 할 때 데이터를 보내고자 하는 PC의 맥 어드레스가 A라고 가정하고, 받는 PC의 맥 어드레스가 B라고 가정한 경우이다. 일단 통신을 위해서는 전송되는 프레임 안에 항상 출발지와 목적지의 주소, 즉 맥 어드레스가 들어있어야 한다. 따라서 위의 경우 프레임 안에 출발지는 A로, 그리고 목적지는 B라고 써넣는 것이다. 이러한 방식이 유니캐스트 통신 방식이다.

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 PC들에 정보를 뿌리는 Shared 방식이기 때문에 그 로컬 네트워크상에 있는 모든 PC는 일단 이 프레임을 받아들여서 랜카드에서 자신의 맥 어드레스와 비교하게 된다. 그다음 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 올려보내게 된다.

#### ▶ 브로드캐스트(Broadcast)

브로드캐스트는 한마디로 로컬 랜에 붙어있는 모든 네트워크 장비들에 보내는 통신이다. 여기서 로컬 랜이란, 라우터에 의해서 구분된 공간, 즉 브로드캐스트 도메인이라고 하는 공간을 뜻한다. 브로드캐스트는 통신의 대상이 특정한 어떤 한 네트워크 장비가 아니고 내가 사는 네트워크 안의 모든 네트워크 장비들에 통신할 때 쓰기 위한 방식이라고 생각하면 된다. 받는 사람이 이 브로드캐스트 도메인 안에 사는 모든 네트워크 장비들이다. 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. 그다음 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.

처음 두 PC 간에 통신하는 경우에는 상대방의 맥 어드레스를 모르기 때문에 이 경우에 상대의 맥 어드레스를 알아내기 위해서 하는 동작이 바로 ARP(Address Resolution Protocol)이다. 이 ARP가 바로 브로드캐스트이다. 그럼 그 IP 주소를 가진 사람이 대답한 후 자신의 맥 어드레스를 보내게 되는데, 이런 과정을 ARP라고 한다.

#### ▶ 멀티캐스트(Multicast)

멀티캐스트는 보내고자 하는 그룹 멤버들에게만 한 번에 보낼 수 있으므로 유니캐스트처럼 여러 번 보낼 필요도 없고, 브로드캐스트처럼 받기 싫어하는 사람에게까지 보낼 필요도 없다. 그 그룹에 속해있는 사람들에게만 선택적으로, 그것도 한 번에 보낼 수 있다.

멀티캐스트는 라우터나 스위치에서 이 기능을 지원해야지만 쓸 수 있다. 만약 라우터나 스위치가 멀티캐스트를 지원하지 않는다면 라우터의 경우는 이러한 멀티캐스트를 마치 브로드캐스트처럼 취급해서 다 막아버리고 스위치의 경우는 모든 포트에 뿌려버린다. 멀티캐스트는 그룹에 포함되고 또 그룹에서 빠져나가는 것을 정의하기 위해 몇 가지 기술을 사용한다. 또한, IP 주소도 클래스 D를 사용한다.

## 7. OSI 7 Layer(레이어, 계층)

통신에 관한 국제적인 표준기구인 International Organization for standardization(ISO)이라는 곳에서 만든 OSI 7 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) : 트랜스포트 계층에서 하는 중요한 일은 주로 플로 컨트롤과 에러 복구 기능이다. 즉 에러 복구를 위해 패킷을 재전송하거나 플로를 조절해서 데이터가 정상적으로 전송될 수 있도록 하는 역할을 한다.
- Network Layer(네트워크 계층) : 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 장비이다.

- **Data Link Layer(데이터 링크 계층)** : 피지컬 레이어를 통하여 송, 수신되는 정보의 오류와 흐름을 관리하여 안전한 정보의 전달을 수행할 수 있도록 도와주는 역할을 한다. 따라서 통신에서의 오류도 찾아주고 재전송도 하는 기능이 있을 뿐만 아니라 맥 어드레스를 가지고 통신할 수 있게 해준다. 이 계층에서 전송되는 단위를 우리는 ‘프레임’이라고 부른다. 이 계층에 속하는 대표적인 장비에는 브리지, 스위치 등이 있다.

- **Physical Layer(피지컬 계층)** : 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 예러가 있는지, 어떻게 보내는 것이 더 효과적인지 하는 것은 전혀 관여하지 않는다. 이 계층에 속하는 대표적인 장비는 통신 케이블, 리피터, 허브 등이 있다.

이렇게 계층을 나눈 이유는 첫 번째로 데이터의 흐름이 한눈에 보인다는 것이다. 즉 우리가 사용하는 애플리케이션 계층부터 맨 마지막 피지컬 계층까지를 나누어 놓으니까 어떻게 데이터가 날아가는지 보기가 쉽다.

두 번째는 문제를 해결하기가 편리하다. 네트워크에서 문제가 발생하면 이 문제 하나를 7개의 작은 문제로 나눈 후 그 문제를 해결하면 훨씬 쉽다는 것이다.

세 번째는 이렇게 계층을 7개로 나누고 층별로 표준화를 하니까 여러 회사 장비를 써도 네트워크가 이상 없이 돌아가는 것이다. 즉 케이블은 국산, 랜카드는 인텔, 스위치나 라우터는 시스코를 써도 계층별로 나누어졌기 때문에 아무 이상 없이 네트워크를 쓸 수 있는 것이다.

## 8. 프로토콜(Protocol)

컴퓨터의 대화에서도 사용하는 언어가 서로 같은 컴퓨터끼리만 대화, 즉 통신할 수 있다. 바로 이때 프로토콜(Protocol)이란 얘기가 나온다. 프로토콜이란, 우리말로 하면 규약, 협약과 비슷한 뜻인데, 컴퓨터끼리는 프로토콜이 서로 같은 그것끼리만 통신할 수 있다.

인터넷을 사용하기 위해서는 모든 PC가 TCP/IP라는 프로토콜을 사용해야 한다. 인터넷을 사용하는 모든 PC가 바로 이 프로토콜을 사용하기 때문에 인터넷을 접속할 수 있는 것이다. 다시 한번 더 정리하자면 프로토콜이란, 컴퓨터끼리 서로 통신하기 위해서 꼭 필요한 서로 간의 통신 규약 또는 통신 방식에 대한 약속으로, 프로토콜이 같은 것끼리만 대화, 즉 통신할 수 있다.

프로토콜에도 여러 종류가 있다. TCP/IP는 Transmission Control Protocol/Internet Protocol의 약자이다. TCP/IP는 인터넷에서 사용하는 프로토콜이다. 그다음은 IPX(Internetwork Packet exchange)라는 프로토콜이다. 예를 들자면, 스타크래프트를 배틀넷에 접속해서 하는 경우, 즉 인터넷에 접속한 게이머들과 게임을 할 때는 TCP/IP를 사용하지만, 같은 게임방에서 친구들끼리 편을 나누어 게임을 할 때는 IPX라는 프로토콜을 사용한다. IPX도 컴퓨터가 통신하는 방법의 하나고, 또 서로 게임을 할 수 있는 건 바로 이 프로토콜을 사용하기 때문이다. 그리고 매킨토시가 사용하는 AppleTalk가 있다. ‘맥’이라고도 부르는 매킨토시들이 서로 간의 통신을 위해 사용하는 프로토콜이 바로 애플토크이다.