네트워크 기초 지식

용어 정리

#컴퓨터_네트워크 : 두 대 이상의 컴퓨터가 연결되어 컴퓨터 간에 필요한 데이터를 서로 주고받는 것으로 네트워크로 표현한다. (= 컴퓨터 간의 연결)
#인터넷 : 세계 최대 규모의 네트워크로 전 세계 컴퓨터를 서로 연결하여 정보를 교환할 수 있도록 만든 하나의 거대한 컴퓨터 통신망

패킷

#패킷 : 컴퓨터 간에 데이터를 주고받을 때 네트워크를 통해 전송되는 데이터의 작은 조각으로 네트워크에서 전송하는 데이터의 기본 단위
#대역폭 : 네트워크에서 이용 가능한 최대 전송 속도로 정보를 전송할 수 있는 단위 시간당 전송량

네트워크나 인터넷에서 데이터를 패킷으로 나누어 보내는 규칙을 사용한다.

- 큰 데이터를 전송하면 네트워크 대역폭을 너무 많이 차지해서 다른 패킷의 흐름을 막을 수 있기 때문
- 목적지에서는 원래 데이터로 되돌리는 작업을 수행 (이를 위해 송신 측에서 패킷을 보낼 때 패킷에 순서를 부여하고 수신 측에서는 순서대로 조합)

비트와 바이트

#디지털_데이터 : 컴퓨터에서 사용하는 0과 1의 집합
#비트 : 0과 1의 정보를 나타내는 최소 단위
#바이트 : 컴퓨터에서 데이터를 다룰 때 사용하는 기본 단위로 8비트
#문자_코드 : 숫자와 문자의 대응표로 0과 1을 사용하는 컴퓨터가 문자를 인식할 수 있게 해준다. ex. ASCII(아스키 코드) - A : 65

LAN과 WAN

네트워크를 접속할 수 있는 범위에 따라 #LAN 과 #WAN 으로 나눌 수 있다.
#LAN : Local Area Network(근거리 통신망)의 약자로, 지리적으로 제한된 공간을 범위로 하는 네트워크 ex. 가정이나 사무실 등
#ISP : Internet Service Provider(인터넷 서비스 제공자)의 약자로 인터넷 상용 서비스 사업을 하는 KT, U+, SK 브로드밴드와 같은 통신 회사를 말함.
#WAN : Wide Area Network(광역 통신망)의 약자로, 지리적으로 넓은 범위에 구축된 네트워크 ex. 서울과 부산 사무실을 연결하는 네트워크 등
-> 해당 연결이 가능한 이유? ISP가 LAN과 LAN의 연결을 서비스로 제공

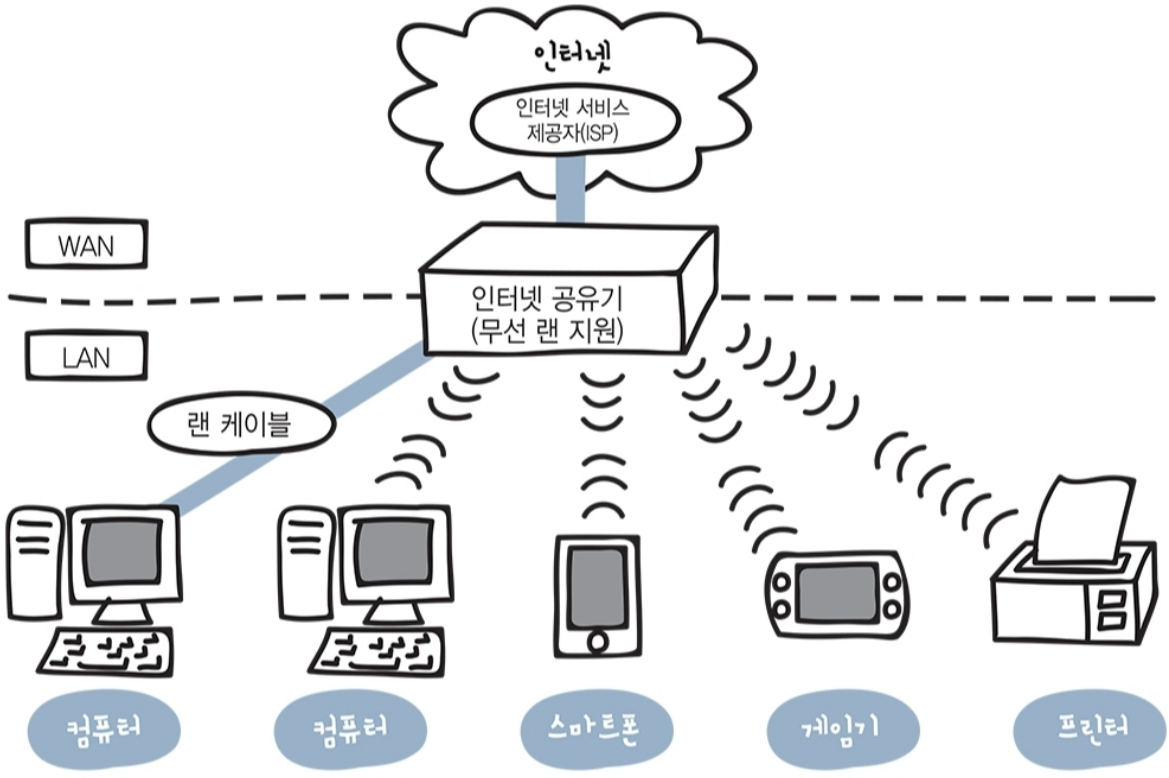
=> WAN은 넓은 범위의 네트워크이자, ISP가 제공하는 서비스를 통해 구축된 네트워크이자 LAN과 LAN을 연결하여 구축된 네트워크

❓ ISP는 어떻게 LAN과 LAN을 연결했지?

LAN과 WAN 비교

	LAN	WAN
범위	좁다 : 지리적으로 제한된 공간	넓다 : LAN과 LAN을 연결
속도 : 거리가 멀어질수록 속도가 떨어진다	빠르다	느리다
오류 : 거리가 멀어지면 신호가 약해지거나 오류가 발생하기 쉽다	적다	많다

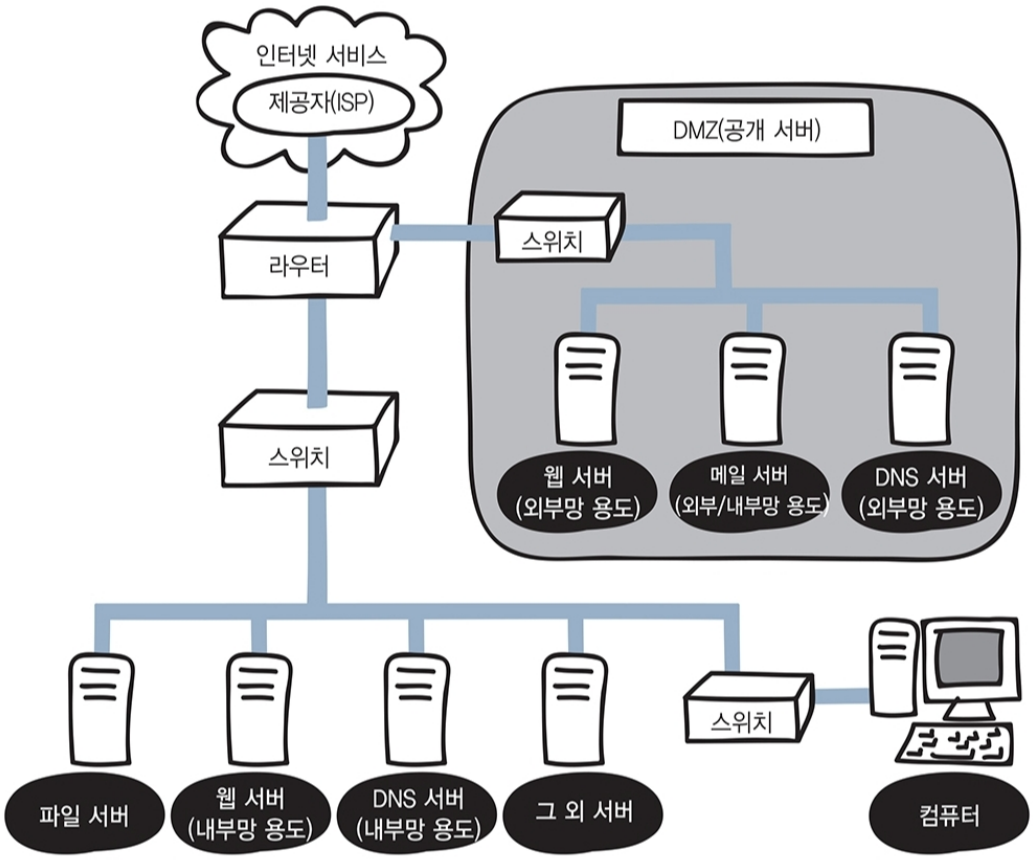
가정에서 하는 LAN 구성



가정용 네트워크는 LAN -> ISP와 인터넷 회선을 결정해야 한다.
#공유기 : ISP와 가정용 네트워크를 연결하기 위한 장치, 가정용으로 만든 일종의 라우터인데 최근에는 라우터 기능뿐만 아니라 허브, 스위칭 허브, 방화벽 등의 기능을 제공한다.

LAN의 연결은 LAN 케이블이 필요한 지에 따라 유선 LAN과 무선 LAN으로 나뉜다.

회사에서 하는 LAN 구성



#소호기업 : SOHO(Small Office/Home Office)의 약어로 소규모 회사를 의미
#DMZ : DeMilitarized Zone의 약어로 외부 네트워크와 내부 네트워크 사이에 위치한 중간 지대를 의미하며 네트워크 보안 영역으로 외부 공격자가 내부 네트워크에 침투하는 것을 막는 역할을 한다.
#서버 : 네트워크에서 다른 컴퓨터에 서비스를 제공하기 위한 컴퓨터 또는 프로그램
#크라이언트 : 서버에서 보내주는 정보를 받거나 요구하는 측의 컴퓨터 또는 프로그램

서버의 운영

#클라우드 : 인터넷을 통해 소프트웨어나 하드웨어 등의 컴퓨팅 서비스를 제공하는 것으로 인터넷에 접속하기만 하면 언제 어디서든 이용할 수 있다.

서버는 사내에 설치하거나 데이터 센터에 두거나 클라우드에 둘 수 있다.

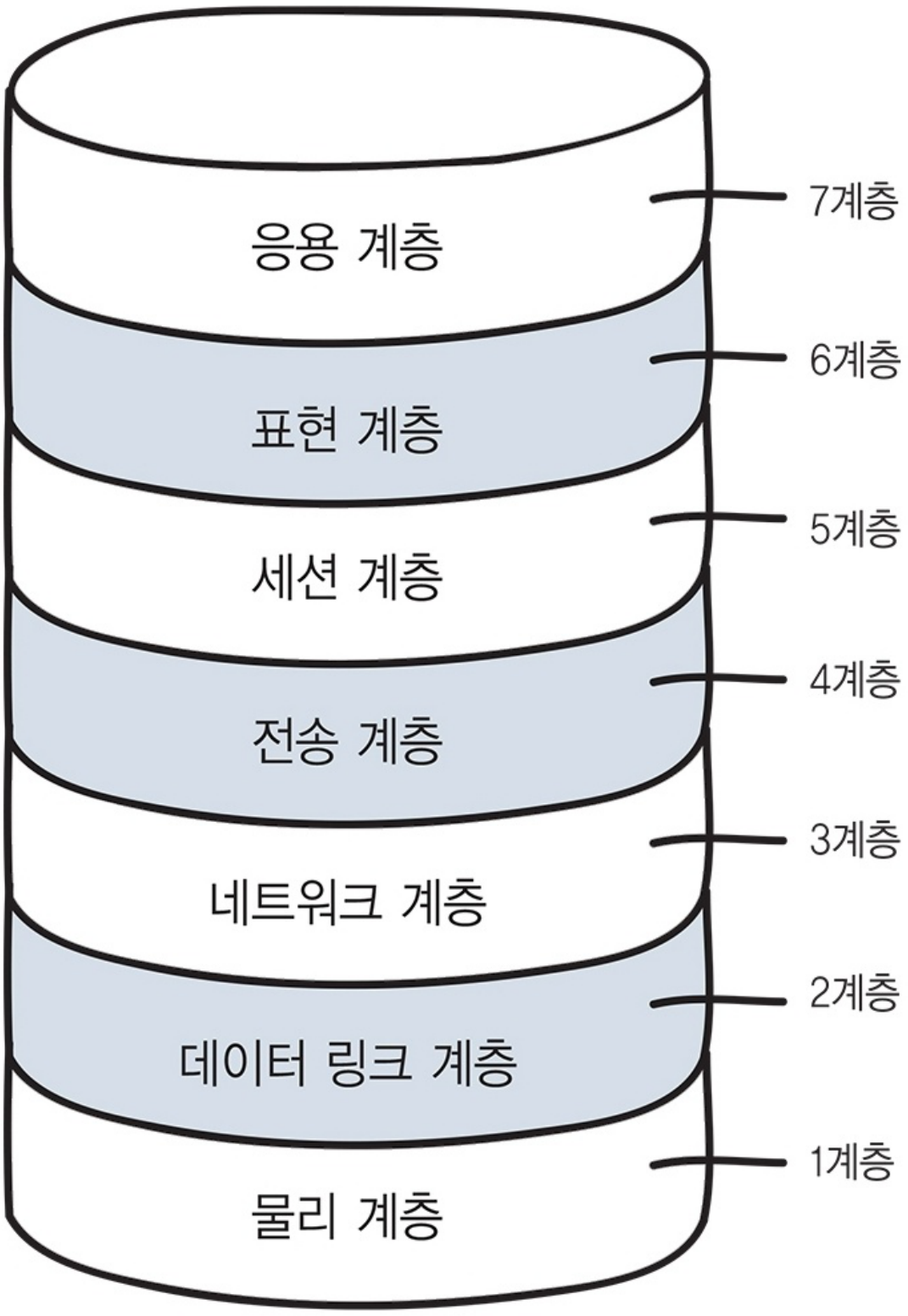
- 사내 설치와 데이터 센터의 이용은 #온프레미스 라고도 부른다.

프로토콜

#프로토콜 : 통신 방법에 대한 규칙이나 표준

OSI 모델

#OSI_모델 : 국제 통신 표준 규약으로 네트워크 기본 구조를 일곱 개 계층으로 나누어 표준화한 통신 규약이다.
등장 배경 : 같은 회사 컴퓨터나 케이블 연결 커넥터끼리 통신이 가능한 시절이 있었고, 공통으로 사용할 수 있는 표준 규격의 필요성이 대두되었다.
-> ISO(International Organization for Standardization)라는 국제 표준화 기구가 OSI 모델이라는 표준 규격을 재정했다.



데이터를 전송할 때는 상위 계층에서 하위 계층으로 데이터를 전달하고, 데이터를 수신할 때는 하위 계층에서 상위 계층으로 각 계층을 통해 전달된 데이터를 받는다.

TCP/IP 모델

#TCP/IP_모델 : OSI 모델 7계층의 네트워크를 4계층으로 단순화하여 사용하는 모델, 인터넷 모델

캡슐화와 역캡슐화

#캡슐화 : 통신에서 상위 계층의 프로토콜 정보를 데이터에 추가하여 하위 계층으로 전달하는 기술

- 데이터를 보낼 때 데이터의 앞부분에 헤더(데이터를 전송하는 데 필요한 정보)를 붙이는 과정
  #역캡슐화 : 상위 계층의 통신 프로토콜에서 하위 계층에서 추가한 정보와 데이터를 분리하는 기술
- 데이터를 수신할 때 헤더를 제거하는 과정
  #헤더 : 저장되거나 전송되는 데이터의 맨 앞에 위치하는 추가적인 정보 데이터로 데이터의 내용이나 성격을 식별 및 제어하는 데에 사용된다.
  #트레일러 : 데이터를 전달할 때 데이터의 마지막에 추가하는 정보

VPN

#VPN : Virtual Private Network(가상 사설망)의 약어

- 가상 통신 터널을 만들어 기업 본사나 지사와 같은 거점 간을 연결하여 통신하거나 외부에서 인터넷으로 사내에 접속하는 것을 말함
- 인터넷 VPN, IP-VPN 두 종류가 있다.

보안을 위한 VPN 사용
: VPN은 암호화된 터널을 통해 데이터를 전송하기 때문에 개인 정보 보호가 가능하다.

- VPN 없이 인터넷을 이용하면, 사용자가 온라인에서 수행하는 모든 것이 노출된다.
- VPN으로 인터넷을 이용하면, ISP는 VPN을 사용하고 있다는 사실만 알 뿐 IP 등의 정보를 알 수 없음.

요즘의 VPN은 보안을 목적으로 사용

- 과거의 VPN은 멀리 떨어진 네트워크 환경을 하나의 안전한 네트워크로 만드는 도구였다.
- 개인의 프라이버시가 중요시 되면서 좀 더 넓은 의미로 '안전하게 인터넷을 사용하는 도구'로 사용되고 있다.
- 과거에는 멀리 떨어진 네트워크끼리 연결하는 데에 집중하였다면 최근에는 안전하게 연결하는 것에 집중하고 있다.
- VPN으로 안전하게 연결할 수 있는 이유
  - VPN은 네트워크 패킷을 암호화하여 VPN 서버에 보내고, VPN 서버가 사용자 대신 인터넷에 접속하여 결과를 돌려준다. 사용자의 컴퓨터와 VPN 서버 사이에는 암호화되어 외부에서 내용을 볼 수 없기 때문에 안전하다.

- VPN 장점
  - 데이터 제한, 대역폭 제한 방지
    - ISP가 데이터 제한 및 대역폭 제한을 걸 수 있는데, VPN을 사용하면 사용 중인 데이터 양을 알 수 없고, 사용자의 장치에서 송수신되는 데이터를 알 수 없기 때문에 해당 제한을 방지할 수 있다.
  - 지리적 차단 서비스에 엑세스
    - 일부 서비스에서 위치에 따른 서비스를 제공하는데, VPN을 사용하면 다른 IP 주소를 받을 수 있다. 이를 통해 허용된 장소에서 서비스를 사용하는 것처럼 사용할 수 있다.
  - 네트워크 확장성

물리 계층 = 데이터를 전기 신호로 변환

물리 계층의 역할과 랜 카드의 구조

#물리_계층 : 컴퓨터와 네트워크 장비를 연결하고 컴퓨터와 네트워크 장비 간에 전송되는 데이터를 전기 신호로 변환하는 계층

- 데이터를 보내는 쪽은 데이터를 0과 1의 비트열 데이터로 보낸다.
- 비트열 데이터는 전기 신호로 변환되어 네트워크를 통해 데이터를 받는 쪽에 도착한다.
- 전기 신호로 변환은 **랜 카드**가 담당
- 받는 쪽에서는 전기 신호를 다시 비트열 데이터로 복원한다.
  #랜_카드 : 컴퓨터의 네트워크 연결 및 데이터 전송을 담당한다.
- 네트워크 카드 / 네트워크 인터페이스 컨트롤러(NIC)라고도 불린다.

케이블의 종류와 구조

트위스트 페어 케이블

#전송_매체 : 데이터가 흐르는 물리적인 선로 -> 유선/무선

- 유선 : 트위스트 페어 케이블, 광케이블
- 무선 : 라디오파, 마이크로파, 적외선

케이블에 전기 신호가 흐르면 노이즈가 발생하여 전기 신호의 형태가 왜곡된다. 이를 막고 싶다면 실드로 전선을 보호해야 한다.

- #UTP_케이블 : 구리 선 여덟 개를 두 개씩 꼬아 만든 네 쌍의 전선으로 실드 로 보호되어 있지 않는다.
  - 노이즈 영향 받기 쉬운 대신 저렴하여 일반적으로 많이 사용된다.
- #STP_케이블 : 두 개씩 꼬아 만든 선을 실드로 보호한 케이블
  - 노이즈 영향을 덜 받지만 가격이 비싸 잘 사용되지 않는다.

❓ 쌍으로 꼬아서 만드는 이유?
: 일직선의 단선을 사용하면 주변에 강한 전자기 신호가 있는 경우 유도기전력에 의해 전기가 흐르게 되고, 이로 인해 케이블의 신호를 왜곡시킬 수 있기 때문에 쌍으로 꼬여 있는 선을 사용하여 전자기적 간섭을 상쇄한다.

#실드 : 금속 호일이나 금속의 매듭 같은 것으로 외부에서 발생하는 노이즈를 막는 역할 담당
#트위스트_페어_케이블 : #랜_케이블 이라고도 불림
#RJ-45 : 랜 케이블 양쪽 끝에 붙은 커넥터로 다양한 네트워크 기기에 연결할 때 사용

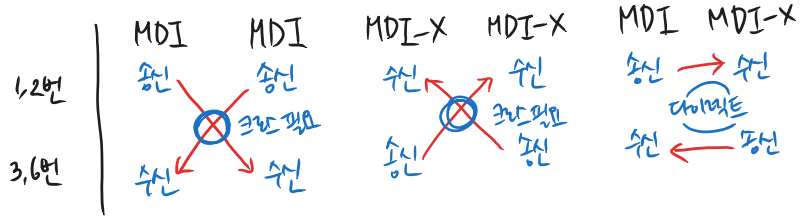
다이렉트 케이블 / 크로스 케이블

랜 케이블에는 #다이렉트_케이블 과 #크로스_케이블 이 있다.

- 컴퓨터, 라우터는 MDI 인터페이스를, 스위치, 허브는 MDI-X 인터페이스를 사용
- MDI끼리 / MDI-X 끼리의 연결에는 크로스 케이블을, MDI와 MDI-X의 연결에는 다이렉트 케이블을 사용한다.
- 최근에는 케이블 배선 실수로 인한 통신 문제를 해결하기 위해 MDI와 MDI-X의 차이를 자동으로 판단하여(auto MDIX) 연결 신호를 전환하는 기능을 가진 스위치나 허브를 사용한다.

다이렉트 케이블과 크로스 케이블

1. 각 케이블이 사용되는 상황
   - 일반적으로 같은 계층의 네트워크 장비와 통신할 때나 다른 기기와 통신할 때는 #다이렉트_케이블 을,
   - 다른 계층의 네트워크 장비와 통신할 때나 다른 기기와 통신할 때는 #크로스_케이블 을 사용한다.
2. 케이블이 사용되는 상황이 다른 이유
   - 네트워크 장비는 DCE와 DTE로 구분된다.
   - DCE = Data Circuit Equipment로 리피터나 허브처럼 신호를 증폭시키거나 분기하는 역할
   - DTE = Data Terminating Equipment로 서버, PC, 라우터처럼 프레임을 생성하는 장치
   - DCE는 MDI-X를, DTE는 MDI를 사용한다.
   - MDI-X는 1, 2번을 수신, 3, 6번을 송신에 사용
   - MDI는 1, 2번을 송신, 3, 6번을 수신에 사용
   - 양쪽에서 동일한 번호로 데이터를 전송하면 데이터가 충돌할 수 있기 때문에,
   - MDI <-> MDI-X 통신이라면 다이렉트 케이블을 사용해야 송신-수신이 올바르게 연결된다.
   - MDI <-> MDI거나 MDI-X <-> MDI-X라면 크로스 케이블을 사용해야 송신-수신이 올바르게 연결된다.



리피터와 허브의 구조

물리 계층에서 동작하는 네트워크 장비 : 리피터, 허브

#리피터 : 네트워크를 중계하는 장치

- 전기신호를 복원하고 증폭하는 기능을 가진 네트워크 장비
- 리피터 기능을 통해 멀리 있는 대상과도 통신할 수 있게 됨
- 요즘 대부분의 네트워크 장비가 리피터 기능을 지원하게 되면서 리피터의 필요성이 사라짐

#허브 : 가까운 거리에 있는 장비들을 케이블을 사용하여 연결하는 장치

- 리피터처럼 전기 신호를 정형하고 증폭하는 기능 수행
- 리피터 허브라고도 불림
- 여러 개의 포트를 통해 컴퓨터끼리 직접 연결하지 않아도 통신할 수 있게 해주지만, 데이터를 송신한 포트를 제외한 나머지 포트로 데이터를 전달한다. -> 더미 허브라고도 불린다.
- 불필요한 데이터 전송으로 인한 비효율을 개선하기 위해 #스위치 라는 네트워크 장비가 존재한다.

데이터 링크 계층 : LAN에서 데이터 전송하기

데이터 링크 계층의 역할과 이더넷

#이더넷 : LAN에서 데이터를 주고 받는 규칙
#데이터_링크_계층 : 네트워크 기기 간에 데이터를 전송하고 물리 주소를 결정

- LAN에서 정상적으로 데이터를 주고 받기 위해 필요함
- 이더넷 규칙이 일반적

허브로 보는 이더넷 역할

1. 허브를 사용하는 랜 환경에서는 특정 컴퓨터에만 데이터를 보낼 수 없고, 다른 모든 컴퓨터에 전기 신호가 전달된다.
    1. 보내려는 데이터에 목적지 정보를 추가해서 보내고 목적지 외의 컴퓨터는 데이터를 받더라도 무시하도록 설계
2. 컴퓨터 여러 대가 동시에 데이터를 보내면 데이터의 충돌이 발생 가능
    1. 여러 컴퓨터가 동시에 데이터를 전송해도 충돌이 일어나지 않도록 데이터를 보내는 시점을 늦춘다.
    2. **CSMA/CD**(Carrier Sense Multiple Access With Collision Detection : 반송파 감지 다중 접속 및 충돌 탐지의 약어)
    3. CS : 데이터를 보내려는 컴퓨터가 케이블에 신호가 흐르고 있는지 확인
    4. MA : 케이블에 데이터가 흐르고 있지 않다면 데이터를 보내도 된다.

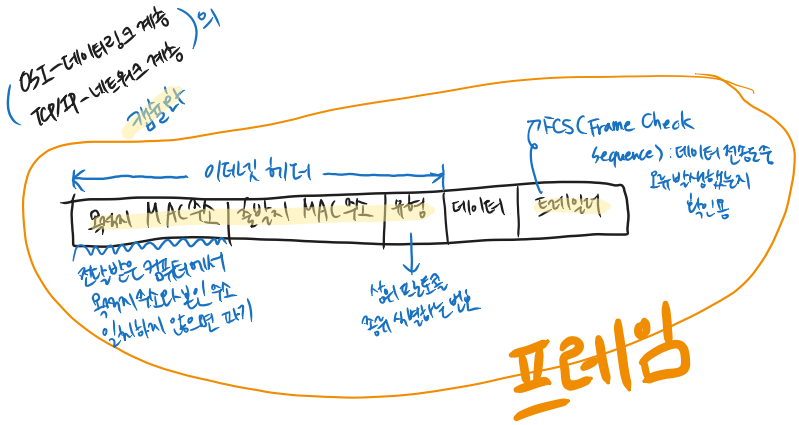
5. CD : 충돌이 발생하고 있는지를 확인한다.
6. 현재는 효율이 좋지 않다는 이유로 #스위치 장비로 대체되고 있다.

MAC 주소의 구조

#MAC_주소 : LAN 카드에 부여된 고유한 번호

- Media Access Control Address의 약어
- 물리 주소라고도 불림
- 전 세계에서 유일한 번호로 할당되어 있다.
  - 중복되지 않게 `LAN 카드 만든 제조사 번호(24비트) + 제조사가 붙인 일련번호(24비트)` 로 이루어짐

MAC 주소를 사용한 통신



OSI 데이터 링크 계층 / TCP/IP 네트워크 계층에서 캡슐화가 일어날 때 이더넷 헤더와 트레일러가 추가된다.

- 데이터에 이더넷 헤더와 트레일러가 붙은 형태를 `프레임` 이라고 한다.
- `이더넷 헤더는 목적지 MAC 주소 + 출발지 MAC 주소 + 유형` 으로 이루어진다.
- 수신한 컴퓨터에서 목적지 MAC 주소가 본인의 주소와 일치하지 않으면 데이터를 파기한다.
- 일치하면 데이터를 수신한다.
- 유형은 상위 프로토콜의 종류를 식별하는 번호가 들어있다.
- 트레일러는 FCS라고도 불리며 데이터 전송 도중에 오류가 발생하는지 확인하는 용도로 사용된다.
  ❓ 트레일러를 헤더에 넣지 않은 이유는 뭐지?

스위치의 구조

#스위치 : LAN을 구성할 때 사용하는 단말기 간 스위칭 기능이 있는 통신망 중계 장치

- 스위칭 허브 또는 레이어 2 스위치라고 한다.
- 데이터 링크 계층에서 동작한다.
- 호스트에서 특정한 다른 장치로 패킷을 보낼 수 있는 기능이 있어 통신 효율이 좋다.

레이어 2 스위치 / 레이어 3 스위치
: 스위치는 OSI 2계층과 3계층에서 쓰일 수 있어 레이어 2 스위치와 레이어 3 스위치로 구분지을 수 있다.

- 레이어 2 스위치는 MAC 주소를 기반으로 데이터를 전달한다.
- 레이어 3 스위치는 IP 주소를 기반으로 데이터를 전달한다.
- 대부분의 스위치는 레이어 2 스위치이다.

스위치의 동작

#MAC_주소_테이블 : 스위치의 포트번호와 MAC 주소가 매핑되어 있는 데이터 베이스

- 브리지 테이블이라고도 불림

0. MAC 주소 테이블에 아무것도 등록되어 있지 않을 때
    1. MAC 주소 학습 기능 발생
    2. 데이터가 전송되면 MAC 주소와 포트를 MAC 주소 테이블에 기입
    3. 플러딩 발생 : 아직 목적지 주소가 등록이 되어 있지 않기 때문에 송신 포트 이외의 포트에 데이터 전송
1. MAC 주소 테이블에 목적지 MAC 주소가 등록되어 있을 때
    1. MAC 주소 필터링 : 목적지에만 데이터 전송

데이터가 케이블에서 충돌하지 않는 구조

전이중 통신과 반이중 통신

통신은 #전이중_통신_방식 과 #반이중_통신_방식 으로 나뉜다.

- 전이중 통신 방식 : 데이터의 송수신을 동시에 진행
    - 서로 다른 회선이나 주파수를 사용하여 데이터 신호가 충돌되는 상황을 방지한다.
- 반이중 통신 방식 : 회선 하나로 송신과 수신을 번갈아가면서 진행
- 전이중 통신 방식은 동시에 데이터를 전송해도 충돌이 발생하지 않지만, 반이중 통신 방식은 데이터를 동시에 전송하면 충돌 발생
- LAN 케이블로 직접 연결 / 스위치 : 전이중 통신 방법
- 허브 : 반이중 통신 방법

허브 대신 스위치를 사용하게 된 이유

- 허브는 목적지에만 데이터를 보내는 것이 아니라 모든 포트에 데이터를 전달하여 비효율적
- 허브는 충돌이 발생할 수 있어 네트워크 지연이 발생
  - #충돌_도메인 : 충돌이 발생할 때 영향이 미치는 범위
  - 허브는 연결되어 있는 컴퓨터 전체가 충돌 도메인
  - 스위치는 하나의 포트가 충돌 도메인
  - 충돌 도메인의 범위가 넓을 수록 네트워크가 지연되기 때문에 충돌 도메인의 범위를 좁히는 것이 중요
  - 연결되는 포트가 많아지면 허브는 충돌 도메인도 커지지만 스위치는 동일
- 스위치는 전송하면서 동시에 수신도 가능하여 효율이 높다.

ARP

#ARP : Address Resolution Protocol의 약자로, 목적지 컴퓨터의 IP 주소를 이용하여 MAC 주소를 찾기 위한 프로토콜

- 네트워크 계층 주소와 데이터 링크 계층 주소 사이의 변환을 담당하는 프로토콜
- `ARP 캐시` : 가장 최근에 변환한 IP 대 하드웨어 주소를 보관하고 있는 RAM의 한 영역

1. 이더넷 프레임을 사용하기 위해선 출발지 컴퓨터가 목적지 컴퓨터의 MAC 주소를 알아야 한다.
2. 목적지 컴퓨터의 MAC 주소를 모를 경우 `ARP 요청` 실행
   1. 네트워크에 브로드 캐스트로 요청을 보냄
3. `ARP 응답` : 지정된 IP 주소를 가진 컴퓨터만 자신의 MAC 주소를 응답으로 보냄
4. 출발지 컴퓨터에서는 MAC 주소와 IP 주소의 매핑 정보를 `ARP 테이블` 이라고 불리는 메모리에 저장
   1. 이후 통신은 ARP 테이블을 참고하여 전송된다.
   2. IP 주소가 변경되면 제대로 통신할 수 없기 때문에 ARP 테이블에서 일정 기간이 지나면 삭제하고 다시 ARP 요청을 수행한다.
   3. 윈도우에서 ARP 명령어
      1. `arp -a` : ARP 캐시 내용 확인

2. `arp -d` : ARP 캐시 강제 삭제

```
C:\Users\lukey>arp -a

인터페이스: 192.168.0.5 --- 0xb
  인터넷 주소           물리적 주소           유형
  192.168.0.1           58-86-94-d1-57-8f     동적
  192.168.0.255         ff-ff-ff-ff-ff-ff     정적
  224.0.0.2             01-00-5e-00-00-02     정적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.251           01-00-5e-00-00-fb     정적
  224.0.0.252           01-00-5e-00-00-fc     정적
  239.255.255.250       01-00-5e-7f-ff-fa     정적
  255.255.255.255       ff-ff-ff-ff-ff-ff     정적
```

이더넷 종류와 특징

이더넷은 케이블 종류나 통신 속도에 따라 다양한 규격으로 분류된다.

`통신 속도 - 전송 방식 - 케이블 종류/케이블 길이`