네트워크 일반

RACOS System

2021.08.23

목차 (Contents)

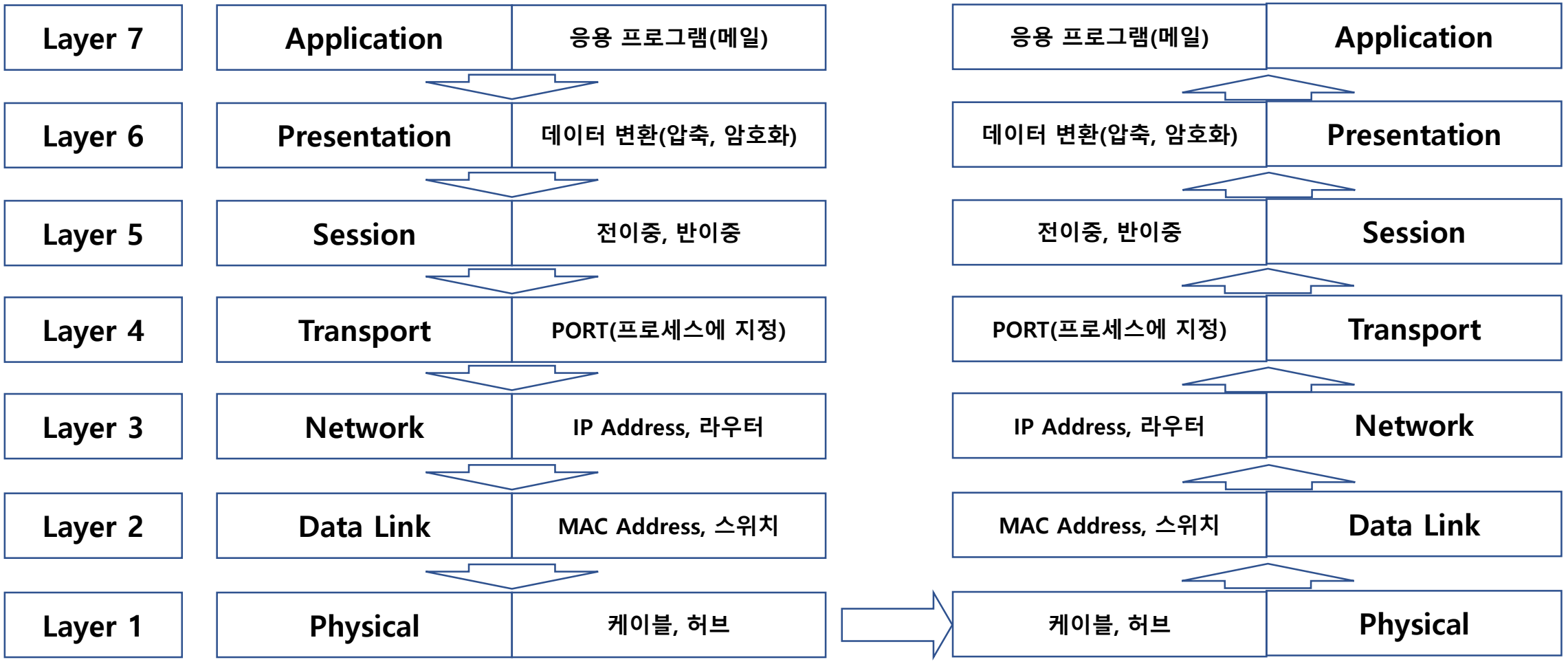
OSI(Open Systems Interconnection) 7 Layer : Overview

OSI 7 Layer : 왜 필요한가?

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

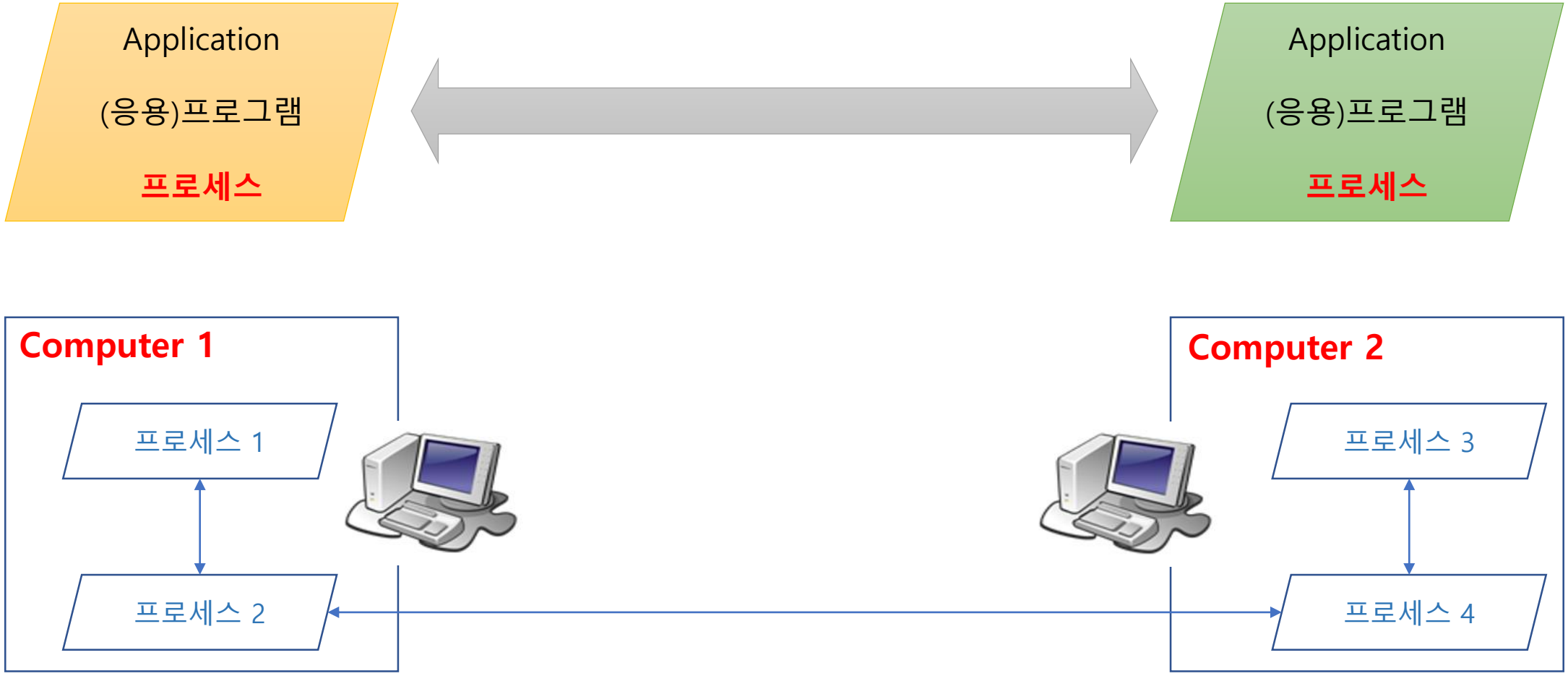
- 국제 표준기구인 ISO 에서 통신에 관한 표준을 수립하기 위해 제정한 것으로 통신이 일어나는 과정을 7개의 단계로 나누었다.
- 데이터의 흐름을 한 눈에 볼 수 있다.
- 네트워크에 문제가 발생할 때 그 원인을 찾는데 용이하다.
- 7개의 단계별로 표준화 하여 그 효율성을 높이기 위한 것이다.
- 이러한 표준화 덕분에 우리는 여러 회사에서 만든 네트워크 장비들을 통합하여 사용할 수 있는 것이다.

OSI 7 Layer : Basic

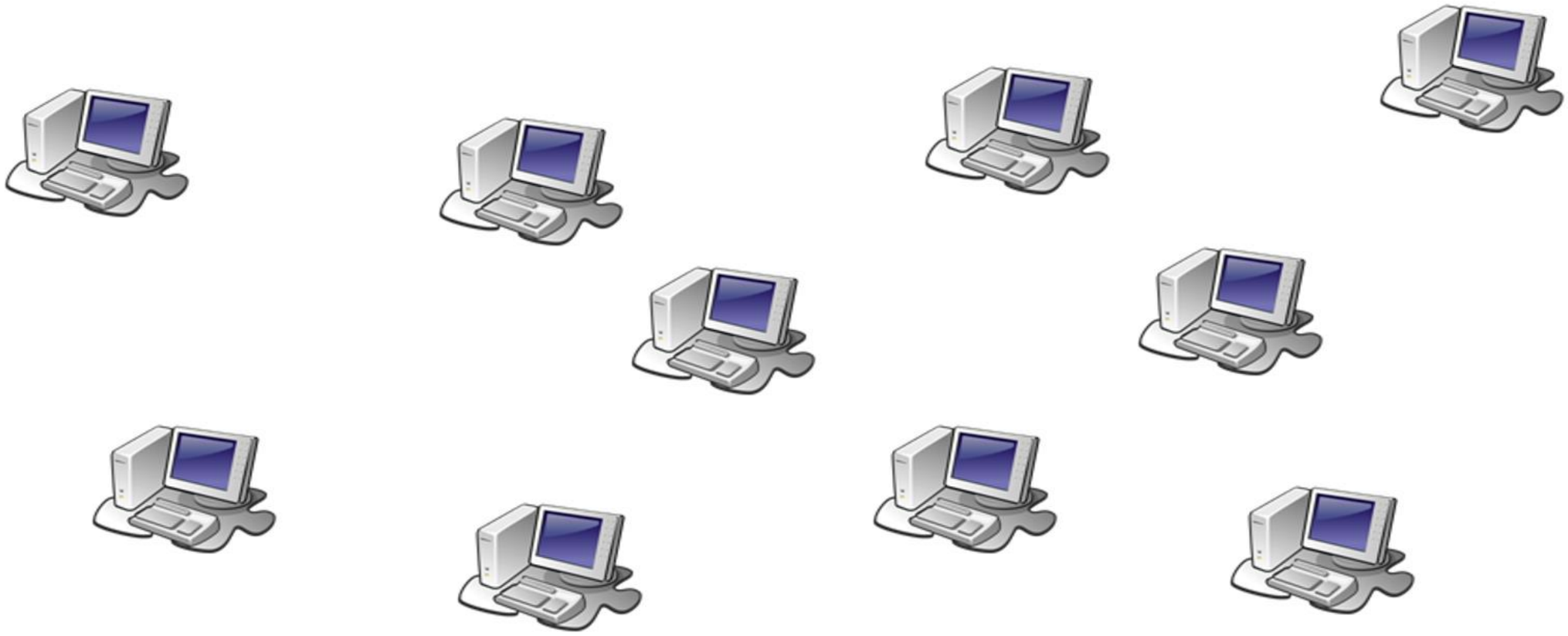


Networking (네트워킹)

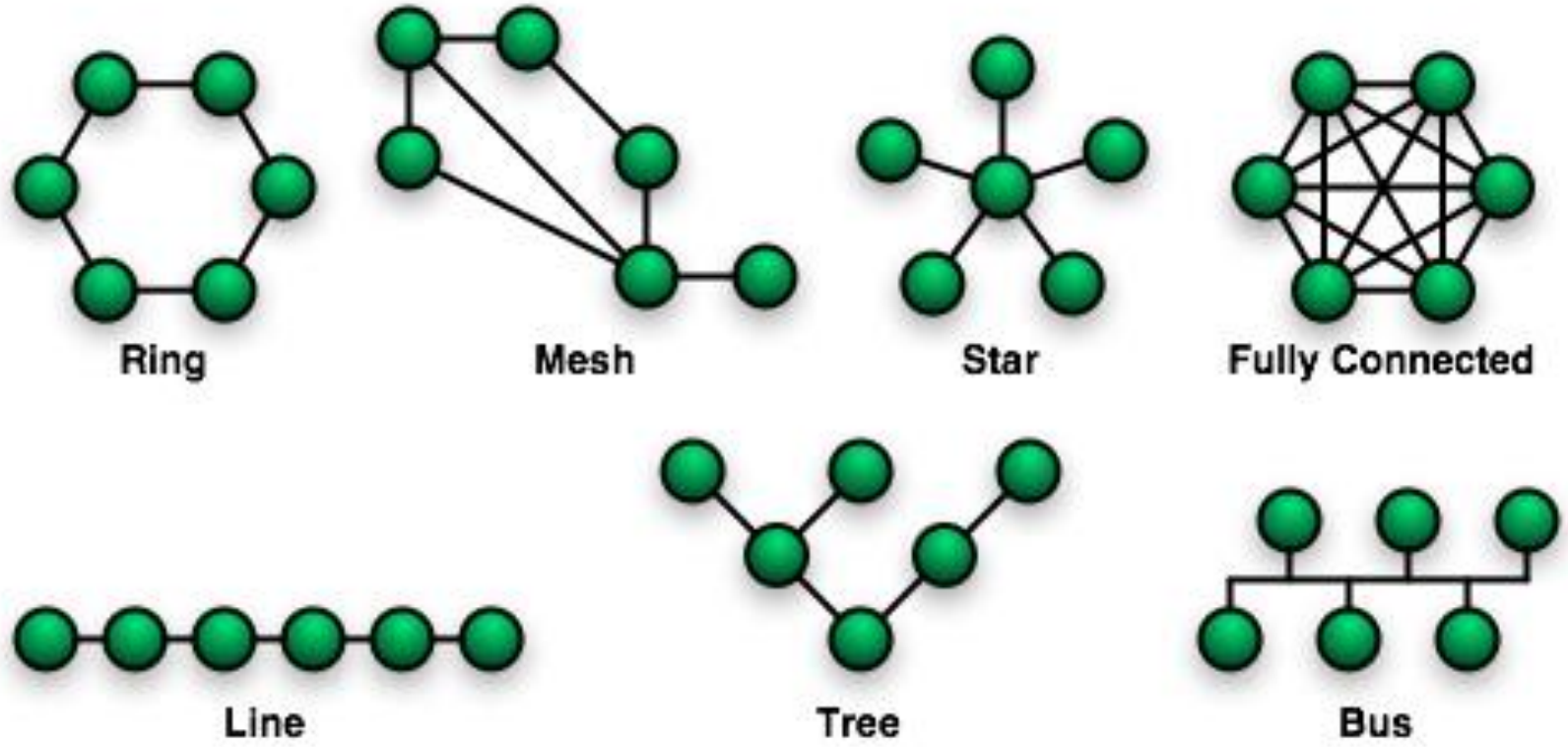
네트워킹(통신) 이란?


Application
(응용)프로그램
프로세스
Application
(응용)프로그램
프로세스
Computer 1
프로세스 1
프로세스 2
Computer 2
프로세스 3
프로세스 4

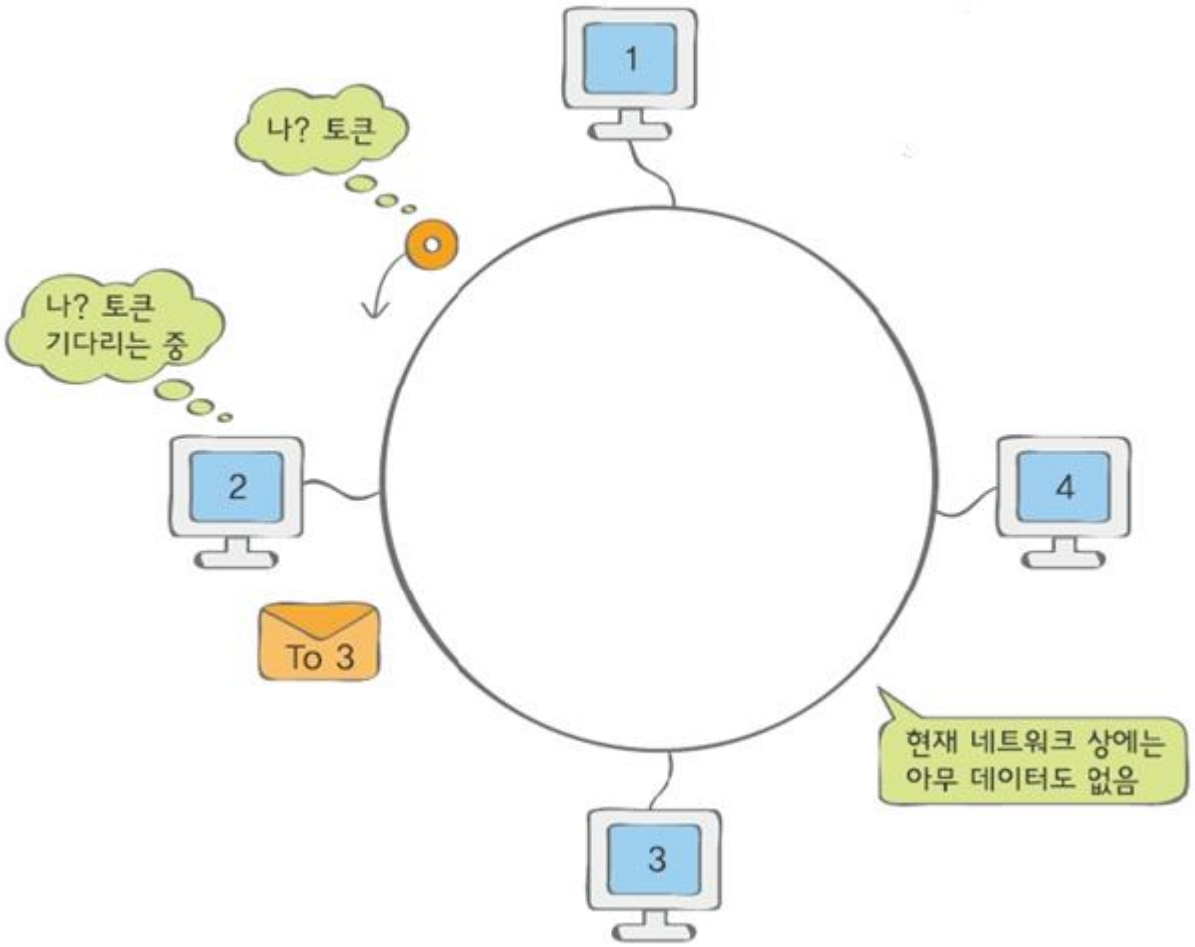
여러 대의 장비와는 어떻게 통신하지?



네트워크 구성 방식 : Topology (토폴로지)



네트워크 통신 방식 : Token-Ring(토큰링)



토큰링은 옆 그림을 보면 쉽게 이해가 간다.

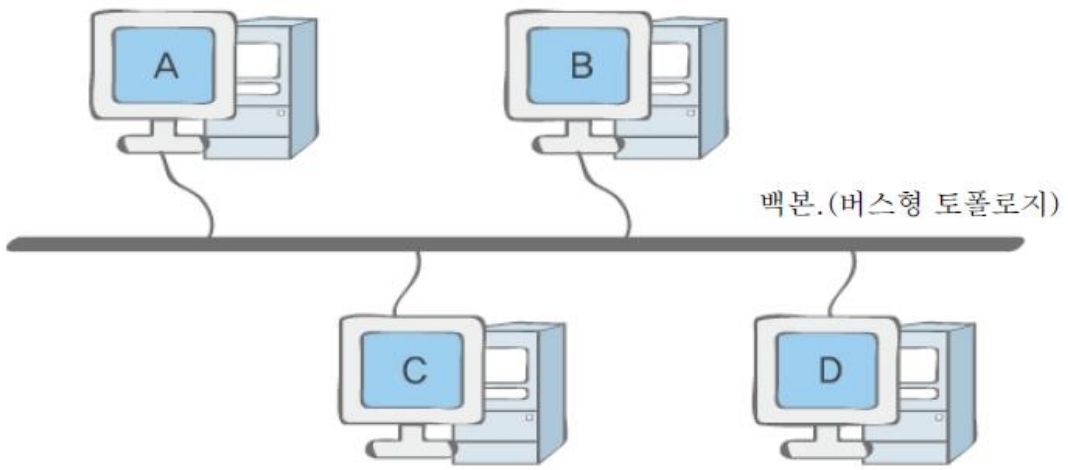
네트워크에서 데이터를 전송하고자 하는 PC는 이더넷처럼 자기 맘대로 보내고 싶을 때 남들이 전송만 하지 않고 있으면 막 보내는게 아니다.

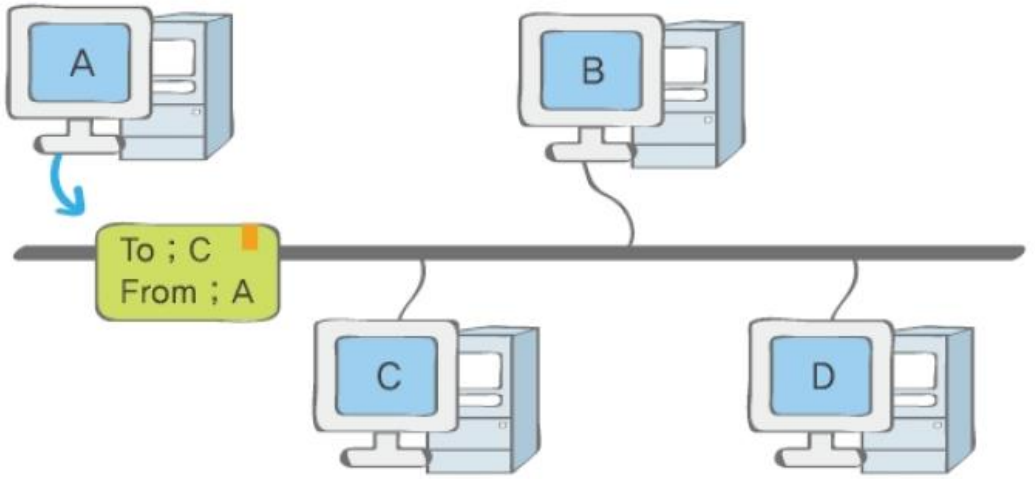
네트워크상에서 오직 토큰을 가진 PC만이 네트워크에 데이터를 실어 보낼 수 있다.

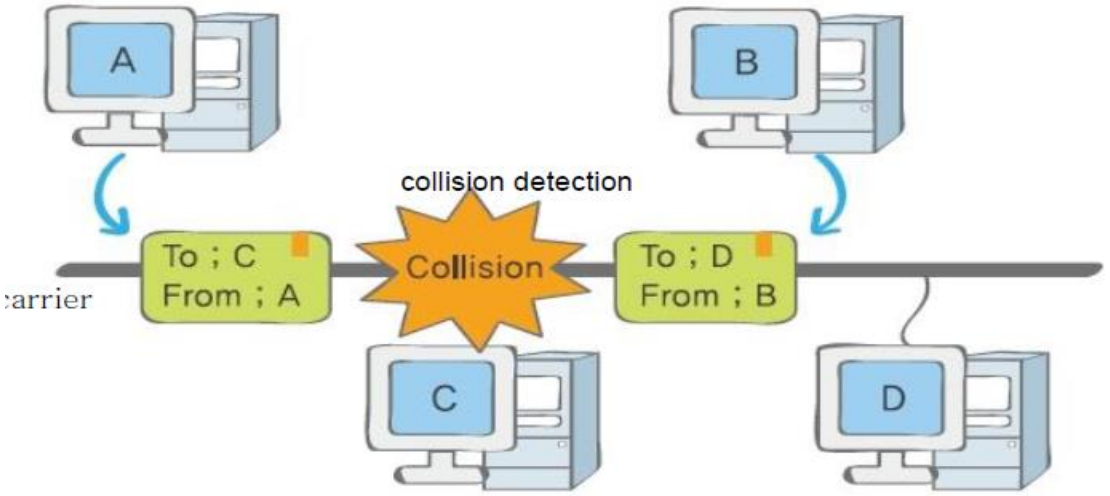
데이터를 다 보내면 토큰을 옆 PC에게 전달되고 이 전달방향은 한방향이다. 따라서 토큰링에서는 충돌이 발생하지 않고 네트워크에 대한 성능을 미리 예측하기도 쉽다.

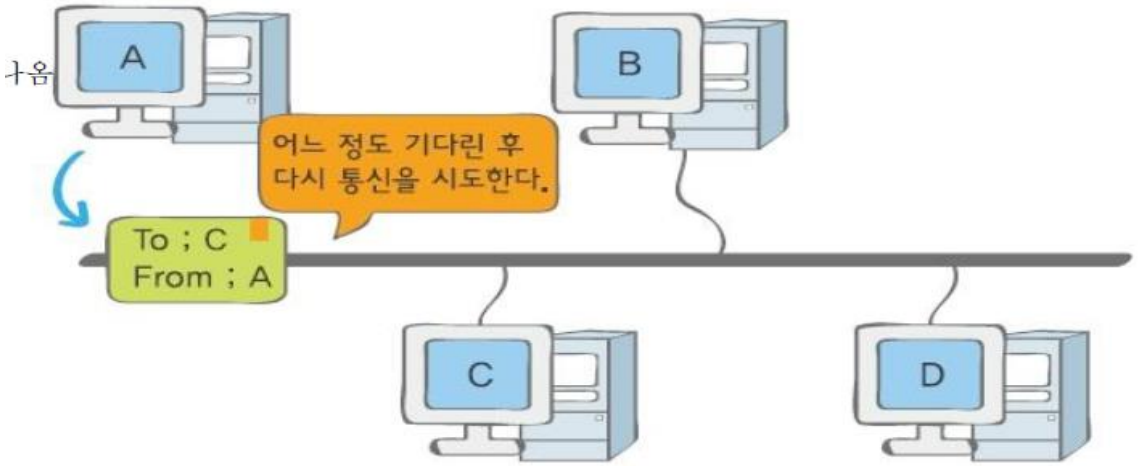
하지만 내가 지금 보내야 할 데이터가 있고 다른 PC들은 보낼 데이터가 하나도 없다고 하더라도 나에게 토큰이 올 때까지 기다려야 한다는 단점이 있다. 이러한 토큰링 방식은 이더넷이 나오고 나서 사라지기 시작했다.

네트워크 통신 방식 : EtherNet(이더넷)









CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

1. Carrier Sense :
현재 네트워크(망)를 쓰고 있는 장비가 있는지를 확인해 보는 것. 만약 캐리어가 감지되면, 다시 말해 누군가가 네트워크 상에서 통신을 하고 있으면 자기가 보낼 정보가 있어도 못 보내고 기다린다. 그러다가 네트워크에서 통신이 없어지면 눈치를 보다가 무조건 자기 데이터를 네트워크 상에 실어서 보낸다.

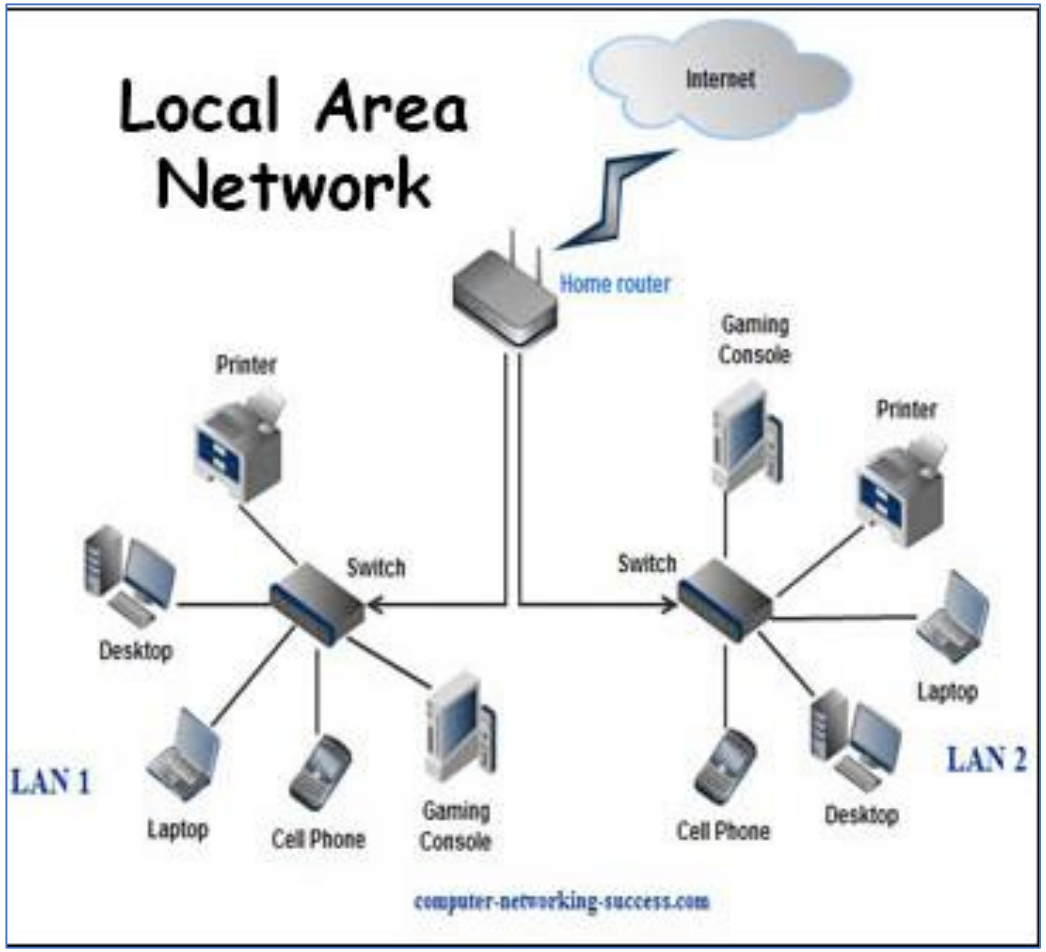
2. Multiple Access :
만약 현재 네트워크 상에서 두 대의 장비가 보낼 데이터를 가지고 눈치를 살피고 있다고 가정해 보자. 네트워크 상에서 통신이 일어나지 않고 있다는 것을 확인하고 바로 두 컴퓨터가 동시에 각자 자신의 데이터를 네트워크 상에 실어서 보내는 경우, 이더넷에서는 이런 경우를 Multiple Access 라고 한다.

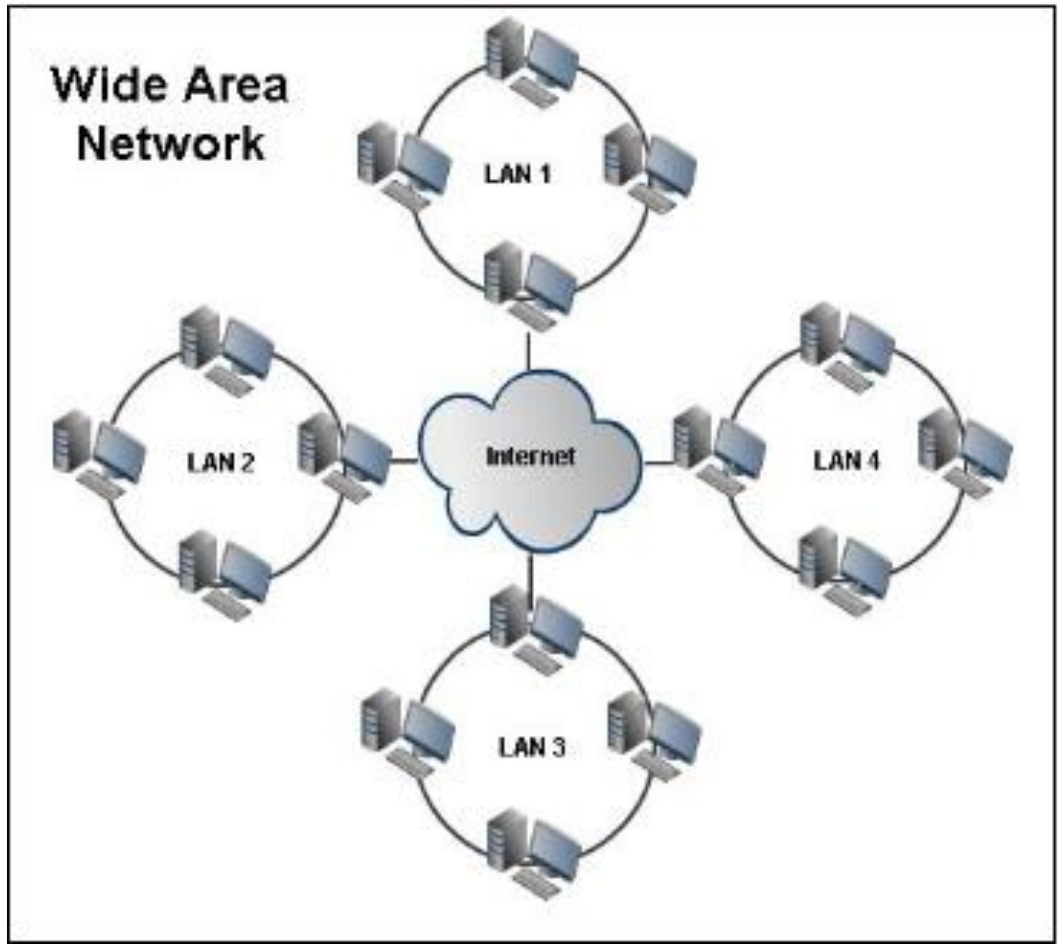
3. Collision Detection :
통신에서 이렇게 두 개의 장비들이 데이터를 동시에 보내다가 부딪치는 경우를 충돌(Collision)이 발생했다고 한다. 따라서 이더넷에서는 데이터를 네트워크에 실어서 보내고 나서도 혹시 다른 PC 때문에 충돌이 발생하지 않았는지를 점검해야 하는데 이것이 Collision Detection 이다

Collision Domain

- 하나의 PC가 데이터를 보내고 있으면 다른 PC는 데이터를 보낼 수 없게 되는 CSMA/CD 효과가 미치는 영역, 즉 Collision이 발생하는 영역을 Collision Domain (콜리전 도메인) 이라고 한다.
- Hub에 붙어 있는 하나의 PC가 Collision이 발생하면 그 Hub에 붙어 있는 모든 PC가 영향을 받는다는 개념이다.
- Collision Detection (충돌 감지) 매커니즘은 NIC에 구현되어 있으며 이는 데이터 송신시 매체에서 다른 호스트와 충돌이 생기는지 확인하는 절차이다.
- 일정 횟수(보통 16회)만큼 시도한 후, 계속 충돌 감지 시 해당 패킷 폐기한다.
- 네트워크 구성 시 Collision Domain 을 최소화 하는 것이 바람직하다.

LAN & WAN


Local Area Network
Internet
Home router
Printer
Gaming Console
Printer
Switch
Switch
Desktop
Laptop
LAN 1
LAN 2
Laptop
Cell Phone
Gaming Console
Cell Phone
Desktop
computer-networking-success.com


Wide Area Network
LAN 1
LAN 2
Internet
LAN 4
LAN 3

MAC (Media Access Control) Address

MAC(Media Access Control) Address

- ✓ 맥(MAC)은 Media Access Control의 약자로, 장비는 네트워크 상에서 통신하려면 서로를 인식할 수 있는 일종의 인식 번호 같은 것이 있어야 하는데 그것이 MAC 주소이다.
- ✓ 표현 형식 : **00-60-97-8F-4F-86** 또는 **00:60:97:8F:4F:86** 또는 **0060.978F.4F86**
- ✓ OUI(Organizational Unique Identifier) : 생산자를 나타내는 코드 (예, 00-60-97)
- ✓ HI(Host Identifier) : 각 메이커에서 각 장비에 분배하여 배정하는 코드 (예, 8F-4F-86)
- ✓ 네트워크 장비에 고정되어 있는 주소이며, 원칙적으로 전세계에서 유일하여야 한다.
  - MAC 등록 및 구매 : https://standards.ieee.org/products-services/regauth/oui/index.html
  - MAC 조회 (OUI) : https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries

2 진수	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1011	1110	1111
10 진수	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16 진수	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

2 진수	0000 0000	0110 0000	1001 0111	1000 1111	0100 1111	1000 0110
16 진수	00	60	97	8F	4F	86

네트워크 전송방식

Unicast

- ✓ Unicast는 1:1로 데이터를 전달하는 통신 방식이다.
- ✓ 구체적으로 데이터를 보내는 PC는, 자신의 MAC Address를 적고, 받는 쪽 PC의 MAC Address도 적어 프레임에 감싸 데이터를 전달한다.
- ✓ 그 다음 같은 지역의 로컬 네트워크 환경은 일반적으로 Shared한 통신 방식을 취하기 때문에, 일단 같은 네트워크 서식지에 있는 모든 PC는 프레임 받게 된다.
- ✓ 각각의 PC는 받는 쪽 MAC Address와 자신의 LAN 카드 MAC Address를 비교하여, MAC Address가 서로 다르다면 CPU에게 보내지 않고 프레임을 폐기 처분한다.
- ✓ 만약 MAC Address가 같다면 PC는 CPU위에 프레임을 올린다(Broadcast 경우 PC 성능이 떨어질 수 있는데, 그 이유는 모든 프레임을 다 CPU에 올리기 때문이다).

Broadcast

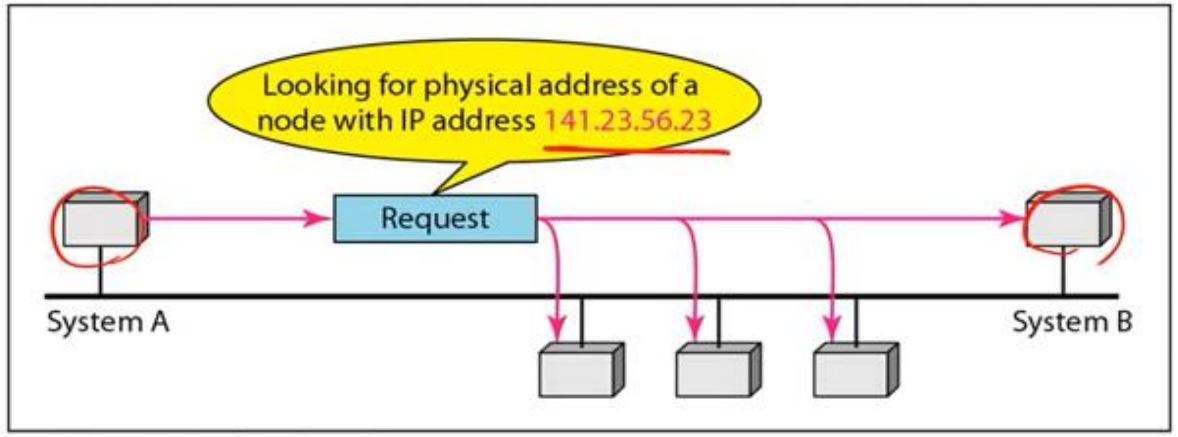
- ✓ Broadcast는 같은 네트워크 서식지에 있는 모든 PC들에게 데이터를 주는 방식이다.
- ✓ 패킷, 프레임을 받는 PC의 MAC Address 주소가 실제 프레임에 적혀 있는 MAC Address와 일치하지 않더라도 폐기하지 않고 CPU에게 인터럽트를 걸어 우선적으로 받은 패킷을 처리하게 한다.
- ✓ 즉, 자신의 LAN 카드 MAC Address 주소와 일치하지 않는 패킷을 받더라도 PC는 CPU에게 패킷을 처리하게 시킨다. 따라서 너무 많은 Broadcast는 같은 서식지의 네트워크에 많은 노드를 발생시켜 혼잡을 야기하며, 그 안에 거주하는 PC의 CPU에 성능을 저하시킬 수 있다. 그럼 보통 이 Broadcast를 왜 이용할까?
- ✓ 만약 받는 PC의 MAC주소는 모르고 IP주소만 알고있을 때 받는 PC의 MAC주소를 알기 위해 Broadcast를 날린다. 즉 같은 네트워크 안에서 "다들 들으세요 여기 이런 IP주소 가진 PC 있으면 알려줘!" 라고 외친다.
- ✓ 그럼 해당 PC는 자신의 MAC주소를 전달해 준다. 결국 IP주소를 MAC주소로 바꾸는 과정 ,얻어내는 과정이를 ARP(Address Resolution Protocol)이라고 한다. 그 외에도 서버가 다수의 클라이언트에게 특정 서비스를 하기 위해서 Broadcast를 사용한다.
- ✓ Broadcast 전송이 닿는 영역을 Broadcast Domain 이라고 하며, 일반적으로 라우터 내의 네트워크를 의미하며, Broadcast용 MAC 주소는 FF-FF-FF-FF-FF-FF

Multicast

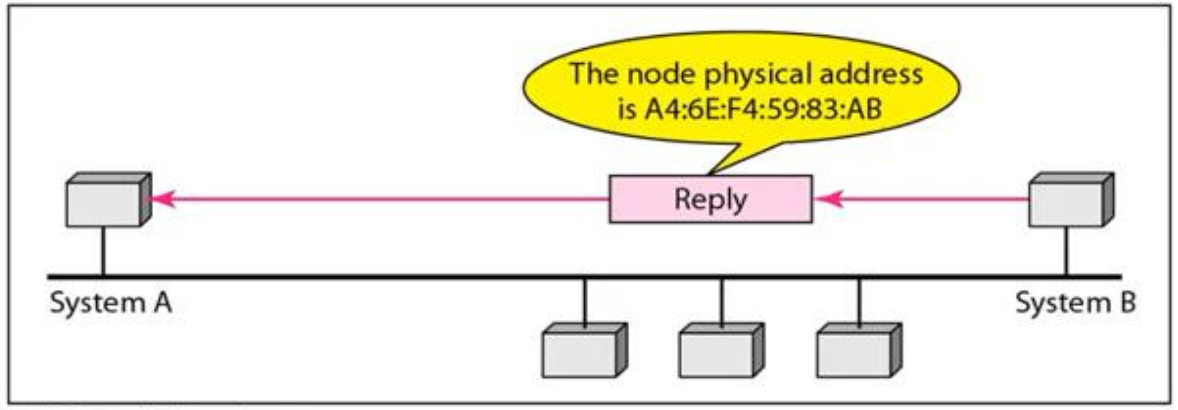
- ✓ 예를 들어, Multicast는 200명에 사용자가 있는 네트워크에서 150명의 사용자에게만 데이터를 주고 싶을 때 사용하는 것으로, 특정 그룹에게 데이터를 보내는 방식이다.
- ✓ Unicast로 150명에게 각각 150번씩 보낼 수 있지만 이것은 서버에게 가혹한 일이다.
- ✓ Broadcast로 한 번에 보낼 수도 있지만, 이것 역시 50명에겐 불필요한 데이터를 주어 CPU에 영향을 준다.
- ✓ 이렇게 특정 그룹에게만 보내는 것을 Multicast 라고 하며, Multicast는 라우터와 스위치가 Multicast 지원을 해줘야 가능하다.
- ✓ 지원하지 않는 라우터는 Multicast를 Broadcast 무조건 버린다. 라우터는 기본적으로 Broadcast를 막는 기능을 가지고 있기 때문이다.
- ✓ 지원하지 않는 스위치는 Multicast를 마치 Broadcast 처럼 모든 포트에게 전부 보내 버린다.
- ✓ Multicast용 MAC 주소 : 01-00-5E-**-**-**

ARP(Address Resolution Protocol)

ARP(Address Resolution Protocol) : LAN 내부



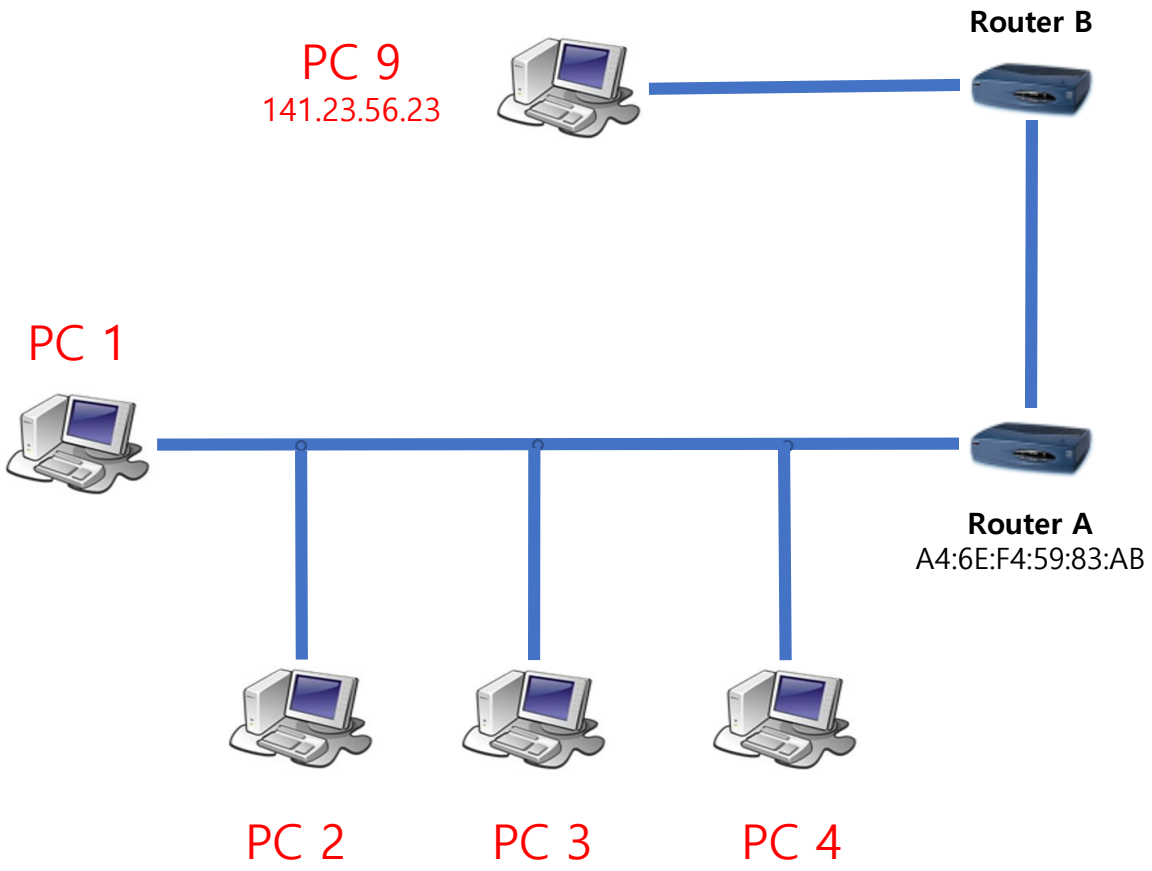
a. ARP request is broadcast



b. ARP reply is unicast

- ✓ ARP란 IP Address를 MAC Address와 매칭시키기 위한 프로토콜이다.
- ✓ 일반적으로 사용하는 IP 주소만 있으면 모든 통신이 될 것 같지만 실제로는 IP주소를 다시 MAC 주소로 바꾸어야 통신이 가능하다.
- ✓ "System A"에서 "System B"로 통신하려고 한다고 가정하자. 이때 "System B"의 IP 주소를 알고 있는 상태이고, 그 주소는 141.23.56.23 이라고 하자.
- ✓ "System A"에서 Broadcast를 이용하여 현재 네트워크(LAN)에 141.23.56.23 IP주소를 가졌으면 MAC주소를 알려 달라고 요청한다. (이때 "System A" MAC 주소를 함께 보낸다)
- ✓ 각 노드는 자기의 IP주소를 확인하고 다르면 반응하지 않고 맞는 노드(System B)가 자기의 MAC 주소(A4:6E:F4:59:83:AB)를 Unicast로 요청자인 "System A" 에게 응답한다.
- ✓ 이후, 보내고자 하는 데이터를 응답 받은 MAC 주소를 이용하여 통신을 시도한다.

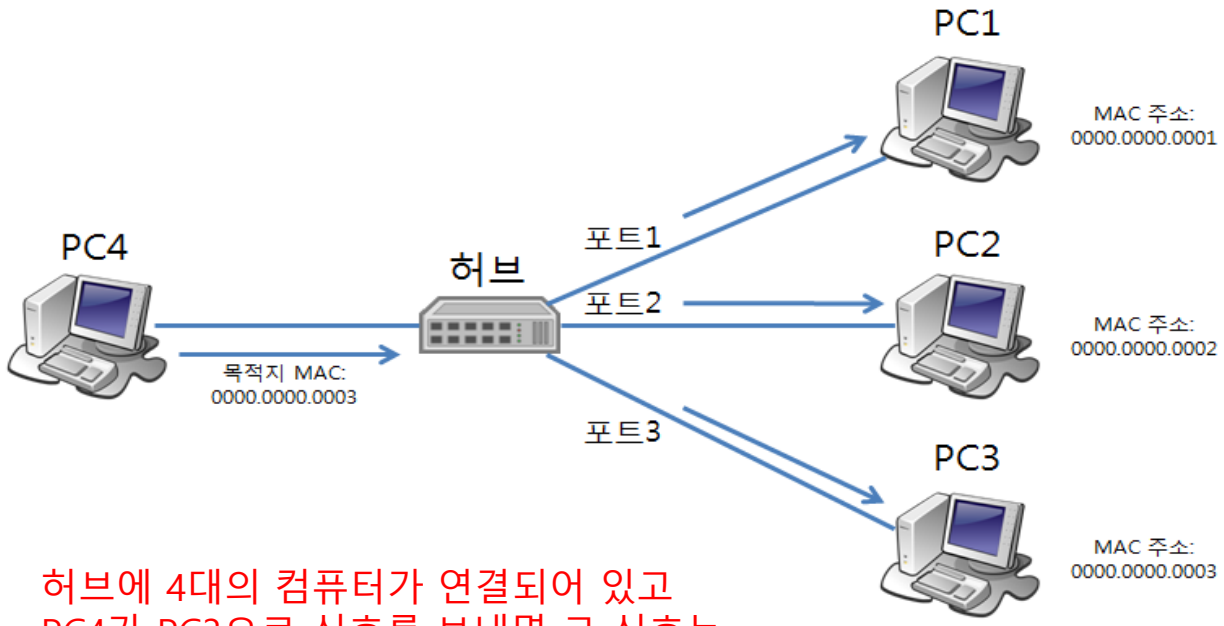
ARP(Address Resolution Protocol) : LAN 외부



- ✓ PC1에서 "IP주소 141.23.56.23 을 갖은 놈(?)이 있으면 MAC 주소를 알려 줘" 라고 현재 네크워크(LAN)에 Broadcast를 보낸다.
- ✓ 그러나 이번에는 "Router A"너머에 그 IP 주소가 있다는 것을 "Router A"가 알고 PC1에게 "Router A" 자신의 MAC Address를 보내 준다.
- ✓ 이후, PC1은 보내고자 하는 데이터를 "Router A"의 MAC Address로 보낸다.
- ✓ 그럼 그 데이터를 "Router A"가 받은 다음 PC9가 있는 네트워크로 넘겨 주기 위해 그 네트워크를 구성하고 있는 "Router B"에게 넘겨 준다.
- ✓ 다시 PC9이 있는 네트워크의 "Router B"가 자기 네트워크에 있는 PC9의 MAC Address 를 앞 페이지의 방식으로 찾게 된다.
- ✓ 이후, PC9의 MAC Address를 이용하여 데이터를 보낸다.

네트워크 장비

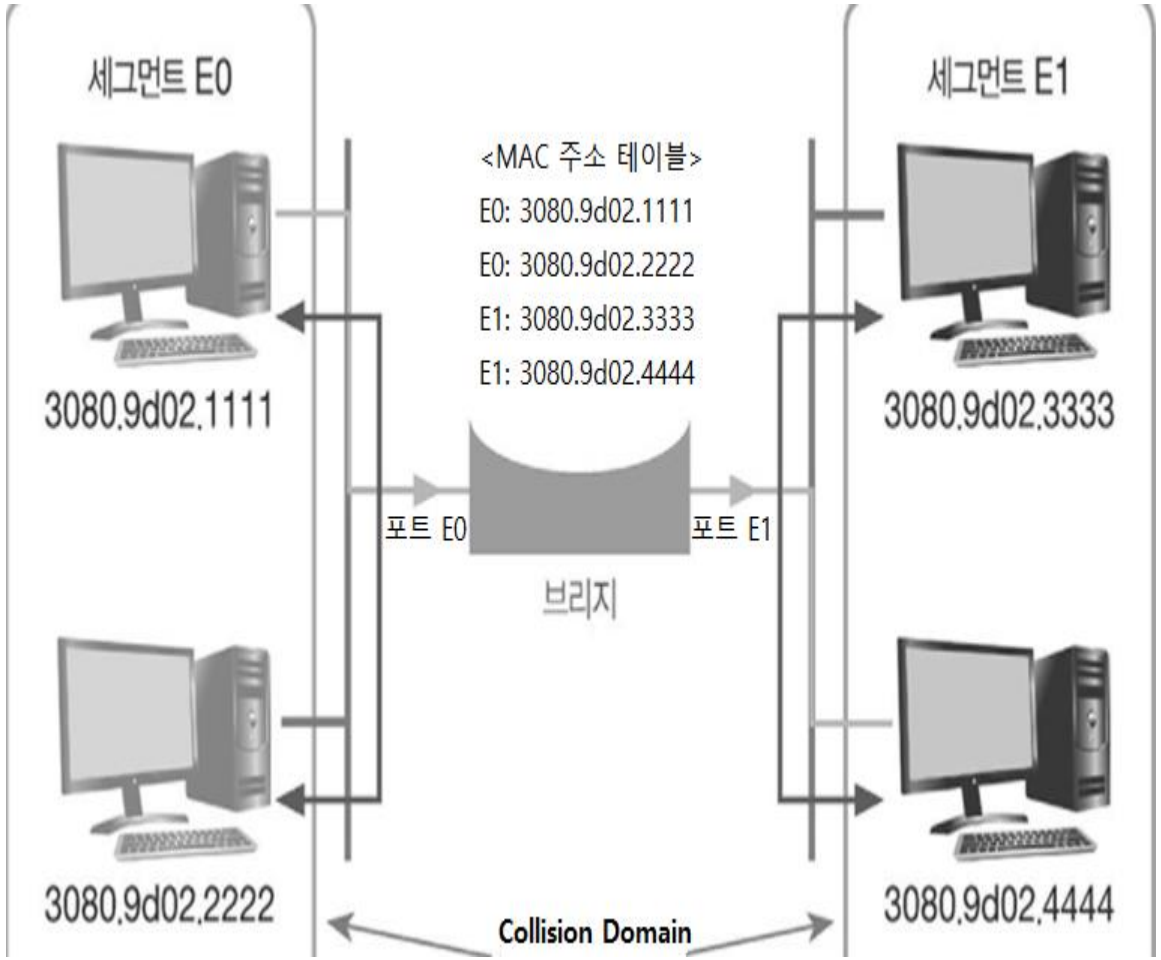
네크워크 장비(Layer 1) : Hub (허브)



허브에 4대의 컴퓨터가 연결되어 있고
PC4가 PC3으로 신호를 보내면 그 신호는
허브에 연결된 모든 컴퓨터로 전송된다.
즉 모두에게 Broadcast 한다는 것이다.

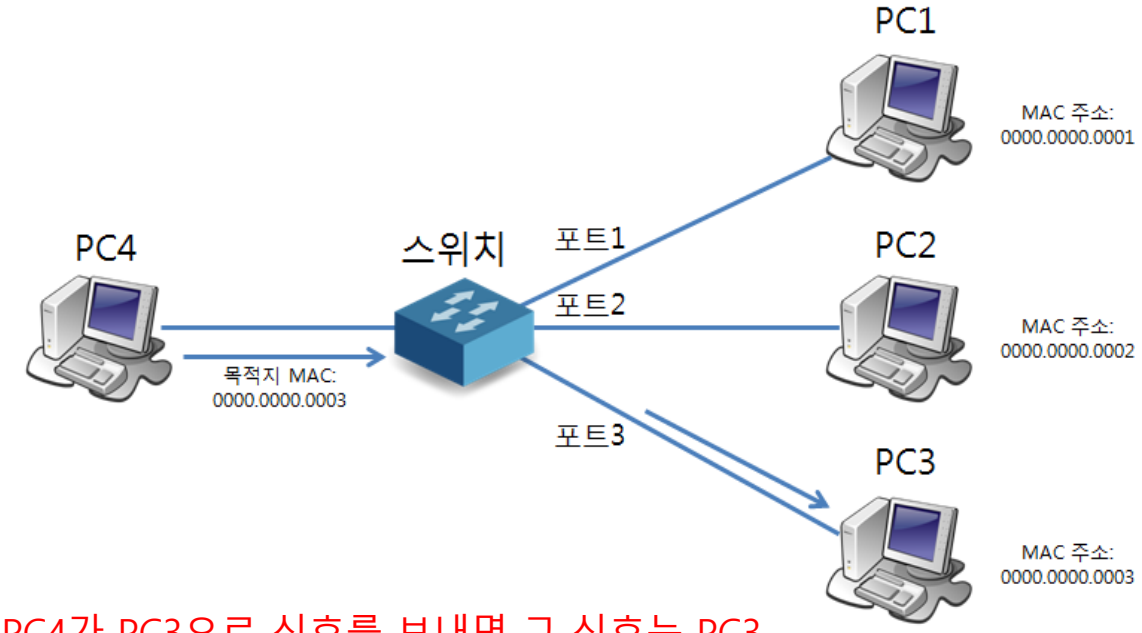
- ✓ 허브와 스위치의 가장 큰 차이점은 각각의 포트에 연결된 컴퓨터나 네트워크 장비의 MAC 주소를 알고 있느냐 이다.
- ✓ 허브의 경우에는 단순히 중계기(멀티포트, 리피터) 역할이며 "더미 허브" 라고도 불린다.
- ✓ 허브는 들어오는 신호의 송신지와 수신지를 구별하지 못하기 때문에 허브를 통해 연결된 모든 컴퓨터에게 신호를 전달한다.
- ✓ 불필요한 트래픽이 발생하므로 대규모 네트워크에는 적합하지 않아 소규모 네트워크에서만 주로 사용된다.
- ✓ 만약 10M의 대역폭을 가진 허브에 컴퓨터가 5대 연결되어 있다면 각 포트에 할당되는 대역폭은 10/5, 즉 2M.
- ✓ 허브를 도로에 비교할 경우, 허브는 왕복 1차선 도로라고 생각하면 된다. 동시에 같은 길에 자동차가 진입하면 사고가 나듯이, 당연히 허브에서도 동시에 신호가 오가면 충돌이 생기게 된다. 따라서 한 쪽 신호가 지나간 후에 다른 포트에서 신호를 보내게 되어 있다.
- ✓ 24 포트 Hub의 Collision Domain 개수는?

네크워크 장비(Layer 2) : Bridge (브리지)



- ✓ 브리지는 스위치의 원조격으로 Collision Domain을 나누어 주는 장비
- ✓ 3080.9d02.1111 PC가 3080.9d02.2222 PC로 통신할 때 3080.9d02.3333 PC가 3080.9d02..4444 PC로 통신 가능하게 하는 장비.
- ✓ 브리지는 Mac주소 테이블을 가지고 있고 이 테이블로 세그먼트 E0와 세그먼트 E1의 통신이 분리되어 Collision domain이 발생하지 않도록 관리한다.
- ✓ 브리지와 스위치는 공통적으로 아래 5가지의 기능 기능을 제공한다.
  - Learning : 송신 측 MAC 주소는 수집 저장한다.
  - Flooding : 모르면(없으면) 들어 온 포트를 제외한 다른 모든 포트에 뿌린다.
  - Forwarding : 해당 포트로 보내 준다.
  - Filtering : 가른 포트로는 못 가게 막는다.
  - Aging : 일정시간(300초, 조정 가능) 동안 통신이 없으면 해당 MAC 주소 삭제하고, 있으면 다시 0초로 초기화하여 시간을 연장해 준다.
- ✓ 브리지는 프레임의 처리를 소프트웨어으로 처리하고, 스위치는 하드웨어로 처리한다.
- ✓ 스위치는 포트별로 다른 속도를 연결해 줄 수 있으나 브리지는 No.
- ✓ 요즘은 거의 스위치로 대체 되었다.

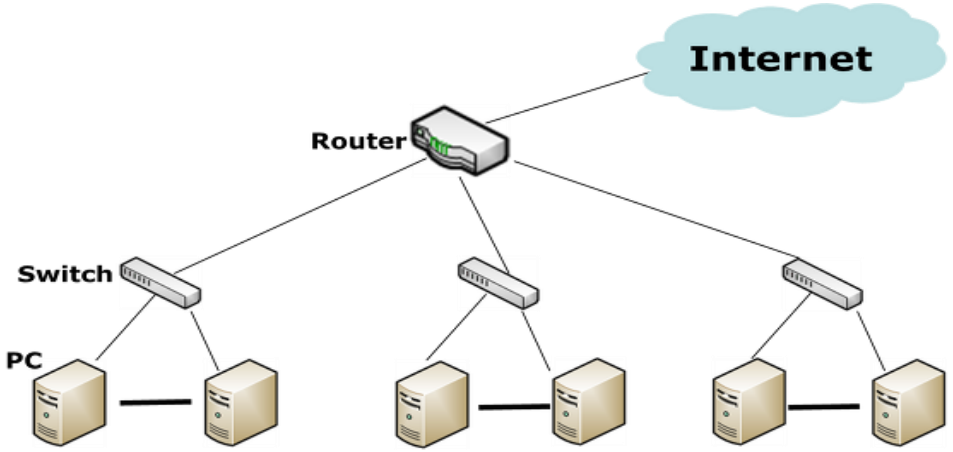
네크워크 장비(Layer 2, 3, 4, 7) : Switch (스위치)

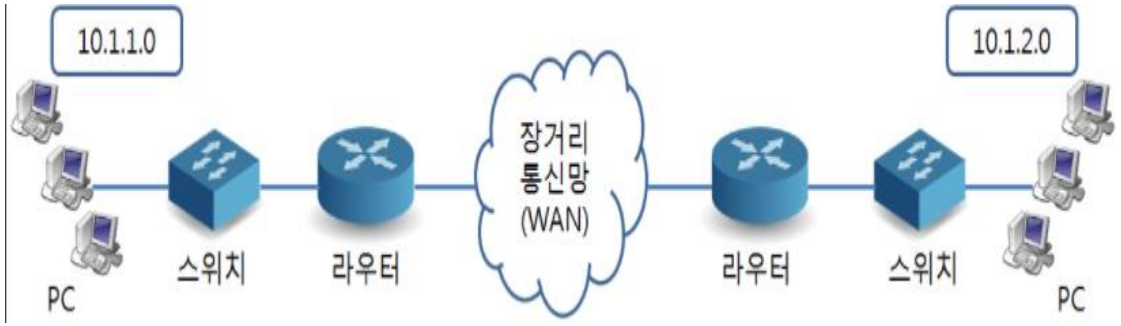


PC4가 PC3으로 신호를 보내면 그 신호는 PC3으로만 전달되고 다른 컴퓨터에는 신호를 보내지 않는다.

- ✓ 스위치는 내부에 메모리를 가지고 있어 각 포트에 연결된 컴퓨터들의 MAC 주소(MAC 주소 테이블)를 기억한다. 즉, 송신지와 수신지의 주소를 구분하여 해당 목적지로만 신호를 전달하며, 데이터 전송 에러 등을 복구해 주는 기능을 가지고 있다.
- ✓ 다만 스위치는 자신의 테이블에 없는 목적지를 가진 프레임이 오면 해당 프레임을 연결된 모든 장치에 포워딩하여, 이 경우 허브와 같은 동작을 한다.
- ✓ 10Mbps 스위치라면 각 포트에 연결된 컴퓨터들은 10Mbps의 속도를 보장 받으면서 통신을 할 수 있다.
- ✓ 허브와 스위치의 차이는 메모리 뿐만 아니라 내부 구조에서도 나타난다. 허브의 경우 내부 연결 통로(버스)를 공유하는 방식이다. 하지만 스위치의 경우 각 포트별로 상대 포트로 향하는 독립적인 통로(버스)를 가지고 있다.
- ✓ L2 스위치를 "스위칭허브" 라고도 불린다.
- ✓ 24 포트 스위치의 Collision Domain 개수는?

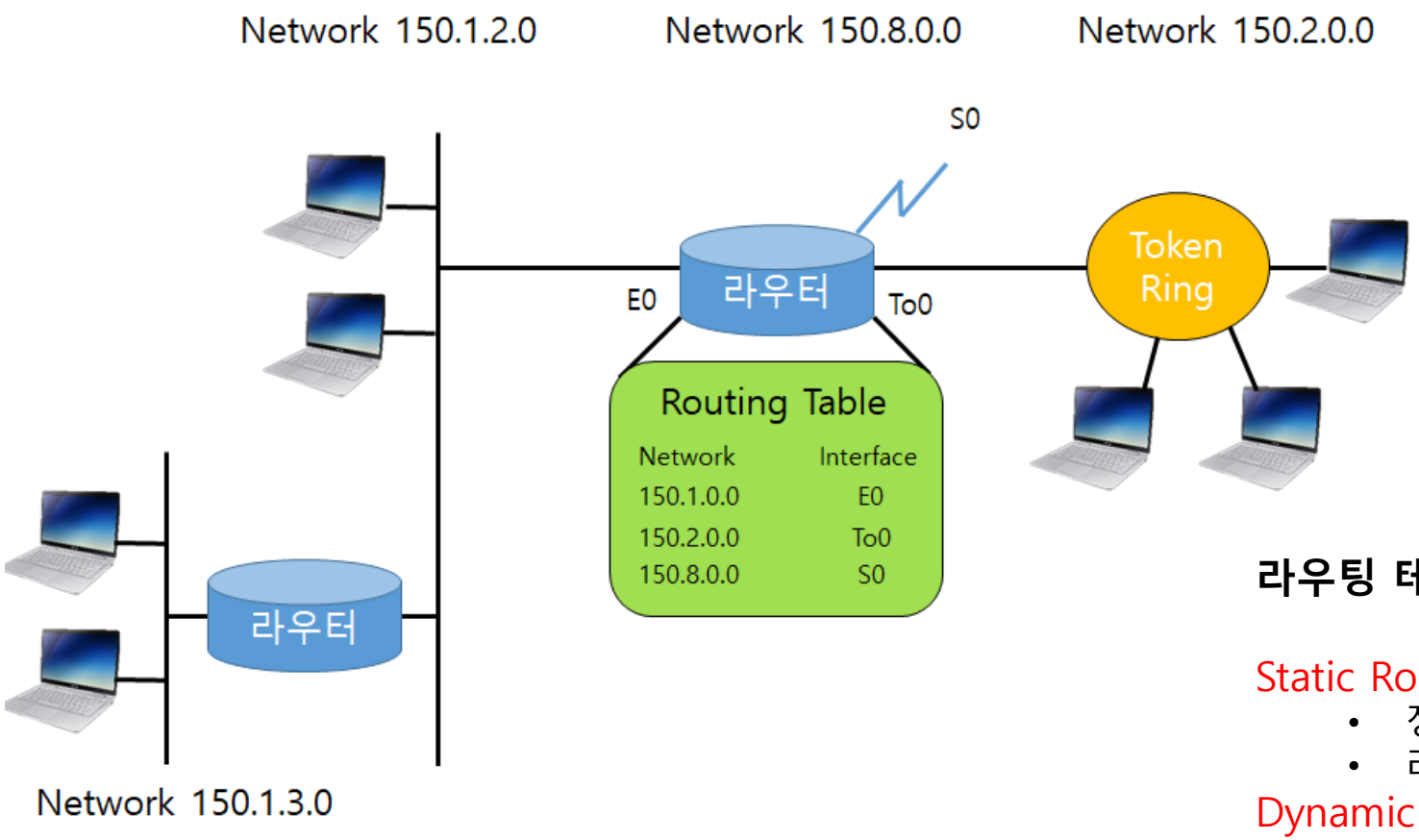
네트워크 장비(Layer 3) : Router (라우터)





- ✓ 서로 다른 네트워크(서브넷 마스크가 다른)를 연결시켜 주는 장비로서, 정보를 주고 받을 때 송신 정보에 담긴 수신처의 주소를 읽고 가장 적절한 통신 경로를 이용하여 다른 통신망으로 전송하는 장치로 주요 기능은 경로설정 및 판단(라우팅 알고리즘), NAT 기능 등이 있다.
- ✓ 라우터는 IP 주소 등 L3에 있는 주소를 참조하여 목적지로 패킷을 전송한다. 또한 서브넷 마스크가 다른 IP 주소를 가진 장비간 통신을 하기 위해서는 반드시 라우터와 같은 L3 장비를 거쳐야만 한다.
- ✓ 서로 다른 프로토콜로 운영하는 통신망에서 정보를 전송하기 위해 경로를 설정하는 역할을 제공하는 핵심적인 통신 장비이다.
- ✓ Web에서 **구글**, **네이버**과 같은 서비스 제공자의 주소에 접속 할 때, 우리가 흔히 알고 있는 '[www.naver.com'와](http://www.naver.com) 같은 도메인을 통하여 접속을 하면, 도메인 서버(DNS)를 통하여 IP를 얻을 수 있다. 이 IP를 이용하여 요청을 보내면, 라우터에서는 **'다음은 여기 라우터로 가야 됩니다!'** 라고 판단하고 데이터 패킷을 다른 라우터에게 전송해 준다. 이런 과정을 여러번 진행하면서 수많은 라우터들을 거치고, 최종 목적지인 **네이버**로 도착하게 되는 것이다.

네트워크 장비 : Routing Table (라우팅 테이블)



라우팅 테이블을 구성하는 것은 라우팅 프로토콜,

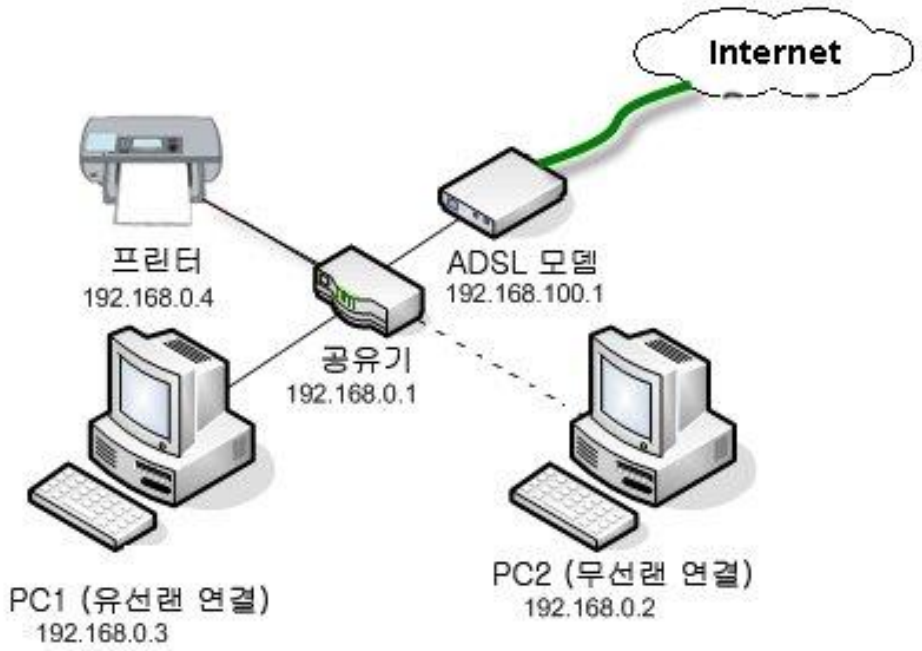
Static Routing Protocol :

- 정적으로 Routing 경로를 지정, 단일 경로에 적합
- 라우터 추가, 변경 등을 자동인지 하지 못한다.

Dynamic Routing Protocol :

- 동적으로 Routing 경로를 지정, 다중 경로에 적합
- 네트워크 변화를 자동 인지하여 재구성 한다.
- RIP, IGRP, EIGRO, OSPF 등이 있다.

네트워크 장비 : IP 공유기



- ✓ ISP(Internet Service Provider) 업체에서 제공하는 한 개의 인터넷 IP Address로 여러 대의 컴퓨터, 노트북, IP폰 등이 인터넷을 공유할 수 있도록 한다.
- ✓ 라우터의 많은 기능 중에 NAT 기능을 특화시켜 저렴화 한 기기로, 사설 IP 할당으로 여러 PC가 인터넷을 사용하게 한다. 그러나 IP 공유기에는 경로설정/판단 기능이 없다.
- ✓ 또한, IP 공유기는 허브 기능을 포함하고 있어서, 여러 대의 PC를 연결할 수 있다. 대부분의 인터넷 공유기는 4포트를 내장하고 있는데, 4대 이상의 PC가 하나의 인터넷 IP를 공유하기 위해서는 인터넷 공유기와 스위칭 허브를 이용하면 된다.
- ✓ 공유기에는 보통 1개의 WAN 포트와 4개의 LAN 포트가 있는데, 외부에서 들어오는 공인 IP의 LAN 선을 WAN 포트에 연결하고, 나머지 LAN 포트들은 내부 IP (ex 192.168.0.~)로 사용할 장치들에 LAN 선을 연결하는 것이 일반적인 사용법이다.
- ✓ 공유기에서 나오는 LAN 선을 또 다른 하위 공유기에 연결할 수 있는데,
  - 하위 공유기의 WAN 포트에 연결하면 새로운 영역의 네트워크 (ex 192.168.1.~)을 만드는 것이고,
  - 하위 공유기의 LAN 포트에 연결하면 허브로 멀티포트 기능을 사용하는 것 (ex 192.168.0.~)이다.

네트워크 장비 : (L2, L3, L4, L7) 스위치

L2 스위치 : 스위칭 허브

- **MAC Address** 를 보고 스위칭 하는 것.

L3 스위치 : 스위치

- **IP Address(Routing Table)** 를 보고 스위칭 하는 것.

L4 스위치 : 로드밸런서(부하 분산, HA)

- **(IP + Port)** 를 보고 스위칭 하는 것.
- 실제로 우리가 사용하는 많은 온라인 서비스들은 대부분 최소 2개 이상의 같은 서버들로 분산처리 되게끔 구성되어 있는데, 이때 서비스를 분산시켜 주는 장비가 L4 스위치이다.
- "부하 분산" 뿐만 아니라 "클러스터링" 액티브-액티브 구성으로 HA(High Availability, 고가용성) 구현.

L7 스위치 : 웹방화벽, 보안스위치

- **실제 Application에서 활용되는 데이터**를 보고 스위칭 하는 것.
- 패킷의 내용이나 Pattern을 AI, Machine Learning 등의 분석 기법으로 비정상 데이터를 필터링하여 차단하거나 필요한 조치를 취하는 네트워크 보안 장비.

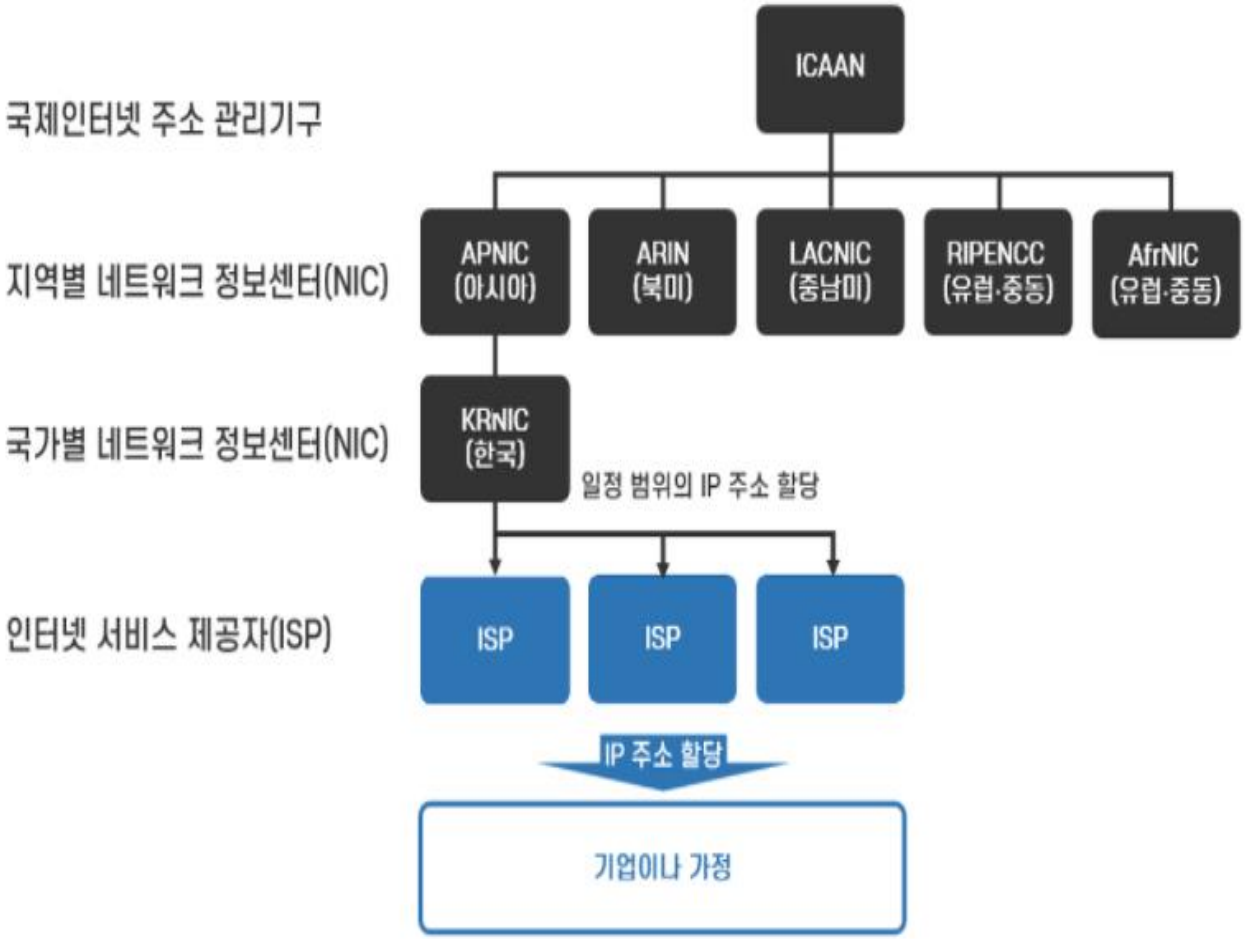
**** 기본적으로 상위 Layer 스위치는 하위 Layer 스위치 기능을 모두 포함한다.**

IP (Internet Protocol) Address

IP Address **vs** MAC Address

- IP 주소는 TCP/IP라는 프로토콜을 사용하는 모든 장비들을 구분해 주기 위해서 만든 주소.
- 그런데 IP 주소가 있는데 MAC 주소는 또 왜 필요한가 (학번 있는데 주민번호 왜 필요해) ?
- 네트워크 계층과 데이터링크 계층의 각각 독립된 주소.
- IP 논리적 주소 MAC은 물리적 주소
- IP 주소는 도로명주소, IPX 주소는 지번주소, mac은 위도/경도 (http://www.dawuljuso.com/)
- 논리적 주소 -> 물리적 주소 바꾸는 절차를 ARP 라고 한다.
- 국가별 IP 주소 : https://xn--3e0bx5euxnjje69i70af08bea817g.xn--3e0b707e/jsp/statboard/IPAS/ovrse/natal/IPaddrBandCurrent.jsp?nationCode1=KR

IP Address 표현 형식 (IPv4)



- 2진수 32 자리로 구성 (IPv4)
- IPv6 는 2진수 128 자리로 구성, IPv6 = IPv4 * 4배
- 00000000.00000000.00000000.00000000 ~ 11111111.11111111.11111111.11111111 : 약 42억 9천개
- 일반적인 표기 방식은 10진수로 4개를 (.) 점으로 구분하여 표기 : 예, 104.35.15.34
- IP 주소 = Network Part + Host Part
- Network Part : Broadcast Domain (라우터를 거치지 않고도 통신할 수 있는 영역)
- Host Part : Broad Domain에 연결된 각각의 PC들의 가리킴.
- Network Part는 모두 동일하고 Host Part는 모두 달라야 정상적인 통신이 되는 영역을 LAN 이라고 한다.

IP Address : Class

- Network Part와 Host Part를 나누는 방법을 약속해 놓은 것이 IP주소의 Class (**Red : Network Part Blue : Host Part**)

- Class A : **0xxx xxxx** . **xxxx xxxx . xxxx xxxx . xxxx xxxx**
  - Network Part 1 ~ 126 으로 시작하며, 허용되는 Host 개수는 16,777,214 개

- Class B : **10xx xxxx . xxxx xxxx** . **xxxx xxxx . xxxx xxxx**
  - Network Part 128.0 ~ 191.255 로 시작하며, 허용되는 Host 개수는 65,534 개

- Class C : **110x xxxx . xxxx xxxx . xxxx xxxx** . **xxxx xxxx**
  - Network Part 192.0.0 ~ 223.255.255 로 시작하며, 허용되는 Host 개수는 254 개

Class	공인 IP : 공인된 기관에서 인증한 공개형 주소	사설 IP : 공인되지 않은 주소로 폐쇄형
A	0.0.0.0 ~ 127.255.255.255	10.0.0.0 ~ 10.255.255.255
B	128.0.0.0 ~ 191.255.255.255	172.16.0.0 ~ 172.31.255.255
C	192.0.0.0 ~ 233.255.255.255	192.168.0.0 ~ 192.168.255.255
D	224.0.0.0 ~ 239.255.255.255 : Multicast용	
E	240.0.0.0 ~ 255.255.255.255 : 연구용	**문제 : 203.54.23.1 의 Network Part는?**

IP Address : Subnet Mask I

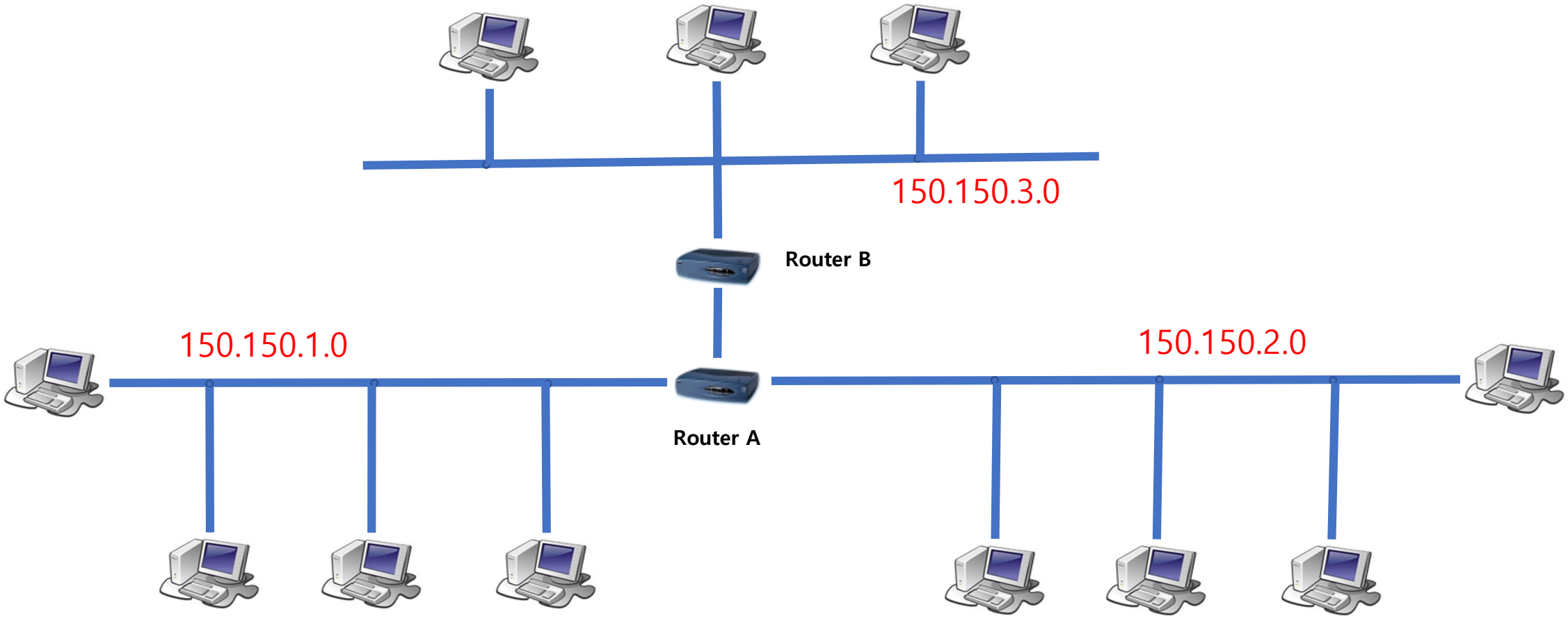
Class B 주소를 할당 받았다고 가정해 보자.

- 하나의 네트워크로 구성하면 65,534 개의 Host를 갖는 네트워크가 생기고, 이 곳에서는 Broadcast의 난무로 실제로 통신이 원활히 이루어질지 의문이다. 즉 Broadcast domain이 너무 커진다는 것이다.
- 큰 고기덩어리를 칼로 잘라 나누듯, Class B와 같이 큰 네트워크를 자르기 위해서 필요한 것이 "Subnet Mask" 또는 NetMask 라고 하기도 한다. 다시 말해, Subnet Mask는 IP주소를 가지고 어디 까지가 Network Part이고 또 어디 까지가 Host Part인지를 나타내는 역할.
- Class B의 기본 Subnet Mask는 255.255.0.0 그러면 Subnet Mask를 255.255.255.0으로 조정하면 어떻게 되는 것인가?

Logical AND	10진수	2진수
IP 주소	150.150.10.3	1001 0110 . 1001 0110 . 0000 1010 . 0000 0011
Subnet Mask	255.255.0.0	1111 1111 . 1111 1111 . 0000 0000 . 0000 0000
Subnet Network	150.150.0.0	1001 0110 . 1001 0110 . 0000 0000 . 0000 0000

Logical AND	10진수	2진수
IP 주소	150.150.10.3	1001 0110 . 1001 0110 . 0000 1010 . 0000 0011
Subnet Mask	255.255.255.0	1111 1111 . 1111 1111 . 1111 1111 . 0000 0000
Subnet Network	150.150.10.0	1001 0110 . 1001 0110 . 0000 1010 . 0000 0000

IP Address : Subnet Mask II



IP Address : Subnet Mask III

이번에는 Class C 주소를 (201.222.10.60) 잘라 봅시다.

255.255.255.248을 Subnet Mask로 사용하면 201.222.10.56 ~ 201.222.10.63 으로 8개의 Host를 갖는 네트워크 구성

Logical AND	10진수	2진수
IP 주소	201.222.10.60	1100 1001 . 1101 1110 . 0000 1010 . 0011 1100
Subnet Mask	255.255.255.248	1111 1111 . 1111 1111 . 1111 1111 . 1111 1000
Subnet Network	201.222.10.56	1100 1001 . 1101 1110 . 0000 1010 . 0011 1000

Logical AND	10진수	2진수
IP 주소	201.222.10.55	1100 1001 . 1101 1110 . 0000 1010 . 0011 0111
Subnet Mask	255.255.255.248	1111 1111 . 1111 1111 . 1111 1111 . 1111 1000
Subnet Network	201.222.10.0	1100 1001 . 1101 1110 . 0000 1010 . 0011 0000

Logical AND	10진수	2진수
IP 주소	201.222.10.64	1100 1001 . 1101 1110 . 0000 1010 . 0100 0000
Subnet Mask	255.255.255.248	1111 1111 . 1111 1111 . 1111 1111 . 1111 1000
Subnet Network	201.222.10.64	1100 1001 . 1101 1110 . 0000 1010 . 0100 0000

IP Address : Subnet Mask IV

Class C 주소를 (201.222.10.60) Subnet Mask로 자르기 위해서는

구성할 수 있는 Host 개수	10진수	2진수
128	255.255.255.128	1111 1111 . 1111 1111 . 1111 1111 . 1000 0000
64	255.255.255.192	1111 1111 . 1111 1111 . 1111 1111 . 1100 0000
32	255.255.255.224	1111 1111 . 1111 1111 . 1111 1111 . 1110 0000
16	255.255.255.240	1111 1111 . 1111 1111 . 1111 1111 . 1111 0000
8	255.255.255.248	1111 1111 . 1111 1111 . 1111 1111 . 1111 1000
4	255.255.255.252	1111 1111 . 1111 1111 . 1111 1111 . 1111 1100
2	255.255.255.254	1111 1111 . 1111 1111 . 1111 1111 . 1111 1110
1	255.255.255.255	1111 1111 . 1111 1111 . 1111 1111 . 1111 1111

기타 네트워크 관련 용어들

Gateway(게이트웨이), DNS, NMS

Gateway

- 게이트웨이란 서로 다른 네트워크를 연결해 주는 역할을 하는 특정 장비나 호스트를 의미.
- 게이트웨이로 사용되는 가장 일반적인 장비가 라우터.
- 일반적인 서버나 호스트는 특정 패킷을 받았을 때 자기 자신의 것이 아니면 그냥 버리는데 반해, 게이트웨이는 라우팅 테이블을 확인하여 받은 패킷을 가장 적합한 다른 네트워크로 전달해 주는 역할을 하며, 이를 "IP 포워딩" 또는 "패킷 포워딩" 이라고 한다.

DNS(Domain Name System)

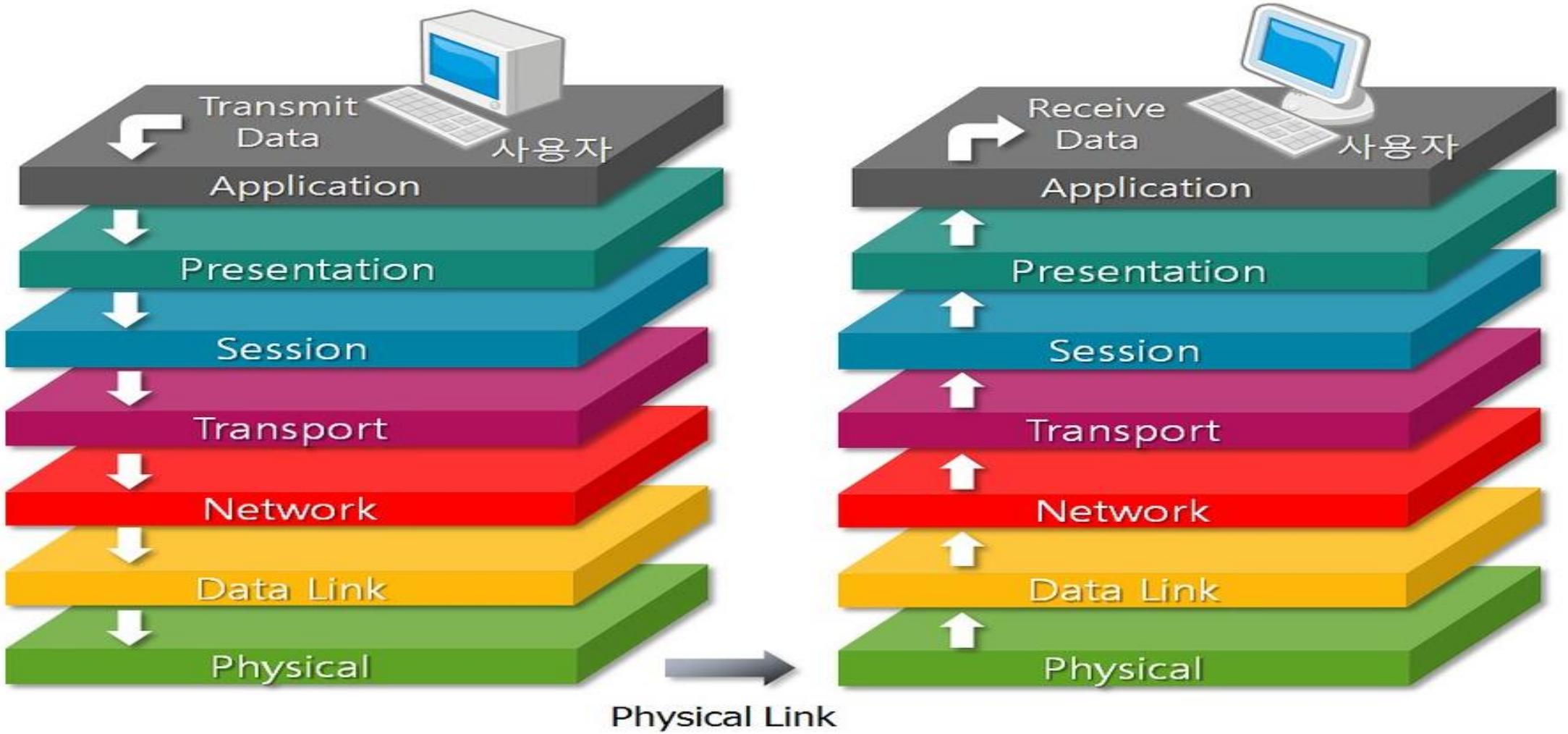
- 인터넷 전화번호부 같은 것으로 도메인이름(naver.com)을 IP 주소로 변환 또는 그 반대 역할을 해주는 시스템.
- DNS가 없다면 우리는 그 많은 IP 주소를 외우고 다녀야 할지도....
- 도메인등록업체에서 도메인에 대한 네임서버를 변경하면, 그 변경내역이 최상위 기관의 DNS에 적용되고 전세계 cache DNS에 전파되는 데에 최대 2~3일까지 소요될 수 있다.

NMS(Network Management System)

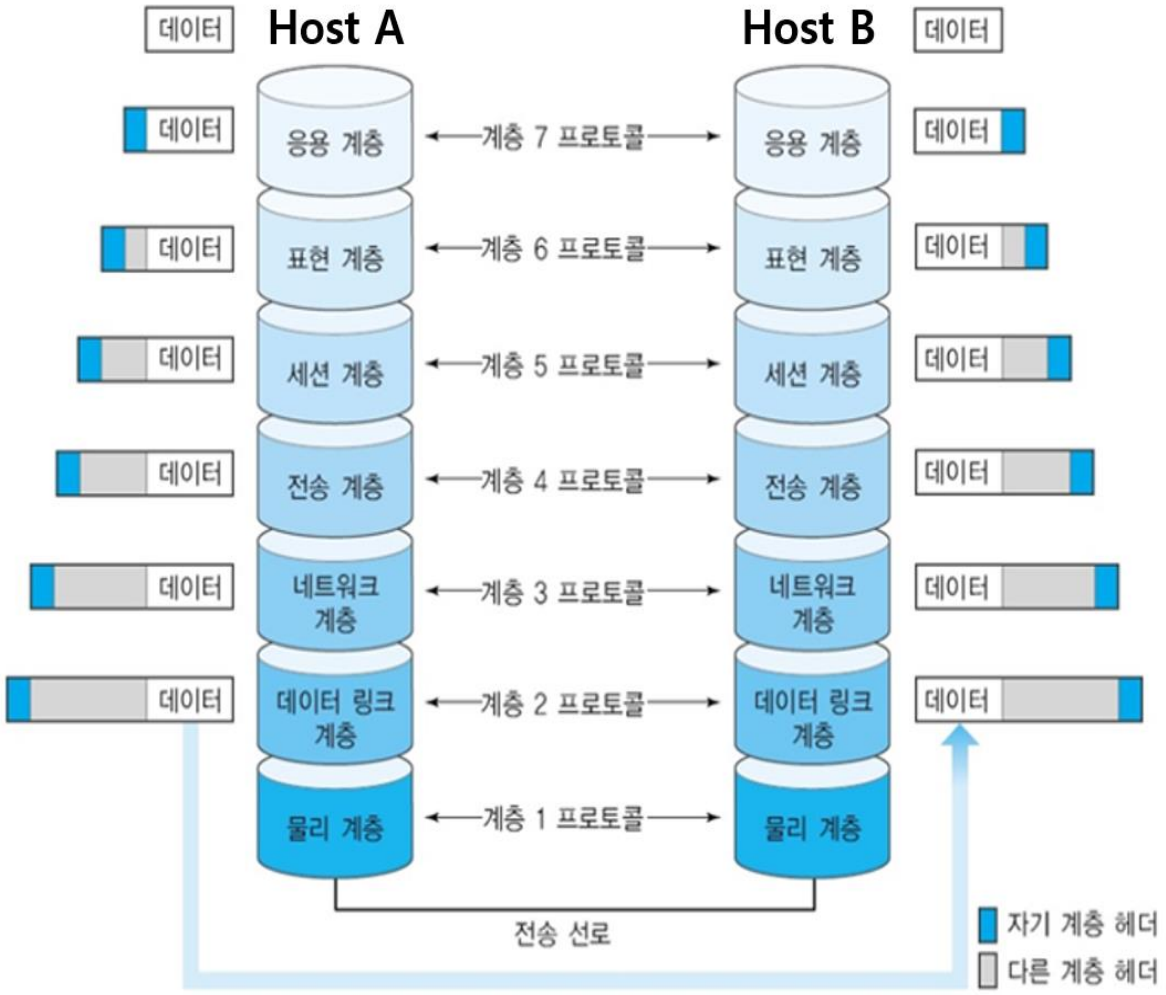
- 하드웨어 또는 소프트웨를 이용하여 LAN/WAN 모니터링, 유지관리, 최적화 시키는 네트워크 시스템.
- 핵심기능으로는 네트워크 모니터링, 장비감지, 성능분석, 장비관리, 장애관리 등

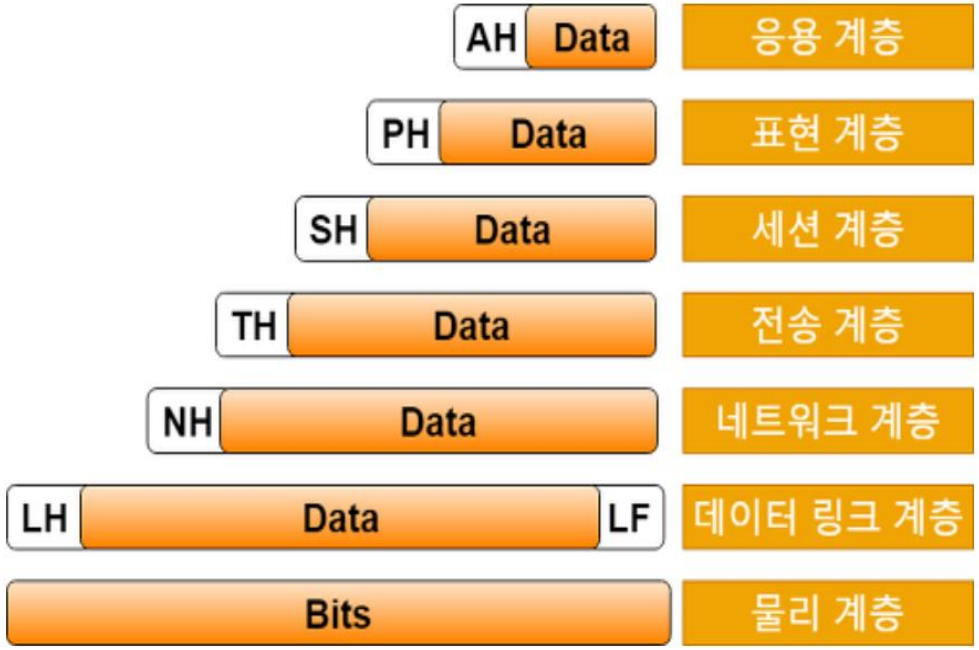
OSI(Open Systems Interconnection) 7 Layer : A few more

OSI 7 Layer

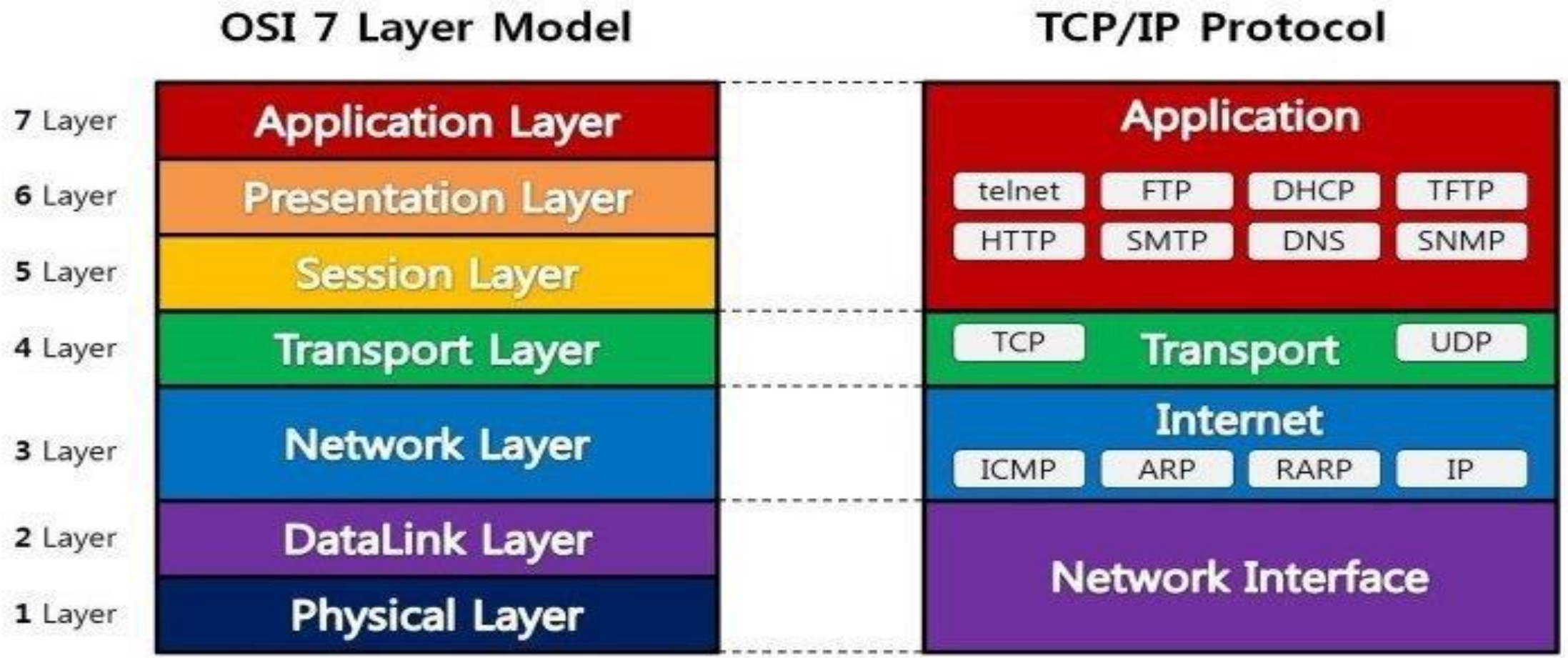

Transmit Data
사용자
Application
Presentation
Session
Transport
Network
Data Link
Physical
Receive Data
사용자
Application
Presentation
Session
Transport
Network
Data Link
Physical
Physical Link

OSI 7 Layer로 표현하는 통신





OSI 7 Layer Model vs TCP/IP Model



OSI 7 Layer : Application Layer(응용 계층, 7계층)

- ✓ 사용자가 어플리케이션에 입력한 정보를 특정 프로토콜(HTTP, SMTP, FTP 등)의 형식에 맞게 표현하는 User Interface를 제공하는 계층.
- ✓ 예를 들어, 누군가에게 편지를 보내는 상황을 가정해 보자. 편지를 보내기 위해서는 먼저 편지지를 구매하고 그 위에 전달할 내용을 작성해야 할 것이다. 여기서 편지지가 바로 우리가 발신하고자 하는 정보를 입력하는 어플리케이션(웹 브라우저 등)에 해당한다고 볼 수 있다.
- ✓ 전송 단위 : Message
- ✓ 프로토콜 스택 : Telnet, FTP, HTTP, SSH
- ✓ Ex : 전자 메일, 웹브라우저(인터넷)

OSI 7 Layer : Presentation Layer(표현 계층, 6계층)

- ✓ 수신자가 이해할 수 있는 형태로 데이터를 변환하고(인코딩), 데이터 전송의 효율성과 안전성을 보장하기 위해 데이터를 압축하고 암호화/복호화 하는 계층.
- ✓ 데이터의 형태를 변환하는 이유는 통신하는 두 기기가 특성이 같다는 보장이 없기 때문이다. 따라서 누구나 이해할 수 있는 공통의 표준 형식으로 데이터를 변환하여 수신자에게 보내고, 이를 받은 수신자는 자신에게 맞는 형태로 해당 데이터를 다시 변환하게 된다.
- ✓ 예를 들어, 미국인이 중국인에게 "One, Two, Three"라는 메시지를 전달하고 싶다면 두 사람 모두 이해할 수 있는 "1, 2, 3"으로 메시지를 변환하여 전송하고, 이를 받은 중국인은 해당 메시지를 "Yī, èr, sān"으로 변환하여 이해하게 될 것이다.
- ✓ 마찬가지로, 압축이나 암호화가 되어 있는 경우도 수신자가 그 과정을 거꾸로 진행하여 원래의 데이터를 복구해야 할 것이다.
- ✓ 전송 단위 : Message
- ✓ 프로토콜 스택 : XDR, SMB, AFP

OSI 7 Layer : Session Layer(세션 계층, 5계층)

- ✓ 통신하는 두 기기 사이의 연결 상태를 관장하는 계층으로, 어떠한 방식으로 두 기기가 상호작용할 것인지를 결정.
- ✓ 예를 들어 통화하는 것처럼 쌍방향으로 동시에 데이터를 주고받을 것인지, 무전기처럼 데이터를 서로 번갈아서 주고 받을 것인지, 아니면 일방적으로 데이터를 받기만 할 것인지 등에 관한 상호작용 방식을 결정한다.
- ✓ 수신자는 세션 계층에서 명시한 정보를 바탕으로 어떤 방식으로 반응을 해야 할지 결정하게 된다. 무전기로 요청이 왔으면 무전기로 응답하고, 우편으로 요청이 왔으면 우편으로 응답하는 셈이다.
- ✓ 전송 단위 : Message
- ✓ 프로토콜 스택 : NetBIOS, RPC

OSI 7 Layer : Transport Layer(전송 계층, 4계층)

✓ 누가 누구에게 보냈는지에 대한 정보를 명시하는 계층으로 최종 도착지에 위치한 어떤 프로세스에게 데이터를 전달할 것인가, 즉 포트 번호를 명시하는 계층.

✓ 최종 도착지가 어디인가를 명시하는 것은 바로 이어서 설명할 네트워크 계층의 역할이다. 전송 계층에 해당하는 대표적인 프로토콜은 바로 TCP와 UDP이다. 이 둘의 차이를 간단하게 설명하면 다음과 같다.

- TCP는 데이터를 발신하는 쪽에서 수신자가 온전한 데이터를 받을 수 있도록 하는 책임을 지니고 있어서, 데이터가 제대로 전달되지 않은 경우 이를 재전송해야 한다.
- 반면에 UDP는 그러한 책임을 지니고 있지 않아서 데이터가 제대로 전달되지 않은 경우에도 특별히 이를 재전송하지 않는다. 편지지가 제대로 전달됐는지 확인이 가능한 등기 우편과 그렇지 않은 일반 우편의 차이인 셈이다.

✓ 전송 단위 : Segment

✓ 프로토콜 스택 : TCP, UDP, SPX, AppleTalk

✓ 장비 : L4 스위치(3계층 트래픽 분석, 서비스 종류 구분)

OSI 7 Layer : Network Layer(네트워크 계층, 3계층)

- ✓ 네크워크를 논리적으로 구분하고 연결하는 계층 – 논리적 주소(IP 주소) 사용
- ✓ 중계 노드를 통하여 전송하는 경우, 어떻게 중계할 것인가를 규정, 즉 데이터를 목적지까지 가장 안전하고 빠르게 전달 (라우팅)
- ✓ 전송 계층이 누구에게 보낼지를 명시한다면, **네트워크 계층은 수신자가 위치해 있는 최종 도착지를 명시**한다.
- ✓ 편지를 보낼 때 받는 사람의 아파트 주소를 적어야 하는 것과 마찬가지이다. IP(Internet Protocol)가 바로 네트워크 계층에 해당하는 대표적인 프로토콜로, 이 경우 최종 도착지를 IP 주소로 명시하게 된다.
- ✓ 최종 도착지 뿐만 아니라 그곳까지 가기 위해 필요한 경로들의 정보도 함께 명시하는 **라우팅 기능**을 수행한다.
- ✓ 참고로 최종 도착지의 경우 수신자에게 도달할 때까지 변하지 않는 정보이지만, 이어서 설명할 데이터 링크 계층에서 명시하는 물리 주소(EX. MAC 주소 등)는 노드를 이동할 때마다 변하는 정보라는 사실을 기억하도록 하자.
- ✓ 전송 단위 : Packet
- ✓ 프로토콜 스택 : IP, ARP, IPX, X.25
- ✓ 장비 : 라우터, L3 스위치

OSI 7 Layer : Data Link Layer(데이터 링크 계층, 2계층)

- ✓ 물리적으로 연결된 두 장치 간의 신뢰성 있는 데이터 전송을 담당
- ✓ 물리 계층에서 담당하지 않는 흐름 제어 및 오류 수정의 기능을 담당하는 계층.
- ✓ 물리 계층에서는 단순히 비트열을 전달할 뿐 데이터의 신뢰성에 대한 특별한 검사를 진행하지 않기 때문에 데이터 링크 계층에서 데이터의 신뢰성을 보장해주는 것이다.
- ✓ 데이터 링크 계층에서는 **물리 주소(EX. MAC 주소)를 명시**함으로써 수신자의 MAC 주소와 일치하지 않는 경우에는 데이터의 전달이 잘못되었음을 판단할 수 있도록 한다.
- ✓ 정보의 오류와 흐름을 관리, 안정된 정보 전달
- ✓ 전송 단위 : Frame
- ✓ 프로토콜 스택 : EtherNet, Token-Ring, ATM, FDDI
- ✓ 장비 : 스위치, 브리지

OSI 7 Layer : Physical Layer(물리 계층, 1계층)

- ✓ 발신할 데이터를 디지털 신호에서 전기 신호로 바꾸고, 수신한 데이터를 전기 신호에서 디지털 신호로 바꾸는 계층.
- ✓ 즉 물리적인 매체를 통해 비트열을 전송할 수 있도록 하는 계층으로, 물리적인 장치 및 인터페이스가 데이터의 전송을 위해 필요로 하는 몇 가지 처리 절차를 담당하고 있다.
- ✓ 전기 신호를 어떻게 만들어서 보낼지, 어떠한 회선을 사용할지, 부호화는 어떤 식으로 할 건지 등등을 정의하게 된다.
- ✓ 전송단위 : bit.
- ✓ 단지 데이터 전달 역할만을 하며 알고리즘, 오류제어 등의 기능은 없음.
- ✓ 장비 : 케이블, 리피터, 허브

전송 단위 : Message, Segment, Packet, Frame