

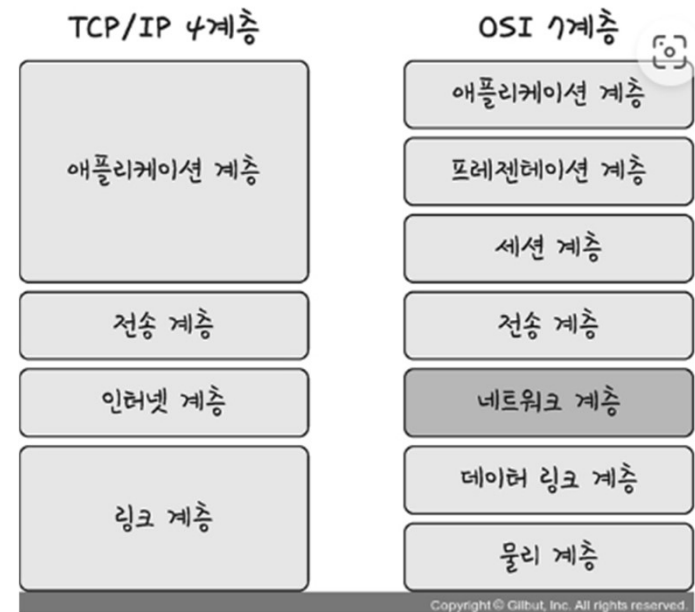
네트워크 기기

- 계층 별 범위 (애플리케이션, 인터넷, 데이터 링크, 물리)
- 개념 정리 (로드밸런스 , 라우터 , 스위치)
- 각각의 계층에 관여하는 네트워크 기기 소개

네트워크 기기

- 계층 별로 처리 범위를 나눌 수 있음
- 상위 계층을 처리하는 기기는 하위 계층을 처리 할 수 있지만 , 그 반대는 불가함

- 애플리케이션 계층: L7 스위치
- 인터넷 계층: 라우터, L3 스위치
- 데이터 링크 계층: 브리지, L2 스위치
- 물리 계층: NIC, 리피터, AP



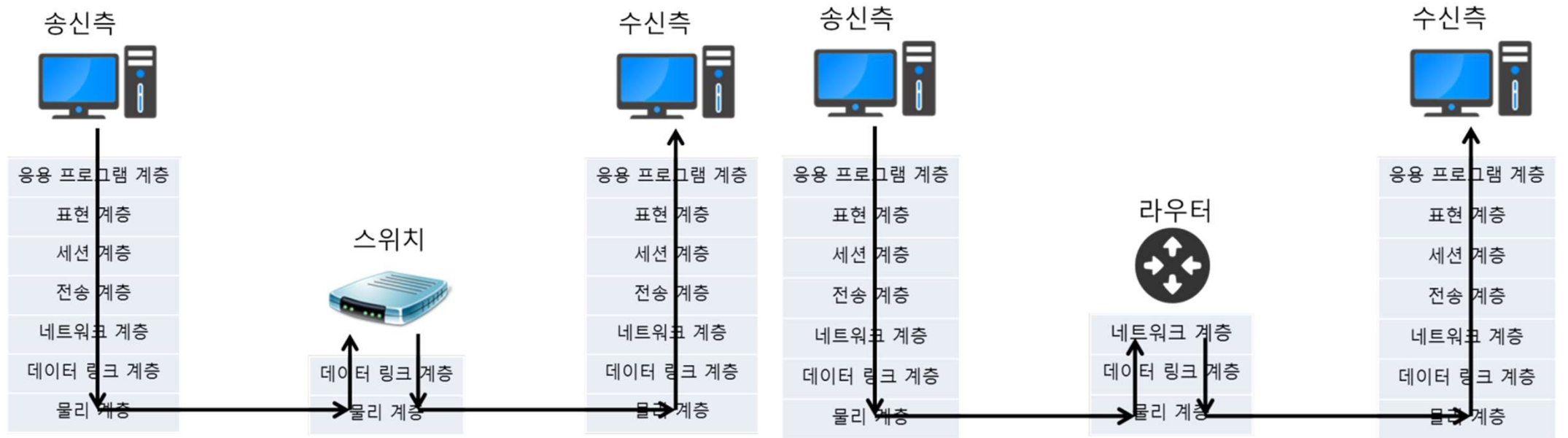
▲ 그림 2-18 TCP/IP 4계층과 OSI 7계층 비교

개념 정리

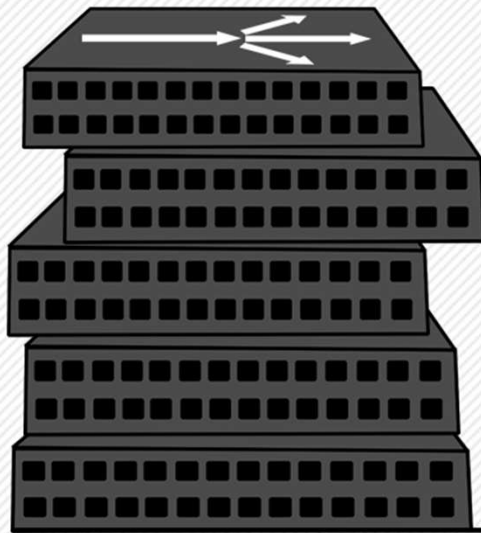
- 스위치 : 데이터 링크 계층(계층 2)에서 작동하며, 물리적 포트에 연결된 기기에서 전송된 패킷을 받아 다시 내보내는데, 패킷이 도달해야 하는 기기로 이어지는 포트를 통해서만 보냄. 여러 장비를 연결하고, 데이터 통신을 중재하며 **목적지가 연결된 포트로만** 전기 신호를 보내 데이터를 전송하는 네트워크 장비 ('내부 네트워크' 간의 통신만이 가능하다는 한계점)
- 라우터: 네트워크 계층(계층 3) 내부와 외부 네트워크 신호를 구분할 줄 아는 라우터만이 외부 네트워크와의 통신 → **서로 다른 네트워크**를 연결하는 기능 -- 굉장히 비쌈



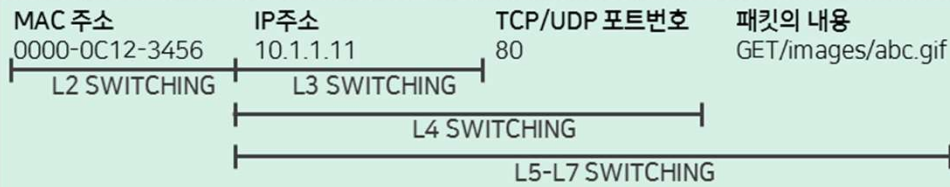
- 네트워크 회선과 서버 컴퓨터를 연결하는 네트워크 장비



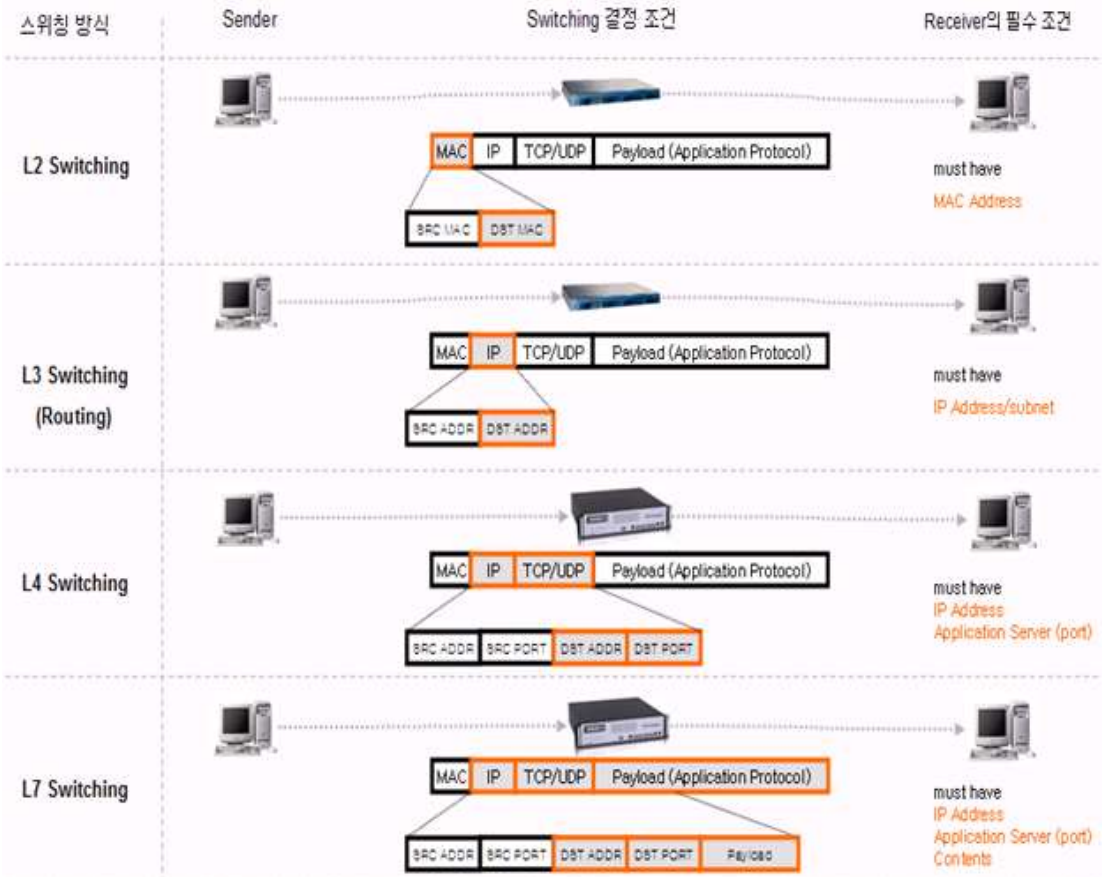
정리해보면,



- L7 Switch**
로드밸런싱, 보안기능
(트래픽 필터, VPN)
- L4 Switch**
포트번호를 이용한 로드밸런싱
- L3 Switch**
IP 주소를 이용한 스위칭,
라우팅&포워딩
- L2 Switch**
MAC 주소를 이용한 스위칭
- L1 Switch**
허브, 플러딩



계층에 따른
스위칭 방식



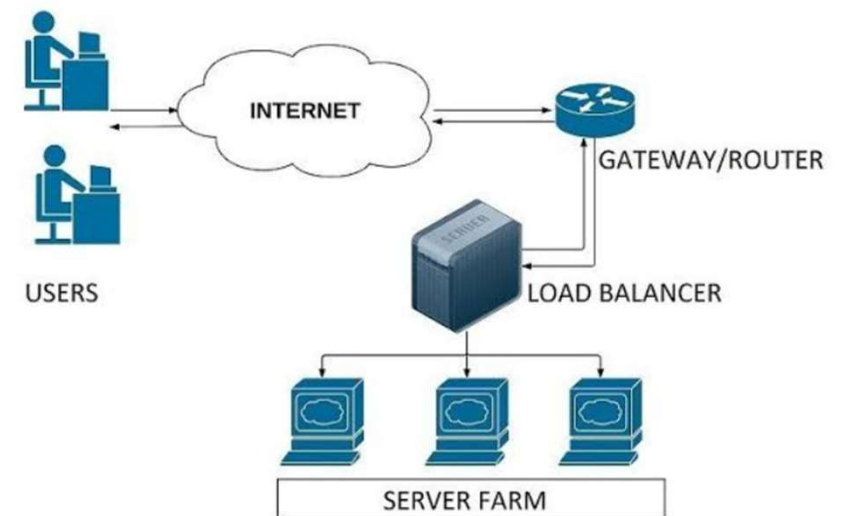
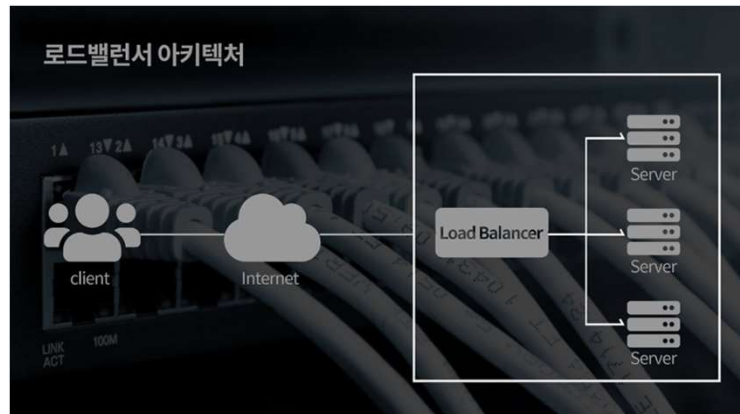
상위 계층을 처리하는 기기는 하위 계층을 처리 할 수 있지만 , 그 반대는 불가능

개념정리

- 수천만 명의 접속자를 감당하기 위해 서비스를 제공하는 측에서 미리 트래픽을 예측하고 서버와 네트워크를 증설하는데, 이때 한 서버의 성능을 높이는 scale-up 작업은 한계가 있으므로,

분산처리를 위해 여러 대의 서버들을 놓게 되는 scale-out 작업을 하게 되는데, 이 때 여러 서버들로 **대규모의 네트워크 트래픽을 분산 처리하는 기술** =

‘로드 밸런싱’



스위치 분류

- L1 스위치 : 가장 하위 계층 (물리 계층)
- L2 스위치 : 데이터 링크 계층 , MAC 주소를 읽은 후 해당 장비를 찾아 전달 해 주는 장비
- L3 스위치 (+라우팅 기능) : MAC + IP 주소
- **라우터 : 네트워크 패킷을 연결해주는 통로 역할 (대역폭 확장)
- L4 스위치 , L7 스위치 (로드밸런서) : IP + 포트 정보

애플리케이션 계층 - L7 스위치

- L7 스위치 (로드 밸런서):
 - <URL , 서버 , 캐시 , 쿠키들을 기반으로 트래픽을 분산한다>
 - 서버의 부하를 분산하는 기기로 시스템이 처리 할 수 있는 트래픽 (서버와 스위치 등 네트워크 장치에서 일정 시간 내에 흐르는 데이터의 양) 증가를 목표로 한다.
1. 바이러스, 불필요한 외부 데이터 등을 걸러내는 **필터링** 기능
 2. 응용 프로그램 (사용자를 위해 특정 기능을 직접 수행하는 포괄적이고 독립적 인 프로그램) 수준의 **트래픽 모니터링**도 가능

헬스 체크

- 장애 발생 시: 트래픽 분산 대상에서 제외하기 위해 정기적으로 헬스 체크(health check)를 이용하여 감시하며 이루어짐
- *헬스 체크*: L4 스위치 또는 L7 스위치 모두 헬스 체크를 통해 정상적인 서버 또는 비정상적인 서버를 판별하는데 헬스 체크는 **전송 주기와 재전송 횟수** 등을 설정한 이후 반복 적으로 서버에 요청을 보내는 것을 의미한다.
- L4 체크: TCP의 3-way handshaking을 통해 각 서버의 포트 상태를 확인한다.
- L7 체크: 애플리케이션 계층에서 체크하는 방법으로 실제 웹 페이지에 통신을 시도해 이상 유무를 파악한다.

L4 스위치와 L7 스위치 차이

- L4 는 인터넷 계층을 처리하는 기기로 스트리밍 관련 서비스에서는 사용할 수 없고 메시지를 기반으로 인식하지 못하며 **IP와 포트**를 기반으로 트래픽을 분산함 반면, L7은 IP, 포트, HTTP 헤더, 쿠키 등을 기반으로 트래픽을 분산함

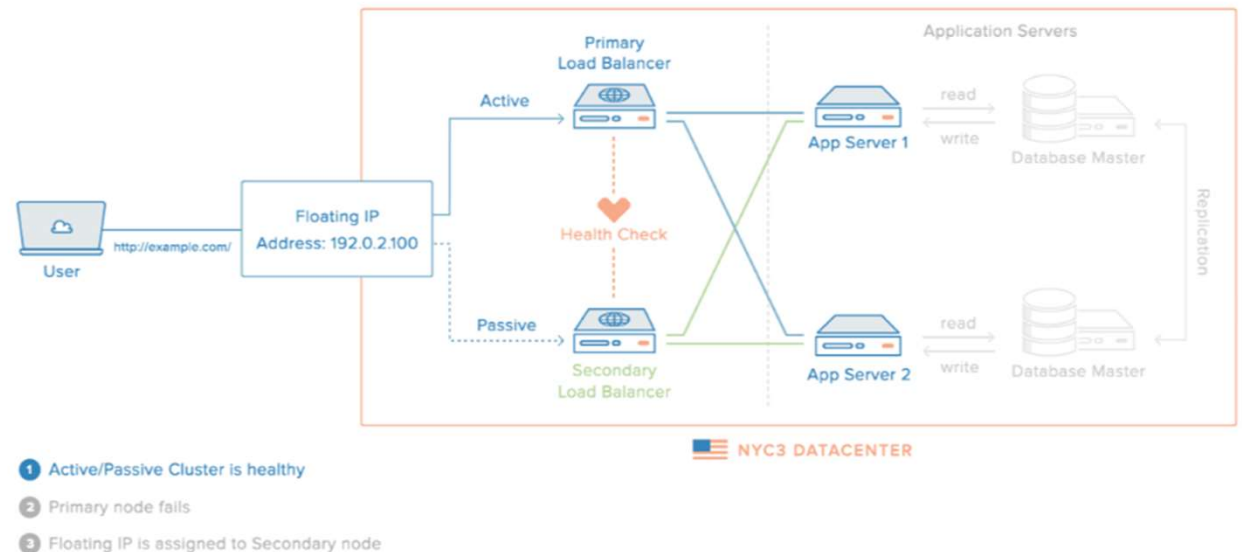
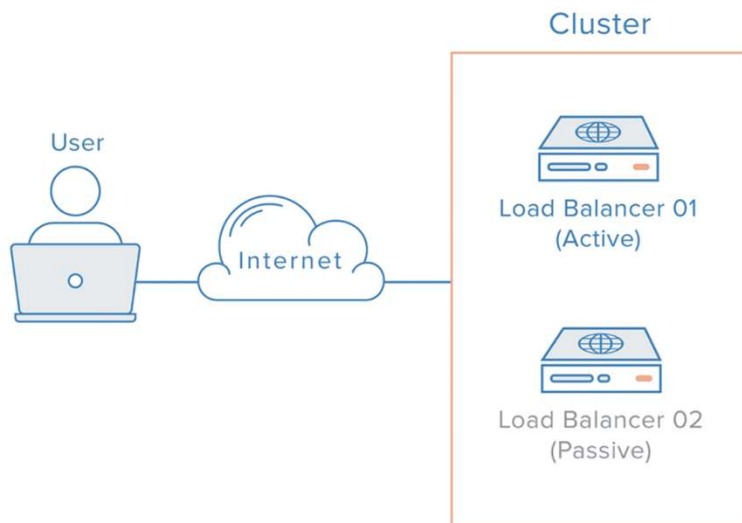
	L4 로드밸런서	L7 로드밸런서
네트워크 계층	Layer 4 전송계층(Transport layer)	Layer 7 응용계층(Application layer)
특징	> TCP/UDP 포트 정보를 바탕으로 함	> TCP/UDP 정보는 물론 HTTP의 URI, FTP의 파일명, 쿠키 정보 등을 바탕으로 함
장점	> 데이터 안을 들여다보지 않고 패킷 레벨에서만 로드를 분산하기 때문에 속도가 빠르고 효율이 높음 > 데이터의 내용을 복호화할 필요가 없기에 안전함 > L7 로드밸런서보다 가격이 저렴함	> 상위 계층에서 로드를 분산하기 때문에 훨씬 더 섬세한 라우팅이 가능함 > 캐싱 기능을 제공함 > 비정상적인 트래픽을 사전에 필터링할 수 있어 서비스 안정성이 높음
단점	> 패킷의 내용을 살펴볼 수 없기 때문에 섬세한 라우팅이 불가능함 > 사용자의 IP가 수시로 바뀌는 경우라면 연속적인 서비스를 제공하기 어려움	> 패킷의 내용을 복호화해야 하기에 더 높은 비용을 지불해야 함 > 클라이언트가 로드밸런서와 인증서를 공유해야하기 때문에 공격자가 로드밸런서를 통해서 클라이언트에 데이터에 접근할 보안 상의 위험성이 존재함

로드 밸런서를 이용한 서버 이중화

- 이중화 : 시스템의 가용성을 높이기 위해 장비를 다중화 시키는 방법
- 가용성 : $(\text{정상 서비스 시간}) / (\text{총 서비스 시간}) = \text{가용성}$
--> 서비스가 다운 되지 않고 유지된 시간
- 2 대 이상의 서버를 기반으로 가상 IP를 제공하고 이를 기반으로 안정적인 서비스를 제공함

서버 이중화

1. 이중화된 로드 밸런서들은 서로 상태를 확인을 한다.
2. Master 서버가 Fail되면 Standby 서버가 자동으로 Master 서버의 역할을 한다.
3. Standby 서버는 정상 시에는 대기 상태로 있다가 Master 서버가 Fail 되었을 경우에만 작동한다.
4. 이 구성을 Fail Over라고 한다.



인터넷 계층 – 라우터 , L3 스위치

- 라우터:
- 여러 개의 네트워크를 연결, 분할, 구분 시켜주는 역할을 하며 "다른 네트워크에 존재하는 장치끼리 서로 데이터를 주고 받을 때 패킷 소모를 최소화 하고 경로를 최적화 하여 최소 경로로 패킷을 포워딩"
- **** 패킷 :정보 기술에서 패킷 방식의 컴퓨터 네트워크가 전달하는 데이터의 형식화된 블록이다. 패킷은 제어 정보와 사용자 데이터로 이루어지며, 이는 페이로드 라고도 한다.**

인터넷 계층 – 라우터 , L3 스위치

- L3 스위치 :
- L2 스위치의 기능과 라우팅(**네트워크에서 경로를 선택하는 프로세스**) 기능을 갖춘 장비를 뜻함
- 네트워크 패킷을 연결해주는 통로 역할을 하며 대역폭 확장이 주 기능이
- — 소프트웨어 기반의 라우팅과 하드웨어 기반의 라우팅을 하는것으로 나뉨
- 하드웨어 기반의 라우팅을 담당하는 장치 : L3 스위치라고 함

데이터 링크 계층 – 브리지, L2 스위치

- L2 스위치:
- 장치들의 MAC 주소를 MAC 주소 테이블을 통해 관리. 연결된 장치로부터 패킷이 왔을 때 패킷 전송을 담당함
- 단순 패킷의 MAC 주소를 읽어 스위칭 하는 역할
- 목적지가 MAC 주소 테이블에 없다면 전체 포트에 전달하고 MAC 주소 테이블의 주소는 일정 시간 이후 삭제하는 기능도 있다.

데이터 링크 계층 – 브리지, L2 스위치

- 브리지 (Bridge):
- 두 개의 근거리 통신망(LAN)을 상호 접속 할 수 있도록 하는 통신망 연결 장치로 , 포트와 포트 사이의 다리역할을 하며 장치에서 받아온 MAC 주소를 MAC 주소 테이블로 관리함
- MAC 주소 기반 필터링 기능을 통해 더 나은 대역폭을 제공하고, 트래픽을 통제한다.
- MAC 주소 기반 리피터 기능을 제공한다.

물리계층 - NIC, 리피터 , AP

- NIC (Network Interface Card)
- **네트워크 카드, 랜카드, 닉카드, 이더넷카드** 등으로 불림
- 네트워크 인터페이스 카드는 2대 이상의 컴퓨터 네트워크를 구성하는 데 사용하며, 네트워크와 빠른 속도로 데이터를 송수신할 수 있도록 컴퓨터 내에 설치하는 확장 카드 고유의 식별번호인 MAC 주소가 있다.

물리계층 - NIC, 리피터 , AP

- 리피터(Repeater) :
- 들어오는 약해진 신호 정도를 증폭해 다른 쪽으로 전달하는 장치
- 긴 케이블일수록 신호가 약해지기 때문에 신호를 멀리 보내기 위한 증폭 장치이다.
- 이를 통해 패킷이 더 멀리 갈 수 있다. 하지만 이는 광케이블이 보급됨에 따라 현재는 잘 쓰이지 않는다.

물리계층 - NIC, 리피터 , AP

- AP(Access Point):
 - 패킷을 복사하는 기기
 - 스위치 허브
- AP에 유선 LAN을 연결한 후 다른 장치에서 무선 LAN 기술(와이파이 등)을 사용하여 무선 네트워크 연결을 할 수 있다.