네트워크 계층 별 장비

2025.08.16 토

최병주

1계층 (물리 계층) 장비

- **리피터 (Repeater)**
  - **특징**
    - 신호 증폭 및 재생
      - 약해진 전기 신호를 원래의 강도로 복원하여 더 먼 거리까지 전송
  - **장점**
    - 저렴한 가격
    - 간단한 설치
    - 전송 거리 확장
  - **단점**
    - 충돌
      - 충돌(Collision)이 발생하면 리피터에 연결된 모든 장비에 영향.
    - 노이즈 증폭:
      - 신호뿐만 아니라 잡음(Noise)까지 함께 증폭하여 전송.
    - 제한적인 확장성
      - 연결할 수 있는 장비의 수에 한계가 있습니다.

현재는 비효율성, 상위 장비에 흡수되어 사용되지 않음.

1계층 (물리 계층) 장비

- **허브 (Hub)**
  - **특징**
    - 여러 장치 연결
      - 리피터와 유사하지만 여러 개의 포트를 통해 여러 장비 한 번에 연결
    - 반이중 통신 (Half-duplex)
      - 송신과 수신이 동시에 불가능한 특성
  - 장점
    - 저렴한 가격
    - 간단한 구조
    - 네트워크 구성 용이
  - **단점**
    - 브로드캐스팅으로 인한 네트워크 부하 → 모든 장치에 데이터 전송
    - 충돌
      - 충돌(Collision)이 발생하면 허브에 연결된 장비에 영향

현재는 비효율성, 상위 장비에 흡수되어 사용되지 않음.

2계층 (데이터 링크 계층) 장비

브릿지 (Bridge)

- **특징**
  - 네트워크 분리
    - 두 개의 독립적인 근거리 통신망(LAN)을 연결
  - MAC 주소 학습
    - 자신의 포트에 연결된 장비들의 MAC 주소를 MAC 주소 테이블에 기록
    - 이를 통해 다시 브로드캐스팅 하지 않음
  - 필터링(Filtering)
    - 트래픽 검사를 통한 불필요한 트래픽 차단
  - 충돌 도메인 분리:
    - 브릿지를 기반으로 한 도메인 분리가 가능
- **장점**
  - 네트워크 성능 향상
  - 충돌 감소
- **단점**
  - 브로드 캐스트를 완전히 방지하지 못함
  - 스위치 대비 부족한 성능
    - 소프트웨어 기반의 데이터 처리

2계층 (데이터 링크 계층) 장비

스위치 (Switch)

- **특징**
  - 고성능 브리지
  - ASIC (Application-Specific Integrated Circuits)를 통한 하드웨어 처리
  - 포트별 충돌 도메인 분리
  - 전이중 통신(FulI-Duplex)
  - 가상 랜(VLAN), 스패닝 트리 프로토콜(STP) 등 고급 기능 지원
    - STP → 네트워크의 루프를 방지(참고)
- **장점**
  - 빠른 속도
  - 높은 효율
    - 포트별 대역폭 할당 가능
  - 확장성
    - 많은 포트를 통한 대규모 네트워크 구성에 유리
- **단점**
  - 브릿지 대비 고비용
  - 브로드캐스트 구성
    - VLAN으로 방지 가능

2계층 (데이터 링크 계층) 장비

	브리지 (Bridge)	스위치 (Switch)	설명
작동 계층	2계층 (데이터 링크)	2계층 (데이터 링크)	**MAC 주소를 읽어 데이터를 처리합니다.**
핵심 기능	네트워크 분리 및 연결	네트워크 분리 및 연결	**LAN.**
충돌 도메인 분할	O	O	**장비를 기반으로 한 도메인 분리**
처리 방식	소프트웨어 기반	**하드웨어(ASIC 칩) 기반**	**하드웨어 vs 소프트웨어로 인한 성능차**
속도	상대적으로 느림	**매우 빠름**	**처리 방식으로 인한 성능차이**
포트 수	소수 (주로 2개)	**다수 (4 ~ 48개 이상)**	**스위치가 더 큰 확장성을 가짐**
통신 방식	반이중(Half-duplex)	**전이중(Full-duplex)**	**반이중의 경우 송/수신 동시 불가**
현재 사용 여부	거의 사용 안 함	**보편적으로 사용**	**스위치로 많이 대체**

3계층 (네트워크 계층) 장비

라우터 (Router)

- **특징**
  - 경로 설정
  - IP 주소 기반으로 IP 주소를 읽어 네트워크 확인
  - 네트워크간의 연결(내부망 <-> 인터넷) 게이트웨이
  - 브로드캐스트 도메인 분리
  - 패킷 필터링
    - IP 주소, 포트 번호 기반의 방화벽 수행 가능
- **장점**
  - 대규모 네트워크를 효율적으로 구성하고 확장 가능
  - 브로드 캐스트 차단과 패킷 필터링을 통한 안정성과 보안
  - 최적 경로 라우팅 프로토콜 제공
- **단점**
  - 스위치 대비 느린 속도
  - 다양한 기능으로 인한 복잡도

라우팅(Routing) 이란?

구분	정적 라우팅 (Static Routing)	동적 라우팅 (Dynamic Routing)
경로 설정	수동 설정	라우터끼리 정보를 교환하여 자동으로 학습
장점	라우팅 테이블에 정해진 경로로만 통신 경로를 매번 계산할 필요 없어 리소스 소모가 적음 네트워크 설정의 직관성	동적 경로 설정을 통한 최적의 경로로 통신 네트워크가 변경/확장시에도 알아서 처리됨
단점	네트워크 변경/확장에 제한적 문제 발생시 수동 조치가 필요함	주기적인 경로 정보 교환 수행으로 자원 소모 잘못된 경로 유입 가능성 초기 설정의 복잡성과 이해가 필요
주요 사용 환경	소규모, 보안이 중요한 단순한 네트워크	대규모이거나 변화가 잦은 복잡한 네트워크
대표 프로토콜	-	RIP, OSPF, EIGRP, BGP 등

4계층(전송 계층) 장비

로드 밸런서 (Load Balancer) / L4 스위치

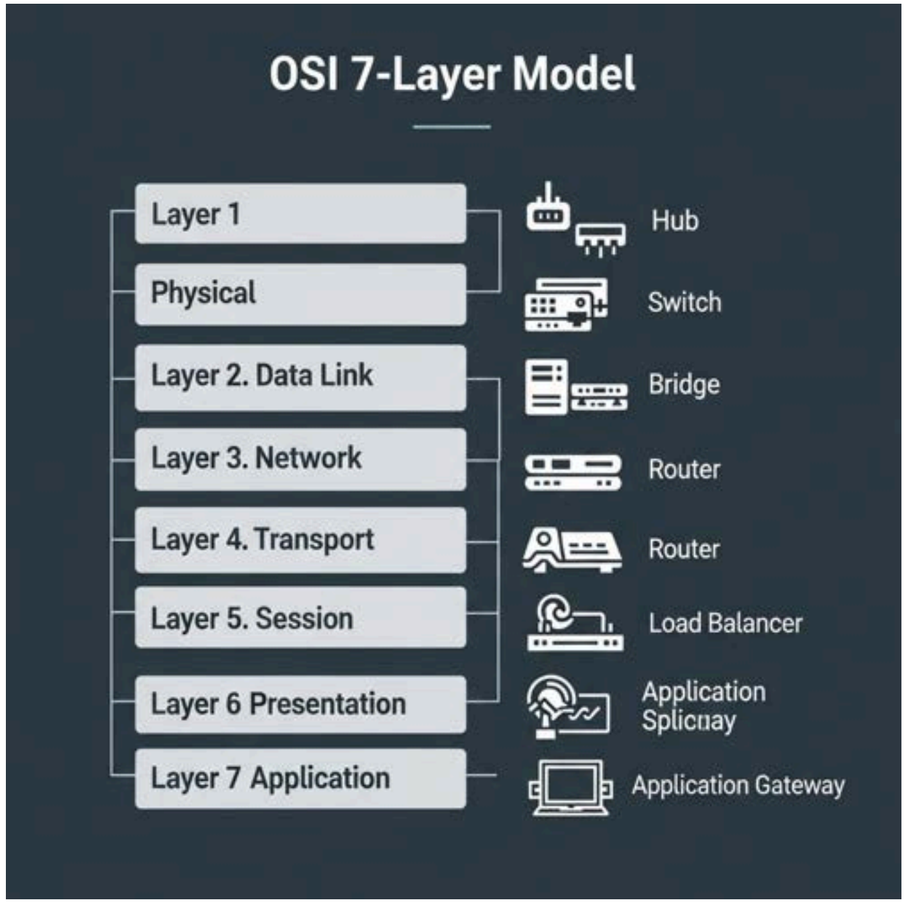
- **특징**
  - 서비스 안정성 확보
    - 특정 서버의 상태를 체크하여 이상시 전송하지 않음
  - 부하 분산
  - 포트 번호 기반의 접근제어(80, 443, 3306...)
- **장점**
  - 가용성 및 안정성
  - 유연한 확장성
- **단점**
  - 로드밸런서 장애 발생시 치명적인 문제 발생 가능 → 단일 장애점(SPOF)
    - 여러 클라우드 서비스에선 이중화 구성이 필수적으로 설정됨
  - 헬스 체크 구성, 포트 번호 분리, 로드밸런싱 알고리즘 등 최적화가 필요

4계층(전송 계층) 장비

방화벽

- **특징**
  - 접근제어
    - IP와 포트 번호 기반의 정책 설정(white list, black list)
  - 네트워크 분리
    - 외부 인터넷과 내부 사설망(Ingress/Egress)를 구분하여 내부를 보호
  - 로깅을 통한 흐름추적
- **장점**
  - 네트워크 보안 강화
  - 불필요한 접근과 유출 통제
- **단점**
  - 모든 트래픽을 검사하므로 성능 저하와 병목 발생 가능성
  - 네트워크에 대한 이해가 필수적임
  - 기본적으로 Ingress에 대한 방어에 중점

네트워크 장비 정리



특징 정리

- 네트워크 장비라고 한다면 다양한 하드웨어 장비뿐만 아니라 소프트웨어 형식도 많음
  - ADC(Application Delivery Controller)
- 계층별 역할을 명확히 나누기보단 상위 장비의 발전으로 유동적으로 통합되고 사라짐
- **계층별 특징**
  - 1계층 (물리 계층 - Physical Layer)
    - 전기적, 기계적 신호를 주고받아 데이터를 전송 (예: 케이블, 허브)
  - 2계층 (데이터 링크 계층 - Data Link Layer)
    - MAC 주소를 사용하여 동일 네트워크 내에서 데이터 전송을 담당(예: 스위치)
  - 3계층 (네트워크 계층 - Network Layer)
    - IP 주소를 사용하여 다른 네트워크로 데이터를 전송하고 최적의 경로 탐색 (예: 라우터)
  - 4계층 (전송 계층 - Transport Layer)
    - 포트 번호를 사용하여 도착지 컴퓨터의 특정 프로세스(서비스)에 데이터 전달(예: L4 스위치)
  - 7계층 (응용 계층 - Application Layer)
    - 응용 프로그램과 상호작용하며 데이터를 처리합니다. (예: 웹 방화벽, L7 스위치)