

2단원. 데이터링크 계층과 스위칭

대상: 전공자 · 정보처리기사 취득자 | 목적: 인프라 직무 기술 면접 대비 중요도: ★★★ 최빈출 · ★★ 자주 출제 · ★ 기본 개념

Q1. MAC 주소란 무엇이고 IP 주소와 어떻게 다른가요? ★★★

답안 MAC 주소는 NIC에 부여된 48비트 물리 주소(예: 00:1A:2B:3C:4D:5E)로, 앞 24비트는 제조사(OUI), 뒤 24비트는 일련번호입니다. **같은 네트워크(L2 세그먼트) 안에서** 장비를 식별하며 원칙적으로 변하지 않습니다. IP 주소는 논리 주소로 네트워크 위치에 따라 바뀌며 **네트워크 간** 전달에 쓰입니다. 통신 시 IP 주소는 종단 간 유지되지만, MAC 주소는 **홉마다** 다음 장비의 것으로 교체됩니다. "IP는 집 주소, MAC은 주민번호" 비유와 함께, 라우터를 거널 때 프레임의 출발/목적 MAC이 어떻게 바뀌는지 설명할 수 있어야 합니다.

관련 개념 OUI, L2 vs L3 주소, 홉 단위 MAC 교체, MAC 스푸핑 가능성

Q2. ARP의 동작 과정을 설명하세요. ★★★

답안 ARP는 IP 주소로 MAC 주소를 알아내는 프로토콜입니다. 목적지 IP가 같은 서브넷이면 그 IP의 MAC을, 다른 서브넷이면 **기본 게이트웨이의 MAC**을 조회합니다. 과정은 ① "이 IP 가진 사람 MAC 알려줘"라는 ARP 요청을 브로드캐스트 → ② 해당 IP 소유자만 자신의 MAC을 유니캐스트로 응답 → ③ 결과를 ARP 캐시에 저장(수 분 TTL)합니다. 보안 관점에서 ARP는 인증이 없어 **ARP 스푸핑**(공격자가 게이트웨이인 척 응답해 트래픽 가로채기)에 취약하며, 정적 ARP나 DAI(Dynamic ARP Inspection)로 방어합니다.

관련 개념 ARP 캐시(arp -a), GARP, ARP 스푸핑과 중간자 공격, DAI

Q3. 스위치는 어떻게 동작하나요? (MAC 학습과 포워딩) ★★★

답안 스위치는 프레임의 **출발지 MAC**을 보고 어느 포트에 어떤 장비가 있는지 **학습**해 MAC 주소 테이블을 만듭니다. 이후 수신 프레임의 **목적지 MAC**이 테이블에 있으면 해당 포트로만 전달(포워딩)하고, 없으면 수신 포트를 제외한 전 포트로 뿌립니다(플러딩). 브로드캐스트 주소(FF:FF:...)도 전 포트로 전달합니다. 허브와 달리 포트별로 충돌 도메인을 분리해 전이중 통신이 가능합니다. 테이블 항목은 에이징 타임(기본 300초)이 지나면 삭제됩니다. 공격 관점에서 MAC 플러딩으로 테이블을 넘치게 하면 스위치가 허브처럼 동작해 스니핑이 가능해집니다(포트 시큐리티로 방어).

관련 개념 MAC 주소 테이블, 플러딩, 충돌 도메인 분리, 포트 시큐리티

Q4. 충돌 도메인과 브로드캐스트 도메인의 차이를 설명하세요. ★★★

답안 **충돌 도메인**은 두 장비가 동시에 전송하면 충돌이 나는 범위입니다. 허브는 전체가 하나의 충돌 도메인이지만, 스위치는 **포트마다** 충돌 도메인을 분리하고 전이중에서는 충돌 자체가 없습니다. **브로드캐스트 도메인**은 브로드캐스트 프레임이 도달하는 범위로, 스위치는 분리하지 못하고 **라우터(또는 VLAN)**가 분리합니다. 정리하면 스위치=충돌 도메인 분

리, 라우터=브로드캐스트 도메인 분리입니다. 브로드캐스트 도메인이 너무 크면 ARP·DHCP 트래픽만으로도 부하가 커지므로 서브넷/VLAN 분할이 필요합니다.

관련 개념 허브 vs 스위치 vs 라우터, CSMA/CD, VLAN의 도메인 분리

Q5. VLAN이란 무엇이고 왜 사용하나요? ★★★

답안 VLAN은 하나의 물리 스위치를 논리적으로 여러 네트워크(브로드캐스트 도메인)로 분할하는 기술입니다. 목적은 ① 브로드캐스트 트래픽 축소, ② 부서·용도별 트래픽 격리로 보안 강화(서버망/사무망/게스트망 분리), ③ 물리 배선 변경 없이 논리적 네트워크 재구성입니다. 스위치 간 VLAN을 넘겨줄 때는 **트렁크 포트**가 프레임에 802.1Q 태그(VLAN ID, 12비트로 최대 4094개)를 붙여 전달합니다. VLAN 간 통신은 L2에서 불가능하고 라우터나 **L3 스위치(SVI)**를 거쳐야 하며, 이를 인터-VLAN 라우팅이라 합니다.

관련 개념 802.1Q 태그, 액세스/트렁크 포트, 인터-VLAN 라우팅, 네이티브 VLAN

Q6. STP(Spanning Tree Protocol)는 왜 필요한가요? ★★

답안 스위치를 이중화하려고 링크를 루프 형태로 구성하면, 이더넷 프레임에는 TTL이 없어 **브로드캐스트 프레임이 무한 순환**하며 네트워크를 마비시킵니다(브로드캐스트 스톰). 또한 MAC 테이블이 계속 요동칩니다. STP는 스위치들이 BPDU를 교환해 루트 브리지를 선출하고, 루프를 만드는 일부 포트를 **차단(blocking)** 상태로 두어 논리적 트리 구조를 만듭니다. 링크 장애 시 차단 포트를 활성화해 우회 경로를 살립니다. 수렴이 느린 원조 STP 대신 RSTP(802.1w)가 표준이며, 데이터센터에서는 STP의 비효율(차단 포트=낭비) 때문에 MLAG나 스판-리프+L3 설계로 대체하는 추세입니다.

관련 개념 브로드캐스트 스톰, 루트 브리지 선출, RSTP, MLAG/vPC

Q7. 이더넷 CSMA/CD의 동작 원리를 설명하세요. ★★

답안 반이중 공유 매체에서의 접근 제어 방식으로, **전송 전 매체를 감지(Carrier Sense)**해 사용 중이면 대기하고, 비어 있으면 전송하되 **전송 중에도 충돌을 감지(Collision Detection)**합니다. 충돌이 나면 잼 신호를 보내 모두에게 알리고, 랜덤한 시간(지수 백오프) 후 재전송합니다. 무선랜은 충돌 감지가 어려워 **CSMA/CA**(충돌 회피: 전송 전 대기과 ACK 확인)를 씁니다. 현대 스위치 기반 전이중 이더넷에서는 충돌이 없어 CSMA/CD가 사실상 비활성이지만, 원리는 여전히 단골 시험 문제입니다.

관련 개념 지수 백오프, 반이중/전이중, CSMA/CA(무선), 잼 신호

Q8. 데이터링크 계층의 오류 검출 방식(패리티, CRC, 체크섬)을 비교하세요. ★★

답안 **패리티 비트**는 1의 개수를 짝수/홀수로 맞추는 가장 단순한 방식으로, 짝수 개 비트 오류는 놓칩니다. **CRC**는 데이터를 생성 다항식으로 나눈 나머지를 붙이는 방식으로, 버스트 오류 검출력이 강력해 이더넷 프레임(FCS 필드)이 사용됩니다. **체크섬**은 데이터를 워드 단위로 합산하는 방식으로 계산이 가벼워 IP/TCP/UDP 헤더가 사용하지만 검출력은

CRC보다 약합니다. 검출 후 처리는 계층에 따라 달라, 이더넷은 오류 프레임을 폐기만 하고 재전송은 상위 계층(TCP)에 맡깁니다.

관련 개념 FCS, 생성 다항식, 버스트 오류, 검출 vs 정정(FEC)

Q9. L2 스위치와 L3 스위치의 차이는 무엇인가요? ★★

답안 L2 스위치는 MAC 주소 기반 프레임 포워딩만 합니다. L3 스위치는 여기에 **하드웨어(ASIC) 기반 IP 라우팅**을 더한 장비로, VLAN 간 라우팅(인터-VLAN)을 라우터 없이 처리합니다. 전통 라우터와 비교하면 L3 스위치는 포트 밀도가 높고 LAN 내부 라우팅이 빠른 대신, WAN 인터페이스·NAT·VPN 같은 기능은 제한적입니다. 일반적 설계는 액세스 계층에 L2, 분배/코어 계층에 L3 스위치를 두고, 인터넷 경계에 라우터/방화벽을 두는 구조입니다.

관련 개념 ASIC 포워딩, SVI, 캠퍼스 3계층 설계(액세스/분배/코어)

Q10. MTU와 점보 프레임, 그리고 MTU 불일치 시 생기는 문제를 설명하세요. ★★

답안 MTU는 한 프레임에 실을 수 있는 최대 페이로드 크기로 이더넷 표준은 1500바이트입니다. **점보 프레임**(약 9000바이트)은 헤더·인터럽트 오버헤드를 줄여 스토리지 네트워크(iSCSI, NFS)나 데이터센터 내부에서 처리량을 높이지만, **경로상 모든 장비**가 지원해야 합니다. 경로 중간에 MTU가 작은 구간이 있으면 IP 단편화가 일어나거나, DF 비트가 설정된 경우 ICMP "Fragmentation Needed"로 통보됩니다. 방화벽이 이 ICMP를 막으면 **PMTUD 블랙홀**(작은 패킷은 되는데 큰 패킷만 조용히 실패)이 발생하는데, "ping은 되는데 파일 전송이 안 돼요" 유형의 실무 장애 단골 원인입니다. VPN·오버레이(VXLAN) 터널은 캡슐화 헤더만큼 실효 MTU가 줄어드는 점도 주의해야 합니다.

관련 개념 IP 단편화, DF 비트, PMTUD, VXLAN 오버헤드(50바이트), MSS 클램핑

Q11. 링크 애그리게이션(LACP)이란 무엇인가요? ★

답안 여러 물리 링크를 하나의 논리 링크로 묶어 **대역폭 합산**과 **링크 이중화**를 동시에 얻는 기술입니다(802.3ad/802.1AX). LACP는 양단이 협상해 묶음을 자동 구성·감시하는 프로토콜입니다. 트래픽은 플로우 단위 해시(출발/목적 MAC·IP·포트)로 멤버 링크에 분산되므로, **단일 플로우에 한 링크 이상의 속도를 낼 수 없다**는 점이 중요합니다. 서버 본딩(리눅스 bonding/teaming), 스위치 업링크에 널리 쓰입니다.

관련 개념 802.3ad, 해시 기반 분산, 리눅스 bonding 모드, MLAG와 조합

Q12. 무선랜(Wi-Fi)과 유선 이더넷의 근본적 차이는 무엇인가요? ★

답안 무선은 **공유·개방 매체**라는 점이 근본 차이입니다. ① 반이중 통신이며 같은 채널의 모든 단말이 에어타임을 나눠 씁니다(밀집 환경 성능 저하). ② 충돌 감지가 불가능해 CSMA/CA와 ACK로 회피·확인합니다. ③ 전파는 도청이 쉬워 암호화(WPA2/WPA3)가 필수입니다. ④ 신호 세기·간섭·거리에 따라 전송률이 계속 변합니다(레이트 어댑테이션). ⑤ 히든 노드 문제(서로 안 들리는 두 단말이 AP에서 충돌)는 RTS/CTS로 완화합니다. 그래서 '표기 속도'와 실제 처리량 차이가 유선보다 훨씬 큼니다.

관련 개념 CSMA/CA, WPA2/WPA3, 히든 노드와 RTS/CTS, 채널 간섭(2.4/5/6GHz)
