

3단원. 네트워크 계층: IP 주소와 서브네팅 (최빈출 단원)

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

Q1. IPv4 주소의 구조와 클래스, 그리고 CIDR가 등장한 배경을 설명하세요. ★★★

답안 IPv4는 32비트 주소로 네트워크 부분과 호스트 부분으로 나뉩니다. 초기에는 A(/8), B(/16), C(/24) 클래스로 고정 분할했지만, B는 너무 크고(6.5만 호스트) C는 너무 작아(254 호스트) 주소가 심하게 낭비됐습니다. **CIDR**는 클래스를 없애고 프리픽스 길이(/22 등)로 **필요한 만큼만** 네트워크를 자르는 방식이며, 여러 네트워크를 하나의 프리픽스로 묶는 **경로 집약(supernetting)**으로 라우팅 테이블 크기도 줄였습니다. 현재 인터넷 라우팅은 전부 CIDR 기반입니다.

관련 개념 클래스풀 vs 클래스리스, 프리픽스 표기, 경로 집약, 주소 고갈

Q2. 서브넷 마스크란 무엇이고, 서브네팅은 왜 하나요? ★★★

답안 서브넷 마스크는 IP 주소에서 **어디까지가 네트워크이고 어디부터가 호스트인지** 구분하는 32비트 값입니다 (255.255.255.0 = /24). IP와 마스크를 AND 연산하면 네트워크 주소가 나오고, 두 IP의 네트워크 주소가 같으면 같은 서브넷(직접 통신), 다르면 게이트웨이를 거칩니다. 서브네팅의 목적은 ① 브로드캐스트 도메인 축소, ② 부서·용도별 망 분리, ③ 주소 공간의 효율적 배분, ④ 계층적 주소 설계로 라우팅 단순화입니다.

관련 개념 AND 연산, 네트워크/브로드캐스트 주소, 기본 게이트웨이 판단 로직

Q3. 192.168.10.0/26 네트워크에서 사용 가능한 호스트 수와 각 서브넷 범위를 구하세요. ★★★

답안 /26은 호스트 비트가 6비트이므로 서브넷당 주소 64개, 사용 가능한 호스트는 64-2(네트워크 주소, 브로드캐스트 주소 제외)=**62개**입니다. 192.168.10.0/24를 /26으로 나누면 4개 서브넷: ① .0~.63(네트워크 .0, 브로드캐스트 .63), ② .64~.127, ③ .128~.191, ④ .192~.255. 각 서브넷의 첫/끝 주소를 뺀 범위가 호스트 할당 가능 구간입니다. 이런 계산은 "255.255.255.192가 마스크", "블록 크기는 256-192=64"로 빠르게 푸는 연습이 필요하며, 정보처리기사와 인프라 면접 양쪽에서 가장 흔한 계산 문제입니다.

관련 개념 $2^n - 2$ 공식, 블록 크기 계산법, /31·/32의 예외(P2P 링크, 호스트 라우트)

Q4. 공인 IP와 사설 IP의 차이, 사설 대역 3가지를 말해보세요. ★★★

답안 공인 IP는 인터넷에서 유일하며 IANA/ISP가 할당합니다. **사설 IP**는 내부망에서 자유롭게 쓰는 주소로 인터넷에서 라우팅되지 않으며, RFC 1918이 **10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16** 세 대역을 정의합니다. 사설 IP 장비가 인터넷에 나가려면 NAT로 공인 IP로 변환해야 합니다. 실무에서는 클라우드 VPC CIDR 설계 시 온프레미스 대역과 겹치지 않게 잡는 것(겹치면 VPN/전용선 연결 시 라우팅 충돌)이 중요한 포인트로 자주 출제됩니다. 추가로 169.254.0.0/16(APIPA, DHCP 실패 시 자동 할당)도 알아두면 좋습니다.

Q5. NAT의 동작 원리와 종류(SNAT/DNAT/PAT)를 설명하세요. ★★★

답안 NAT는 IP 헤더의 주소를 변환해 사설망과 인터넷을 연결합니다. **SNAT**는 출발지 주소를 변환하며, 내부→인터넷 방향에서 사설 IP를 공인 IP로 바꿉니다. **PAT(NAPT)**는 포트 번호까지 활용해 **공인 IP 하나를 수많은 내부 장비가 공유** 하는 방식으로, 가정용 공유기와 클라우드 NAT 게이트웨이가 이것입니다. 변환 테이블(내부IP:포트 ↔ 공인IP:포트)을 유지하며 응답을 역변환합니다. **DNAT**는 목적지 주소를 변환하며, 외부에서 들어온 요청을 내부 서버로 보내는 포트 포워딩·로드밸런서에 쓰입니다. NAT는 주소 절약과 내부망 은닉 효과가 있지만, 종단 간 연결성을 깨서 P2P·IPsec에 문제를 일으키고 상태 테이블이 병목이 될 수 있습니다.

관련 개념 PAT/NAPT, 포트 포워딩, NAT 테이블 고갈, 헤어핀 NAT, STUN(NAT 통과)

Q6. IP 헤더의 TTL 필드는 어떤 역할을 하나요? ★★★

답안 TTL은 패킷이 통과할 수 있는 최대 홉 수로, **라우터를 지날 때마다 1씩 감소**하고 0이 되면 폐기되며 발신자에게 ICMP Time Exceeded를 보냅니다. 목적은 라우팅 루프에 빠진 패킷이 영원히 도는 것을 방지하는 것입니다. **traceroute**는 이를 역이용해 TTL을 1, 2, 3...으로 올려 보내며 각 홉에서 돌아오는 Time Exceeded 응답으로 경로를 알아냅니다. OS별 초기값(리눅스 64, 윈도우 128)이 달라 ping 응답의 TTL로 상대 OS를 추정하기도 합니다.

관련 개념 라우팅 루프 방지, traceroute 원리, ICMP Time Exceeded, IPv6의 Hop Limit

Q7. ICMP는 어떤 프로토콜이고 ping은 어떻게 동작하나요? ★★★

답안 ICMP는 IP 계층의 **오류 통보와 진단용** 프로토콜입니다(포트 개념 없음). 주요 메시지는 Echo Request/Reply(ping), Destination Unreachable(호스트·포트 도달 불가), Time Exceeded(TTL 만료), Fragmentation Needed(PMTUD)입니다. ping은 Echo Request를 보내고 Reply가 오기까지의 RTT와 손실률을 측정합니다. 주의할 점은 방화벽이 ICMP를 차단하는 경우가 많아 "ping 안 됨 ≠ 서비스 다운"이라는 것이며, 반대로 ICMP를 전부 막으면 PMTUD가 깨져 통신 장애를 만들 수 있어 선별적 허용이 바람직합니다.

관련 개념 Echo Request/Reply, Unreachable 코드, PMTUD와 ICMP 차단 부작용, ICMP 플러드

Q8. IPv6의 특징과 IPv4 대비 개선점을 설명하세요. ★★

답안 IPv6는 **128비트** 주소로 고갈 문제를 근본 해결합니다(2^{128} 개). 개선점은 ① 헤더 단순화·고정 길이(40바이트)로 라우터 처리 효율화, ② **NAT 불필요**한 종단 간 연결성 복원, ③ SLAAC로 주소 자동 구성(DHCP 없이 RA 기반), ④ IPsec 지원 내장, ⑤ 브로드캐스트 제거(멀티캐스트로 대체), ⑥ 라우터에서 단편화 금지(출발지만 수행)입니다. 표기는 콜론 16진수(2001:db8::1, 연속된 0은 ::로 축약 1회 가능)입니다. 전환 기술로 듀얼 스택(양쪽 동시 운영, 주류), 터널링, NAT64/DNS64가 있습니다.

관련 개념 SLAAC/RA, 링크로컬(fe80::/10), 듀얼 스택, NAT64, 주소 축약 규칙

Q9. 기본 게이트웨이가 없으면 어떤 통신이 안 되나요? ★★

답안 같은 서브넷 내 통신은 ARP와 L2 포워딩만으로 가능하므로 정상 동작하지만, 다른 서브넷·인터넷으로 나가는 모든 통신이 불가능해집니다. 호스트는 목적지 IP를 서브넷 마스크와 비교해 외부라고 판단하면 패킷을 게이트웨이 MAC으로 보내는데, 그 대상이 없기 때문입니다. 실무 트러블슈팅에서 "내부 서버끼리는 되는데 인터넷만 안 돼요"의 1순위 점검 항목이 게이트웨이 설정(및 게이트웨이 장비의 상태)이며, ip route(리눅스), route print(윈도우)로 확인합니다.

관련 개념 라우팅 판단 로직, 기본 경로(0.0.0.0/0), ip route, 게이트웨이 이중화(VRRP)

Q10. DHCP의 동작 과정(DORA)을 설명하세요. ★★★

답안 DHCP는 IP 주소, 서브넷 마스크, 게이트웨이, DNS 서버를 자동 할당합니다. 과정은 DORA: ① **Discover** — 클라이언트가 브로드캐스트로 서버 탐색, ② **Offer** — 서버가 사용 가능한 IP 제안, ③ **Request** — 클라이언트가 특정 제안 수락을 브로드캐스트(서버 여럿일 때 선택 알림), ④ **Ack** — 서버가 임대(lease) 확정. 임대 기간의 50% 시점에 갱신을 시도합니다. 서브넷마다 브로드캐스트가 같으므로, 중앙 DHCP 서버를 쓸 때는 라우터에 **DHCP 릴레이**를 설정합니다. 보안 이슈로 비인가 DHCP 서버(rogue)가 잘못된 게이트웨이를 뿌리는 공격이 있으며 DHCP 스누핑으로 방어합니다.

관련 개념 DORA, 임대 갱신(T1/T2), DHCP 릴레이, DHCP 스누핑, 고정 임대(reservation)

Q11. IP 단편화는 언제 발생하고 왜 피해야 하나요? ★★

답안 패킷이 링크 MTU보다 크면 라우터(IPv4)나 출발지가 패킷을 조각으로 나눕니다. 재조립은 최종 목적지에서만 수행합니다. 피해야 하는 이유는 ① 조각 하나만 유실돼도 전체 패킷 재전송, ② 라우터·호스트의 처리 부담, ③ 방화벽이 조각을 차단하거나 조각을 악용한 공격(티어드롭 등)이 존재, ④ IPv6는 라우터 단편화를 아예 금지하기 때문입니다. 실무 대응은 PMTUD로 경로 MTU를 탐지하고, TCP는 **MSS**를 조정(터널 구간에서 MSS 클램핑)해 단편화 자체를 예방하는 것입니다.

관련 개념 단편화 오프셋/식별자, PMTUD, MSS 클램핑, VPN 구간 MTU 이슈

Q12. VRRP 같은 게이트웨이 이중화 프로토콜은 왜 필요한가요? (인프라 연계) ★★

답안 기본 게이트웨이는 서브넷의 단일 장애점입니다. 라우터가 죽으면 해당 서브넷 전체가 외부와 단절됩니다. **VRRP**는 라우터 두 대 이상이 **가상 IP(VIP)**와 **가상 MAC**을 공유하고, 마스터가 광고(advertisement)를 보내다 죽으면 백업이 수 초 내 마스터로 승격해 같은 VIP로 서비스를 잇는 표준 프로토콜입니다. 호스트 입장에서는 게이트웨이 IP가 그대로라 무중단 전환됩니다. 시스코 전용 HSRP, 로드 분산이 가능한 GLBP도 같은 계열이며, 방화벽·로드밸런서 이중화에도 동일한 VIP 개념이 쓰입니다. keepalived가 리눅스에서 VRRP를 구현한 대표 도구입니다.

관련 개념 VIP, 마스터/백업 선출, keepalived, HSRP, 프리엠션

Q13. 클라우드 VPC 설계 시 CIDR와 서브넷은 어떻게 잡아야 하나요? (인프라 연계) ★★★

답안 ① **CIDR 크기**: 향후 확장을 고려해 넉넉히(/16 권장), 단 온프레미스·타 VPC와 **겹치지 않게** 잡습니다. 겹치면 VPN·피어링 시 라우팅이 불가능합니다. ② **서브넷 분할**: 가용영역(AZ)별 × 용도별(퍼블릭/프라이빗/DB)로 나눕니다. 퍼블릭 서브넷은 IGW 경로를, 프라이빗은 NAT 게이트웨이 경로를 갖습니다. ③ **예약 주소**: AWS는 서브넷당 5개(네트워크, 라우터, DNS, 예약, 브로드캐스트)를 제외하고 할당됩니다. ④ **쿠버네티스**를 쓰면 파드가 IP를 대량 소비하므로 (EKS의 VPC CNI) 서브넷을 크게 잡아야 합니다. IP 고갈은 실제로 흔한 운영 장애입니다.

관련 개념 VPC 피어링과 CIDR 중복, 퍼블릭/프라이빗 서브넷, NAT 게이트웨이, 파드 IP 고갈

Q14. 같은 서브넷의 두 호스트 통신과 다른 서브넷 간 통신의 패킷 흐름 차이를 설명하세요. ★★★

답안 **같은 서브넷**: 출발 호스트가 목적지 IP를 마스크와 비교해 같은 네트워크임을 확인 → 목적지 IP의 MAC을 ARP로 조회 → 프레임의 목적지 MAC=상대방 MAC으로 직접 전송(스위치 공유). **다른 서브넷**: 외부 네트워크로 판단 → **게이트웨이 MAC**을 ARP로 조회 → 목적지 IP는 최종 상대로 유지한 채 목적지 MAC만 게이트웨이로 설정해 전송 → 라우터가 IP를 보고 다음 홉으로 라우팅하며 홉마다 MAC 재작성. 핵심 문장은 "IP 주소는 끝까지 유지되고, MAC 주소는 홉마다 바뀐다"이며, 이 원리를 정확히 설명하면 L2/L3 이해를 한 번에 증명할 수 있습니다.

관련 개념 온링크 판단, ARP 대상 결정, 홉바이홉 포워딩, 라우터의 TTL 감소·체크섬 재계산

Q15. 0.0.0.0, 127.0.0.1, 255.255.255.255는 각각 어떤 주소인가요? ★★

답안 **0.0.0.0**은 '모든 인터페이스' 또는 '미지정 주소'입니다. 서버가 0.0.0.0:80에 바인드하면 모든 NIC에서 요청을 받고, 라우팅 테이블의 0.0.0.0/0은 기본 경로를 뜻합니다. **127.0.0.1**은 루프백으로, 자기 자신과의 통신이며 패킷이 NIC 밖으로 나가지 않습니다(127.0.0.0/8 전체가 루프백). **255.255.255.255**는 제한된 브로드캐스트로 로컬 세그먼트의 전체에게 전달되며 라우터를 넘지 않습니다(DHCP Discover가 사용). 면접에서 "서버가 127.0.0.1에만 바인드되어 외부 접속이 안 되는 장애"(bind 주소 확인)는 흔한 실무 사례입니다.

관련 개념 바인드 주소, 루프백 인터페이스, 제한된/지향성 브로드캐스트, ss -tlnp 확인