↑ 목록으로 다음 단원 →

1단원. 네트워크 기초 개념 (실무 관점)

> 대상: 전공자 · 정보처리기사 취득자 | 목적: 인프라 직무(네트워크·클라우드·시스템·보안) 기술 면접 대비 중요도: ★★★ 최빈출 · ★★ 자주 출제 · ★ 기본 개념

> **Q1. VLAN**을 사용하는 이유와 트렁크 포트의 역할을 설명하세요.
> ★★★

답안 **VLAN(Virtual LAN)**은 물리적으로 하나의 스위치에 연결된 장비들을 논리적으로 여러 개의 브로드캐스트 도메인으로 분리하는 기술입니다. 부서별·업무별로 트래픽을 격리해 불필요한 브로드캐스트 확산을 줄이고 보안성을 높이며, 물리적 배선 변경 없이 네트워크 구성을 유연하게 바꿀 수 있다는 실무적 장점이 있습니다. 액세스 포트는 하나의 VLAN에 속한 단말이 연결되는 포트이고, 트렁크 포트는 여러 VLAN의 트래픽을 하나의 링크로 동시에 전달해야 할 때(스위치 간 연결, 스위치-라우터 연결) 사용하며 프레임에 **802.1Q** 태그를 붙여 어느 VLAN에 속한 프레임인지 구분합니다. 실무에서는 트렁크 포트에 허용 VLAN 목록을 명시적으로 지정하고 네이티브 VLAN을 기본값(VLAN1)에서 변경해 보안 사고를 예방합니다.

관련 개념 802.1Q 태깅, 네이티브 VLAN, 브로드캐스트 도메인, 스위치 포트 모드(access/trunk), VLAN 홉핑 공격

Q2. ARP의 동작 원리와 **ARP** 스푸핑(**ARP Poisoning**)이 발생하는 이유를 설명하세요. ★★★

답안 **ARP(Address Resolution Protocol)**는 같은 네트워크 세그먼트 안에서 목적지의 **IP** 주소에 대응하는 **MAC** 주소를 알아내기 위한 프로토콜로, 송신 호스트가 브로드캐스트로 ARP 요청을 보내면 해당 IP를 가진 호스트가 자신의 MAC 주소를 유니캐스트로 응답합니다. 이 응답 값은 **ARP** 캐시(테이블)에 일정 시간 저장되어 이후 통신 시 재활용됩니다. **ARP** 스푸핑은 ARP 프로토콜에 인증 절차가 없다는 점을 악용해 공격자가 위조된 ARP 응답을 보내 특정 IP에 대한 MAC 주소를 자신의 것으로 속이는 공격으로, 이를 통해 중간자 공격(**MITM**)이 가능해집니다. 실무에서는 스위치의 **Dynamic ARP Inspection(DAI)**이나 정적 ARP 등록, 포트 보안 기능으로 대응합니다.

관련 개념 ARP 캐시, 중간자 공격, DAI(Dynamic ARP Inspection), 포트 시큐리티, 게이트웨이 ARP 스푸핑

Q3. DHCP의 **IP** 할당 과정(**DORA**)을 설명하고, **DHCP Snooping**이 왜 필요한지 설명하세요. ★★★

답안 DHCP는 **DORA(Discover-Offer-Request-Acknowledge)** 4단계로 동작합니다. 클라이언트가 브로드캐스트로 **Discover**를 보내면, DHCP 서버가 사용 가능한 IP를 담아 **Offer**로 응답하고, 클라이언트가 그 중 하나를 선택해 **Request**를 보내면 서버가 **ACK**로 최종 할당을 확정합니다. 이 과정에서 인증 절차가 없기 때문에 공격자가 가짜 DHCP 서버를 네트워크에 올려 잘못된 게이트웨이나 DNS 정보를 배포하는 **Rogue DHCP** 공격이 가능합니다. **DHCP Snooping**은 스위치에서 신뢰할 수 있는 포트(정상 DHCP 서버가 연결된 포트)만 DHCP 응답 트래픽을 통과시키도록 제한하는 보안 기능으로, 실무에서는 액세스 스위치 단에서 이를 활성화해 비인가 DHCP 서버로부터 클라이언트를 보호합니다.

관련 개념 DORA 프로세스, Rogue DHCP, DHCP Snooping, 임대 시간(lease time), 릴레이 에이전트

> **Q4. NAT**의 종류(**Static NAT, Dynamic NAT, PAT**)를 비교하고 실무에서 어떤 상황에 사용되는지 설명하세요. ★★★

답안 **Static NAT**는 내부 사설 IP와 외부 공인 IP를 1:1로 고정 매핑하는 방식으로, 외부에서 접근해야 하는 서버(웹서버 등)에 사용합니다. **Dynamic NAT**는 공인 IP 풀 중 사용 가능한 주소를 그때그때 할당하는 방식이지만 공인 IP 개수만큼만 동시 접속이 가능해 실무에서는 잘 쓰이지 않습니다. **PAT(Port Address Translation, NAT Overload)**는 하나의 공인 IP를 포트 번호로 구분해 여러 내부 호스트가 동시에 공유하는 방식으로, 가정용 공유기나 사내 인터넷 게이트웨이에서 가장 널리 사용됩니다. NAT는 IPv4 주소 고갈 문제를 완화하고 내부 네트워크 구조를 외부에 숨기는 보안 효과도 있지만, 종단 간 연결성이 깨져 IPsec이나 일부 P2P 프로토콜에서는 별도 처리(NAT Traversal)가 필요합니다.

관련 개념 PAT/NAT Overload, 사설 IP 대역(RFC 1918), NAT Traversal, 포트포워딩, IPv4 고갈

> **Q5.** 스패닝 트리 프로토콜(**STP**)이 필요한 이유와 기본 동작 방식을 설명하세요. ★★

답안 이중화를 위해 스위치를 여러 경로로 연결하면 루프(**loop**)가 발생할 수 있고, 이는 브로드캐스트 스톰과 MAC 주소 테이블 불안정으로 이어져 네트워크 전체가 마비될 수 있습니다. **STP(Spanning Tree Protocol)**는 이러한 물리적 루프 구조에서 논리적으로 트리 형태의 경로만 활성화하고 나머지 경로는 차단(**Blocking**) 상태로 두어 루프를 방지합니다. 동작 과정에서 루트 브리지를 선출하고, 각 스위치는 루트까지의 최단 경로 포트(Root Port)와 세그먼트별 대표 포트(Designated Port)를 결정하며 나머지는 차단합니다. 실무에서는 수렴 속도가 느린 전통적 STP 대신 **RSTP(Rapid STP)**를 주로 사용하며, 링크 장애 시 대체 경로로 빠르게 전환됩니다.

관련 개념 루트 브리지, BPDU, 포트 상태(Blocking/Listening/Learning/Forwarding), RSTP, 브로드캐스트 스톰

> **Q6.** 라우팅 테이블에서 목적지를 결정하는 우선순위(롱기스트 매치)와 기본 게이트웨이의 역할을 설명하세요. ★★

답안 라우터나 호스트는 패킷을 전달할 때 라우팅 테이블에서 목적지 IP와 일치하는 여러 경로가 있으면 최장 프리픽스 일치(**Longest Prefix Match**) 원칙에 따라 서브넷 마스크가 가장 긴(가장 구체적인) 경로를 우선적으로 선택합니다. 예를 들어 10.0.0.0/24와 10.0.0.0/16이 동시에 존재하면 /24 경로가 우선합니다. 목적지 네트워크와 일치하는 경로가 테이블에 없을 경우 기본 게이트웨이(**default route,** 0.0.0.0/0)로 패킷을 전달해 외부 네트워크로 나가도록 합니다. 실무 트러블슈팅 시 라우팅 테이블 확인은 통신 장애의 원인을 파악하는 가장 기본적인 절차이며, 잘못된 정적 경로나 게이트웨이 미설정이 흔한 장애 원인입니다.

관련 개념 최장 프리픽스 일치, 디폴트 라우트, 정적/동적 라우팅, 서브넷 마스크, 라우팅 메트릭

> **Q7.** 서브넷팅이 필요한 이유와 **CIDR** 표기법을 예시와 함께 설명하세요. ★★

답안 서브넷팅은 하나의 큰 네트워크 대역을 여러 개의 작은 네트워크로 분할하는 것으로, IP 주소 낭비를 줄이고 브로드캐스트 도메인을 축소해 트래픽 효율과 보안을 높이는 목적으로 사용됩니다. **CIDR(Classless Inter-Domain Routing)** 표기법은 IP 주소 뒤에 `/24`처럼 네트워크 부분의 비트 수를 표시하는 방식으로, 클래스 기반 주소 체계의 한계를 극복하고 유연한 대역 분할을 가능하게 합니다. 예를 들어 192.168.1.0/24는 호스트 비트가 8비트이므로 254개의 호스트 주소를 사용할 수 있고, 이를 /26로 나누면 4개의 서브넷(각 62개 호스트)으로 분할할 수 있습니다. 실무에서는 부서별·용도별로 서브넷을 나누어 VLAN과 매칭시키고 접근 정책을 서브넷 단위로 적용하는 경우가 많습니다.

관련 개념 CIDR, 서브넷 마스크, 네트워크 주소/브로드캐스트 주소, VLSM, 호스트 비트 계산

> **Q8.** 게이트웨이 이중화를 위한 **HSRP/VRRP**의 개념을 설명하세요. ★★

답안 서버나 클라이언트는 통상 하나의 기본 게이트웨이만 설정하므로, 그 게이트웨이 역할을 하는 라우터/L3 스위치가 장애 나면 외부 통신이 전면 중단됩니다. **HSRP(Hot Standby Router Protocol, Cisco 독자)**와 **VRRP(Virtual Router Redundancy Protocol,** 표준)는 여러 대의 라우터가 하나의 가상 **IP·**가상 **MAC**을 공유하도록 그룹을 구성해, 평소에는 우선순위가 높은 라우터(Active/Master)가 트래픽을 처리하다가 장애 발생 시 대기 라우터(Standby/Backup)가 자동으로 그 역할을 이어받는 게이트웨이 이중화 기술입니다. 클라이언트 입장에서는 게이트웨이 IP가 바뀌지 않으므로 장애 전환이 투명하게 이루어집니다. 실무에서는 데이터센터 코어 스위치나 방화벽 이중화 구성에서 필수적으로 사용됩니다.

관련 개념 가상 IP/가상 MAC, Active/Standby, 우선순위(priority), Preempt, 게이트웨이 이중화

> **Q9.** 네트워크 연결 장애 발생 시 트러블슈팅 절차를 **OSI** 계층 관점에서 설명하세요. ★★

답안 실무 트러블슈팅은 보통 하위 계층부터 상위 계층 순서로 접근합니다. 먼저 물리 계층에서 케이블 연결, 링크 램프, 포트 상태를 확인하고, 데이터링크 계층에서 스위치 포트의 VLAN 설정과 MAC 주소 테이블, STP 상태를 점검합니다. 이후 네트워크 계층에서 `ping`, `traceroute`로 IP 연결성과 라우팅 경로를 확인하고, 전송 계층에서 포트가 열려 있는지, 방화벽에서 차단되지 않는지를 확인합니다. 마지막으로 애플리케이션 계층에서 DNS 해석, 서비스 자체의 응답 여부를 점검합니다. 이렇게 계층별로 원인을 좁혀가면 문제 범위를 빠르게 특정할 수 있으며, 실무에서는 `ping` → `traceroute` → `telnet/nc`로 포트 확인 → 애플리케이션 로그 확인의 순서가 흔히 사용됩니다.

관련 개념 ping/traceroute, 계층별 장애 분리, telnet/nc 포트 테스트, DNS 트러블슈팅, MTU 문제

> **Q10.** 인터페이스 이중화 기술인 링크 애그리게이션 **(EtherChannel/LACP)**의 목적을 설명하세요. ★

답안 링크 애그리게이션은 여러 개의 물리 링크를 하나의 논리적 링크로 묶어 대역폭을 증가시키고 회선 장애 시에도 나머지 링크로 트래픽을 지속 전달할 수 있게 하는 기술입니다. 표준 프로토콜인 **LACP(Link Aggregation Control Protocol)**는 양쪽 장비가 자동으로 묶을 링크를 협상하고 장애 링크를 감지해 그룹에서 제외하는 역할을 합니다. 트래픽 분산은 보통 출발지/목적지 MAC이나 IP, 포트 정보를 해시하는 방식으로 이루어지며, 완벽한 균등 분산이 보장되지는 않습니다. 실무에서는 서버-스위치 간, 스위치-스위치 간 업링크 구간에서 대역폭 확장과 이중화 목적으로 널리 사용됩니다.

관련 개념 LACP, EtherChannel, 로드밸런싱 해시 알고리즘, 포트 채널, 이중화(redundancy)
