

1.IPv4와 IPv6의 헤더 구성, 단편화 처리 및 관련 필드에 관한 다음 설명 중 옳지 않은 것은 무엇인가?

- ① IPv4 헤더 구성: IPv4 헤더는 기본적으로 20바이트의 고정 길이를 가지며, 단편화를 위해 식별자, 플래그(DF: 단편 금지, MF: 단편 이어짐)와 단편 오프셋 필드를 포함한다. 단편 오프셋은 8바이트 단위로 측정된다.
- ② IPv6 헤더 및 확장 헤더: IPv6 헤더는 고정 40바이트이며, 기본 헤더에는 단편화 관련 필드가 존재하지 않고, 단편화가 필요한 경우 Fragment 확장 헤더를 사용하여 처리한다.
- ③ TTL과 홉 제한: IPv4는 TTL(Time To Live) 필드를 사용해 패킷의 생명주기를 관리하며, 각 라우터 통과 시 1씩 감소하여 0이 되면 폐기된다. IPv6에서는 동일한 역할을 홉 제한(Hop Limit) 필드가 수행한다.
- ④ IPv6 단편화 처리: IPv6에서는 중간 라우터가 패킷의 크기가 MTU보다 클 경우 자동으로 단편화를 수행하여, 경로 상의 MTU 제약에 맞게 패킷을 분할한다.
- ⑤ 상위 계층 프로토콜 지정: IPv4는 프로토콜(Protocol) 필드를, IPv6는 다음 헤더(Next Header) 필드를 사용하여 상위 계층 프로토콜(예: TCP, UDP 등)을 지정한다.

2.다음 중 ARP (Address Resolution Protocol)의 동작 및 메시지 구조에 관한 설명 중 옳지 않은 것은 무엇인가?

- ① ARP 요청 전송: ARP 요청은 Ethernet 프레임의 목적지 MAC 주소를 ff:ff:ff:ff:ff:ff(브로드캐스트)로 설정하여 동일 서브넷 내 모든 호스트에 전송되며, 각 호스트는 자신의 IP 주소와 비교하여 응답 여부를 결정한다.
- ② ARP 응답 처리: ARP 응답은 대상 호스트가 자신의 MAC 주소를 포함하여 요청을 보낸 호스트로 유니캐스트 전송되며, 이를 수신한 호스트는 해당 IP-MAC 매핑 정보를 ARP 캐시에 동적 항목으로 저장한다.
- ③ ARP 캐시 관리: 동적 ARP 캐시는 설정된 타임아웃 시간이 경과하면 만료되어 자동으로 삭제되며, 이후 해당 IP에 대한 통신이 필요할 때 새로운 ARP 요청을 통해 갱신된다.
- ④ Gratuitous ARP의 역할: Gratuitous ARP는 자신이 네트워크에 새로 진입하거나 IP 변경 시 자신의 IP와 MAC 주소 매핑 정보를 브로드캐스트로 전송하여, 다른 호스트들의 ARP 캐시를 업데이트하고 IP 충돌을 감지하는 데 사용된다.
- ⑤ ARP 메시지 헤더: ARP 요청 및 응답 메시지의 헤더에는 송신자의 IP와 MAC 주소, 그리고 수신자의 IP와 MAC 주소가 모두 포함되며, 이 중 수신자의 MAC 주소는 요청 메시지에서도 항상 정확한 값으로 기재된다.

3. 다음 중 IP 주소의 네트워크와 호스트 구분, 클래스풀 및 클래스리스 주소 체계, 그리고 서브네팅 과정에 관한 설명 중 옳지 않은 것은 무엇인가?

- ① 클래스풀 주소 체계: 클래스풀 주소 체계에서는 IP 주소가 클래스 A, B, C 등으로 구분되며, 기본적으로 클래스 A는 8비트, 클래스 B는 16비트, 클래스 C는 24비트가 네트워크 주소로 할당되어 네트워크와 호스트 부분의 경계가 고정된다.
- ② 클래스리스 주소 체계 및 CIDR: 클래스리스 주소 체계에서는 IP 주소의 네트워크 부분을 고정된 클래스 경계에 의존하지 않고, CIDR 표기법($/n$)을 사용하여 서브넷 마스크에서 연속된 n 개의 1로 네트워크와 호스트 부분을 구분한다.
- ③ 서브네팅 원리: 서브네팅은 IP 주소와 서브넷 마스크 간의 비트 단위 AND 연산을 통해 네트워크 주소를 도출하며, 서브넷 마스크에서 1로 표시된 비트는 네트워크 부분, 0으로 표시된 비트는 호스트 부분을 의미한다.
- ④ 클래스풀 주소 체계와 서브네팅: 클래스풀 주소 체계에서는 네트워크와 호스트 비트의 길이가 기본적으로 고정되어 있으므로, 별도의 서브넷 마스크를 적용하여 네트워크 내에서 추가적인 서브네팅을 수행하는 것은 불가능하다.
- ⑤ 주소 할당 예시: 예를 들어, IP 주소 172.16.12.45의 경우 클래스풀 주소 체계에서는 기본적으로 네트워크 주소가 16비트(172.16)로 고정되며, 클래스리스 주소 체계에서는 서브넷 마스크 설정에 따라 네트워크와 호스트 부분의 경계가 유연하게 결정될 수 있다.

4.다음 중 공인/사설 IP 주소 관리 및 DHCP를 통한 동적 IP 할당과 관련된 설명 중, 네트워크 운영 및 보안 관점에서 부적절하거나 잘못된 설명은 무엇인가?

- ① 공인 IP 주소의 특성: 공인 IP 주소는 전 세계에서 고유하게 할당되며, 외부와의 직접 통신에 사용된다. 이로 인해 공격 표면이 넓어질 수 있으므로, 방화벽이나 침입 차단 시스템 등으로 보안이 강화되어야 한다.
- ② 사설 IP 주소와 NAT: 사설 IP 주소는 내부 네트워크에서 사용되며, 외부와 통신 시 라우터의 NAT 기능을 통해 공인 IP 주소로 변환된다. 이로 인해 내부 IP는 외부에 노출되지 않아 보안성이 향상된다.
- ③ 정적 IP 할당의 장단점: 정적 IP 할당은 관리자가 수동으로 IP를 부여하여, 서버나 네트워크 장비와 같이 지속적인 주소가 필요한 경우에 유리하다. 다만, 수동 관리로 인한 주소 충돌이나 관리 부담이 발생할 수 있다.
- ④ DHCP를 이용한 동적 IP 할당: 동적 IP 할당은 DHCP 프로토콜(DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK 메시지 교환)을 통해 자동으로 이루어지며, 임대 기간 동안 클라이언트에 IP 주소가 할당된다. 임대 기간 만료 전에 클라이언트는 갱신 절차를 진행하여 주소를 유지한다.
- ⑤ DHCP 임대 기간 만료 시 처리 방식: DHCP 동적 할당 방식에서는 임대 기간이 만료되면 클라이언트는 반드시 새로운 IP 주소를 즉시 할당받아야 하며, 만약 재할당에 실패하면 기존의 IP 주소는 즉시 회수되어 네트워크 연결이 중단된다.

5.라우터가 패킷 전달 경로를 결정할 때, 여러 후보 경로가 존재한다면 아래 기준들을 차례로 고려한다. 이와 관련하여, 최종 경로 선택 시 고려되지 않는 요소로 옳은 것은 무엇인가?

- ① Longest Prefix Match: 목적지 IP와 가장 긴 네트워크 프리픽스(서브넷 마스크)를 가진 경로가 우선 선택된다.
- ② 관리 거리 (Administrative Distance): 서로 다른 라우팅 프로토콜로 학습된 경로 간 우선순위를 결정하는 데 사용된다.
- ③ 메트릭 (Cost): 동일 프로토콜 내에서 경로 비용(예: hop 수, 대역폭 등)을 비교하여 최적 경로를 선택한다.
- ④ 라우팅 프로토콜의 신뢰도: 경로를 학습한 라우팅 프로토콜의 신뢰도가 경로 선택에 영향을 준다.
- ⑤ 패킷의 TTL 값: 패킷의 생명주기를 나타내는 TTL은 경로 선택 기준에 포함되지 않는다.

6. 다음 중 RIP와 OSPF 라우팅 프로토콜에 대한 설명 중 잘못된 것은 무엇인가?

- ① RIP: 거리 벡터 프로토콜로, 홉 수를 메트릭으로 사용하며 최대 홉 수 15로 제한하여 루프를 방지한다.
- ② OSPF: 링크 상태 프로토콜로, 각 링크의 비용(대역폭 등)을 기반으로 최적 경로를 계산하며 Dijkstra 알고리즘을 활용한다.
- ③ 정보 교환 방식: RIP는 주기적으로 전체 라우팅 테이블을 업데이트하는 반면, OSPF는 링크 상태 광고(LSA)를 통해 변화된 토폴로지만 업데이트한다.
- ④ 업데이트 방식: OSPF는 네트워크 토폴로지 변경 시 전체 네트워크에 브로드캐스트 방식으로 업데이트를 전파하여, 모든 라우터가 동일 정보를 받는다.
- ⑤ 부하 분산: OSPF는 동일 비용 경로가 여러 개 있을 경우, 부하 분산(Load Balancing)을 지원한다.

7. 다음 중 정적 라우팅과 동적 라우팅의 운영 및 관리 측면에 관한 설명 중 잘못된 것은 무엇인가?

- ① 정적 라우팅의 한계: 관리자가 수동으로 라우팅 테이블을 구성하므로, 네트워크 토폴로지 변경에 자동 대응하지 못해 관리 부담이 크다.
- ② 동적 라우팅의 장점: 라우팅 프로토콜을 통해 경로 정보를 자동으로 교환하고, 네트워크 변화에 빠르게 수렴할 수 있다.
- ③ 보안 측면: 정적 라우팅은 외부로부터의 라우팅 정보 조작 공격에 상대적으로 취약하지 않아 보안성이 높다고 평가된다.
- ④ 동적 라우팅의 비용: 라우팅 업데이트에 따른 네트워크 트래픽과 계산 부하로 인해, 소규모 네트워크에서는 오히려 비효율적일 수 있다.
- ⑤ 대규모 네트워크 운영: 정적 라우팅은 대규모 네트워크에서 동적 라우팅보다 관리 및 유지보수 비용이 낮으며, 빠른 장애 복구를 보장한다.

1.정답: ④

해설: IPv6에서는 라우터가 패킷을 단편화하지 않습니다. IPv6는 단편화를 보내는 호스트가 사전에 Path MTU Discovery를 통해 적절한 패킷 크기를 결정하도록 설계되었으며, 중간 라우터에서는 단편화를 수행하지 않기 때문에 ④번 설명은 옳지 않습니다.

2.정답: ⑤

해설: ARP 요청 메시지의 경우, 수신자의 MAC 주소는 아직 결정되지 않았으므로 일반적으로 0으로 설정된다. 따라서 "수신자의 MAC 주소가 요청 메시지에서도 항상 정확한 값으로 기재된다"는 설명은 옳지 않으며, ARP 응답 메시지에서만 대상 호스트의 정확한 MAC 주소가 포함된다.

3.정답: ④

해설: 클래스풀 주소 체계에서는 기본 네트워크/호스트 비트 길이가 고정되어 있더라도, 네트워크 내에서 서브넷 마스크를 변경하여 추가적인 서브네팅(예, 서브넷 마스크의 오버래핑)을 수행할 수 있습니다. 즉, 클래스풀 주소 체계에서도 서브네팅은 가능하므로 ④번 설명은 옳지 않습니다.

4.정답: ⑤

해설: DHCP에서는 임대 기간 만료 시 클라이언트가 새로운 IP 주소를 할당받기 위해 갱신을 시도하지만, 갱신이 실패하더라도 클라이언트는 일정 시간 동안 기존 IP 주소를 계속 사용할 수 있습니다. 임대 기간이 만료되었다고 해서 즉시 네트워크 연결이 차단되지는 않으므로 ⑤번 설명은 부적절합니다.

5.정답: ⑤ 해설: 라우팅 결정 과정에서는 목적지 IP의 Longest Prefix Match, 관리 거리, 메트릭, 그리고 라우팅 프로토콜의 신뢰도 등을 고려하지만, 개별 패킷의 TTL 값은 경로 선택 기준에 포함되지 않습니다.

6.정답: ④ 해설: OSPF는 네트워크 토폴로지 변경 시 브로드캐스트 대신 멀티캐스트(예: 224.0.0.5)를 이용해 효율적으로 링크 상태 정보를 전달합니다. 전체 네트워크에 브로드캐스트하는 방식은 RIP의 특성과도 거리가 있습니다.

7.정답: ⑤ 해설: 대규모 네트워크에서는 정적 라우팅의 수동 관리로 인한 오류 가능성 및 유지보수 비용이 매우 높아지므로, 동적 라우팅이 일반적으로 선호됩니다. ⑤번 설명은 정적 라우팅의 한계를 간과한 부적절한 설명입니다.