

IP

IP(Internet Protocol)란

IP 주소

- Internet Protocol Address
- 논리적으로 변하는 주소
- 컴퓨터 네트워크에서 장치 간 통신을 위해 사용되는 특수한 번호
- IPv4 (32비트) 또는 IPv6 (128비트)

MAC 주소

- Media Access Control Address
- 물리적 주소로 네트워크 인터페이스에 할당된 고유 식별자

ARP와 RARP

- ARP (Address Resolution Protocol) : IP주소를 MAC 주소로 변환하는 프로토콜
 - 브로드캐스팅 통해서 해당 IP 주소에 대한 MAC 주소 찾아냄
 - 브로드캐스팅 : 네트워크 내 모든 장치가 확인하는 브로드캐스팅 주소로 요청을 보내기
- RARP (Reverse Address Resolution Protocol)
 - MAC 주소를 IP 주소를 변환하는 프로토콜

IPv4와 IPv6

IPv4

- 32비트 주소 체계로 2^{32} 주소 표현
- 8비트 단위로 4개의 옥텟 . 으로 구분됨

IPv6

- 128비트 주소 체계로 2¹²⁸개의 주소 표현
- 16비트씩 8개로 구분되며 각 16비트는 16진수로 표현
- 빠르고 보안이 강화되며 주소 부족 문제 해결
- Checksum이 없음 → 속도 향상

IPv4 vs IPv6

- IPv6가 더 많은 주소 표현 가능
- IPv6에 불필요한 헤더가 없기 때문에 빠르고 IPSec 이라는 네트워크 보안이 포함되어 있음

아직 IPv4 체계를 사용하는 이유

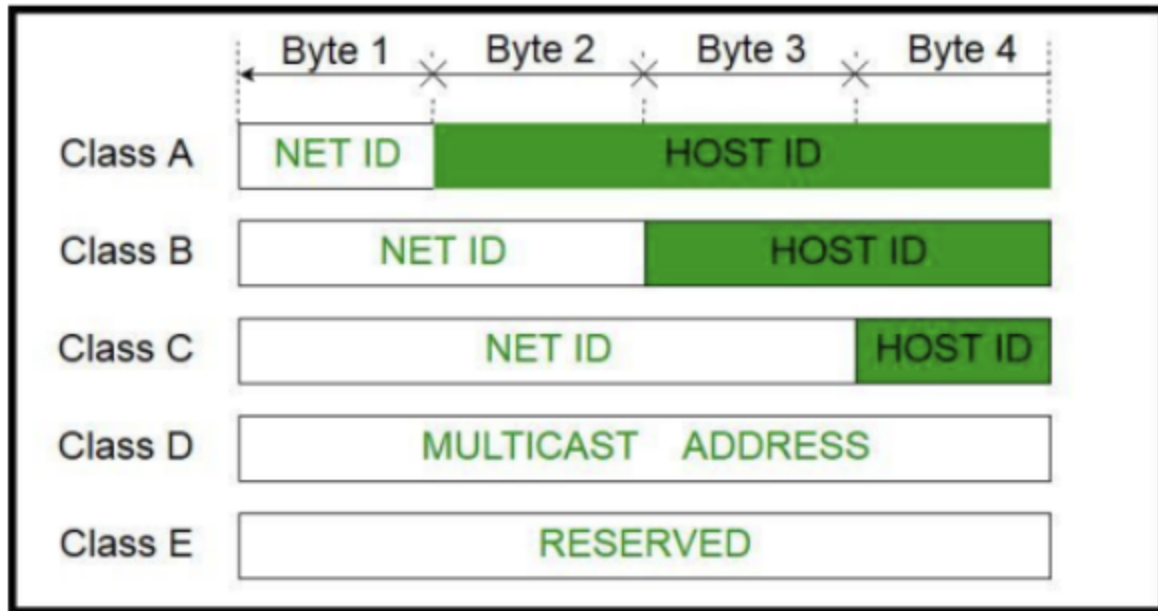
1. 기존 IPv4 인프라를 전부 바꾸기에는 시간과 비용이 많이 소요
2. IPv4와 IPv6 서로 호환되지 않는 프로토콜이기 때문에 한번에 모두 바꾸는 것이 아니면 두 가지 프로토콜을 도ით에 지원하는 시스템을 사용해야함
3. 주소 부족 문제가 있지만 NAT, 서브네팅 등 다양한 기술 발전으로 필요성이 줄어듦

Tunneling

- IPv4와 IPv6를 모두 사용하는 통신 기법
- IPv6로 이루어진 네트워크 패킷을 IPv4로 캡슐화하여 통신에 사용하는 기법

클래스풀 (Classful IP Addressing)

- IPv4 체계에서 클래스로 구분하여 IP를 관리하는 방법



- 클래스 단위가 내려갈 수록 하위 지역
- ex) Class A : 대륙, B: 국가, C: 지역, D: 시/군
- E : 예약된 IP

호스트 ID 개수 구할 때 2개를 제외하는 이유

- 사용 가능한 IP 주소 중 가장 첫 번째는 네트워크 주소로 사용
- 사용 가능한 IP 주소 중 가장 마지막은 브로드캐스팅 주소로 남겨놓음

단점

- 주소 부족 문제 / 사용하지 않는 남는 IP 주소들 발생
- 서로 다른 네트워크 크기에 대한 유연성 부족 ex) 미국, 대한민국 국토 넓이

클래스리스와 서브넷마스크, 서브네팅

클래스리스

- 서브넷마스크를 사용하여 네트워크 크기를 나누는 대신 더 유연한 IP 주소 할당 가능

서브넷마스크

- 네트워크 주소와 호스트 주소를 구분하여 세분화한 비트 마스크

- 클래스풀에서는 8비트 씩 사용

서브네팅

- 네트워크를 나누어 유연한 IP 주소 할당
- 각 서브넷은 독립된 네트워크로 간주되어 라우팅 가능

공인 IP와 사설 IP와 NAT

공인 IP

- 인터넷에서 공개적으로 사용되는 IP 주소

사설 IP

- 내부 네트워크에서 사용되는 비공개 IP 주소

NAT

- 사설 IP와 공인 IP간의 주소 변환을 수행하여 주소 부족 문제 해결
- 여러 사설 IP 주소를 하나의 공인 IP 주소에 연결하여 인터넷에 접속 가능
- 공유기를 통해 여러 호스트가 하나의 공인 IP 주소를 공유하며 NAT를 통해 주소 변환을 수행하여 인터넷에 접속함

NAT 사용하는 이유

- 공인 IP의 포트에 사설 IP를 매핑하여 IP 주소 부족 문제 해결
- 네트워크 보안 강화
 - 내부 네트워크 구조를 외부에 숨길 수 있음
- 네트워크 관리 및 유연성 향상
 - 공인 IP 변경 없이 사설 IP 변경 가능
- 사설 IP 주소의 재사용

단점

- 성능 저하

- IP 주소를 변환하는 과정에서 트래픽 발생
- 종단 간 통신 문제
 - 사설 IP주소를 알수가 없기 때문에 별개 네트워크의 각 장치끼리 직접적인 통신이 어려움
- 복잡한 설정
 - 포트 포워딩 필요
 - Application Layer Gateways
- 보안 문제
 - 모든 사설 IP가 하나의 공인 IP에 몰려있기 때문에 Dos 공격에 취약함
- 로그 및 추적 어려움
 - 사설 IP가 모두 하나의 공인 IP 주소로 변환되기 때문에 로그 분석이 복잡하다
- IPv6 전환 지연