IP 주소

ARP (Address Resolution Protocol)

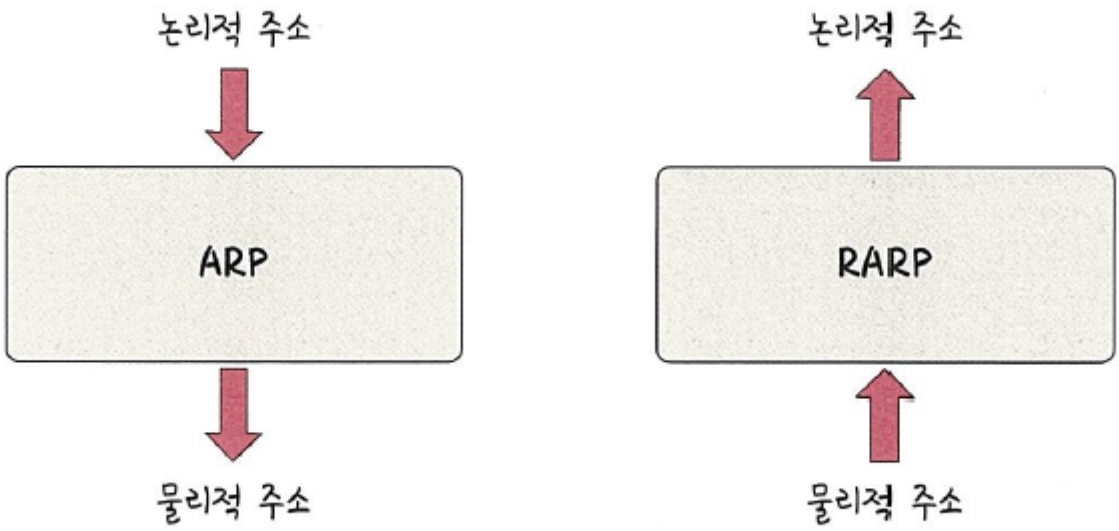
컴퓨터와 컴퓨터 간의 통신은 일반적으로 IP 주소 기반으로 통신하는 것으로 알고 있으나, 정확히는 IP 주소에서 ARP를 통해 MAC 주소를 찾아 MAC 주소를 기반으로 통신하는 것

ARP

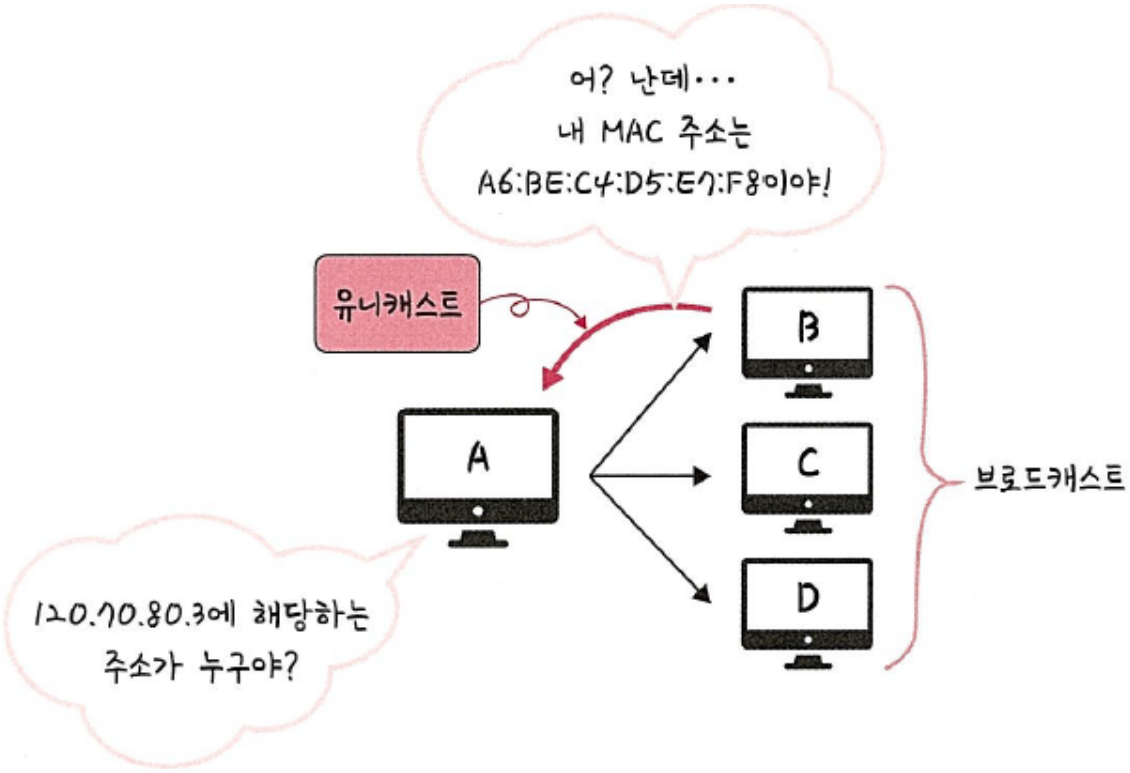
IP 주소로부터 MAC 주소를 구하는 IP 와 MAC 주소의 다리 역할을 하는 프로토콜

ARP 를 통해 가상 주소인 IP 주소를 실제 주소인 MAC 주소로 변환

RARP를 통해 실제 주소인 AMC 주소를 가상 주소인 IP 주소로 변환하기도 함



ARP의 주소를 찾는 과정

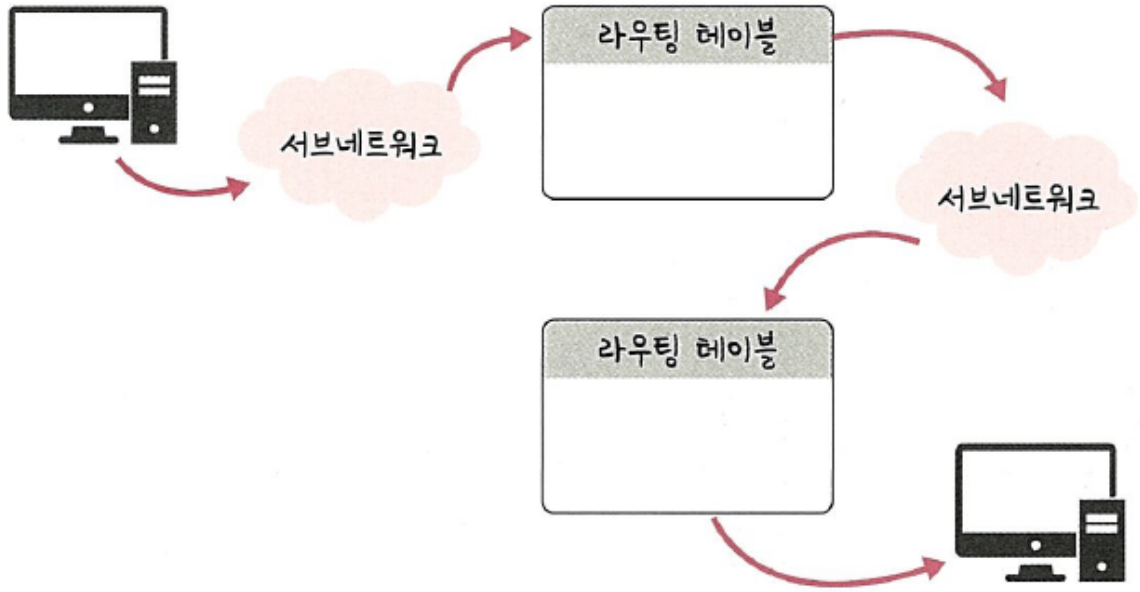


장치 A 가 ARP Request 브로드캐스트를 보내서 IP 주소에 해당하는 MAC 주소를 찾음

해당 주소에 맞는 장치 B 가 ARP reply 유니캐스트 를 통해 MAC 주소를 반환하는 과정을 거쳐 IP 주소에 맞는 MAC 주소를 찾게 됨

- 브로드캐스트 : 송신 호스트가 전송한 데이터가 네트워크에 연결된 모든 호스트에 전송되는 방식
- 유니캐스트 : 고유 주소로 식별된 하나의 네트워크 목적지에 1:1로 데이터를 전송하는 방식

홉바이홉(Hop By Hop) 통신



IP 주소를 통해 통신하는 과정

홉(Hop)

건너뛰는 모습

통신망에서 각 패킷이 여러 개의 라우터를 건너가는 모습을 비유적으로 표현한 것

각각의 라우터에 있는 라우팅 테이블의 IP를 기반으로 패킷을 전달하고 다시 전달해나감

즉, 통신장치에 있는 라우팅 테이블의 IP 를 통해 시작 주소부터 시작하여 다음 IP로 계속해서 이동하는 라우팅 과정을 거쳐 패킷이 최종 목적지까지 도달하는 통신

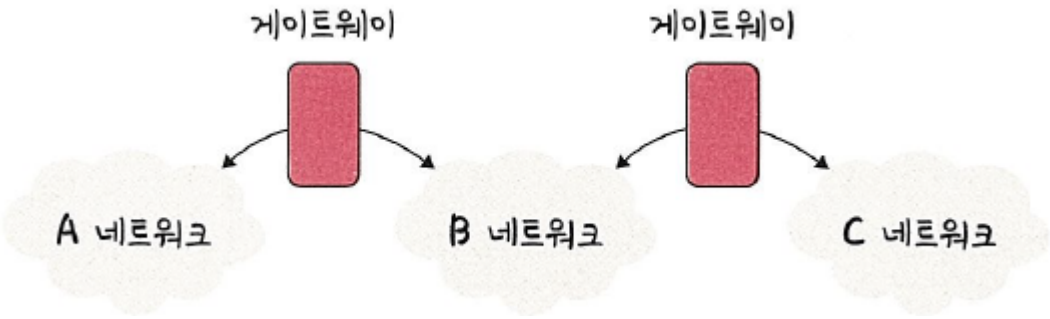
라우팅 테이블 (Routing Table)

송신지에서 수신지까지 도달하기 위해 사용

라우터에 들어가 있는 목적지 정보들과 그 목적지로 가기 위한 방법이 들어 있는 리스트

게이트웨이와 모든 목적지에 대해 해당 목적지에 도달하기 위해 거쳐야할 다음 라우터의 정보를 가지고 있음

게이트웨이 (Gateway)



서로 다른 통신망, 프로토콜을 사용하는 네트워크 간의 통신을 가능하게 하는 관문 역할을 하는 컴퓨터나 소프트웨어의 통칭

사용자는 인터넷에 접속하기 위해 게이트웨이를 거쳐야하며, 게이트웨이는 서로 다른 네트워크상의 통신 프로토콜을 변환해주는 역할을 하기도 함

게이트웨이는 라우팅테이블을 통해 확인할 수 있음

IP 주소 체계

IP 주소는 IPv4 와 IPv6 로 나뉨

IPv4

32비트를 8비트 단위로 점을 찍어 표기

123.45.67.89 와 같은 방식으로 IP 주소를 나타냄

IPv6

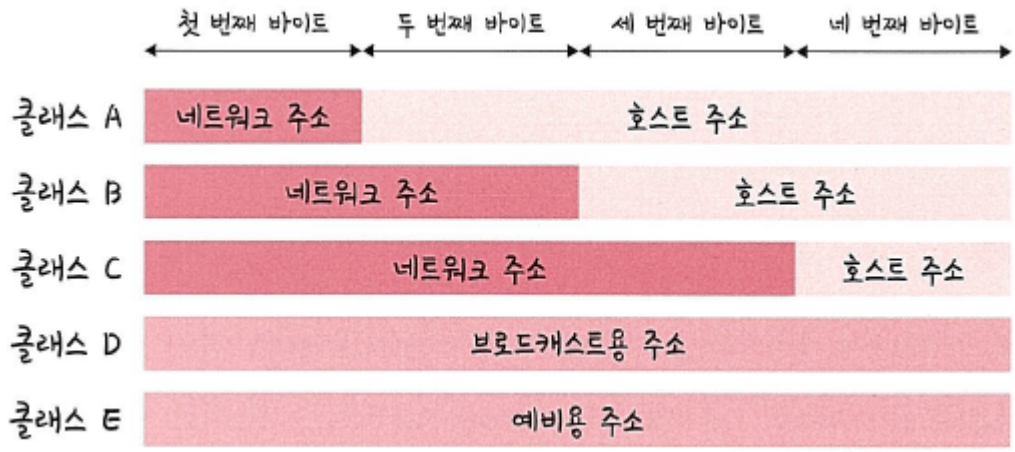
64비트를 16비트 단위로 점을 찍어 표기

2001:db8::ff00:42:8329 와 같은 방식으로 IP 주소를 나타냄

현재 가장 많이 쓰이는 체계는 IPv4. 추세는 IPv6 로 가고 있기는 함

이하 설명은 IPv4 기준

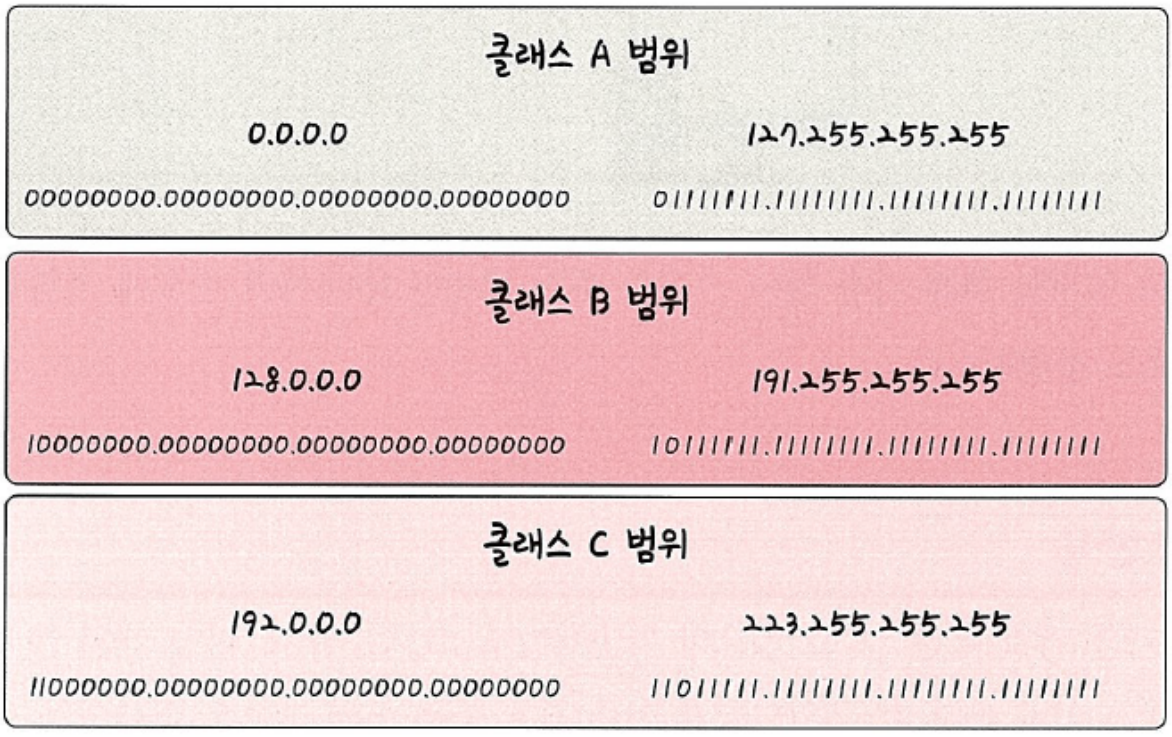
클래스 기반 할당 방식 (CIDR)



초기에는 A, B, C, D, E 다섯 개의 클래스로 구분하는 클래스 기반 할당 방식을 사용하였음

앞에 있는 부분을 네트워크 주소, 뒤에 있는 부분을 컴퓨터에 부여하는 주소인 호스트 주소로 놓아서 사용함

클래스 A, B, C는 일대일 통신으로 사용되고 클래스 D 는 멀티캐스트 통신, 클래스 E는 앞으로 사용할 예비용으로 쓰는 방식



구분 비트: 가장 왼쪽에 있는 비트

A 의 구분 비트 : 0

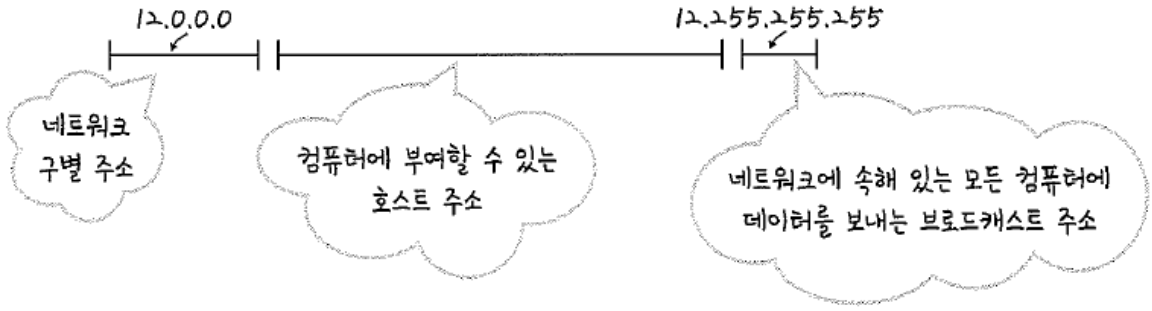
B 의 구분 비트 : 10

C 의 구분 비트 : 110

네트워크의 첫번째 주소 : 네트워크 주소로 사용

가장 마지막 주소 : 브로트캐스트용 주소로 사용 → 네트워크에 속해 있는 모든 컴퓨터에 데이터를 보낼 때 사용됨

클래스 A 로 12.0.0.0 이란 네트워크를 부여받은 경우



첫번째 주소인 12.0.0.0 은 네트워크 구별 주소 → 사용 불가

가장 마지막 주소인 12.255.255.255 는 브로드캐스트용으로 남겨두어야 함 → 사용 불가

12.0.0.1 ~ 12.255.255.254 의 호스트 주소를 부여 받은 것

사용하는 주소보다 버리는 주소가 많다는 단점이 존재함 ⇒ 이를 해소하기 위해 DHCP 와 IPv6, NAT 가 등장

DHCP (Dynamic Host Configuration Protocol)

IP 주소 및 기타 통신 매개변수를 자동으로 할당하기 위한 네트워크 관리 프로토콜

이를 통해 네트워크 장치의 IP 주소를 **수동으로 설정할 필요 없이 인터넷 접속 시마다 자동으로 IP 주소를 할당할 수 있음**

많은 라우터와 게이트웨이 장비에 DHCP 기능이 있음

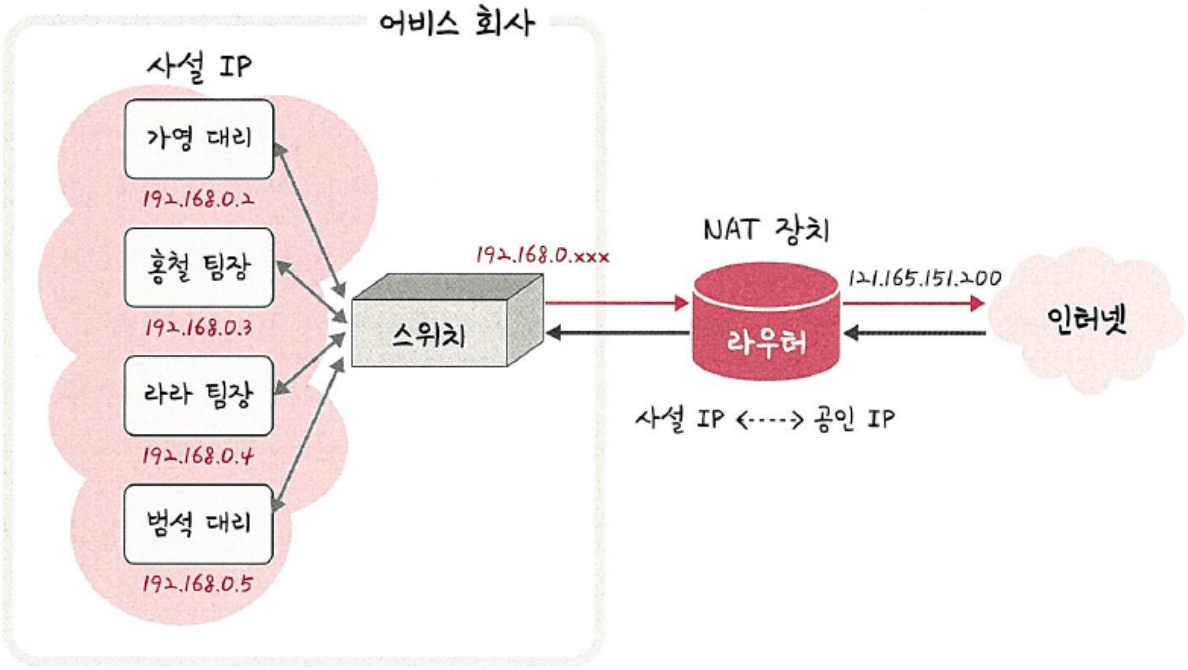
이를 통해 대부분의 가정용 네트워크에서 IP 주소를 할당함

NAT (Network Address Translation)

패킷이 라우팅 장치를 통해 전송되는 동안 패킷의 IP 주소 정보를 수정하여 IP 주소를 다른 주소로 매핑하는 방법

IPv4 주소 체계만으로는 많은 주소들을 감당하지 못하는 단점을 해결하기 위해 NAT 로 공인 IP 와 사설 IP 로 나눠서 많은 주소를 처리함

NAT 를 가능하게 하는 소프트웨어 : ICS, RRAS, Netfilter 등



각각의 사원들은 192.168.0.xxx를 기반으로 서로 다른 IP 를 가짐 → 이를 사설 IP 라고 함

NAT 장치를 통해 하나의 공인 IP 인 121.165.151.200 으로 외부 인터넷에 요청할 수 있음

이를 통해 각 사원들은 하나의 공인 IP를 기반으로 각각의 다른 IP를 가지는 것처럼 인터넷을 사용할 수 있음

NAT 장치를 통해 사설 IP를 공인 IP로 변환하거나 공인 IP를 사설 IP로 변환하는 데 쓰임

공유기와 NAT

NAT 를 쓰는 이유 : 주로 여러대의 호스트가 하나의 공인 IP 주소를 사용하여 인터넷에 접속하기 위함

ex) 인터넷 회선 하나를 개통하고 인터넷 공유기를 사용하여 여러 PC 를 연결하여 사용할 수 있음

→ 인터넷 공유기에 NAT 기능이 탑재되어 있기 때문

NAT를 이용한 보안

NAT 를 이용하면 내부 네트워크에서 사용하는 IP주소와 외부에 드러나는 IP 주소를 다르게 유지할 수 있으므로 내부 네트워크에 대한 어느정도의 보안이 가능해짐

NAT의 단점

NAT는 여러명이 동시에 인터넷을 접속하게 되므로 실제로 접속하는 호스트 숫자에 따라서 접속 속도가 느려질 수 있다는 단점이 있음

IP 주소를 이용한 위치 정보

IP 주소는 인터넷에서 사용하는 네트워크 주소 → 위치 추적이 가능함