#cs #study #network

0) 목차

- 네트워크의 큰 그림
- 물리 및 데이터링크 계층
- IP 계층

1) 네트워크의 큰 그림

네트워크의 기본구조

- 네트워크는 노드와 간선으로 이루어진 "그래프" 형태를 띄고 있다.
  - 노드 : 네트워크에 연결된 기기
  - 간선 : 정보를 교환하는 네트워크 선
- 네트워크 위상(network topology) : 네트워크가 연결된 형태. 노드와 간선이 이루어진 형태에 따라 망형, 트리형, 링형, 성형, 버스형으로 구분
- 호스트(host) : 네트워크 가장자리에 위치해 네트워크를 통해 주고 받는 정보를 최초로 송신하고 마지막에 수신하는 노드
  - 클라이언트(client) : 정보 요청(request)을 보내는 호스트
  - 서버(server) : 클라이언트 요청에 응답(response)하여 정보를 보내주는 호스트

네트워크 규모

- 네트워크의 규모에 따라 LAN과 WAN으로 구분
- LAN(Local Area Network)
  - 비교적 가까운 거리를 연결하는 네트워크
  - 집이나 사무실에 있는 공유기를 통해 모든 네트워크 기기가 통신하고 있으면 LAN이 공유기를 중심으로 구축된 것
    - 외부 네트워크 기기들은 위 공유기에 연결된 네트워크 기기들을 모두 하나의 LAN에 연결된 걸로 인식한다
- WAN(Wide Area Network)
  - 원거리 네트워크로 LAN 간 통신을 맡는다. 소위 인터넷이라고 부르는 네트워크가 WAN 네트워크다.
  - ISP(Internal Service Provider) 업체가 맡아서 관리하며 한국에서는 통신사가 ISP 업체다.

네트워크 정보 전송 방식

- 네트워크에서는 데이터 전송 단위인 패킷(packet)을 기준으로 정보를 송수신한다.
- 패킷은 페이로드(payload), 헤더(header)가 기본적으로 포함되어 있으며 가끔 트레일러(trailer)도 포함한다.

    - 페이로드(payload) : 패킷에서 송수신하려는 데이터
    - 헤더(header), 트레일러(trailer) : 패킷에 추가되는 부가 정보
- 주소(address) : 호스트 간 서로를 인식하기 위한 정보. 패킷의 헤더에 들어가 있으며 이를 통해 네트워크 내에 상대의 위치를 알고 그 쪽으로 정보를 보낼 수 있다.
- 캐스트(cast) : 수신자의 범위를 지정한다.
    - 유니캐스트(unicast) : 송신자와 수신자가 일대일로 메세지를 주고 받는 방식
    - 브로드캐스트(broadcast) : 네트워크 상의 모든 호스트에게 메세지를 전송하는 방식. 브로드캐스트 전송 범위를 브로드캐스트 도메인(broadcast domain)이라 하며 호스트가 같은 브로드캐스트 도메인에 속해 있으면 같은 LAN에 속해 있음
    - 멀티캐스트(multicast) : 네트워크 내의 동일 그룹에 속한 호스트에게만 전송
    - 애니캐스트(anycast) : 네트워크 내의 동일 그룹에 속한 호스트 중 가장 가까운 호스트에게 전송

패킷 전송 과정

- 프로토콜(protocol) : 두 호스트 간 패킷 전송 방식에 대한 규약. 수신자와 송신자 전부 같은 프로토콜을 준수하지 않으면 송수신한 정보를 제대로 해석할 수 없다.
    - 종류 : IP, ARP, TCP, UDP, HTTP, SSL 등
    - 각 프로토콜마다 목적과 특징이 다르다. 예를 들어 IP는 네트워크에 속한 기기들의 주소를 지정하기 위한 규약이며 ARP는 IP와 MAC 주소를 대응시키는 규약이다.
    - 위와 같이 목적이 다르기에 패킷의 내용도 달라진다.
- 네트워크 참조 모델(network reference model) : 패킷을 주고 받는 방식을 거시적으로 추상화한 것. 대표적으로 OSI 7계층이 있다.
    - OSI 모델 : 국제 표준화 기구(ISO)에서 만들었으며 1 ~ 7 계층으로 구분한다.
        - 물리 계층(physical layer, 1계층) : 비트 신호를 주고 받는 계층. 이진수로 이루어진 신호를 받으면 이를 유무선 통신 기기를 통해 운반한다.
        - 데이터 링크 계층(data link layer, 2계층) : 동일 LAN에 속한 호스트끼리 올바르게 정보를 주고 받기 위한 계층. MAC 주소를 사용하여 호스트끼리 구별하고 물리 계층 정보에 대한 오류를 검증한다.
        - 네트워크 계층(network layer, 3계층) : 네트워크 간 통신을 위한 계층. 각 네트워크를 인식하기 위해 IP를 사용한다.
        - 전송 계층(transport layer, 4계층) : 네트워크 간 패킷 전송에 관여하는 계층. 패킷 신뢰성 검증을 수행하며 포트(port)를 통해 기기 내부의 응용프로그램으로 연결해준다. TCP/UDP가 여기에 속한다.
        - 세션 계층(session layer, 5계층) : 응용 프로그램 간 연결 상태를 나타내는 세션(session)을 관리하는 계층.
        - 표현 계층(presentation layer, 6계층) : 인코딩, 압축, 암호화 같은 번역 업무를 수행하는 계층.
        - 응용 계층(application layer, 7계층) : 사용자에게 가장 가까운 계층으로 사용자의 눈에 보이는 네트워크 서비스를 제공한다. HTTP, HTTPS, DNS가 속한다.
    - TCP/IP 모델 : TCP/IP 4계층이라 불리며 OSI에서 3, 4계층을 중심으로 해석한 모델

        - 네트워크 액세스 계층(network access layer, 1계층) : 링크 계층 또는 네트워크 인터페이스 계층이라 부른다. OSI의 데이터 링크 계층과 유사함.
        - 인터넷 계층(internet layer, 2계층) : OSI 모델의 네트워크 계층과 유사함.
        - 전송 계층(transport layer, 3계층) : OSI 모델의 전송 계층과 유사함.
        - 응용 계층(application layer, 4계층) : OSI 모델의 5 ~ 7계층을 합쳐놓은 것과 유사함.
- 캡슐화와 역캡슐화
    - 캡슐화(encapsulation) : 송신 과정에서 발생. 상위 -> 하위 계층(응용 -> 물리)으로 정보 전송 시에 상위 계층이 보낸 패킷을 페이로드로 삼고 그 위에 헤더와 트레일러를 덧붙인다.
    - 역캡슐화(decapsulation) : 수신 과정에서 발생. 캡슐화 과정에서 붙인 헤더를 각 계층에서 확인하고 제거한다.
    - OSI 모델에서는 계층마다 패킷을 지칭하는 이름이 다르다
        - 물리 계층 : 심볼(symbol), 비트(bit)
        - 데이터 링크 계층 : 프레임(frame)
        - 네트워크 계층 : 패킷 또는 데이터그램
        - 전송 계층 : TCP 기반에서는 세그먼트, UDP 기반에서는 데이터그램
        - 그 외 : 데이터 또는 메시지

Quiz

- 같은 아파트에 같은 공유기를 사용하는 영희와 철수가 서로 메시지를 교환하고 있다. 이 때, 영희와 철수는 다른 LAN 대역의 바둑이가 보았을 때 같은 IP로 보이는가?

2) 물리 계층과 데이터 링크 계층

이더넷

- 이더넷은 통신 매체를 통해 신호를 송수신하고 데이터 링크 계층에서 주고 받는 형식 등을 정의한다. 즉, LAN 내의 호스트들이 올바르게 정보를 주고 받을 수 있도록 도와주는 것.
- 이더넷 표준
    - IEEE 802.3을 기준으로 하였으며 이더넷의 속도에 따라 802.3 뒤에 알파벳을 붙여 구분한다.
    - 이더넷 표준이 달라지면 통신 매체 종류, 신호 송수신 방법, 최대 지원 속도가 달라질 수 있다.
    - 대다수의 LAN 장비는 이더넷 표준을 준수하고 있다
- 이더넷 프레임 : 이더넷 기반의 네트워크에서 주고 받는 프레임
    - 프레임은 헤더, 페이로드, 트레일러로 구분하며 각 구성요소는 다음과 같다
    - 헤더
        - 프리앰블(preamble) : 송수신지 동기화를 위해 사용하는 8byte 정보. 이 값을 통해 이더넷 프레임으로 정보를 받고 있는 걸 알 수 있다.
        - 송수신지 MAC 주소 : 송신지와 수신지를 특정할 수 있는 6byte 길이의 MAC 주소를 명시한다. MAC 주소는 쌍점(:)을 기준으로 16진수로 이루어진 두 자리 숫자 6개로 구성한다. MAC 주소는 네트워크 인터페이스마다 하나씩 부여한다.
            - 네트워크 인터페이스 : 네트워크를 향하는 통로, 연결 매체와의 연결 지점을 추상화한 것

        - 타입/길이 : 프레임의 타입/길이를 나타내며 주어진 크기에 따라 타입인지 길이인지 나타내는 종류가 다르다. 주어진 영역의 크기가 10진수 기준으로 1500이하인 경우 프레임의 크기, 1536이상이면 프레임 유형을 나타낸다.
            - 프레임 유형을 나타낼 때, 16진수 기준으로 0800이면 IP, 0806이면 ARC를 나타낸다.
    - 페이로드
        - 데이터 : 상위 계층으로 전달하거나 전달 받을 내용물을 넣는다. 영역의 최대 크기는 1500byte이며 이 크기를 MTU라고 부른다.
    - 트레일러
        - FCS(frame check sequence) : 프레임의 오류가 있는 지 여부를 확인하는 영역. CRC라는 오류 검출용 값이 들어가 있다. 송신지에서 전송할 데이터에 대한 CRC 값을 만들어 보내면 수신지에서 전달받은 데이터를 통해 CRC를 계산하고 두 값이 같은 지 확인한다.

유무선 통신 매체

- 아무리 소프트웨어를 기깔나게 작성해서 네트워크 성능을 살려도 하드웨어가 성능이 낮으면 결국 최대 성능은 하드웨어를 따라간다. 그렇기에 본인이 만드는 소프트웨어가 속한 네트워크 기기의 성능을 파악하는 것도 중요하다.
- 유선 매체 - 트위스티드 페어 케이블
    - 공유기에 꽂는 네트워크 선을 본 적 있는가? 그 선이 바로 트위스티드 페어 케이블이다.
    - 카테고리(category)를 통해 성능을 구분하며 Cat5(100Mbps), Cat6(1Gbps) 등 빨라질 수록 뒤의 숫자를 높여부른다.
    - 구리선을 통해 전기 신호를 직접 주고 받기에 신호에 왜곡을 줄 수 있는 주변 잡음에 취약하다. 그래서 철사나 포일로 감싸서 차폐(sheieding)를 수행하며 이 철사와 포일을 각각 브레이크 실드와 포일 실드라고 부른다.
    - 브레이크 실드로 왜곡을 감쇄한 케이블을 STP, 포일 실드로 감쇄한 케이블을 FTP, 둘 다 사용하지 않고 구리선만 있으면 UTP라고 부른다.
- 무선 매체 - 전파와 WiFi
    - 전파 : 3kHz에서 3THz 사이의 진동수를 갖는 전자기파. 와이파이에서는 2.4GHz와 5GHz를 사용한다.
    - 와이파이(WiFi) : 무선 LAN에서 대중적으로 사용하는 기술. IEEE 802.11 표준을 따르며 이더넷 표준 규격처럼 뒤에 알파벳을 붙여서 규격을 구분한다.
    - 주파수 대역이 겹치면 신호 간섭이 발생할 수 있음. 이를 극복하기 위해 채널(channel)이라는 하위 주파수 대역으로 구분하여 서로의 채널이 겹치지 않게끔 신호 중첩을 최대한 막는다.
- 네트워크 인터페이스 : NIC
    - 네트워크 상에서 노드와 통신 매체가 연결되는 지점
    - 네트워크 인터페이스마다 MAC 주소를 받으며 NIC 하드웨어가 네트워크 인터페이스 역할을 맡는다.
    - NIC는 통신 매체의 신호를 호스트가 이해하는 프레임으로 변환하거나 반대로 프레임을 통신 매체의 신호로 변환한다.
    - NIC의 패킷 입출력(수신, 송신)은 시스템 콜과 커널을 거쳐서 수행한다. 그렇기에 입출력이 끝나면 인터럽트를 통해 작업 종료 알림을 보내고 DMA도 지원한다.

허브와 스위치

- 물리 계층과 데이터 링크 계층의 중간에 위치한 노드
- 물리 계층 : 허브
  - 여러 대의 호스트를 연결하는 장치. 허브에서 케이블의 커넥터가 꽂히는 부분을 포트(port)라고 한다
  - 허브의 역할
    - 전달받은 신호를 모든 포트로 내보낸다
    - 반이중(half durex) 모드로 송수신을 수행한다. 반이중 모드는 송신 또는 수신을 번갈아가면서 통신하는 것. 즉, 동시 송수신이 불가하다.
      - 참고) 전이중(full durex) 모드 : 송수신이 동시에 가능한 통신
  - 충돌(collsion) : 허브를 향해 동시에 호스트들이 메세지를 보내는 경우에 발생한다. 허브는 반이중 모드여서 동시에 송수신이 불가하기 때문이다.
    - 충돌 도메인(collision domain) : 충돌이 발생할 수 있는 영역. 허브에 연결된 모든 호스트가 해당된다.
- 데이터 링크 계층 : 스위치
  - 허브의 한계인 충돌을 보완하기 위해 만들어진 장비. 전이중 모드를 지원하기에 충돌 영역이 허브에 비해 좁다.
  - 스위치의 역할
    - 신호를 받으면 목적지 호스트에게 신호를 전송한다. 스위치는 포트, 연결된 호스트의 MAC 주소의 관계를 MAC 주소 테이블에 저장한다. 이를 통해 전달받은 신호가 어느 호스트로 가는 지 파악하고 해당 호스트에만 신호를 보낼 수 있다.
    - VLAN(Virtual LAN)을 통해 동일 스위치에 연결된 호스트를 여러 논리적인 네트워크로 분할하여 각각 독립된 네트워크 개체로 취급한다.

Quiz

- 철수는 무선 이어폰을 착용하고 WiFi가 연결된 노트북을 통해 음악을 듣는 걸 즐기는 백수다. 오늘 새로운 카페가 열려서 아메리카노 한 잔과 함께 음악 감상을 하려는 데 자꾸 무선 이어폰이 끊기는 거 아닌가? 이 때, 철수의 무선 이어폰에 생긴 문제점이 무엇인지 통신 관점에서 분석하고 답을 내시오.
- 영희는 서버를 구축하는 일을 맡았다. 그런데 사장님이 허브만 잔뜩 사오고 스위치는 하나도 사온 게 없지 않는가. 사표를 내고 싶은 밤이었으나 박터지는 경쟁률을 보고 눈물을 삼키며 영희는 일을 시작했다. 허브만 이용해 허브에 연결된 호스트 간 내부 네트워크를 구성할 시, 발생할 수 있는 문제점과 그 문제점을 줄이기 위해 강구할 수 있는 해결책을 생각하시오.

3) 네트워크 계층 - IP 계층

IP의 목적과 특징

- IP의 목적 : 주소 지정과 단편화
  - 주소 지정 : 네트워크 간 통신 과정에서 호스트를 구별하는 것
    - IP 주소 : IP 패킷 헤더에 위치하며 크기는 총 4byte로 1byte 당 점(.)으로 구분한다. 점으로 구분한 각 숫자는 10진수로 0 ~ 255 사이값으로 표기한다. 이 때, 각 숫자를 옥텟

(octet)이라 한다.(IPv4 기준)
        - 예시) 255.255.255.255
    - IP와 MAC 차이 : IP는 네트워크에서 부여한 추상적인 주소이고 MAC은 NIC라는 장비에 부과된 물리적인 주소다. 즉, IP는 네트워크에서 어떻게 부과하느냐에 따라 주소가 변경될 수 있지만, MAC은 장비를 바꾸지 않는 이상에야 바뀌지 않는다.
    - 라우터 : 서로 다른 네트워크 간 경로를 설정해주는 장치. 라우터를 통해 최적의 경로를 설정하고 그 경로를 따라 IP 패킷을 전송한다.
  - 단편화 : 데이터를 여러 IP 패킷으로 잘 쪼개서 보내는 것
    - mtu 단위로 패킷을 분리한다.
    - 헤더에는 단편화와 관련된 내용이 들어가며 식별자, 플래그, 단편화 오프셋이 있다.
      - 식별자 : 특정 패킷이 어떤 데이터에서 쪼개진 패킷인지 식별
      - 플래그 : 3비트로 구성된 영역으로 첫번째 비트를 제외한 두번째와 세번째 비트 사용. 두번째 비트는 DF라고 불리며 'IP 단편화 수행 여부'를 나타낸다. 세번째 비트는 MF라고 불리며 '단편화된 패킷 다수 존재 여부'를 나타낸다.
      - 단편화 오프셋 : 특정 패킷이 초기 데이터에서 얼마나 떨여지 있는가를 나타낸다.
- IP 특징
  - 신뢰할 수 없는 통신 : 패킷이 수신지까지 제대로 전송되었는 지 알 수 없다. 왜냐하면 목적지까지 가서 정보 손실이 발생해도 이에 대한 조치가 없기 때문이다.
  - 비연결형 통신 : 패킷을 주고 받기 전에 사전 통신 과정을 거치지 않는다. 즉, 수신자가 받을 준비가 되었는 지 확인을 하지 않고 그냥 보내는 것.
- 경로 MTU(path MTU)
  - 최근에는 IP 단편화 없이 주고 받을 수 있는 크기 내에서 정보를 보낸다.
  - 즉, 단편화를 하기 전에 네트워크에서 최대 크기가 어느 정도까지 인지 확인하고 그에 맞춰서 정보를 쪼개 보내는 것

IP 주소의 구조

- 네트워크 주소와 호스트 주소
  - IP주소는 IPv4 기준으로 1byte로 이루어진 값이 4개 모여서 총 4byte이다. 그리고 byte 기준(옥텟)으로 네트워크 주소 영역과 호스트 주소 영역으로 구분할 수 있다.
  - 네트워크 주소는 호스트가 속한 네트워크를 특정한다. 호스트 주소는 네트워크에 속한 호스트를 특정한다.
  - 네트워크 주소와 호스트 주소의 영역은 유동적이다. 상황에 따라 네트워크 주소가 클 수도 있고 호스트 주소가 클 수도 있기 때문이다.
- 클래스폴 주소 체계
  - 네트워크의 크기에 따라 유형별로 IP 주소를 분류하는 기준. 클래스는 A, B, C, D, E, F로 나뉘며 이중에서 가장 많이 사용하는 클래스가 A, B, C이다.
  - A 클래스 : 네트워크(1옥텟), 호스트(3옥텟). 0.0.0.0 ~ 127.255.255.255
    - 이진수로 보았을 때, 첫번째 옥텟 주소가 0으로 시작한다
  - B 클래스 : 네트워크(2옥텟), 호스트(2옥텟). 128.0.0.0 ~ 191.255.255.255
    - 이진수로 보았을 때, 첫번째 옥텟 주소가 10으로 시작한다.

    - C 클래스 : 네트워크(3옥텟), 호스트(1옥텟). 192.0.0.0 ~ 223.255.255.255
        - 이진수로 보았을 때, 첫번째 옥텟 주소가 110으로 시작한다.
- 예약 주소 : 미리 목적에 따라 할당된 주소. 이 주소는 사용자가 임의로 설정해서 쓸 수 없다.
    - 네트워크 주소 : 호스트 주소 영역이 전부 0인 주소 또는 전부 1인 주소. 해당 네트워크 영역이 시작하는 걸 알린다.
    - 브로드캐스트 주소 : 호스트 주소 영역이 전부 255인 주소. 해당 네트워크 영역에 속한 모든 호스트에게 패킷을 전송할 때 사용한다.
    - 루프백 주소 : 첫번째 옥텟 주소가 127인 주소. 자기 자신을 가리키는 주소로 localhost라고 부름. 자기 자신한테 패킷을 전송할 때 사용한다.
    - 사설 네트워크 주소 : 첫번째 옥텟 주소가 10, 172, 192인 주소. 공유기, 온프레미스 서버 등 자체적으로 만들어 놓은 서버에서 사용하는 주소.
- 클래스리스 주소 체계와 서브넷 마스크
    - 클래스리스 주소 체계(classless addressing) : 클래스 없이 주소를 구분하여 유연성을 높인 체계. 주소 구분을 위하여 서브넷 마스크를 사용한다.
    - 서브넷 마스크(subnet mask) : 네트워크 주소와 호스트 주소를 구분하기 위해 만든 비트마스킹. 이진수 기준으로 네트워크 주소 비트는 전부 1, 호스트 주소 비트는 전부 0으로 표기한 뒤에 클래스리스 주소와 AND 연산을 해서 네트워크 주소를 파악한다.
        - 즉, 서브넷 마스크를 통해 네트워크 속의 네트워크를 구성할 수 있다. 왜냐하면 A클래스 주소 체계에서 서브넷을 B클래스로 설정하면 특정 영역대에서 더욱 쪼개진 B클래스 주소 영역을 하나 만들 수 있지 않는가?
- 공인 IP주소와 사설 IP주소
    - 공인 IP 주소 : ISP 기관에서 정식으로 할당받은 주소
    - 사설 IP 주소 : 외부 네트워크에 공개되지 않은 네트워크에서 받은 주소. 공유기가 이에 해당되며 바깥에서 보면 공유기에 연결된 기기 대수가 얼마가 되었든 하나의 기기로 보인다.

IP 주소 할당

- 정적 할당
    - 정적 IP 주소(static IP address)는 수작업으로 설정한다.
    - 필요한 값은 IP주소, 서브넷 마스크, 게이트웨이 주소, DNS 주소이다. 게이트웨이 주소는 외부에 노출된 주소이며 이는 공유기 또는 라우터 주소를 의미한다. DNS 주소는 IP주소에 별칭으로 붙은 이름이며 별도의 DNS 서버에 IP주소와 DNS 이름이 매칭된 테이블이 존재한다.
- 동적 할당
    - 동적 IP 주소(dynamic IP address)는 자동으로 설정된다.
    - 보통 DHCP(Dynamic Host Configuration Protocol) 프로토콜을 통해 DHCP에서 동적 IP 주소를 할당해준다. 가정에서는 보통 공유기(라우터)가 이 역할을 수행한다.
    - 특징
        - 동적 IP 주소는 임대 기간이 정해져 있음
        - 동적 IP 주소는 할당 받을 때마다 다른 주소를 받을 수 있음

IP 전송 특징 보완 : ICMP

- ICMP(Internet Control Message Protocol)는 IP 패킷 전송 과정에 대한 피드백 메세지를 얻기 위해 사용한다. 전송 과정에 대한 오류 정보와 네트워크에 대한 진단 정보를 받아 볼 수 있다.
- ICMP를 통해 비연결적 통신의 문제점을 보완할 수 있으나, 완전히 문제없이 만드는 건 불가능하다. 결국, 전송 계층의 신뢰성 보장이 필요함.
- TTL : IP헤더에 들어가 있으며 패킷의 수명을 나타내는 영역. TTL이 0이 되면 패킷은 폐기되고 ICMP에서 호스트 쪽으로 시간 초과 메세지를 보낸다.
    - 홉(hop) : 패킷이 호스트 또는 라우터에 이동하는 것. 한 번 이동할 때마다 홉이 1 씩 감소하며 TTL에 이 값이 들어가 있다. 즉, 기존에 정한 횟수보다 더 많이 이동하는 경우에는 시간 초과 오류가 발생할 수 있다.

IP 주소와 MAC 주소 대응 : ARP

- ARP(Address Resolution Protocol)은 IP 주소를 통해 MAC 주소를 알아낼 때 사용한다.
- 패킷을 송신하기 위해서는 IP와 MAC 주소를 둘 다 알아야 하는데 모르는 경우에 사용.
- 브로드캐스트 메세지를 통해 찾으려는 MAC 주소에 대응하는 IP주소를 ARP 요청에 담아 보낸다. 이를 통해 본인의 IP주소가 ARP요청에 있는 IP주소와 같은 경우, 호스트는 ARP 응답 메세지에 자신의 MAC 주소를 기입하여 보낸다.
- 각 호스트는 ARP 요청 - 응답 과정을 통해 알아낸 IP주소 - MAC 주소 쌍을 ARP 테이블에 추가하고 일정 시간이 지나면 삭제한다.

Quiz

- 바둑이는 서버 엔지니어다. 바둑이가 관리하는 서버의 라우터 IP주소가 25.3.2.5이며 서브넷 마스크가 /18이다. 네트워크 주소는 몇이고 호스트 주소 범위는 몇인지 구하시오. 그리고 왜 네트워크 주소와 호스트 주소 범위가 그렇게 나오는 지 설명하시오.
- 컴퓨터 내부에 백엔드 서버 컨테이너, 프론트 엔드 서버 컨테이너, DB 서버 컨테이너를 만들었다. 이때, IP주소 상으로는 어떤 주소를 사용하여 서로 통신을 하는 지 고민해보시오. (세부적인 통신 방식은 TCP/UDP까지 배우고서 논할 겁니다.)