네트워크 공통 질문

1. HTTP 프로토콜에 대해 설명해주세요.

- HTTP란 서버와 클라이언트가 서로 데이터를 주고 받기 위한 프로토콜이며, 상태 정보를 저장하지 않는 Stateless의 특징과 클라이언트의 요청에 맞는 응답을 보낸 후 연결을 끊는 Connectionless의 특징을 가지고 있다.
- 장점으로는 통신 간의 연결 상태 처리나 정보를 관리 할 필요가 없어 서버 디자인이 간단하고 HTTP 요청에 따라서 독립적으로 응답만 보내주면 된다. 단점으로는 요청을 보낼 때마다 이전 정보를 모르기 때문에 매번 인증을 해줘야 하는데 이를 해결하기 위해 쿠키나 세션을 사용해서 데이터를 처리한다.

2. HTTP와 HTTPS의 차이점은 무엇인가요?

- HTTP로 중요한 정보를 주고 받는 중에 제 3자에 의해서 조회 될 수 있는데 이를 해결하기 위해 HTTP에 암호화를 추가한 프로토콜이 HTTPS이다.
- HTTP는 SSL을 덮어쓴 HTTP이며 원래는 TCP와 직접 통신했지만 HTTPS에서는 HTTP와 SSL이 통신하고 SSL이 TCP와 통신함으로써 암호화와 증명서, 안전성 보호를 받을 수 있게 된다.

3. 쿠키와 세션의 차이점에 대해 말해주세요.

- 쿠키는 사용자의 컴퓨터에 저장하는 작은 기록 정보 파일이다. HTTP에서 클라이언트의 상태 정보를 PC에 저장했다가 필요 시 정보를 참조하거나 재 사용 할 수 있다.
- 세션은 일정 시간 동안 같은 사용자로부터 들어오는 일련의 요구를 하나의 상태로 보고, 그 상태를 유지 시키는 기술이다.
- 방문자가 웹 서버에 접속해 있는 상태를 하나의 단위로 보고 그것을 세션이라고 한다.

4. www.naver.com에 접속할 때 생기는 과정에 대해 설명해주세요.

1. 사용자가 브라우저에 URL을 입력
2. DNS 서버가 도메인 네임으로 서버의 진짜 IP주소를 찾음
3. IP 주소로 웹 서버에 TCP 3way-handshake로 연결 수립
4. 클라이언트는 웹 서버로 HTTP 요청을 보냄
5. 웹 서버는 HTTP응답 메세지를 보냄
6. 도착한 HTTP 응답 메세지는 웹 페이지 데이터로 변환되고, 웹 브라우저에 의해 출력

5. TCP와 UDP의 차이를 설명해주세요.

- TCP는 연결형 지향형 서비스로 3-way handshaking 과정을 통해 연결을 설정하기 때문에 높은 신뢰성을 보장하지만 속도가 비교적 느리다.
- UDP는 비연결 지향형 서비스로 3-way handshaking을 사용하지 않기 때문에 신뢰성이 떨어지는 단점이 있지만, 데이터 수신 여부를 확인하지 않기 때문에 속도가 빠르다는 장점이 있다.
- 따라서 TCP는 신뢰성이 중요한 파일 교환과 같은 경우에 쓰이고 UDP는 실시간성이 중요한 스트리밍에 자주 사용 된다.

6. 3 way-handshaking을 통신이 종료 되었을 때도 사용하나요?

- TCP는 3-way handshaking 과정을 통해 연결을 설정하고,4 way-handshaking 과정을 통해 연결을 해제한다.

7. 3 way-handshake와 4 way-handshake를 설명해주세요.

- 3 way-handshake는 TCP 네트워크에서 통신하는 장치가 서로 연결이 잘 되었는지 확인하는 방법
- 4 way-handshake는 TCP 네트워크에서 통신 하는 장치의 연결을 해제하는 방법

8. OSI 7 계층과 각 계층에 대해 아는 대로 설명해주세요.

- 7계층(응용 계층) : 사용자에게 통신을 위한 서비스 제공, 인터페이스 역할

- 6계층(표현 계층) : 데이터의 형식을 정의하는 계층(코드간 번역 담당 : 응용 ←→ 세션)
- 5계층(세션 계층) : 컴퓨터끼리 통신을 하기 위해 세션을 만드는 계층
- 4계층(전송 계층) : 최종 수신 프로세스로 데이터의 전송을 담당하는 계층
- 3계층(네트워크 계층) : 패킷을 목적지까지 가장 빠른 길로 전송하기 위한 계층
- 2계층(데이터링크 계층) : 데이터의 물리적인 전송과 에러 검출, 흐름 제어를 담당하는 계층
- 1계층(물리 계층) : 데이터를 전기 신호로 바꾸어 주는 계층

9. HTTP Method와 각각이 사용되는 경우에 대해서 설명해주세요.

- GET - 데이터 조회
- POST - 요청 데이터 처리(보통 데이터 등록 사용)
- PUT - 데이터 변경(해당 데이터가 없으면 생성)
- PATCH - 일부 데이터만 변경
- DELETE - 데이터 삭제

10. GET과 POST의 차이에 대해 설명해 주세요.

- GET은 데이터를 조회하기 위해 사용되는 방식이며 헤더에 추가하며 전송하는 방식이다. URL에 데이터가 노출됨
- POST는 데이터를 추가 또는 수정하기 위해 사용되는 방식으로 데이터를 바디에 추가하여 전송하는 방식, 완전히 안전하다는 것은 아니지만 URL에 데이터가 노출되지 않아 GET보다는 안전하다.

11. 세션 기반 인증과 토큰 기반 인증의 차이에 대해 얘기해 주세요.

- 세션 기반 인증은 클라이언트로 부터 요청을 받으면 클라이언트의 상태 정보를 저장하므로 Stateful한 구조를 가지고, 토큰 기반 인증은 상태 정보를 서버에 저장하지 않으므로 Stateless한 구조를 가진다.

12. Stateful한 세션 기반의 인증 방식을 사용하게 된다면 어떤 단점이 있을까요?

- 서버에 세션을 저장하지 않기 때문에 사용자가 증가하면 서버에 과부하를 줄 수 있어 확장성이 낮다.
- 해커가 훔친 쿠키를 이용해 요청을 보내면 서버는 올바른 사용자가 보낸 요청인지 알 수 없다.

13. 그렇다면 세션 기반 인증과 토큰 기반 인증은 각각 어느 경우에 적합한가요?

- 단일 도메인이라면 세션을 관리할 때 사용되는 쿠키는 단일 도메인 및 서브 도메인에서만 작동하도록 설계되어 있기 때문에 세션 기반 인증을 사용하는 것이 적합하다.

14. JWT 토큰에 대해 설명해주세요.

- JWT는 JSON 포맷을 이용하는 Claim 기반의 웹 토큰이며, 토큰 자체를 정보로 사용하는 Self-Contained 방식으로 정보를 안전하게 전달한다.
- JWR는 헤더.내용.서명으로 구성되며 각 파트를 점으로 구분한다.
- 헤더 - 토큰의 타입과 해시 암호화 알고리즘으로 이루어져 있다.
- 내용 - 토큰에 사용자가 담고자 하는 정보를 키-벨류 형태의 한쌍으로 담는다.
- 서명 - 토큰을 인코딩하거나 유효성 검증할 때 사용하는 고유한 암호화 코드이다. 헤더와 내용의 값을 인코딩 한다.

15. 대칭키, 비대칭키 암호화 방식에 대해 설명해주세요.

- 대칭키는 암호화와 복호화에 같은 암호화 키를 쓰는 알고리즘이다. 따라서 누군가 암호 키를 가로채면 복호화를 할 수 있어 정보가 유출 될 수 있다.
- 비대칭키는 암호화와 복호화를 할 때 서로 다른 키를 사용하는 암호화 알고리즘이다.

16. Connection Timeout과 Read Timeout차이에 대해 설명해주세요.

- 서버 자체에 클라이언트가 어떤 이유로 실패했을 시에 적용되는 것이 Connection Timeout이다. 즉, 접근을 시도하는 시간 제한

- 클라이언트가 서버에 접속을 성공했으나 서버가 로직을 수행하는 시간이 너무 길어 제대로 응답을 하지 못한 상태에서 클라이언트가 연결을 해제 했을 경우 Read Timeout이라고 한다. 즉, 서버와 클라이언트간 싱크가 맞지 안아 문제가 발생할 확률이 높다.

17. 공인IP와 사설IP의 차이에 대해 설명해주세요.

- 공인 IP는 ISP가 제공하는 IP주소이며, 외부에 공개되어 있는 IP주소 이다.
- 사설 IP는 일반 가정이나 회사 내 등에 할당 된 네트워크 IP 주소이며, IPv4의 주소부족으로 인해 서브넷팅 된 IP이기 때문에 라우터에 의해 로컬 네트워크상의 PC나 장치에 할당 된다.
- 사설 IP 주소만으로는 인터넷에 직접 연결할 수 없고, 라우터를 통해 1개의 공인 IP를 할당하고, 라우터에 연결된 개인 PC는 사설 IP를 각각 할당 받아 인터넷에 접속할 수 있다.