Quiz

- 혼잡 제어를 통해 네트워크 내부 정보량 폭주를 제어한다. 가장 단순한 AIMD에 비유하면 평시에 정상적으로 정보가 전송될 때는 수신량을 1씩 늘리다가 송신 오류가 발생하면 송신 가능한 정보량을 절반 줄인다.
- SYS-SENT는 클라이언트가 서버에게 연결 요청 메시지를 보낸 것이다. SYS-SENT가 지속되는 건 곧 서버로부터 연결 수립이 가능한 지 여부를 못 받은 것이다. 정상적이라면 서버가 SYN-RECEIVED를 보내서 클라이언트에게 수신 확인 및 연결 수립 여부 검증을 시도한다. 그리고 클라이언트가 이를 받으면 ESTABLISEHD 즉, 둘의 연결이 성사된다.
- 웹소켓은 최초 연결 수립 시에 HTTP 1.1을 사용한다. 몰론, 지속 가능한 연결을 할 수 있는 HTTP 2.0과 HTTP 3.0도 할 수는 있지만 내부 구조가 좀 달라서 제한적이다. 그리고 최초 연결이 수행되면 HTTP 1.1 -> websocket 프로토콜로 변경하여 통신을 지속한다.
- 401이 나온 건 서버에서 요구하는 인증값이 아니거나 인증값 자체를 포함하지 않은 것이다. 여기서는 tokenValue라고 서버에서 요구한 인증값 변수명이 있으므로 변수에 저장된 값이 문제다.
- 영희가 입력한 사용자 정보가 해당 API를 이용할 수 있는 권한이 없다. 권한이 있는 사용자를 넣으면 문제없이 이용할 수 있다.
- 철수의 컴퓨터가 저장소이고 영구적으로 내용물이 저장되어 있다. 로컬 스토리지를 활용했으므로 당연하게도 별도 처리를 하지 않은 이상에야 내용이 지워지지 않는다. 그렇기에 영구 보관이 필요없는 정보는 별도 수명을 지정할 수 있는 쿠키나 세션 기간이 끝나면 정보를 삭제하는 세션 스토리지를 이용하는 게 좋다.

Test

- 도메인 이름을 제공하는 DNS 서비스 업체의 이름 서버에 접속하여 DNS 자원 레코드를 추가한다. 레코드에 기록된 도메인 이름에 해당하는 IP주소를 대응하면 끝.
- 쿠키를 이용한다. 쿠키에 해당 정보를 띄우는 팝업창에 대한 플래그를 저장하고 프론트에서 페이지를 다시 불러오는 이벤트에서 플래그 검증 과정을 거치면 끝.
- 콘텐츠 협상을 통해서 클라이언트가 선호하는 언어의 우선순위를 알 수 있기 때문이다. 페이지 요청 시 클라이언트에서 우선 순위를 지정하여 인코딩 언어를 보내주면 서버에서 지원하는 언어를 확인하고 그 언어에 맞는 페이지 정보를 넘겨주는 식.
- HTTPS는 TLS를 통해 보안이 더해졌다. 기존 HTTP가 TCP handshakes -> HTTP로 넘어가면 HTTPS는 TCP handshakes -> TLS handshakes -> HTTP로 보안 검증 과정을 한 단계 거치는 방식이다.