(4) HTTP/3의 특징은 무엇이며, 이전 버전들과의 차이점은 무엇인가?

HTTP/3은 QUIC 프로토콜을 기반으로 한다. 이전 버전들과의 가장 두드러지는 차이점은 바로 이 전송 프로토콜이다. 기존의 버전들은 모두 TCP 프로토콜 위에서 동작했는데, HTTP/3에서는 QUIC 프로토콜 위에서 동작한다. 그 이유는 기능을 확장하기 위해 TCP의 구조를 살펴봤더니 OPTION 필드의 제한으로 인해 한계가 생겼다. 또한, 이미 오랫동안 사용해 온 헤더 자체가 암호화되지 않은 상태로 전달되다 보니 외부에서 관찰하거나 패킷을 수정할 수 있어서 보안성에 취약해졌다. 라는 것을 이유로 들 수 있다. QUIC 프로토콜은 UDP 위에서 동작하는데 UDP란, User Datagram Protocol의 준말이다. UDP 프로토콜의 전송 방식은 매우 단순해서 정보 전달의 신뢰성이 떨어지는데, 순서가 섞이거나 중복 혹은 손실되기도 한다. 이러한 특징 때문에 일반적으로 오류의 검사나 수정이 필요 없는 곳에서 쓰이는데 그 예로는 DNS 서비스, IPTV, VoIP 등이 있다.

HTTP/3의 특징은 다음과 같다.

1) QUIC 프로토콜을 기반으로 하여 처리 속도가 빠르다.

QUIC 프로토콜의 가장 큰 특징이자 장점은 0-RTT(Round Trip Time)과 1-RTT인데, 이는 새로운 커넥션을 생성하기 위해서 요구되는 시간을 줄이기 위해서 클라이언트가 이전에 연결했던 서버의 커넥션 캐시를 바탕으로 특정한 파라미터를 가져오는 것이다. 이것 덕분에 클라이언트에게 즉시 정보를 보낼 수 있어서 지연 시간이 단축된다. 또한 이것은 UDP 프로토콜의 원칙이므로 UDP 위에서 동작하는 QUIC 프로토콜에서도 적용된다.

반면에, 이전 버전들이 TCP 위에서 동작하면서 커넥션을 새로 만들기 위해 여러 단계의 송수신 과정을 거쳐야 하는데 이 단계를 거치면서 실제 필요한 데이터를 전송하기도 전에 여러 단계에서 왕복이 발생하게 된다. 따라서 커넥션 생성을 위한 오버헤드가 증가하고 지연 시간이 증가한다. 반면에 0-RTT인 HTTP/3에서는 오버헤드가 감소하는 것을 알 수 있다.

오버헤드(overhead) : 어떤 처리를 하기 위해 들어가는 간접적인 처리 시간이나 메모리 등을 말한다.

2) 향상된 보안성.

QUIC은 TLS 1.3 버전의 암호화를 기본적으로 사용하고 있다. 또한, 불안전하거나 암호화되지 않은 곳에서 존재하지 않는다.

TLS(Transport Layer Security) : 컴퓨터 네트워크에 통신 보안을 제공하기 위해 설계된 암호 규약이다. TCP/IP를 사용하는 통신에 적용된다.

3) 이전보다 향상된 멀티플렉싱 및 오류 정정 방법.

멀티플렉싱은 HTTP/2의 가장 큰 특징 중 하나인데, TCP 프로토콜에서는 데이터가 체인처럼 연결되어 있기에 여러 개별 데이터를 하나로 전송할 때, 첫 번째 패킷이 전송 도중에 손실되거나 없어지면 그 패킷 다음에 오는 패킷들은 손실된 패킷이 서버 측에서 다시 보내지거나 다시 찾아질 때까지 기다려야 한다. 이를 Head-Of-Line Blocking이라 하는데, QUIC에서는 같은 상황에서 별다른 블로킹없이 지속적으로 데이터를 처리할 수 있다. 이렇게 데이터를 처리하는 것은 FEC(Forward Error Correction)이라 하며 이전 버전에 비해 향상되었다.

HTTP/3와 HTTP/2의 공통점은 스트림(stream), 서버 푸시, 헤더 압축(이때, HTTP/3은 QPACK를, HTTP/2는 HPACK를 사용한다. 둘다 비슷함.), 멀티플렉싱(multiplexing), 스트림 우선순위 설정 등등이 있다. 두 버전의 차이점을 살펴보면 다음과 같다. HTTP/3은 QUIC 프로토콜 기반이며 스트림을 자체적으로 처리 가능하다. 반면에 HTTP/2는 TCP 프로토콜 기반이며 HTTP 계층에서 스트림을 다룬다.