

HTTPS와 HTTP/3

☰ 태그	
🕒 생성 일시	@2023년 12월 27일 오후 5:34

▼ 목차

[HTTPS](#)

[SSL/TLS](#)

[보안 세션](#)

[인증 메커니즘](#)

[SEO에 도움이 되는 HTTPS](#)

[SEO를 높이는 방법](#)

[HTTPS 구축 방법](#)

[HTTP/3](#)

[QUIC \(Quick UDP Internet Connections\)](#)

[초기 연결 설정 시 지연 시간 감소](#)

HTTPS

- HTTP/2는 HTTPS 위에서 동작
- HTTPS는 애플리케이션 계층과 전송 계층 사이에 신뢰 계층인 SSL/TLS 계층을 넣은 신뢰할 수 있는 HTTP 요청을 말합니다.

SSL/TLS

- SSL(Secure Socket Layer)은 SSL 1.0, 2.0, 3.0, TLS(Transport Layer Security Protocol) 1.0, 1.3까지 버전이 올라가며 마지막으로 TLS로 명칭이 변경되었으나, 보통 이를 합쳐 SSL/TLS로 많이 부릅니다.
- SSL/TLS는 전송 계층에서 보안을 제공하는 프로토콜입니다.
- 클라이언트와 서버가 통신할 때, SSL, TLS를 통해 제 3자가 메시지를 도청하거나 변조하지 못하도록 합니다.

보안 세션

- 보안 세션이란?
보안이 시작되고 끝나는 동안 유지되는 세션
- SSL/TLS는 핸드셰이크를 통해 보안 세션을 생성하고 이를 기반으로 상태 정보 등을 공유합니다.

인증 메커니즘

- 인증 메커니즘은 CA(Certificate Authorigies)에서 발급한 인증서를 기반으로 이루어집니다.
- CA에서 발급한 인증서는 안전한 연결을 시작하는 데 있어 필요한 ‘공개키’를 클라이언트에 제공하고 사용자가 접속한 서버가 ‘신뢰’할 수 있는 서버임을 보장합니다.
- 인증서는 서비스 정보, 공개키, 지문, 디지털 서명 등으로 구성

SEO에 도움이 되는 HTTPS

HTTPS로 전환하게 되면 검색엔진 최적화(SEO)에 있어서도 큰 혜택을 볼 수 있습니다.

- 이는 구글이 SSL 인증서를 강조해왔고 HTTPS 웹사이트에 가산점을 주기 때문이기도 하지만 사용자들이 결국에는 가장 안전하다고 생각하는 사이트를 더 많이 방문하기 때문이기도 합니다.
- 또한 가속화된 모바일 페이지(*AMP, Accelerated Mobile Pages)를 만들고 싶을 때도 HTTPS 프로토콜을 사용해만 합니다.

구글의 SERP(검색 결과 페이지)를 보면 스마트폰과 태블릿의 사용자들이 모바일에서 사용하기 편하도록 AMP 콘텐츠들이 두드러져 보이는 것을 볼 수 있습니다

즉, **모바일 친화적인 웹사이트를 만드는 것과 모바일 검색순위 및 지역에 SEO를 증가시키는 것**이 점점 더 중요해지고 있는 요즘, HTTP를 HTTPS로 전환하는 것이 필수라고 볼 수 있습니다.

▼ AMP란?

구글이 만든 모바일 기기에서 훨씬 빠르게 콘텐츠를 로딩 하기 위한 방법입니다. AMP는 HTML에서 불필요한 부분을 없앴 것이라고 볼 수 있습니다.

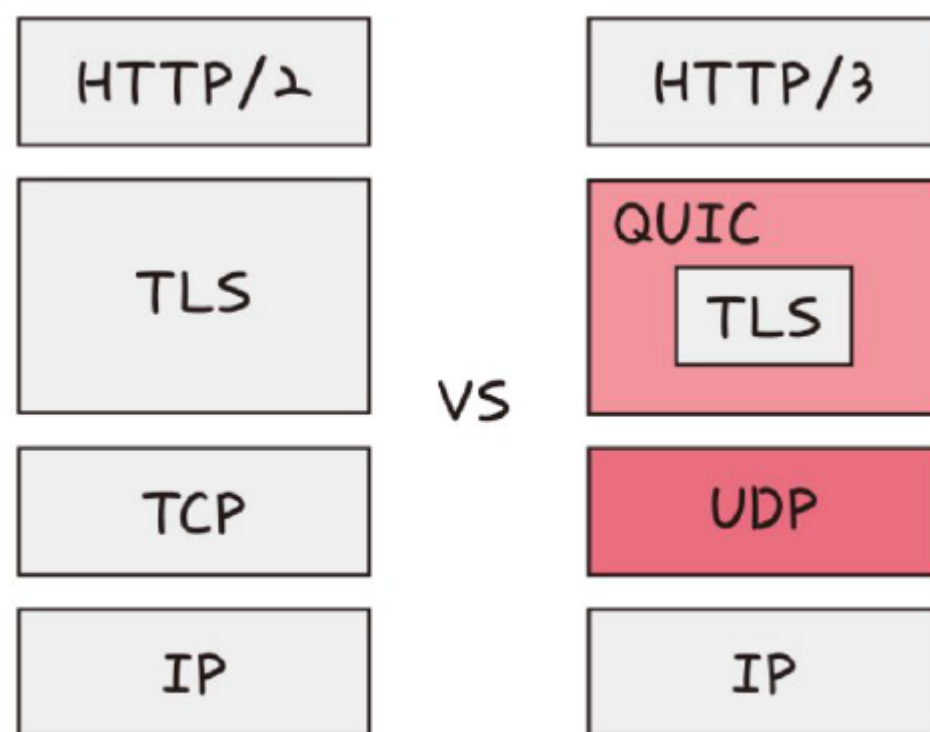
SEO를 높이는 방법

- 캐노니컬 설정
- 메타 설정
- 페이지 속도 개선
- 사이트맵 관리

HTTPS 구축 방법

1. 직접 CA에서 구매한 인증키를 기반으로 HTTPS 구축
2. 서버 앞단의 HTTPS를 제공하는 로드밸런서 두기
3. 서버 앞단에 HTTPS를 제공하는 CDN을 두기

HTTP/3



▲ 그림 2-68 UDP 기반으로 돌아가는 HTTP/3

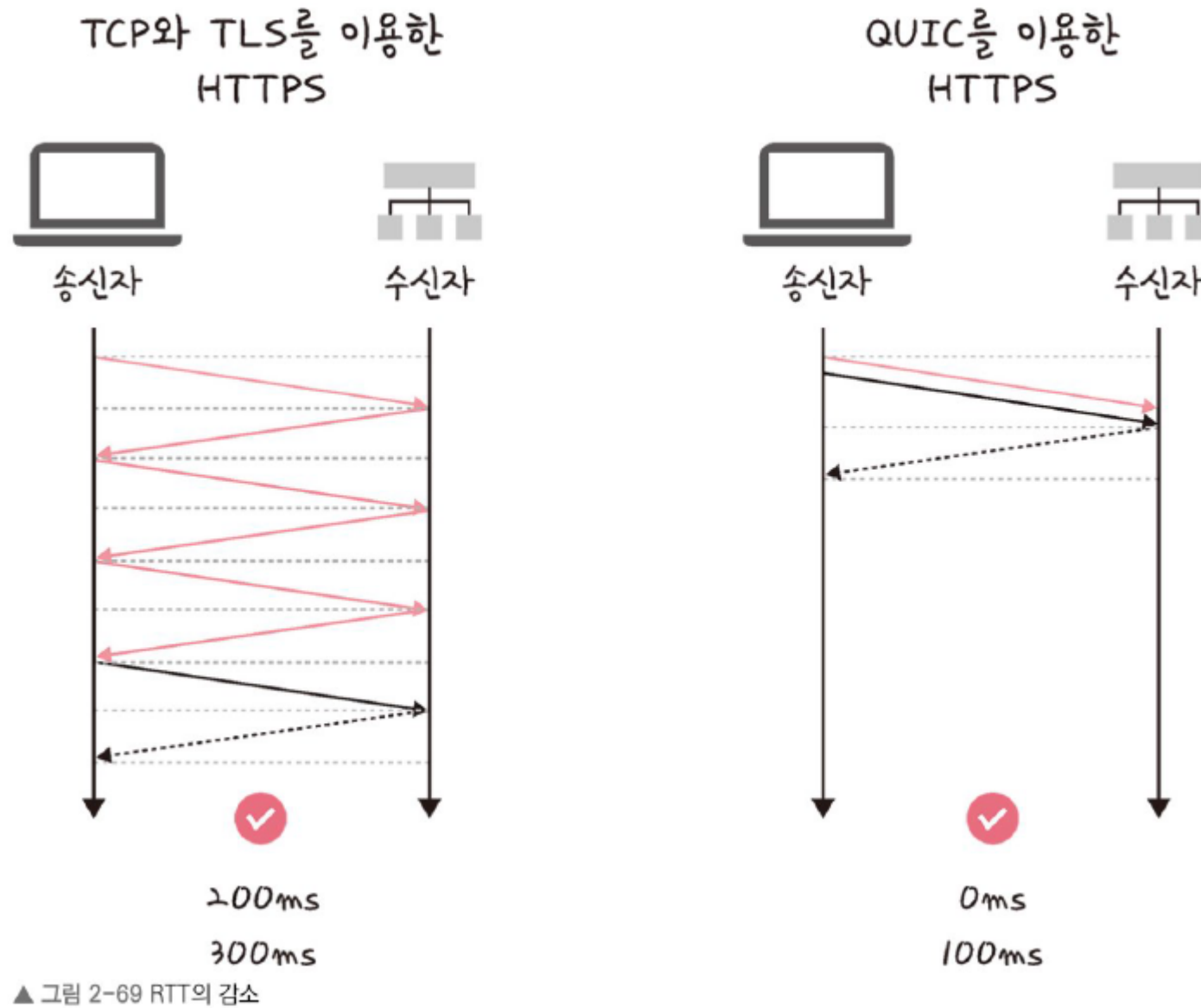
- HTTP/3은 HTTP/1.1 및 HTTP/2와 함께 WWW에서 정보를 교환하는 데 사용되는 HTTP의 세 번째 버전입니다.
- TCP 위에서 돌아가는 HTTP/2와는 달리 HTTP/3는 **QUIC**라는 계층 위에서 돌아가며, TCP 기반이 아닌 **UDP 기반**으로 돌아갑니다.
- HTTP/2의 장점이었던 멀티플렉싱을 가지고 있으며 **초기 연결 설정 시 지연 시간 감소**라는 장점이 있습니다.

QUIC (Quick UDP Internet Connections)

- UDP 기반 응답 속도를 개선하고 TCP 기반 다중화와 신뢰성 있는 전송이 가능한 차세대 HTTP 프로토콜(HTTP/3)

- 즉, UDP는 처리 속도가 빠른 반면 데이터의 신뢰성 확보가 어렵지만, QUIC 계층을 추가하여 TCP만큼 신뢰성을 제공할 수 있게 하였습니다.
- 게임, 스트리밍 미디어, VoIP 서비스에 자주 쓰이며, 지연 시간이 적은 인터넷 전송 프로토콜입니다.

초기 연결 설정 시 지연 시간 감소



- QUIC는 TCP를 사용하지 않기 때문에 통신을 시작할 때 번거로운 3-Way Handshake 과정을 거치지 않아도 됩니다.
- QUIC는 첫 연결 설정에 1-RTT만 소요됩니다.

클라이언트가 서버에 어떤 신호를 한 번 주고 서버도 거기에 응답하기만 하면 바로 본 통신을 할 수 있다는 말입니다.

▼ RTT란?

- RTT = 왕복 시간(Round Trip Time)
- 인터넷 상에서 송신지부터 목적지까지 패킷이 왕복하는데 걸리는 시간
- QUIC는 순방향 오류 수정 메커니즘(FEC, Forward Error Correction)이 적용되어 있습니다.

▼ FEC란?

전송한 패킷이 손실되었다면 수신 측에서 에러를 검출하고 수정하는 방식. 열악한 네트워크 환경에서도 낮은 패킷 손실률을 자랑함

참고

도서- 면접을 위한 CS 전공지식 노트

<https://blog.skby.net/quic-quick-udp-internet-connection/>