11 MASQUE 기술 표준화 - IETF미러포럼

□ 개요

○ MASQUE(Multiplexed Application Substrate over QUIC Encryption)는 Transport QUIC 기반의 HTTP/3 프로토콜을 활용하여 기존 전송 프로토콜 프록시 기술의 제약점을 해결하고, 임의의 데이터가 Transport QUIC를 통해 터널링 될 수 있도록 Transport QUIC를 기반(Substrate) 프로토콜로 사용하는 표준 기술임

▸ MASQUE는 (1) Transport QUIC 데이터그램이 HTTP/3에서 사용되는 방식에 대한 정의와 (2) 대상 서버에 UDP 소켓을 시작하는 새로운 종류의 HTTP 요청, 이 두 가지 표준 기술로 UDP 터널링 문제를 해결하고자 함

▸ OSI 7레이어 중 응용계층과 전송계층이 연계되는 기술

○ Transport QUIC 및 HTTP/3 표준화 완료와 역사적 의미

- 원래 QUIC은 구글에서 개발된 기술로서 웹페이지 로딩 속도 개선은 물론 혼잡 제어와 손실 복구를 향상시키기 위한 기술임
- QUIC은 기존 HTTP/2에서 TCP+TLS(3-Way Handshake 과정)에 해당하며, 보안 및 향상된 성능을 제공하는 UDP 기반 전송 계층 프로토콜임
- QUIC은 상당히 가볍고 성능과 보안성을 모두 고려해서 설계되었으며, 암호화된 전송을 통해 멀티플렉싱된 스트림을 제공함
- 또한, QUIC는 독립적인 TCP 연결과 거의 동일하지만 대기 시간이 훨씬 단축되기 때문에 클라이언트 연결 초기화 시간을 줄일 수 있으며, TCP의 HOL 차단 현상을 제거할 수 있음
- 2016년 후반 QUIC WG이 승인 되어 본격적인 논의가 시작되었으며 이후 많은 관심을 받으면서 약 5년간 IETF에서 표준화를 진행하였음
- QUIC WG에서 IETF 버전 QUIC은 HTTP 뿐만 아닌 다른 프로토콜을 전송할 수 있어야 한다고 결정하여 (HTTP-over-QUIC) Hypertext Transfer Protocol (HTTP) over QUIC와 (Transport QUIC) QUIC: A UDP-Based Multiplexed and Secure Transport으로 나누어 개발을 시작하였음
- 지난 2021년 5월 다음과 같이 Transport QUIC 프로토콜 및 관련 표준기술들이 일련의 RFC로 공식 배포되었음

· QUIC: A UDP-Based Multiplexed and Secure Transport(RFC 9000, May 2021)

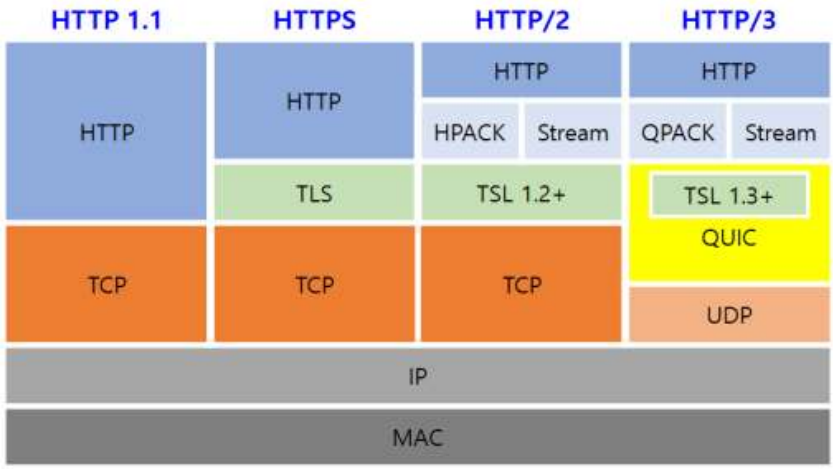
· Version-Independent Properties of QUIC(RFC 8999, May 2021)

· Using TLS to Secure QUIC(RFC 9001, May 2021)
· QUIC Loss Detection and Congestion Control(RFC 9002, May 2021)

- 한편, HTTP-over-QUIC는 2019년 Hypertext Transfer Protocol Version 3(HTTP/3)으로 표준명 변경하여 진행되었고, 2021년 2월 마지막 업데이트 되었으며 최근 2022년 6월 RFC로 최종 출판되었음

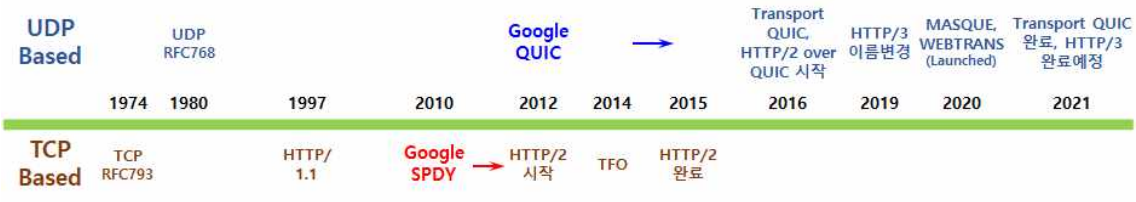
· Hypertext Transfer Protocol Version 3 (HTTP/3) (RFC 9114, June 2022)

- QUIC 기반의 HTTP/3와 기존 TCP 기반의 HTTP/1.1, HTTPS, HTTP/2와 비교는 〈그림 1〉과 같음

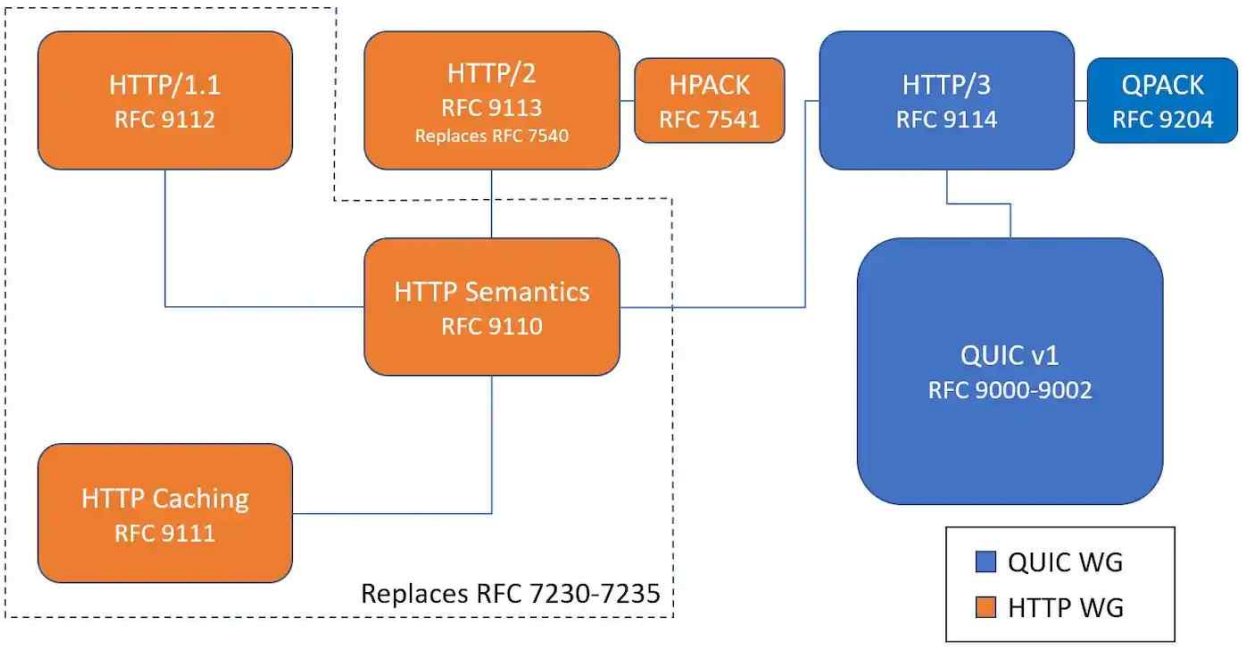


〈그림 1〉 IETF 표준 HTTP 프로토콜의 스택 구조 비교

- Transport QUIC과 HTTP/3 프로토콜은 상호 협력적이고 반복적인 표준화 프로세스를 통해 발전하였음
- 2016년 WG이 설립된 이후로 5년 동안 26번의 대면 회의, 약 1,800 건의 이슈 제기 및 수천 건의 이메일을 주고받은 끝에 표준화를 마무리한 것임
- 이는 Transport QUIC이 대체하고자 하는 기본 전송 프로토콜이며 현재 대부분의 인터넷 서비스에서 쓰여지고 있는 TCP가 완성 된지 40년만의 일이고 HTTP/2 표준이 출판(배포)된지 6년만의 일임
- 결국, 구글은 SPDY를 통해 HTTP/2를, QUIC을 통해 HTTP/3를 이끎으로서 IETF에서 큰 영향력을 미친 기업이 되었음
- 〈그림 2〉는 TCP로부터 HTTP/3까지의 IETF 표준화 역사를 나타내며, 〈그림 3〉 Transport QUIC와 HTTP/3 표준기술들의 연관성을 나타냄



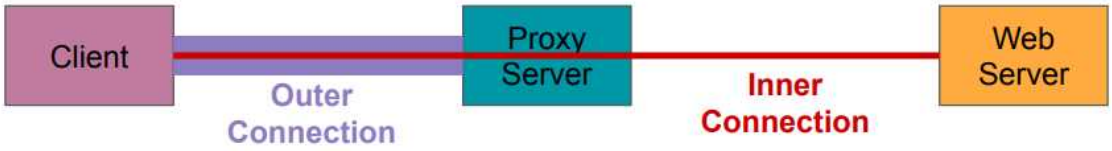
〈그림 2〉 TCP로부터 HTTP/3까지의 IETF 표준화 역사



〈그림 3〉 기존 표준기술과 Transport QUIC, HTTP/3 표준기술과의 상호 관련성

○ Transport QUIC 및 HTTP/3의 필수 요구 사항인 암호화로 인한 도전과제 해결을 위한 프록시(Proxy) 기법

- Transport QUIC와 이를 기반으로 하는 HTTP/3은 모두 암호화를 필수로 요구하는데, 이 때문에 단대단 연결이 불가능하거나(예 : 인터넷 검열), 실행 가능하지 않거나(예 : 위성 링크), 원하지 않는(예 : 개인 정보 보호 문제) 등의 특수한 적용 사례에서 도전과제(Challenges)를 야기함
- 이러한 도전과제를 해결하기 위한 하나의 방법으로 프록시 기능을 고려할 수 있으며, 많은 네트워크 토폴로지에서 전송 프로토콜 프록시가 유용하게 사용될 수 있음
- 예를 들어, VPN과 같이 프록시를 사용하면 단대단 연결이 불가능할 때 엔드 포인트가 통신하거나 원하는 경우 추가 암호화를 적용 할 수 있음
- 프록시 기능은 또한 대상 서버로부터 클라이언트의 IP 주소를 숨겨 클라이언트 개인 정보를 향상시킬 수 있음



〈그림 4〉 프록시 서버의 역할 개념도

- 하지만, 기존의 몇몇 전송 프로토콜 프록시 기술은 제약점을 가지고 있음

· 기본 HTTP 프록시는 암호화되지 않으며 TCP 기반으로 한정됨
· 소켓 보안인 SOCKS는 TCP/UDP 기반이기는 하지만 암호화 되지 않음
· Transparent TCP 프록시는 On-path가 의무이며 TCP 기반(must be on-path, mandatory to use, TCP)으로 한정됨
· HTTP CONNECT는 암호화가 선택 사항이며 TCP 기반으로 한정됨

- 한편, QUIC 기반의 HTTP/3는 단일 연결에서 암호화된 안전한 연결, 다중화된 스트림, 주소 마이그레이션 및 통합 혼잡 제어기를 제공하기 때문에 임의의 트래픽을 프록시할 수 있는 프로토콜 중 하나임
- 또한, UDP 기반의 QUIC 프레임 위에서 동작되는 HTTP/3 데이터그램 구조는 비신뢰성 데이터 전송을 제공하고 프록시를 통해 UDP 및 기타 비신뢰성 플로우를 전송할 수 있게 하며, 이종의 서비스에 대한 플로우를 설정 및 구성 할 수 있는 요청-응답 시멘틱을 지원함

ㅇ MASQUE WG의 설립 배경 및 목표
- Transport QUIC 기반의 HTTP/3 프로토콜을 활용하여 기존 전송 프로토콜 프록시 기술의 제약점을 해결하고, 임의의 데이터가 QUIC를 통해 터널링 될 수 있도록 QUIC를 기반(Substrate) 프로토콜로 사용하고자 함
- MASQUE WG은 서비스 제공 업체(Cloudflare 등) 및 콘텐츠 제공 업체(Apple 등)의 관심속에 2020년 107차 회의에서 BOF가 진행되었고 이후 WG으로 승인이 되었으며 Cloudflare의 Christopher A. Wood와 Apple의 Eric Kinnear가 공동 의장을 맡게 되었음
- MASQUE WG의 주요 목표는 “To allow configuring and concurrently running multiple proxied stream-based and datagram-based flows inside an HTTP/3 connection concurrently”, 즉 단일 HTTP/3 연결 내에서 다중의 프록시 스트림 및 데이터그램 기반 플로우를 구성하고 동시에 실행할 수 있는 메커니즘을 개발하는 것임
- 명시적인 클라이언트-개시(Client-initiated) 시그널링을 사용하여 단일 HTTP/3

연결 내에서 임의의 연결들을 터널링 할 수 있는 메커니즘을 개발하는데, 우선적으로 CONNECT-UDP HTTP와 IP 프록시을 다루며 추가적인 내용으로 확장할 계획임

- 서버-개시(Server-initiated) 프로토콜은 다루지 않는다. 또한, UDP 및/또는 HTTP/3가 인터넷 연결상에 존재하는 기존(Legacy) 클라이언트-프록시에서 자동적으로 차단되는 상황, 즉 프로토콜 고착화(Ossification)로 인한 문제를 해결하기 위해서 우회 프로토콜, 즉 폴백(Fallback) 프로토콜로 원래의 TCP 기반 HTTPS를 고려하고 있음
- 또한, 제3자의 검열(Censorship)이슈를 해결하기 위해 터널링된 데이터는 유선상에서 임의의 암호화된 HTTP 연결과 구별되지 않으며, 이를 통해 연결의 특성을 검열 하고자 하는 대상에게 노출시킬 수 있는 힌트를 방지함. 다시 말해서, 터널링된 데이터가 일반적인 암호화된 HTTP 연결과 구분이 안되어 검열하는데 어려움이 있을 것임

ㅇ MASQUE WG의 주요기술 1 : 데이터그램 캡슐화(Encapsulating datagrams)

- 클라이언트와 프록시 사이의 UDP 페이로드를 캡슐화하는 방법 (프록시가 캡슐화를 해제하고 실제 UDP 데이터그램에서 대상서버으로 전달)
- QUIC의 신뢰할 수 없는 데이터그램 확장(Unreliable datagram extension)은 이름에서 알 수 있듯이 신뢰할 수 없는 새로운 DATAGRAM 프레임을 추가함
- 여러 용도가 있는데 그 중 중요한 하나가 고성능 UDP 터널링을 위한 빌딩 블록을 제공한다는 것이며, 특히 이 확장에는 다음과 같은 속성이 있음

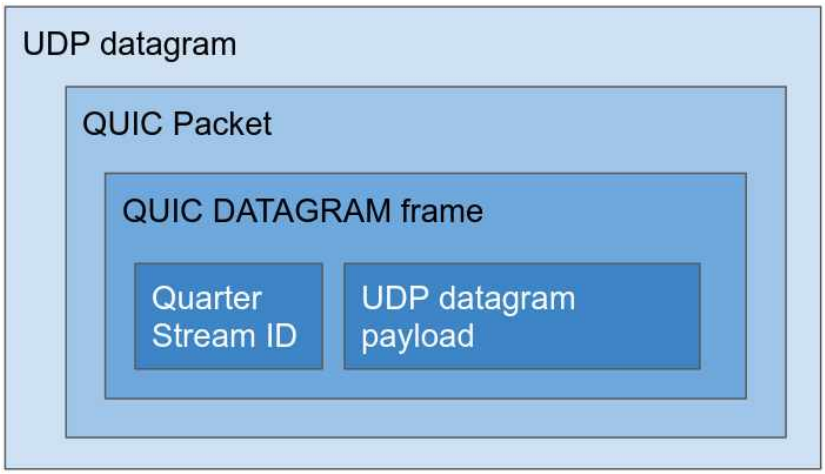
  · DATAGRAM 프레임은 긴 QUIC 스트림과 달리 개별 메시지임
  · DATAGRAM 프레임에는 QUIC의 스트림 ID와 달리 다중화 식별자가 포함되어 있지 않음
  · 모든 QUIC 프레임과 마찬가지로 DATAGRAM 프레임은 QUIC 패킷 내부에 완전히 맞아야 함
  · DATAGRAM 프레임은 혼잡 제어의 대상이 되므로 발신자가 네트워크 과부하를 피할 수 있음
  · DATAGRAM 프레임은 수신자가 승인하지만 중요한 것은 발신자가 손실을 감지하면 QUIC가 손실된 데이터를 재전송하지 않는다는 것임

- "An Unreliable Datagram Extension to QUIC" 표준은 지난 2022년 3월 RFC9221로 발행되었음
- 이 기능은 이미 Cloudflare의 quiche 라이브러리를 통해 이미 지원되어 왔으며,

이제 QUIC에 신뢰할 수 없는 메시지 전송을 지원하는 기본 요소가 있으므로 내부에서 UDP를 효과적으로 터널링하는 표준 방법이 있게 된것임

- QUIC는 프록시 목표를 지원하는 STREAM 및 DATAGRAM 전송 프리미티브를 제공함
- MASQUE WG에서는 위에서 설명한 QUIC 데이터그램이 HTTP/3에서 사용되는 방식을 다음 문서에서 다루고 있음 (이 문서는 원래 QUIC WG 내에서 처음 제안되어 MASQUE WG으로 이관되었음)

· HTTP Datagrams and the Capsule Protocol (draft-ietf-masque-h3-datagram-11, 17 June 2022)



〈그림 5〉 MASQUE에서 데이터그램 캡슐화 개념도

ㅇ MASQUE WG의 주요기술 2 : HTTP/3를 위한 CONNECT 메소드 (HTTP UDP CONNECT)

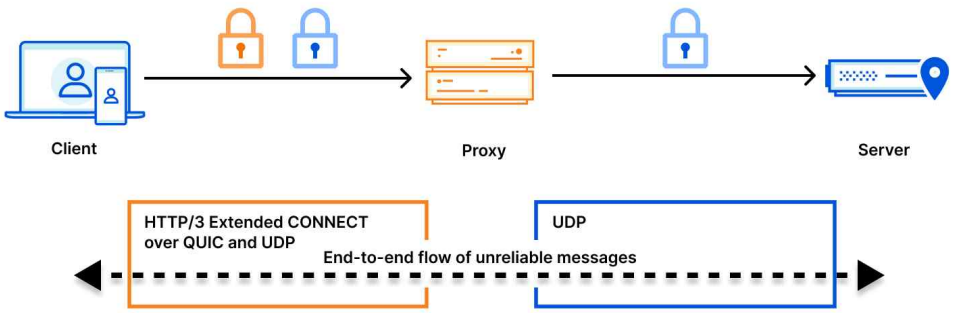
- 클라이언트가 프록시를 통해 대상 서버와 HTTP/3로 통신을 하는 경우 필요한 두 번째 요구사항 : 캡슐화 해제된 페이로드를 전달할 위치를 알 수 있도록 프록시가 대상에 대한 UDP 연결을 열도록 지시하는 방법
- 응용 프로그램은 UDP 데이터그램을 보낼 위치와 수신 위치를 프록시 서버에 알리면서 종단 간 터널을 어떻게 설정하는가에 대한 표준 기술이 필요하며 이를 다루고 있는 MASQUE WG 문서는 다음과 같음

· UDP Proxying Support for HTTP(draft-ietf-masque-connect-udp-15, 17 June 2022)

- 위 문서는 대상 서버에 UDP 소켓을 시작하는 새로운 종류의 HTTP 메소드인

CONNECT에 관한 것임(이하 HTTP UDP CONNECT라고 부름)

- WG에서 핵심적으로 다루고 있는 표준 기술이며 TCP-only HTTP CONNECT 방법에 대한 UDP 기반 대응 기법이라고 할 수 있음
- 이 메소드는 원래 “Bootstrapping WebSockets with HTTP/2(RFC8441)”에서 HTTP/2를 위해 처음 도입 되었으며 현재는 HTTP/3을 위한 확장된 CONNECT로 표준화 중임
- 확장된 CONNECT인 HTTP UDP CONNECT에서는 클라이언트가 요청하는 의도를 나타내는데 사용할 수 있는 :protocol pseudo-header를 새롭게 정의함
- 원래 초기 사용 사례는 RFC8441에서 기술했듯이 HTTP/2 기반 WebSocket이었지만, 현재는 UDP 상에서 동작하는 QUIC 기반 HTTP/3 응용프로그램 용도로 확장하고 있음



〈그림 6〉 MASQUE에서 HTTP UDP CONNECT 동작도

ㅇ MASQUE WG의 주요기술 3 : IP Proxying

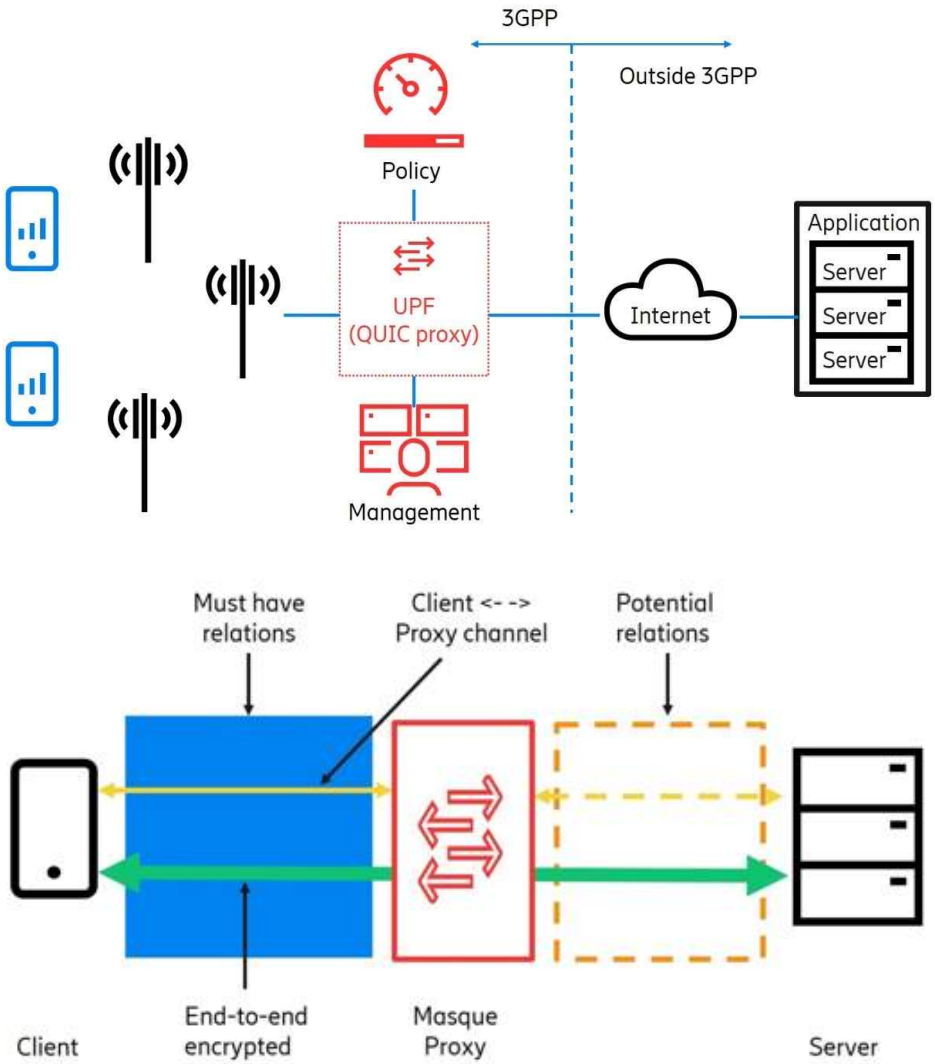
- MASQUE WG은 기존 VPN 사용 사례를 다루는 일반 IP 프록시에 대한 요구 사항을 다루고 있음
- IP Proxying 기술은 다른 CONNECT 프로토콜 설계와 유사하지만 몇 가지 차이점이 있음
- QUIC 데이터그램 프레임을 사용하는 HTTP/3의 멀티플렉싱 기능을 활용하여 단일 HTTP 연결을 통해 여러 IP 프록시 연결을 실행
- 결국 CONNECT 기반 프록시는 이미 TLS 및 기존 WebPKI에 많이 투자된 생태계 및 환경에 더 적합하므로 IP 터널을 위한 CONNECT 기반 솔루션이 미래에 표준이 될 것으로 기대하고 있는 것인데 아직 초기 단계이며 MASQUE WG 문서는 다음과 같음

· IP Proxying Support for HTTP(draft-ietf-masque-connect-ip-02, 11 July 2022)

□ 현황

○ 기술개발 현황 및 전망

- (국제) MASQUE 기술 사양의 설계 세부 사항은 계속 업데이트 중이지만 지금까지 여러 구현이 개발되었으며 그 중 일부는 IETF 해커톤 동안 상호 운용성 테스트를 거쳤음. 해커톤을 통한 실행 코드는 표준사양의 지속적인 개발을 알리는 데 도움이 될 것으로 전망, 세부 사항은 표준화 프로세스가 종료되기 전에 계속 업데이트 될 가능성이 높지만 전체적인 접근 방식은 유사하게 유지될 것으로 예상함. 참고로 최근 에릭슨에서 3GPP와 MASQUE의 연계 아키텍쳐를 제안하여 발표하였음.

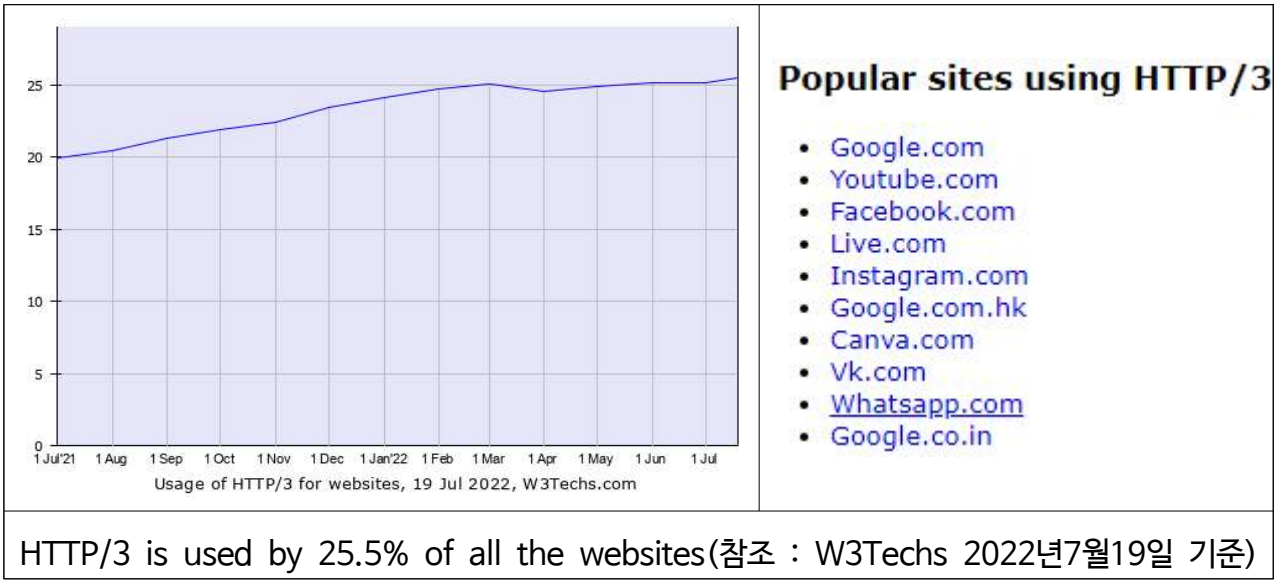


〈그림 7〉 에릭슨에서 제시한 3GPP-MASQUE 연계 구성도

- (국내) MASQUE 기술에 대한 표준화 및 개발이 초기 단계이기 때문에 국내의 경우 관련 기술 개발은 진행되고 있지 않으나, 국내에서도 Transport QUIC와 HTTP/3 기술에 대한 확산이 시작되고 있기 때문에 관련 기술에 대한 기술개발이 곧 시작될 것으로 예상함

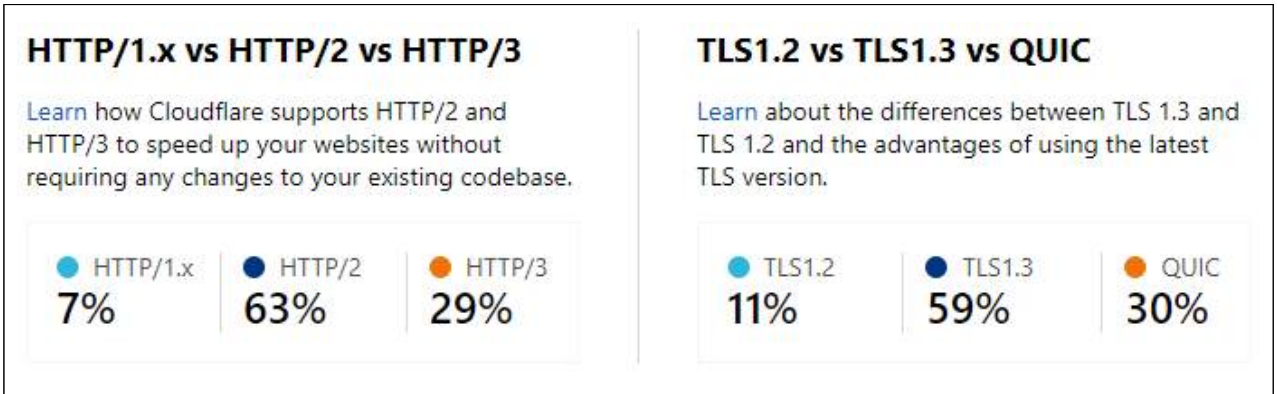
ㅇ 시장 및 산업체 현황 및 전망

- (국제) MASQUE의 기반 프로토콜인 Transport QUIC와 HTTP/3의 확산 현황에서 향후 MASQUE의 시장에서 전망을 예측 할 수 있음. 〈그림 8〉~〈그림 10〉에서 확인할 수 있듯이 두 표준은 최근에 마무리 되었음에도 불구하고 그 이전부터 확산이 진행되었으며, 그 확산 속도가 매우 빠름을 확인할 수 있음
- (국내) MASQUE 기술에 대한 표준화 및 개발이 초기 단계이기 때문에 국내의 경우 국제 시장과 마찬가지로 형성이 되어 있지 않음. 다만, 국내에서도 Transport QUIC와 HTTP/3 기술에 대한 확산이 시작되고 있어 이에 대한 시장 형성의 초기 단계라 할 수 있음



HTTP/3 is used by 25.5% of all the websites(참조 : W3Techs 2022년7월19일 기준)

〈그림 8〉 MASQUE의 기반 기술인 HTTP/3의 확산 현황



HTTP/1.x vs HTTP/2 vs HTTP/3, TLS1.2 vs TLS1.3 vs QUIC,

(참조 : Cloudflare Radar 2022년 7월 기준)

〈그림 9〉 MASQUE의 기반 기술인 HTTP/3과 QUIC의 기존기술 대비 사용률

Popular sites using QUIC

- Google.com
- Youtube.com
- Google.com.hk
- Google.co.in
- Google.com.br
- Google.co.jp
- Google.de
- Google.fr
- Google.ru
- Google.it

QUIC is used by 8.3% of all the websites(참조 : W3Techs 2022년7월19일 기준)

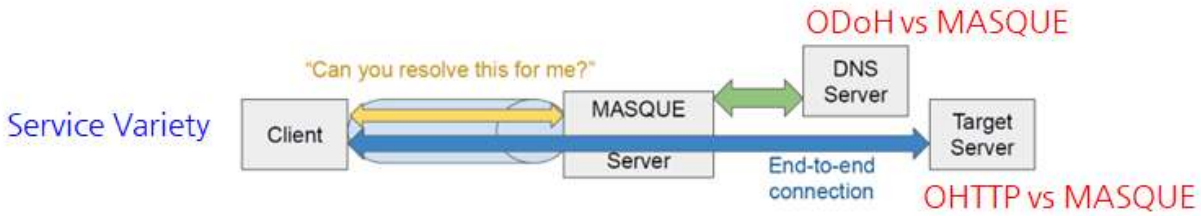
〈그림 10〉 MASQUE의 기반 기술인 Transport QUIC의 확산 현황

○ 표준화 현황 및 전망

- (국제) MASQUE WG에서 다루어진 문서들에서 확인할 수 있듯이, 현재 다뤄지고 있는 문서들은 구글(Google), 클라우드플레어(Cloudflare), 애플(Apple), 에릭슨(Ericsson) 등 인터넷 서비스 및 인프라 시장의 대표적인 글로벌 선두 기업들이 주도함으로써 HTTP/3, QUIC 기술은 물론 이와 연계된 기술인 MASQUE 기술이 향후 다양한 인터넷 서비스에서 비중 있게 활용될 것임을 짐작할 수 있음
- (국제) 최근 IETF 내 전송/응용 계층 기술을 다루는 Area에서 MASQUE 기술의 기본 개념이라 할 수 있는 Proxy 기법을 기반으로 하는 다양한 새로운 표준화 활동이 시작되고 있음. Proxy의 개념으로 사용하는 용어가 Oblivious라는 것인데 '의식하지 못하는'이라는 사전적 의미를 가지며, 2018년 Oblivious DNS-Strong Privacy for DNS Queries라는 IETF Internet Draft에서 처음 사용되었음. 대표적인 첫 번째 활동이 이 Oblivious라는 개념을 기존 DOH(DNS over HTTPS)에 적용하는 Oblivious DNS Over HTTPS(ODoH) 기술인데 애플, 패스틀리(Fastly), 클라우드플레어가 주도하고 있음. 더 나아가 Oblivious 개념을 더 확대하기 위해서 기존 HTTP에 Oblivious 개념을 적용한 Oblivious HTTP Application Intermediation (OHAI) WG이 2021년 10월 설립되어 최근 본격적인 표준화 활동을 진행하고 있음. 〈그림 11〉과 〈그림 12〉은 MASQUE, ODoH, OHTTP의 비교와 활용 사례를 나타냄

	ODoH	OHTTP	MASQUE
IETF WG	DPRIVE	OHAI	MASQUE
Substrate Protocol	HTTPS	HTTP(S)	HTTP(S)/3
Service	DNS Transaction	Web Transaction	Unlimited
Connection	Short lived	Short lived	Long lived

〈그림 11〉 MASQUE, ODoH, OHTTP의 비교

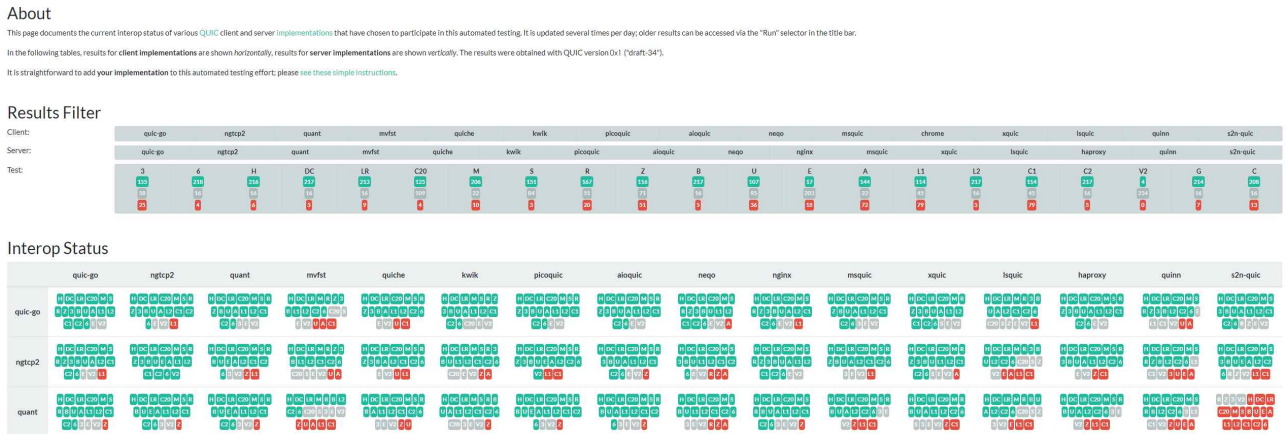


〈그림 12〉 MASQUE, ODoH, OHTTP의 적용 사례

- (국내) IETF 미러포럼 차원에서 관련 표준 이슈를 Follow-up 하고 있으며 MASQUE WG은 물론 이와 연관성이 높은 OHAI WG과 연계하는 표준화 활동을 계획하고 있음. 올해 내에 MASQUE WG에 Path MTU Discovery 관련 기고문을 준비하여 제출 예정임

ㅇ 시험인증 현황 및 전망

- (국제) MASQUE의 표준화가 시작된지 얼마되지 않아 공식적인 시험인증 논의는 없으나 조만간 시험인증에 대한 논의가 진행될 것으로 예상됨. 이러한 예상의 근거로는 QUIC Interop Runner의 상시 운영이라고 할 수 있음. 〈그림 13〉과 같이 MASQUE의 기반 표준 기술인 Transport QUIC와 HTTP/3에 대한 자동화된 상호 운용성 테스트 시스템인 QUIC Interop Runner이 24시간 지속적으로 실행되고 있으며 구글, 애플, 마이크로소프트, 모질라, Fastly와 같은 세계적인 선두 기업들은 자체 구현을 위해 주기적으로 모여 서로 구현을 테스트를 진행중임
- (국내) 국제 현황과 마찬가지로 현재 MASQUE 기술에 대한 시험인증 현황은 없지만, TTA SW시험인증연구소에서 QUIC Interop Runner와 연계하여 인증이 가능할 것으로 예상됨



〈그림 13〉 MASQUE의 기반 기술인 Transport QUIC의 상호 운용성 테스트 현황

□ 주요이슈 및 대응방안

○ 인터넷 분야 글로벌 빅테크 기업들 주도의 표준화가 진행됨

- 구글은 자사가 직접 개발하고 검증까지 마무리한 QUIC 기술을 IETF에 표준 문서로 들고 나타났으며, 이를 기반으로 2016년 QUIC WG이 공식 설립된 이후 QUIC 기술의 표준화는 물론 이를 HTTP에 적용하는 표준화를 진행함으로써 뜨거운 관심과 많은 이슈를 이끌었음. 최근까지 IETF에서 표준화가 진행되었고, Transport QUIC은 2021년에 HTTP/3은 2022년에 각각 표준화가 마무리 되었음
- 구글은 과거 자사의 SPDY라는 기술로 HTTP/2 표준을 이끌었던 것처럼, 자사의 QUIC 기술로 HTTP/3 표준을 이끌게 되어 IETF 표준화 기구의 역사는 물론 인터넷 역사에 중요한 이정표를 세우는데 큰 역할을 하게 되었음
- 구글의 SPDY와 QUIC 프로토콜의 목표 중 하나가 제공하는 인터넷 서비스들의 응답 속도를 빠르게 하는 것이였으며 결국 HTTP/2과 HTTP/3 모두 웹서비스 시장에서 구글이 주도한 진정한 시장 중심의 사실 표준화라 할 수 있음
- MASQUE 기술 역시 Transport QUIC 및 HTTP/3 표준화 완료로 인한 다음 단계의 표준화로서 구글, 클라우드플레어, 애플, 에릭슨 등 인터넷 서비스 및 인프라 분야 글로벌 선두 기업에서 주도하기 시작한 기술임

○ Transport QUIC 및 HTTP/3 표준화 완료로 인한 다양한 새로운 표준화 활동 증가

- 최근, MASQUE 외에도 Transport QUIC 및 HTTP/3 표준화 완료로 인한 다음 단계의 표준화로서 구글, 모질라 등 글로벌 선두 기업들 중심으로 새로운 표준 WG인 Webtransport WG, OHAI WG 등이 신설되어 본격적인 활동 시작됨

○ (대응방안) 최근 표준화 활동은 단순 시장 중심의 표준화가 아닌 표준화 패권 경쟁의 관점에서 세력 중심의 표준화 활동에 대응 필요

- 구글, 클라우드플레어, 애플, 모질라, 에릭슨, 패스틀리와 같은 인터넷 분야 세계적인 선두 기업들은 자체 구현을 위해 열심히 노력해 왔으며 대부분은 이제 상당히 성숙된 상태
- 이러한 기업들은 주기적으로 모여 서로 구현을 테스트하며 대부분은 MASQUE, Webtransport, ODoH, OHAI 등의 기반 기술이 되는 Transport QUIC 및 HTTP/3 관련하여 QUIC Interop Runner라고 하는 지속적으로 실행되는 자동화된 상호 운용성 테스트 시스템에 참여하고 있음
- 현재 구글, 모질라, 애플 중심으로 하는 글로벌 빅테크 세력이 IETF 내에서 인터넷 응용/전송 계층 중심으로 다양한 시장 중심의 표준화를 주도하고 있으며 이를 통해 표준화 패권 경쟁에서 우위를 두고자 하고 있음
- 우리나라도 인터넷 서비스 업체와 웹서비스 업체는 물론 표준화 분야 관련자들의 관심과 대응이 적극 필요한 분야라 할 수 있음

[약어표]

IETF	Internet Engineering Task Force	TCP	Transmission Control Protocol
MASQUE	Multiplexed Application Substrate over QUIC Encryption	UDP	User Datagram Protocol
ODoH	Oblivious DNS Over HTTPS	OHAI	Oblivious HTTP Application Intermediation

[참고문헌]

[1] Y. Cui, T. Li, C. Liu, X. Wang, and M. Kühlewind, “Innovating transport with QUIC: Design approaches and research challenges,” IEEE Internet Computing, vol. 21, no. 2, pp. 72–76, 2017

[2] A. Z. Sarker et al., S. Kim, A collaborative approach to encrypted traffic, Ericsson Blog, June 2020

[3] M. Kosek, T. Shreedhar, V. Bajpai, “Beyond QUIC v1 – A First Look at Recent Transport Layer IETF Standardization Efforts”, IEEE Communications Magazine, vol. 59, issue 4, pp. 24~29, April 2021

[4] M. Kühlewind et al., “Evaluation of QUIC-based MASQUE proxying”, EPIQ '21: Proceedings of the 2021 Workshop on Evolution, Performance and Interoperability of QUIC, pp. 29~34, December 2021

[5] P. S. Kim, “A Survey on Transport Layer IETF Standardization Works for Resolving Limitations of TCP”, ICIC Express Letters, vol. 16, no. 2, pp. 169~176, 2022

[6] L. Pardue and C. Wood, Unlocking QUIC’s proxying potential with MASQUE, The Cloudflare Blog, March 2022

[7] IETF MASQUE WG, https://datatracker.ietf.org/wg/masque/about/