امیرمهدی کوششی

دکتر فصحتی

ارائه پروتکل QUIC

۹۸۱۷۱۰۵۳

پروتکل QUIC

۱. مقدمه

پروتکل QUIC (Quick UDP Internet Connections) یک پروتکل لایه‌ی انتقال جدید است که توسط **گوگل** برای بهبود عملکرد **HTTP/2** توسعه داده شد. این پروتکل جایگزینی برای **TCP + TLS + HTTP/2** محسوب می‌شود که ارتباطات سریع‌تر، ایمن‌تر و کم‌تأخیرتری را فراهم می‌کند.

QUIC مبتنی بر **UDP** بوده و دارای ویژگی‌هایی مانند **Multiplexing بدون Head-of-line blocking**، **Zero-RTT Handshake**، و **Connection Migration** است.

۲. معماری پروتکل QUIC

QUIC شامل چندین لایه‌ی اصلی است که در ادامه بررسی می‌شوند:

۲.۱ لایه‌ی انتقال (Transport Layer)

- **Multiplexed Streams**: چندین جریان داده هم‌زمان بدون تأخیر مسدودکننده (**Head-of-line blocking**) ارسال می‌شوند.
- **Flow Control**: هر جریان دارای محدودیت‌های نرخ ارسال و دریافت داده است.

۲.۲ لایه‌ی امنیتی (Security Layer)

- **TLS 1.3 Encryption**: تمامی ارتباطات **QUIC** رمزنگاری شده‌اند.
- **Zero-RTT Handshake**: تأخیر کم برای ایجاد ارتباطات جدید.

۲.۳ لایه‌ی شبکه (Network Layer)

- **UDP-based Communication**: مبتنی بر **UDP** برای کاهش سربار پروتکل و افزایش سرعت.

- **Connection Migration**: امکان جابجایی ارتباطات بین **WiFi** و **4G** بدون قطع اتصال.

۳. ویژگی‌های کلیدی QUIC

۳.۱ ارتباطات سریع‌تر با Zero-RTT Handshake

در **TCP**، ارتباط نیازمند سه مرحله‌ی دست‌دهی (**Three-Way Handshake**) است. اما در **QUIC**، این فرآیند به **Zero-RTT** کاهش یافته و در اولین پیام، اطلاعات کلیدی امنیتی ارسال می‌شود.

۳.۲ Multiplexing بدون Head-of-line Blocking

در **HTTP/2**، اگر یکی از فریم‌های **TCP** از بین برود، تمامی جریان‌های دیگر منتظر دریافت مجدد آن بسته خواهند ماند (**Head-of-line blocking**). اما در **QUIC**، هر جریان به‌صورت مستقل اداره شده و از این مشکل جلوگیری می‌شود.

۳.۳ Connection Migration

با تغییر شبکه‌ی کاربر (مثلاً از **WiFi** به **4G**)، ارتباط **TCP** قطع می‌شود. اما در **QUIC**، از یک **Connection ID** استفاده می‌شود که امکان مهاجرت اتصال بدون ایجاد اختلال را فراهم می‌کند.

۴. امنیت و رمزنگاری در QUIC

تمام ارتباطات در **QUIC** به‌صورت پیش‌فرض رمزنگاری‌شده و از **TLS 1.3** برای تأمین امنیت داده‌ها استفاده می‌شود. برخی از ویژگی‌های امنیتی آن عبارتند از:

- **Encryption-by-default**: داده‌های ارسال‌شده همیشه رمزنگاری می‌شوند.
- **Forward Secrecy**: جلوگیری از رمزگشایی بسته‌ها حتی در صورت دسترسی به کلید خصوصی.

- **Authenticated Headers**: جلوگیری از تغییر غیرمجاز اطلاعات در هدرها.

۵. مدیریت Congestion Control و Flow Control

۵.۱ کنترل ازدحام

QUIC از الگوریتم‌های مختلفی مانند **Cubic** و **BBR** برای کنترل ازدحام استفاده می‌کند. برخلاف **TCP**، این کنترل ازدحام بر روی **UDP** اجرا شده و قابلیت بهینه‌سازی بهتری دارد.

۵.۲ کنترل جریان (Flow Control)

این قابلیت تضمین می‌کند که فرستنده داده‌ای بیشتر از ظرفیت گیرنده ارسال نکند. **QUIC** از **Stream-level** و **Connection-level Flow Control** بهره می‌برد.

۶. تفاوت‌های QUIC با TCP + TLS + HTTP/2

TCP + TLS + HTTP/2	QUIC	پروتکل انتقال
TCP	UDP	ویژگی
TCP بر روی TLS	TLS 1.3	رمزنگاری
نیاز به چندین مرحله handshake	Zero RTT (بسیار کم)	تاخیر اولیه
بله، اما Head-of-line Blocking دارد	بله، بدون Head-of-line Blocking	Multiplexing
اتصال در تغییر شبکه قطع می‌شود	onnection Migration دارد	اتصال پایدار

۷. موارد استفاده و کاربردهای QUIC

- **Google Services** (مانند **Gmail**، **YouTube**، و **Google Search**)

- **HTTP/3** (استاندارد جدید HTTP مبتنی بر **QUIC**)
- **Cloudflare** و **Akamai** برای تسریع انتقال داده‌ها
- **بازی‌های آنلاین** و **ویدئو کنفرانس‌ها** به دلیل نیاز به تأخیر کم و سرعت بالا

۸. پیاده‌سازی‌های مختلف QUIC

پروتکل **QUIC** توسط چندین پروژه و سازمان اجرا شده است، از جمله:

- **Google QUIC (gQUIC)**: اولین نسخه‌ی **QUIC** توسط گوگل.
- **IETF QUIC**: نسخه‌ی استانداردشده توسط IETF.
- **LiteSpeed QUIC**: برای بهینه‌سازی عملکرد سرورهای **LiteSpeed**.
- **Cloudflare quiche**: پیاده‌سازی سریع برای وب‌سرورها و CDNها.

۹. نتیجه‌گیری

پروتکل **QUIC** با ترکیب ویژگی‌های **TLS**، **TCP** و **HTTP/2**، باعث افزایش سرعت، کاهش تأخیر و بهبود امنیت اینترنت شده است. این پروتکل در **HTTP/3** به استانداردی برای ارتباطات امن و سریع تبدیل شده و بسیاری از شرکت‌های بزرگ مانند **Facebook**، **Google**، و **Cloudflare** در حال استفاده از آن هستند.