HTTP یا HyperText Transfer Protocol، یک پروتکل لایه کاربرد (Application) بوده و کاربرد اصلی آن ارتباط با یک وب سرور است. پروتکل HTTP در وب استفاده شده و امکان باز کردن صفحات را فراهم می کند. این پروتکل در دهه های ۸۰ و ۹۰ میلادی توسعه یافت و اولین نسخه آن HTTP/1 در سال ۱۹۹۶ و دومین نسخه آن HTTP/2 در سال ۲۰۱۵ معرفی شد. HTTP/2 با استفاده از Pipeline و فشرده سازی، باعث شد تا سرعت ارتباط افزایش پیدا کند.

HTTP/3 به عنوان آخرین نسخه این پروتکل توسط IETF (Internet Engineering Task Force) معرفی شده است. این پروتکل از چندین تکنولوژی به صورت ترکیبی و در کنار یکدیگر استفاده می کند که موجب افزایش سرعت و امنیت می شود. HTTP/3 داده ها را سریع تر انتقال داده و تاخیر را کاهش می دهد تا سرعت آغاز بارگذاری صفحه را افزایش می دهد. HTTP/3 به صورت پیش فرض از TLS 1.3 برای رمزگذاری اطلاعات استفاده می کند تا دیگر نیازی به استفاده از HTTPS وجود نداشته باشد.

HTTPs/3 سومین نسخه اصلی پروتکل انتقال ابرمتن است که در کنار HTTP1 و HTTP2 برای تبادل اطلاعات در شبکه جهانی وب استفاده می‌شود. HTTP3 بر روی QUIC اجرا می شود که با نام RFC 9000 منتشر شده است.

هر دو HTTP1 و HTTP2 از TCP به عنوان انتقال خود استفاده می کنند.

یک تفاوت مهم در HTTP/3 این است که روی QUIC، یک پروتکل انتقال جدید، اجرا می شود. QUIC یک پروتکل شبکه لایه انتقال رمزنگاری شده نوین است که برای بهبود ایمنی، کارایی و سرعت ترافیک HTTP استفاده می‌شود.

درواقع QUIC مخفف Quick UDP Internet Connections همان پروتکل تحت وب Http ورژن 3 می باشد .

QUIC بر پایه پروتکل UDP می باشد و از پروتکل TLS به منظور تامین امنیت آن استفاده می کند.

این پروتکل یک بازنویسی از پروتکل HTTP/2 می باشد QUIC. ترکیبی از سه پروتکل زیر است

TCP

TLS

HTTP/2

در سال 2018 از طرف تیم سازنده QUIC و IETF درخواستی به منظور تقییر نام QUIC-Over-Http به HTTP/3 ارسال شد و QUIC-Over-Http با نام HTTP/3 ارائه شد.

هنوز مرورگر های بسیاری هستند که از ورژن Stable این پروتکل پشتیبانی نمیکنند و باید آن را به صورت دستی فعال کرد مانند مرورگر های همچون FireFox و Chrome

QUIC به رفع برخی از بزرگترین کاستی های HTTP/2 کمک می کند:

ایجاد راه حلی برای عملکرد ضعیف هنگام تغییر تلفن هوشمند از WiFi به داده های تلفن همراه (مانند هنگام خروج از خانه یا دفتر)

کاهش اثرات از دست دادن بسته - زمانی که یک بسته از اطلاعات به مقصد خود نمی رسد، دیگر تمام جریان های اطلاعات را مسدود نمی کند (مشکلی که به عنوان "مسدود کردن سر خط" شناخته می شود)

مزایای دیگر عبارتند از:

برقراری اتصال سریعتر QUIC

زمان رفت و برگشت صفر

رمزگذاری جامع تر

رمزگذاری به طور پیش فرض چیست؟

نیاز به رمزگذاری در لایه انتقال، به جای لایه برنامه، پیامدهای مهمی برای امنیت دارد. این بدان معنی است که اتصال همیشه رمزگذاری خواهد شد. پیش از این، در HTTPS، اتصالات رمزگذاری و لایه انتقال به طور جداگانه انجام می شد. اتصالات TCP می‌توانستند داده‌های رمزگذاری شده یا رمزگذاری نشده را حمل کنند، و دست دادن TCP و TLS رویدادهای متمایز بودند. با این حال، QUIC اتصالات رمزگذاری شده را به طور پیش فرض در لایه انتقال تنظیم می کند - داده های لایه برنامه همیشه رمزگذاری می شوند.

آیا HTTP/3 در حال حاضر موجود است؟

در حالی که استاندارد هنوز در حال توسعه است، صاحبان وب سایت و بازدیدکنندگان می توانند از طریق مرورگرها، سیستم عامل ها و سایر مشتریان، از HTTP/3 پشتیبانی دریافت کنند. البته، احتمالاً تغییرات بیشتری برای این استاندارد وجود دارد که قبلاً چندین پیاده سازی را پشت سر گذاشته است.

پس از انتشار HTTP/3، کل وب به یکباره تغییر نخواهد کرد. بسیاری از سایت‌ها هنوز بر روی HTTP/2 نیستند.

از نوامبر 2021، پروتکل HTTPs/3 هنوز به طور رسمی یک پیش نویس اینترنتی است، اما در حال حاضر توسط 74٪ مرورگرهای وب در حال اجرا و، طبق W3Techs، 23٪ از 10 میلیون وب سایت برتر، پشتیبانی می شود.

از آوریل 2020 توسط Google Chrome (از جمله Chrome for Android و Microsoft Edge که بر اساس آن ساخته شده است)[5] و از می 2021 توسط Mozilla Firefox پشتیبانی می‌شود.

HTTP/3 اولین ارتقاء عمده پروتکل انتقال فرامتن از زمان تایید HTTP/2 در سال 2015 خواهد بود.