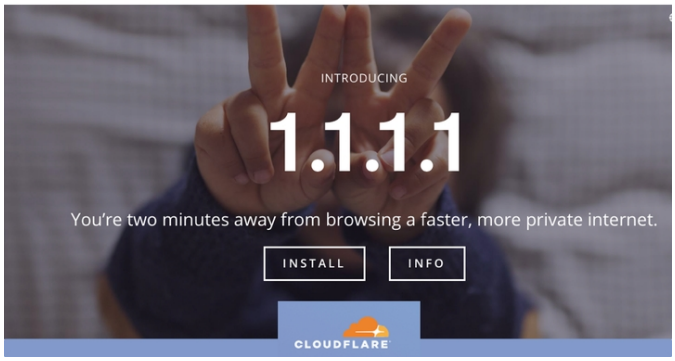
Written by Alice Marshall
05 April 2018

As customers look to improve their internet experience Cloudflare presents the 1.1.1.1 Domain Name System (DNS) resolver, a freely available service promising to both secure and accelerate online traffic.



For the unfamiliar, a DNS resolver "resolves" (or connects) IP addresses to domain names. Most consumers get DNS resolutions as part of the standard ISP package. The process is surprisngly lengthy, with an average DNS lookup taking around 32 milliseconds. As such some companies offer an own fast DNS service, such as Cisco OpenDNS and Google DNS.

Developed in partnership with APNIC (Asia Pacific Network Information Centre) Labs, the 1.1.1.1 service is superior because it runs on the Cloudflare global anycast network powered by 149 datacentres across the world. Thus, the company claims, the DNS is faster than any alternative, including 8.8.8.8 from Google.

Further boosting performance is Knot Resolver-- an open-source resolver implementation offering aggressive caching and "negative caching" to speed up the delivery of IP addresses with less errors.

On the security side, the Cloudflare DNS integrates a pair of protocols to the standard DNS resolution-- DNS-over-TLS (Transport Layer Security) and DNS over HTTPS. Both transmit DNS queries over an encrypted data link, whereas regular DNS is unencrypted, allowing anyone to monitor a network connection.

"The DNS resolver, 1.1.1.1, is also supporting privacy-enabled TLS queries on port 853 (DNS over TLS), so we can keep queries hidden from snooping networks," the company says. "Furthermore, by offering the experimental DoH (DNS over HTTPS) protocol, we improve both privacy and a number of future speedups for end users, as browsers and other applications can now mix DNS and HTTPS traffic into one single connection."

Cloudflare also commits to never use DNS browsing data to target adds, as well as not recording IP addresses and wiping all DNS logs within 24 hours. To ensure this actually takes place the company has KPMG annually audit the code before publishing a confirmation report.

The curious can try out the 1.1.1.1 DNS by following the instructions in the link below.

Go 1.1.1.1