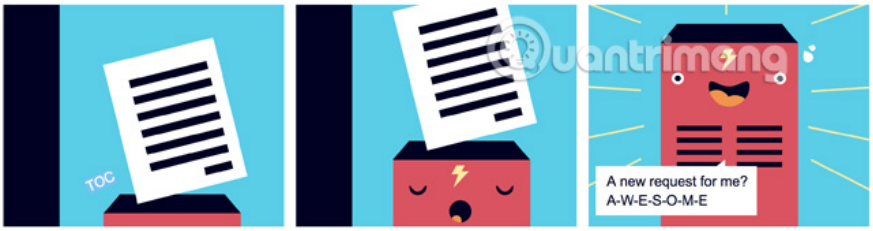
Introducing DNS Resolver 1.1.1.1

Yesterday (1/4/2018) Cloudfare launched DNS Resolver 1.1.1.1, a DNS service that helps speed up the Internet. This service was developed to overcome the Internet platform by building a faster, safer, and more secure DNS resolver service.

Yesterday (1/4/2018) Cloudfare launched DNS Resolver 1.1.1.1, a DNS service that helps speed up the Internet. This service was developed to overcome the Internet platform by building a faster, safer, and more secure DNS resolver service. Anyone can use the DNS resolver 1.1.1.1 service, the first Cloudflare service for consumers. Cloudflare uses very memorable IPv4 addresses for resolver 1.1.1.1 and 1.0.0.1 provided by APNIC.

1. How to change DNS Quad9 to block malicious domain
2. The best, fastest DNS list of Google, VNPT, FPT, Viettel, Singapore

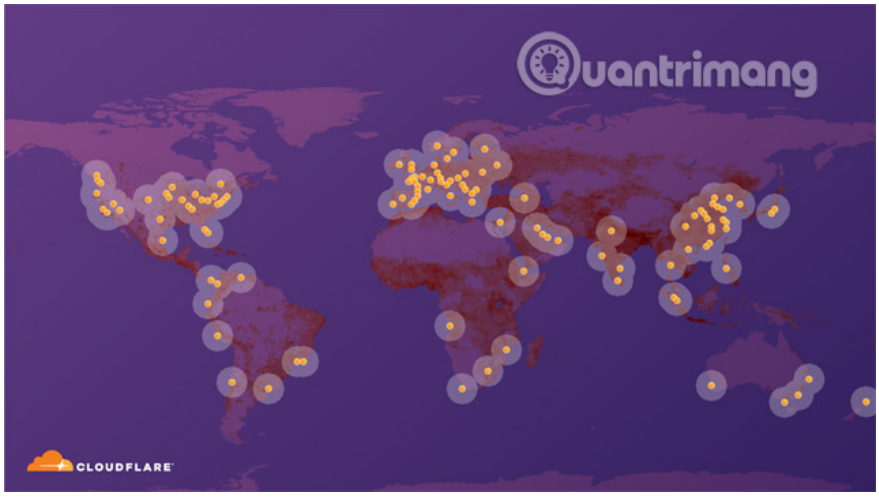
Role of resolver in DNS



When resolving a domain name, a query will move from the terminal system (ie, a web browser) to a recursive DNS service. If the DNS record is not in the local cache of the service, recursion will query the trusted DNS hierarchy to find the IP address information you are looking for. Recursion is a part of DNS 1.1.1.1, so it needs to be fast and secure.

The goal of DNS Resolver service 1.1.1.1

Cloudflare's goal is to operate the world's fastest public resolver, while enhancing the privacy protection standard for users. To speed up the Internet, the company has built data centers around the globe to reduce the distance (ie latency) from users to content.



In March alone, Cloudflare activated 31 new data centers across the globe (Istanbul, Reykjavík, Riyadh, Macau, Baghdad, Houston, Indianapolis, Montgomery, Pittsburgh, Sacramento, Mexico City, Tel Aviv, Durban, Port Louis, Cebu City, Edinburgh, Riga, Tallinn, Vilnius, Calgary, Saskatoon, Winnipeg, Jacksonville, Memphis, Tallahassee, Bogotá, Luxembourg City, Chi?in?u) and like every other city in this network, new sites run DNS Resolver, 1.1 .1.1 on the first day.

This fast and extensive distribution network is built to serve any protocol and currently Cloudflare is the fastest, most reliable DNS provider on the Internet. In addition, the company also provides Anycast service for two of the thirty root nameservers (root domain resolution service) and provides recursive DNS services for users. Recursion can take advantage of trusted servers (authoritative server) in the same location to make searching all domains faster.

Although DNSSEC ensures data integrity between trusted resolver and server, it does not protect the privacy of the last mile for users. However, the DNS Resolver 1.1.1.1, supports new DNS security standards - DNS-over-TLS and DNS-over-HTTPS, provides last mile encryption to keep users' DNS queries private and not fake.

Resolver privacy protection

Previously, recursion sent the full domain name to any intermediary to find its way to trusted root or DNS DNS. This means that if you access the website quantrimang.com, the root server and the .com server will be queried with the full domain name (ie, quantrimang and com part), even though the original servers only need redirection. converted to .com (independent of the full domain). Easy access to all of this personal browsing information via DNS is a concern for many people. This problem is solved by some software packages of resolver, although not everyone knows these solutions.

DNS Resolver service, 1.1.1.1, provides all DNS protection mechanisms defined and proposed to use between resolver resolver and recursive resolver. Stub resolver is a component of the operating system, "talking" with recursive resolver. By using only Query Name Minimization DNS identified in RFC7816, the DNS resolver 1.1.1.1 makes the leakage of information to less intermediate DNS servers, such as root and TLDs. That means the DNS resolver 1.1.1.1, just send enough names to the resolver to know the next question.

DNS resolver, 1.1.1.1 also supports private TLS queries on port 853 (DNS over TLS), so it can keep hidden queries from leaking networks. In addition, by providing DNS over HTTPS, this service has improved both privacy and speed in the future for users, as browsers and other applications can connect to it. Combine DNS and

HTTPS traffic into a single connection.

With the use of negative cache (Negative cache is the cache of "negative" responses, meaning bugs) in DNS is increasing, as described in RFC8198, Cloudflare can continue to reduce the load on the system. Global DNS. This technique first uses the negative cache for the available resolver to keep the negative information (or nonexistent) for a period of time. For DNSSE signed zones and from memory NSEC records, the resolver can find the requested name does not exist without any further queries. Therefore, if you type wwwwwww dot and write something, then wwww dot and write something, the second query is answered 'no' very quickly (NXDOMAIN in the DNS world). Negative cache only works with DNSSEC signed zones, including root and 1400 of 1544 TLD signed yesterday.

The company uses DNSSEC authentication because this allows to ensure that the answers are correct, with low signature verification costs and savings. Cloudflare always wants users to trust the answers they receive and perform all possible tests to avoid bad answers for customers.

However, errors in DNSSEC configuration caused by DNS operators can cause domains to be misconfigured. To fix this problem, Cloudflare will configure the ' **Negative Trust Anchor** ' on domains with identified and corrected DNSSEC errors, and delete them when the operator modifies the configuration. This limits the impact of corrupted DNSSEC domains by disabling temporary DNSSEC authentication for a specific misconfigured domain, restoring access for the end customer.

How is DNS resolver 1.1.1.1 service formed?

Initially, Cloudflare thought about building their own resolver, but the idea was later rejected because of the complexity and considerations regarding go-to-market (GTM) strategy - bringing value. unique to customers and gaining competitive advantage. After they considered all the open source resolver on the market, from this long list, they narrowed down the choice to two or three options that fit most of the project goals. Finally, the company decided to build the system on Knot Resolver of CZ NIC, this resolver was released two and a half years ago. With the selection of Knot Resolver, the variety of software is also increased. The highlight is that it has more core features than Cloudflare wants. With modular architecture similar to OpenResty, Knot Resolver is being used and developed.

Interesting things make Cloudflare's resolver different

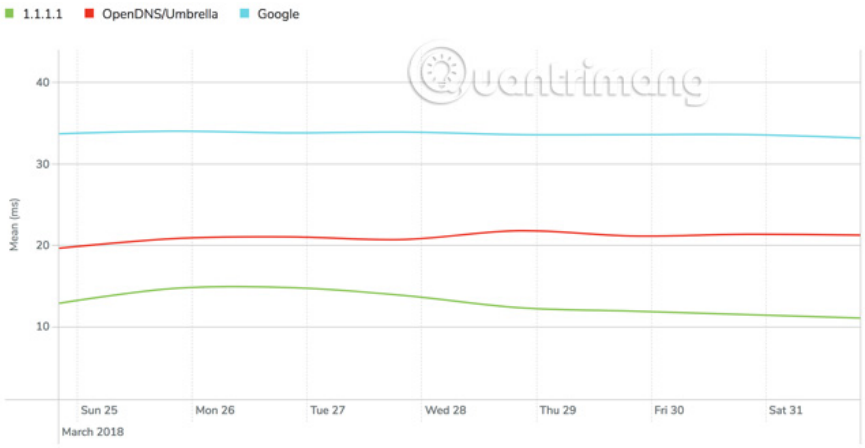
The advanced features of the DNS resolver service 1.1.1.1 are:

1. Query Minimization RFC7816
2. DNS-over-TLS (Transport Layer Security) RFC7858
3. DoH DNS-over-HTTPS protocol
4. The answer 'negative' RFC8198

Note, the main developer of Knot Resolver, Marek Vavruša worked for the Cloudflare DNS team for more than two years.

How to make the resolver faster

There are many factors that affect the speed of the resolver. First and foremost is: Can it answer from cache? In case it is possible, the time to respond is only "round-trip" time for a package from client to resolver.



When the resolver needs an authority answer, things get a little more complicated because the resolver needs to monitor the DNS hierarchy to resolve the domain, which means it has to talk to many trusted servers. head from the root server. For example, resolver in Buenos Aires, Argentina will take more time to monitor DNS hierarchy than resolver in Frankfurt, Germany because it is close to reliable servers. To solve this problem, we must pre-populate the cache, in addition to the frequency band for common names, meaning that when a query is actually entered, the responses can be retrieved from the cache. Much faster.

One problem with extended networks is that the cache access rate is inversely proportional to the number of nodes configured in each data center. If there is only one node in the nearest datacenter, you can be sure that when you ask the same query twice, you will get a cached answer a second time. However, because there are hundreds of nodes in each data center, users can receive unresolved responses, delaying each request. A common solution is to put the cache load balancer in front of all resolver, but this way will become a single-point-of-failure for the whole system and Cloudflare. do not do it. Instead of relying on a centralized cache, the DNS resolver 1.1.1.1, uses an advanced distributed cache.

Data policy

Cloudflare insists that it will never store a customer IP address and only use the query name to improve the performance of DNS resolver (such as filling in all memory based on common domains in an area and / or after blurring).

Cloudflare will never store any information in the log to determine the end user and all collected records will be deleted within 24 hours. The airline insists it will continue to follow the privacy policy and ensure that no user data is sold to advertisers or used to target consumers.

How to set up DNS resolver 1.1.1.1

See Cloudflare's new 1.1.1.1 DNS service article, more secure, surf the web faster to learn how to set up this service.

Something about the address of the DNS resolver

Cloudflare worked with APNIC and used IPv4 1.0.0.1 address and 1.1.1.1 (everyone agrees this address is easy to remember). Without years of research and experimentation, these addresses will not be put into production.

For IPv6, the company chose 2606: 4700: 4700 :: 1111 and 2606: 4700: 4700 :: 1001 for this service. As you all know, it is not easy to get IPv6 addresses, however, they chose an address that uses only numbers.

But why use an easy-to-remember address? What's special about this public resolver? The first thing to do in this process is to put these numbers in. They need a number that is entered into any computer or connected to the user device used to find the resolver service.

Anyone on the Internet can use this public resolver and you can see how to do it by visiting https://1.1.1.1/ and clicking **GET STARTED** .

Why are you announcing the release of DNS resolver in April?

For most people in the world, Sunday is April 1, 2018 (In America in the form of a date written will be the month before the date after 4/1/2018). Do you see 4 and 1? That's why Cloudflare announced on this day, number four (1.1.1.1).

See more:

1. Fake IP, IP change software, best anonymous surfing
2. Instructions for deleting DNS on Windows 7 / 8.1 / 10
3. 3 "legitimate" reasons to change DNS Server