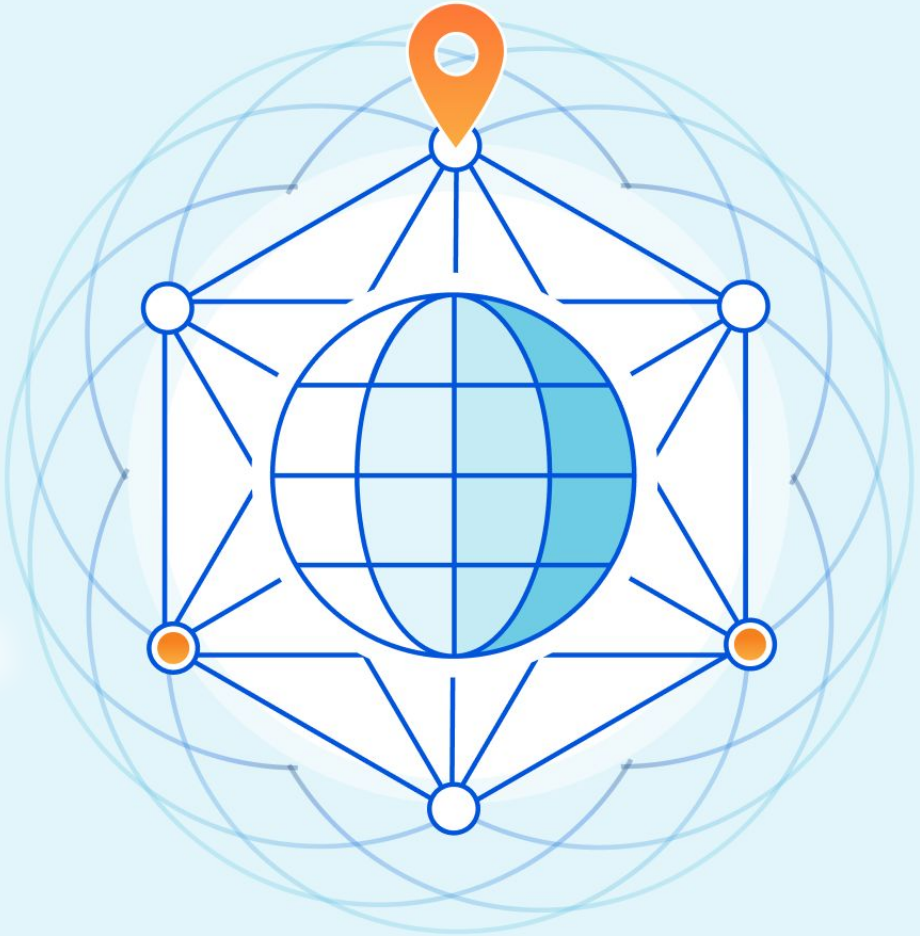
CLOUDFLARE



Exploring

DNS Essentials

Carlos Rodrigues
Systems Engineer @ Cloudflare

About

Cloudflare leverages its large global network to provide security, reliability, and speed to a big part of the Internet. It's best known for content distribution, attack protection, and the serverless Workers* platform.

335 cities in **125 countries**

13,000 interconnects with other networks

348 terabits/s of network capacity

71 million HTTP requests per second → **6.1 trillion** per day

44 million DNS queries per second → **3.8 trillion** per day

CLOUDFLARE

* *workers.cloudflare.com*

When you browse to **www.example.com**, how does your computer figure out which IP address it should connect to?

CLOUDFLARE

When Dinosaurs Roamed the Earth

«The Stanford Research Institute [...] maintained a text file named **HOSTS.TXT** that mapped host names to the numerical addresses of computers on the ARPANET.

[...] **Computers**, including their hostnames and addresses, **were added** to the primary file by contacting the SRI Network Information Center [...] **via telephone during business hours**.»

— from Wikipedia (DNS)

```
HOST : 46.0.0.12 : UCBCALDER : VAX-11/750 : UNIX : TCP/TELNET,TCP/FTP,UDP :
HOST : 46.0.0.13 : UCBDALI : VAX-11/750 : UNIX : TCP/TELNET,TCP/FTP,UDP :
HOST : 46.0.0.14 : UCBMATISSE : VAX-11/750 : UNIX : TCP/TELNET,TCP/FTP,UDP :
HOST : 46.0.0.15 : UCBMEDEA : VAX-11/750 : UNIX : TCP/TELNET,TCP/FTP,UDP :
HOST : 46.0.0.19 : UCBINGRES : VAX-11/780 : UNIX : TCP/TELNET,TCP/FTP,UDP :
HOST : 47.0.32.3 : SAC-VAX,SRI-SPUD,SPUD : VAX-11/780 : UNIX : TCP/TELNET,TCP/FTP,TCP/SMTP,UDP,…
HOST : 48.3.1.41 : NDRE1,NDRE : LSI-11/23 : FUZZ : TCP/TELNET,TCP/SMTP,TCP/FTP,UDP :
```

— excerpt from HOSTS.TXT, May 1983

CLOUDFLARE

When Dinosaurs Roamed the Earth

Maintaining a **centralized** hosts database obviously **didn't scale**, and DNS was invented in **1983** as a **distributed** solution to that problem. The first RFCs describing it date from November of that year:

- RFC 882 — "*Domain names: Concepts and facilities*"
- RFC 883 — "*Domain names: Implementation specification*"

Although it's been 40 years, you still have a descendant of HOSTS.TXT on your computer, in the form of **/etc/hosts** in Unix-like operating systems and **C:\Windows\System32\drivers\etc\hosts** on Windows.

```
127.0.0.1 localhost
255.255.255.255 broadcasthost
::1 localhost
127.0.0.1 kubernetes.docker.internal
```

— excerpt from the /etc/hosts file on my laptop, November 2023

CLOUDFLARE

The Domain Name System (DNS)

The DNS is a **distributed system** both **technically** (made up of many different servers around the globe) and **administratively** (separate organizations managing different parts of it independently of each other).

In the DNS, fully-qualified names are made of **domain components** glued together with dots. The leftmost component is the **host name**, and the rest is the **domain name** (*i.e.* the path to the host).

www.example.com.

There's always an **invisible dot** at the end. The nameless domain to its right is called the **root**.

CLOUDFLARE

The Domain Name System (DNS)

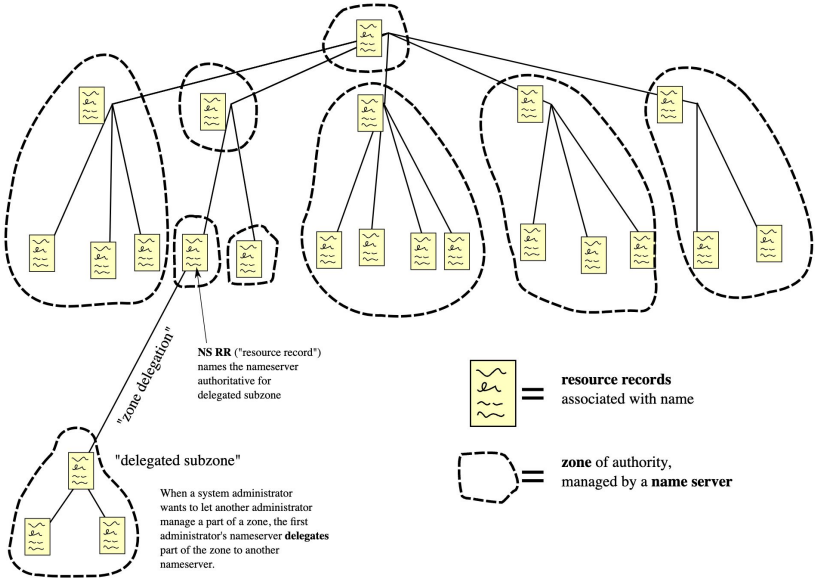
The DNS is a tree and each branch is called a **zone**.

- "**.**" (the root) is a zone
- "**.com**" is a zone under the root
- "**.example.com**" is a zone under ".com"

www.example.com is not a zone, because "www" is just the name of a particular host. But **example.com** can be both a zone *and* the name of a host.

Confused?

You can call zones "**domains**" if that makes it easier.



CLOUDFLARE

Discovering Which DNS Servers to Use

To avoid a **chicken-and-egg** problem, your system needs to be bootstrapped with the **IP address** of **at least one** DNS server… somehow.

In the most common case, your computer **gets an IP address automatically** when it connects to the network and, along with it, **also gets the IP address(es) of one or more DNS servers**.

You can also configure DNS servers manually in your operating system, in which case those are used instead — *e.g.* using **1.1.1.1** instead of your ISP's servers for added performance, privacy, etc.

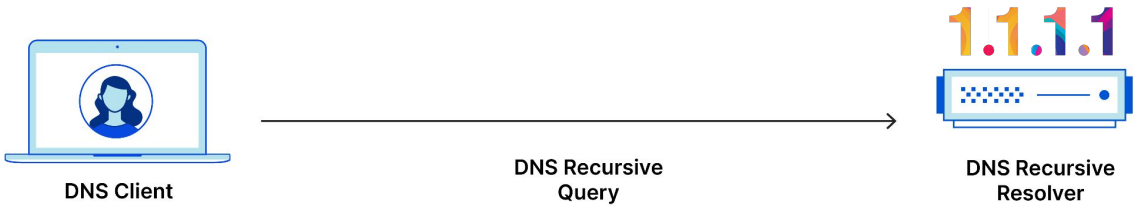
Some applications (*i.e.* web browsers) also have set of DNS servers pre-configured, which they may use instead of the servers configured in the operating system.

CLOUDFLARE

The Different Flavors of DNS Servers

The DNS servers your operating system uses to look up names are called **recursive resolvers**.

Why "recursive" in the name? We'll get to that soon...



In turn, **recursive resolvers** reach out to third-party DNS servers in order to answer client queries. These other DNS servers are called **nameservers** or, more often, **authoritative nameservers**.

CLOUDFLARE

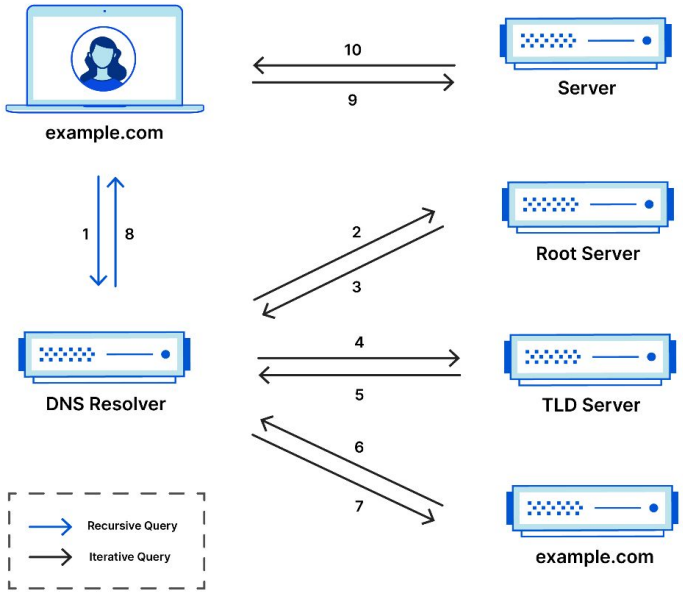
Looking up Names in DNS

Querying DNS means going down from the root until the **authoritative nameserver** holding the answer we want is found.

The **recursive resolver** does this on the client's behalf. It then **caches** the answer(s) and any intermediate steps to speed up subsequent queries.

How long things stay in cache is defined by the **time-to-live** (TTL) attached to each DNS record.

More on caching later…



Nothing stops you from running your own recursive resolver at home, if you want.

CLOUDFLARE

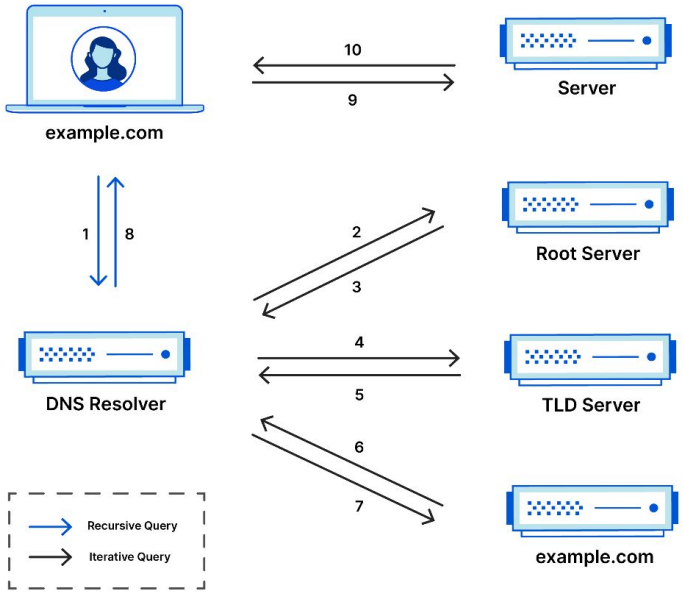
Looking up Names in DNS

DNS queries must specify the **type** of answer they're looking for. These are some common query types:

- **A** — IPv4 address for a name
- **AAAA** — IPv6 address for a name
- **NS** — names of the nameservers for the domain
- **MX** — names of the email servers for the domain
- **TXT** — text associated with the name (*e.g.* email policies)
- **PTR** — name for an IP address (reverse lookup)

DNS responses often contain additional (related) records of types that don't match the requested type (*e.g.* CNAME, DNAME, SOA).

The most important of these extra answers are the **glue records**.



CLOUDFLARE

The Transport Protocols Used in DNS

DNS mostly* still uses **unencrypted UDP**. The query is a single UDP packet, and the response is also a single UDP packet. It's fast, but has some limitations.

When the **response is too big** to fit a single UDP packet (uncommon), the server will return a truncated response. The client must query again using **unencrypted TCP** to get a full response.

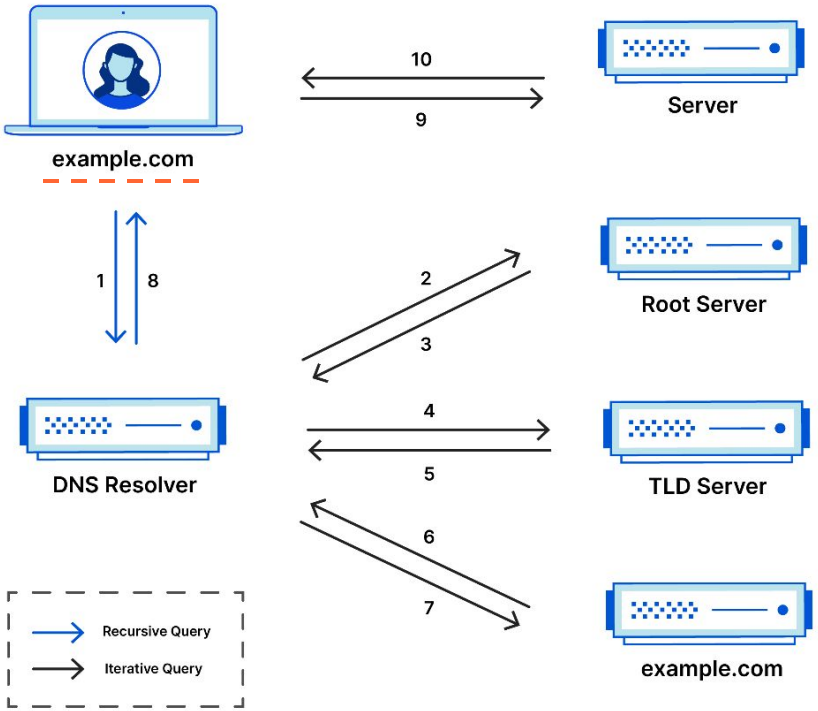
DNS-over-TLS (**DoT**) and DNS-over-HTTPS (**DoH**) provide encryption. DoT and DoH have their own specific advantages and disadvantages. Which one is better depends on the situation.

For traffic between **recursive resolvers** and **authoritative nameservers** there is no standard for encrypted communications (yet). Unencrypted **UDP** and **TCP** are the **only options****.

CLOUDFLARE

** More than **80%** of the time.*
*** DNSSEC is used to prevent tampering by signing responses (but adoption is still lacking).*

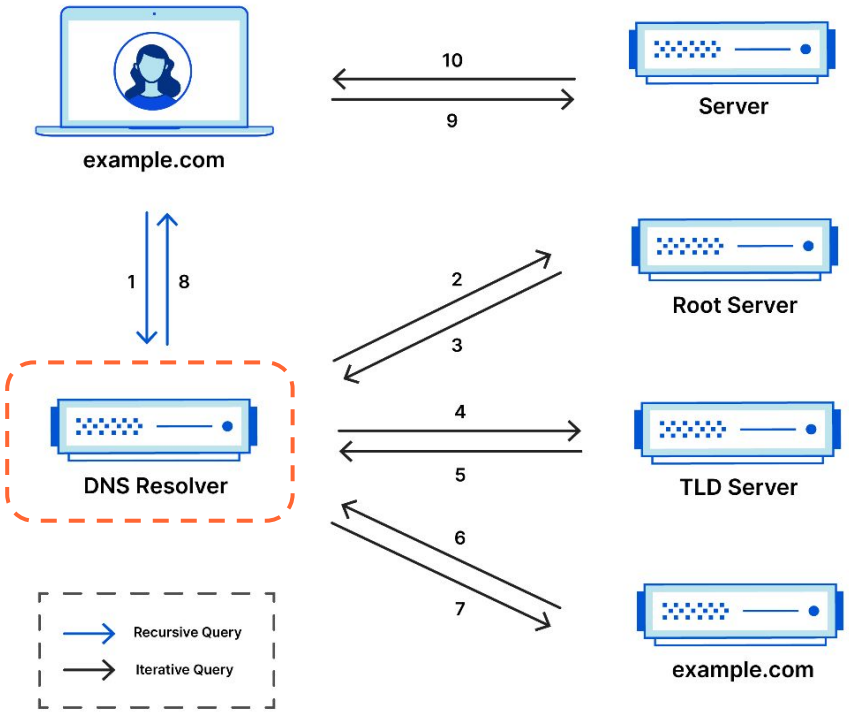
The Recursive Lookup Process



***TLD** means a top-level domain.*

CLOUDFLARE

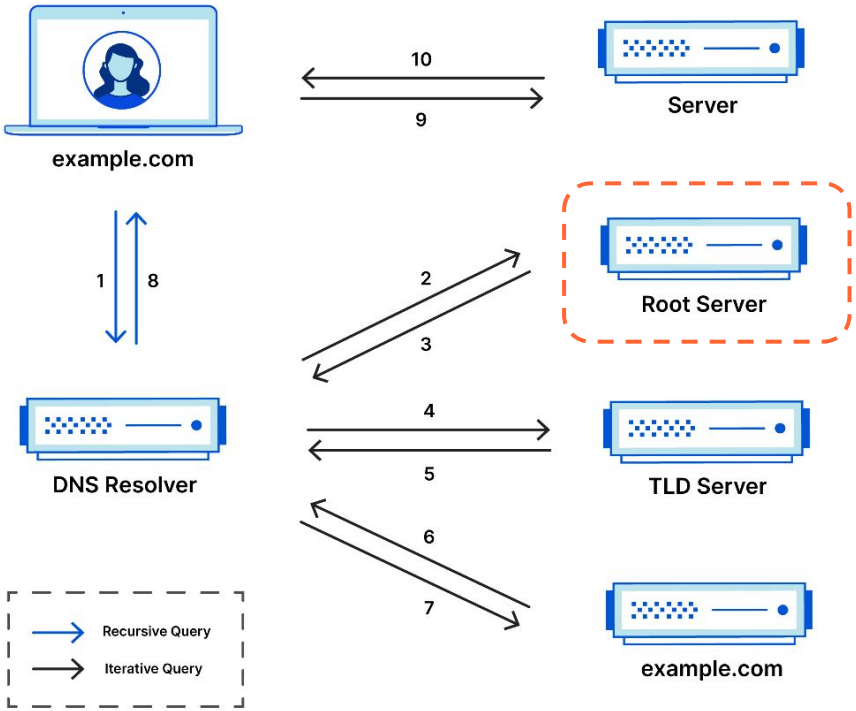
The Recursive Lookup Process



CLOUDFLARE

TLD means a top-level domain.

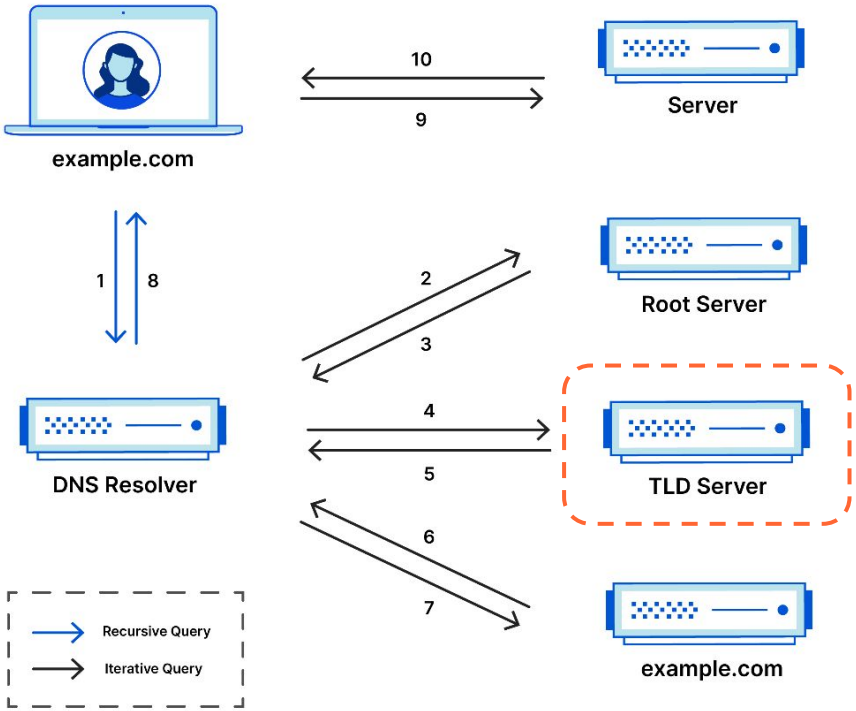
The Recursive Lookup Process



***TLD** means a top-level domain.*

CLOUDFLARE

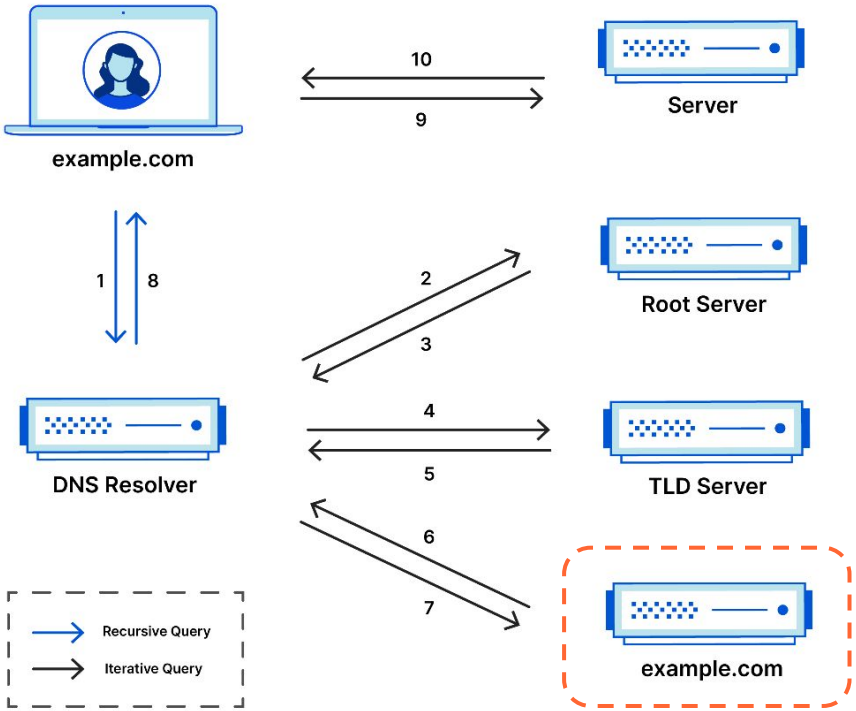
The Recursive Lookup Process



***TLD** means a top-level domain.*

CLOUDFLARE

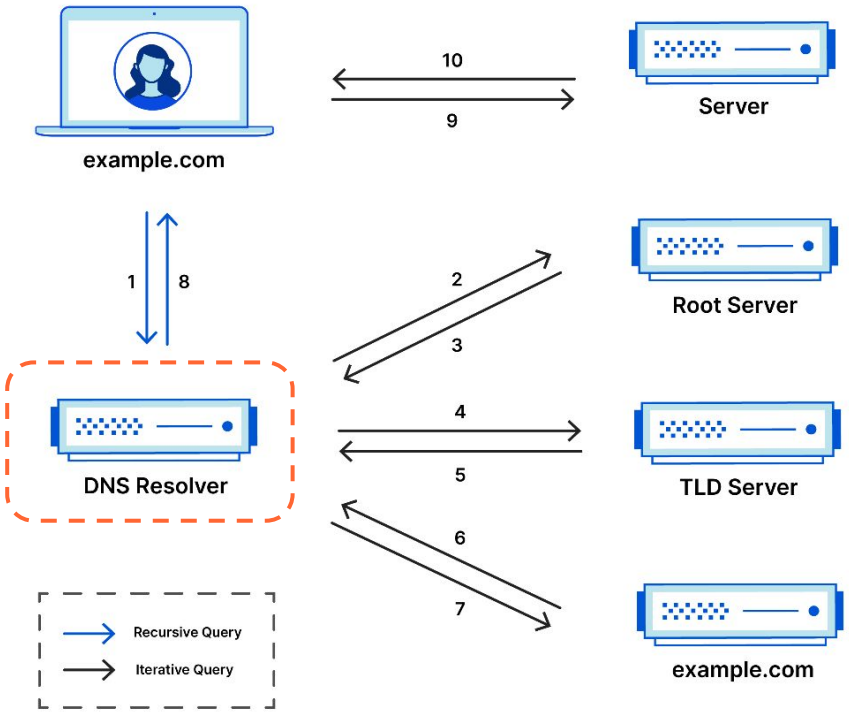
The Recursive Lookup Process



***TLD** means a top-level domain.*

CLOUDFLARE

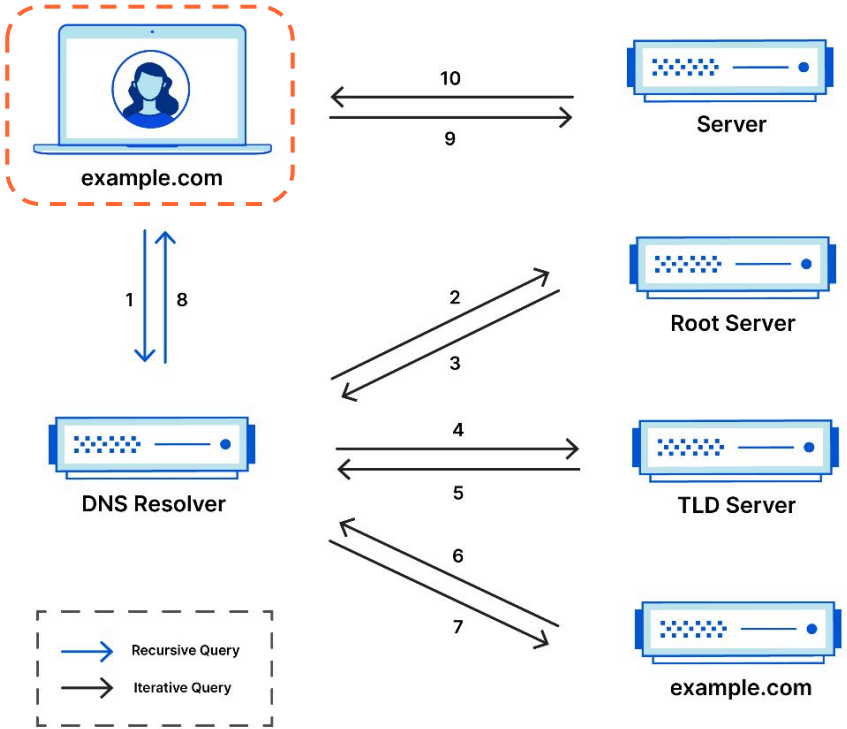
The Recursive Lookup Process



CLOUDFLARE

TLD means a top-level domain.

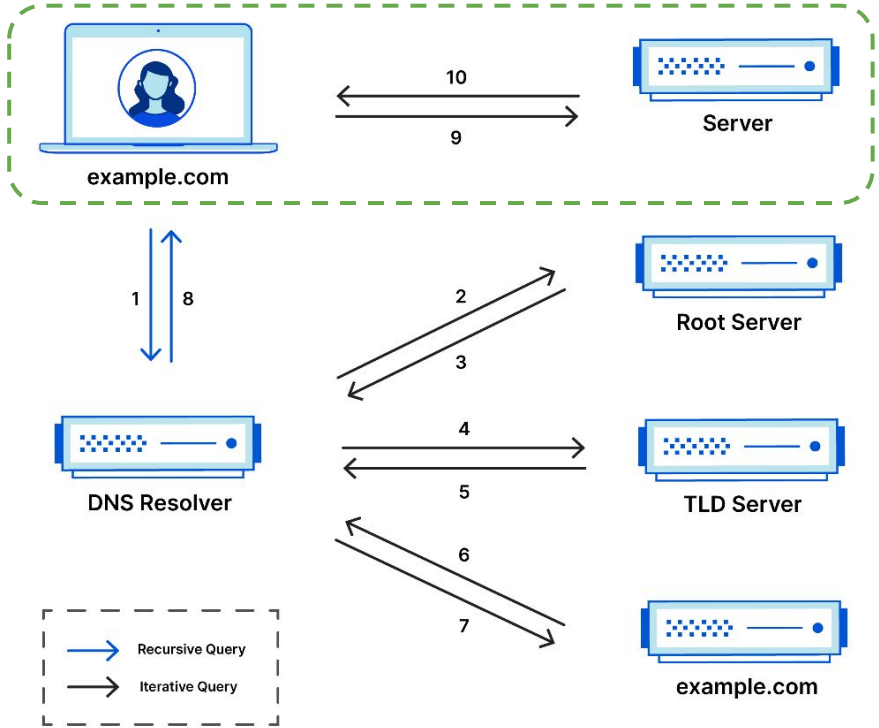
The Recursive Lookup Process



***TLD** means a top-level domain.*

CLOUDFLARE

The Recursive Lookup Process



***TLD** means a top-level domain.*

f.root-servers.net

```
$ dig +nord A www.cloudflare.com @192.5.5.241
```

1

```
; <<>> DiG 9.10.6 <<>> A +nord www.cloudflare.com @192.5.5.241
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35635
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.cloudflare.com.            IN      A

;; AUTHORITY SECTION:
com.                    172800  IN      NS      i.gtld-servers.net.
[...]

;; ADDITIONAL SECTION:
i.gtld-servers.net.     172800  IN      A       192.43.172.30
i.gtld-servers.net.     172800  IN      AAAA    2001:503:39c1::30
[...]

;; Query time: 22 msec
[...]
```

i.gtld-servers.net

```
$ dig +nord A www.cloudflare.com @192.43.172.30
```

2

```
; <<>> DiG 9.10.6 <<>> A +nord www.cloudflare.com @192.43.172.30
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56977
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 21

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cloudflare.com.            IN      A

;; AUTHORITY SECTION:
cloudflare.com.         172800  IN      NS      ns3.cloudflare.com.
[...]

;; ADDITIONAL SECTION:
ns3.cloudflare.com.     172800  IN      A       162.159.0.33
ns3.cloudflare.com.     172800  IN      A       162.159.7.226
ns3.cloudflare.com.     172800  IN      AAAA    2400:cb00:2049:1::a29f:21
ns3.cloudflare.com.     172800  IN      AAAA    2400:cb00:2049:1::a29f:7e2
[...]

;; Query time: 147 msec
[...]
```

ns3.cloudflare.com

```
$ dig +nord A www.cloudflare.com @162.159.0.33

; <<>> DiG 9.10.6 <<>> A +nord www.cloudflare.com @162.159.0.33
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51039
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.cloudflare.com.            IN      A

;; ANSWER SECTION:
www.cloudflare.com.  300    IN      A       104.16.123.96
www.cloudflare.com.  300    IN      A       104.16.124.96

;; Query time: 114 msec
[...]
```

time-to-live (TTL)

3

```
$ dig +nord A www.cloudflare.com @162.159.0.33

; <<>> DiG 9.10.6 <<>> A +nord www.cloudflare.com @162.159.0.33
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51039
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.cloudflare.com.            IN      A

;; ANSWER SECTION:
www.cloudflare.com.  300    IN      A       104.16.123.96
www.cloudflare.com.  300    IN      A       104.16.124.96

;; Query time: 114 msec
[...]
```

3

4

```
$ curl --head --resolve www.cloudflare.com:443:104.16.123.96 \
                                https://www.cloudflare.com/cdn-cgi/trace

HTTP/2 200
date: Mon, 10 Mar 2025 16:46:00 GMT
content-type: text/plain
server: cloudflare
cf-ray: 91e449244b77e3b0-LIS
[...]
```

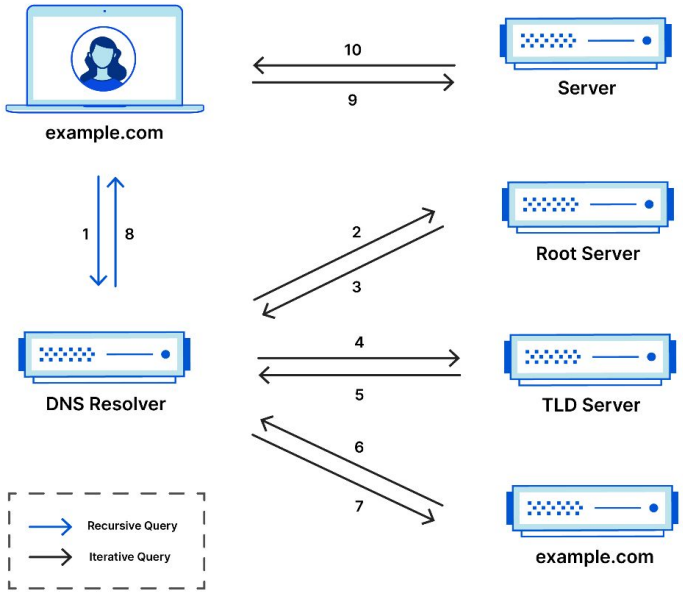
About Caching...

Caching in DNS is present **at every level**, not only in recursive resolvers: your operating system also caches DNS responses, and your home router* does too.

The authoritative nameservers return a **canonical TTL** on each record. Other levels return **adjusted TTLs** by subtracting the amount of time they've had the record in their caches.

This multi-level caching gives the **illusion of propagation**. For a DNS record to be present in a cache, it must have been requested by a client at some point.

When a response comes back empty (*e.g.* an AAAA query for a name that exists but doesn't have an IPv6 address), that can still be cached using the minimum TTL defined in the SOA record.



CLOUDFLARE

* *Clients at home usually get the local router as their DNS resolver, which forwards queries to the recursive resolvers.*

Less Obvious Uses of DNS

It's easy to think of DNS as a static database, but there are plenty of things it can do if you choose DNS server software with fully-programmable backends (*e.g.* PowerDNS*****).

Returning different answers based on the client's location is the most common, but far from the most imaginative.

It's also easy to think of DNS as an Internet-centric service, but there are some less known use-cases out there, such as call routing in 4G/5G mobile networks******.

When your phone does a call using VoLTE ("HD" icon on Android), there are good chances that DNS with ENUM/NAPTR records was involved.

CLOUDFLARE

***** *doc.powerdns.com/authoritative/backends/pipe.html*
****** *wikipedia.org/wiki/telephone_number_mapping*

Learn more about DNS:

cloudflare.com/learning/dns/what-is-dns

radar.cloudflare.com/dns

Experiment with DNS:

messwithdns.net

Thank You

cloudflare.com/careers/jobs

Carlos Rodrigues
crodrigues@cloudflare.com

Coimbra, March 11, 2025