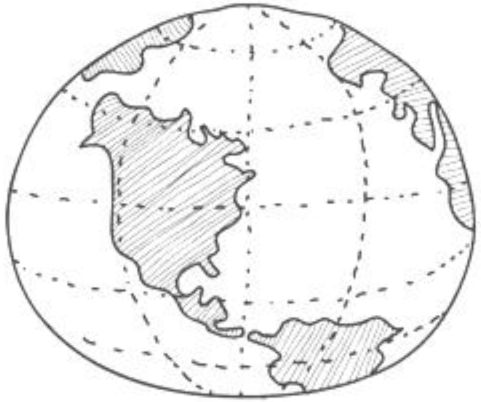
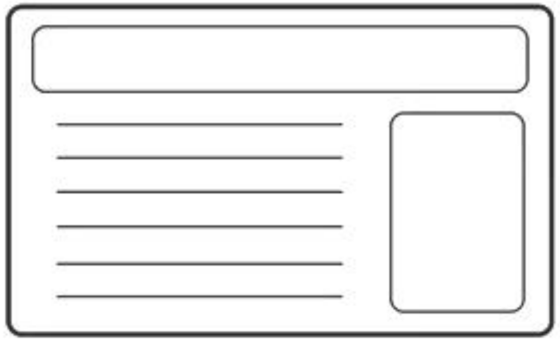
DNS

Dr. Darryl J D’Souza

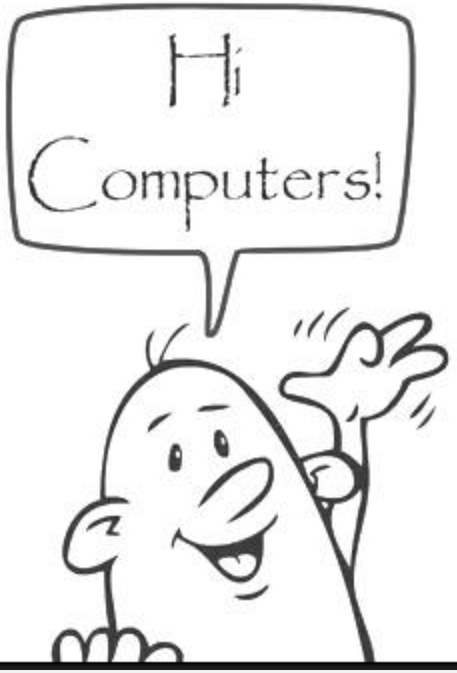


www.facebook.com



192.168.1.2

IP address



DOMAIN NAME SYSTEM

- Every website on the Internet has its own unique address. It’s called an IP address. But unlike the physical street address for a house or building, an IP address consists of a set of numbers strung together and separated by periods. A typical IP address in the IPv4 address space looks like: 123.123.123.2.
- If customers had to memorize the IP addresses of every website they visited, they wouldn’t spend much time on the Internet. Thankfully, we use URLs instead. And behind the scenes, there’s an “address book” of sorts that helps convert these user-friendly URLs and web addresses into the IP addresses that computers understand. It’s called a Domain Name System, or DNS.
- In the simplest form, a DNS is a directory of domain names that align with IP addresses. They bridge the gap between computer language and human language – keeping both servers and people happy.

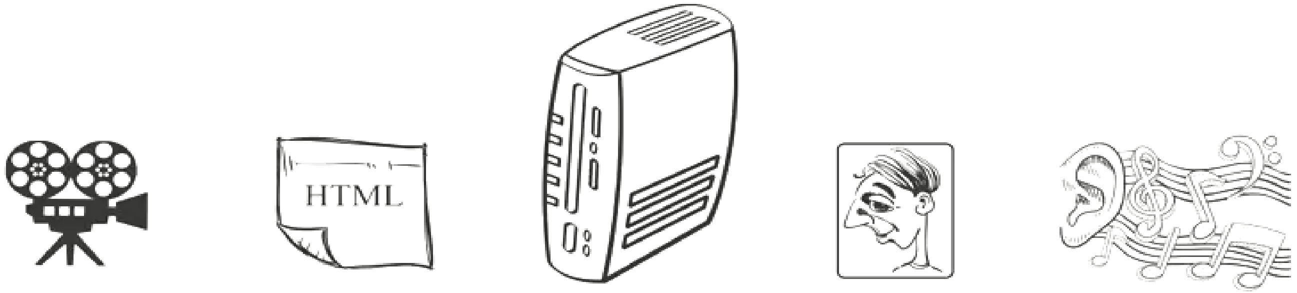
BEYOND WEBSITES, DNS IS USED FOR ALL ONLINE RESOURCES, INCLUDING:

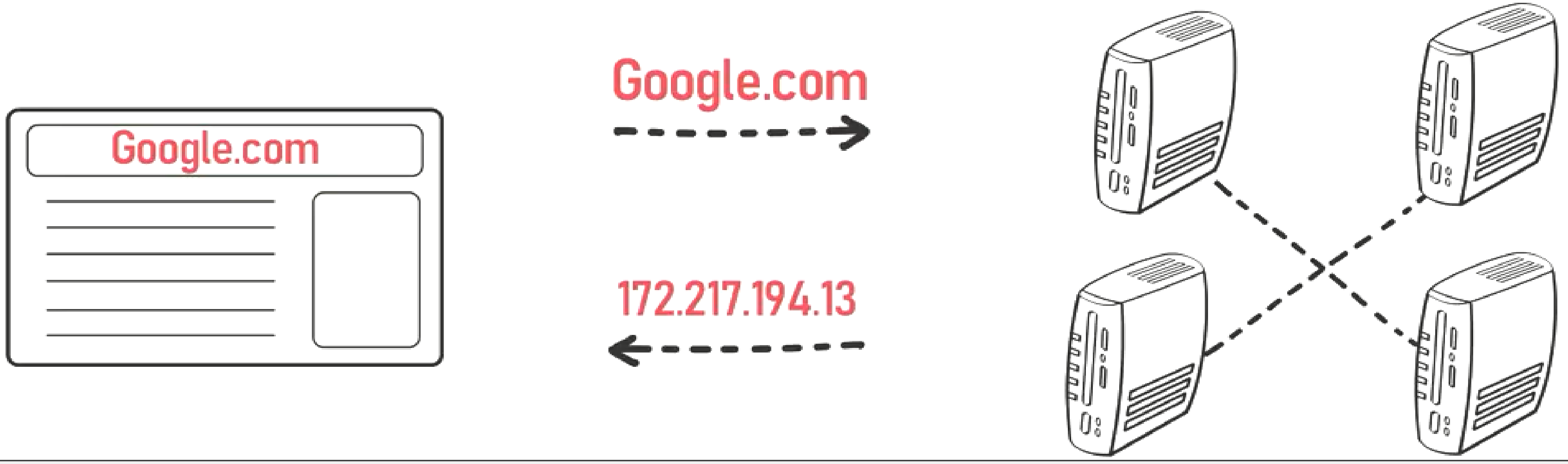
- Email: When sending an email, your email client uses DNS to look up the Mail Exchange (MX) records of the recipient’s domain. This is how it knows where to send the email.
- Video conferencing: Apps like Zoom and Microsoft Teams use DNS to connect users to their servers for video meetings.
- Mobile apps: Apps on your smartphone that connect to the internet use DNS to convert the domain of the web service into an IP address.
- Online gaming: Games played online use DNS to connect players to game servers.
- Internet of things (IoT) devices: Smart home devices use DNS to turn a service’s website name into an IP address so they can use internet services.
- Cloud: Many cloud services rely on DNS to route traffic and perform load balancing across multiple servers or data centers.
- Content delivery networks (CDNs): CDNs use DNS to direct a client request to the nearest server holding the cached content.
- VPNs: VPNs use DNS to resolve the domain names of their servers so that users can connect to them.

DNS is a distributed database, which means that the IP data it holds is spread out across many servers, rather than being stored in one central place. DNS servers are distributed worldwide, managed by different organizations and internet service providers (ISPs.)

How DNS works internally?

DNS Servers




Google.com

Google.com

172.217.194.13

Types of DNS Servers:

- ☞ DNS recursive resolver/DNS resolver
- ☞ Root name server
- ☞ Top Level Domain/TLD name server
- ☞ Authoritative name server

HOW DNS WORKS

1. **User Request**: When you type a web address (URL) into your browser, the browser needs to know the IP address of the server hosting that website.

2. **Query the Local DNS Resolver**: The request first goes to a DNS resolver, which is usually provided by your Internet Service Provider (ISP) or a third-party service like Google Public DNS.

3. **Check Cache**: The resolver checks its cache to see if it already knows the IP address of the requested domain. If the address is cached, it sends the IP address back to your browser, and the process ends here.

4. **Recursive Query to Root Servers**: If the resolver does not have the answer cached, it starts a series of queries. It first contacts one of the root DNS servers, which handle the top of the DNS hierarchy.

5. **Root Server Response**: The root server doesn’t know the IP address but directs the resolver to the appropriate Top-Level Domain (TLD) server (e.g., for .com, .org).

6. **TLD Server Query**: The resolver queries the TLD server, which responds with the authoritative DNS server for the domain.

7. **Authoritative DNS Server Query**: The resolver contacts the authoritative DNS server for the domain, which has the actual IP address of the website.

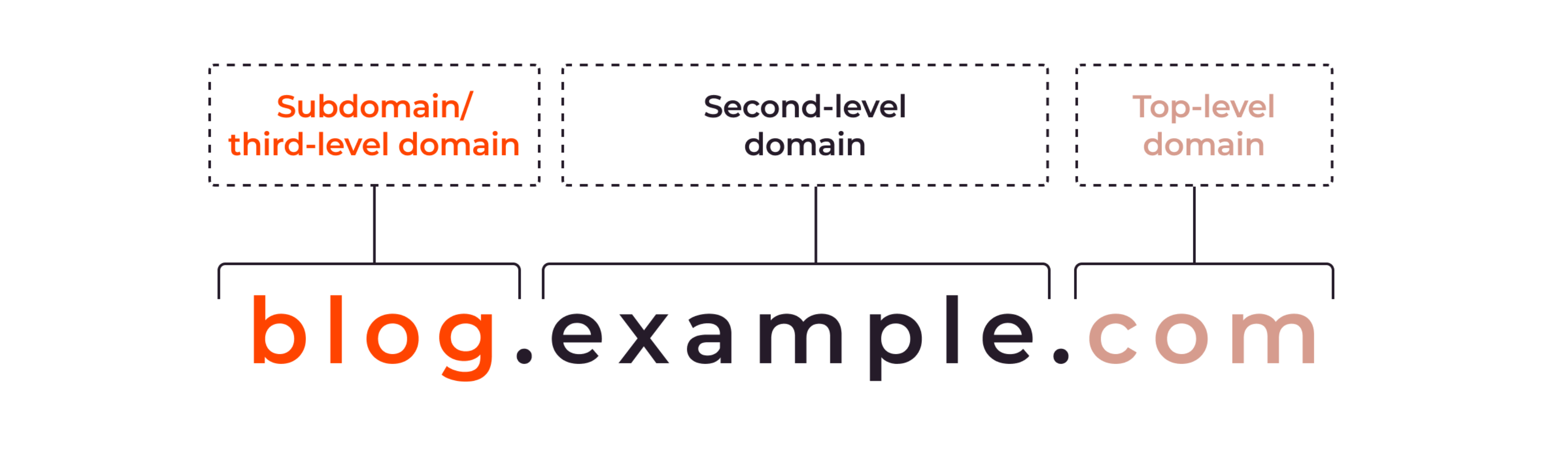
8. **Response to Resolver**: The authoritative DNS server responds with the IP address.

9. **Return to Browser**: The resolver then sends this IP address back to your browser.

10. **Connect to Website**: The browser uses the IP address to connect to the web server hosting the website.

DOMAIN NAME

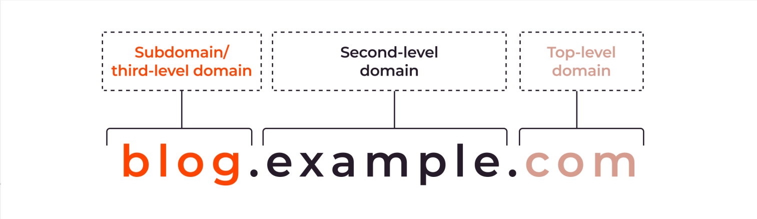
A domain is structured into different parts, separated by dots. Each part has a specific purpose and contributes to the overall hierarchical structure of the domain name. Here's the typical structure of a domain name.



Root domain. The root domain is the base domain name without any subdomains. It is the main part of the domain name that represents the website's identity. For example, in the "www.example.com," "example.com" is the root domain.

DOMAIN NAME

Top-level domains (TLDs): This is the last part of a domain name that appears to the right of the furthest right “dot” symbol. TLDs are essential for categorizing and organizing domain names on the internet. Here are some common examples of TLDs:



Top Level Domains (TLD)	**Description**
.com	Commercial; commonly used for businesses and commercial websites
.org	Organization; often used by non-profit organizations and non-commercial entities
.net	Network; originally intended for network-related websites
Country-code top-Level Domains (ccTLDS)	**Description**
.in	Country code TLD for India
.us	Country code TLD for United States
.uk	Country code TLD for United Kingdom
.ca	Country code TLD for Canada

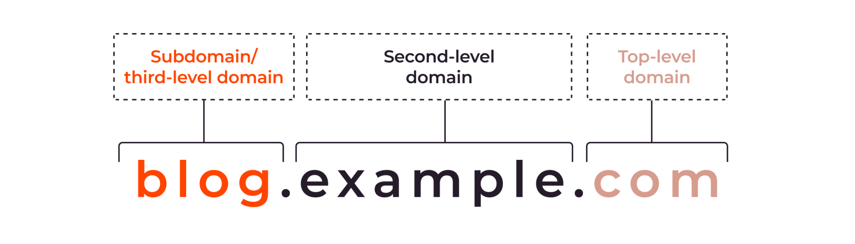
DOMAIN NAME

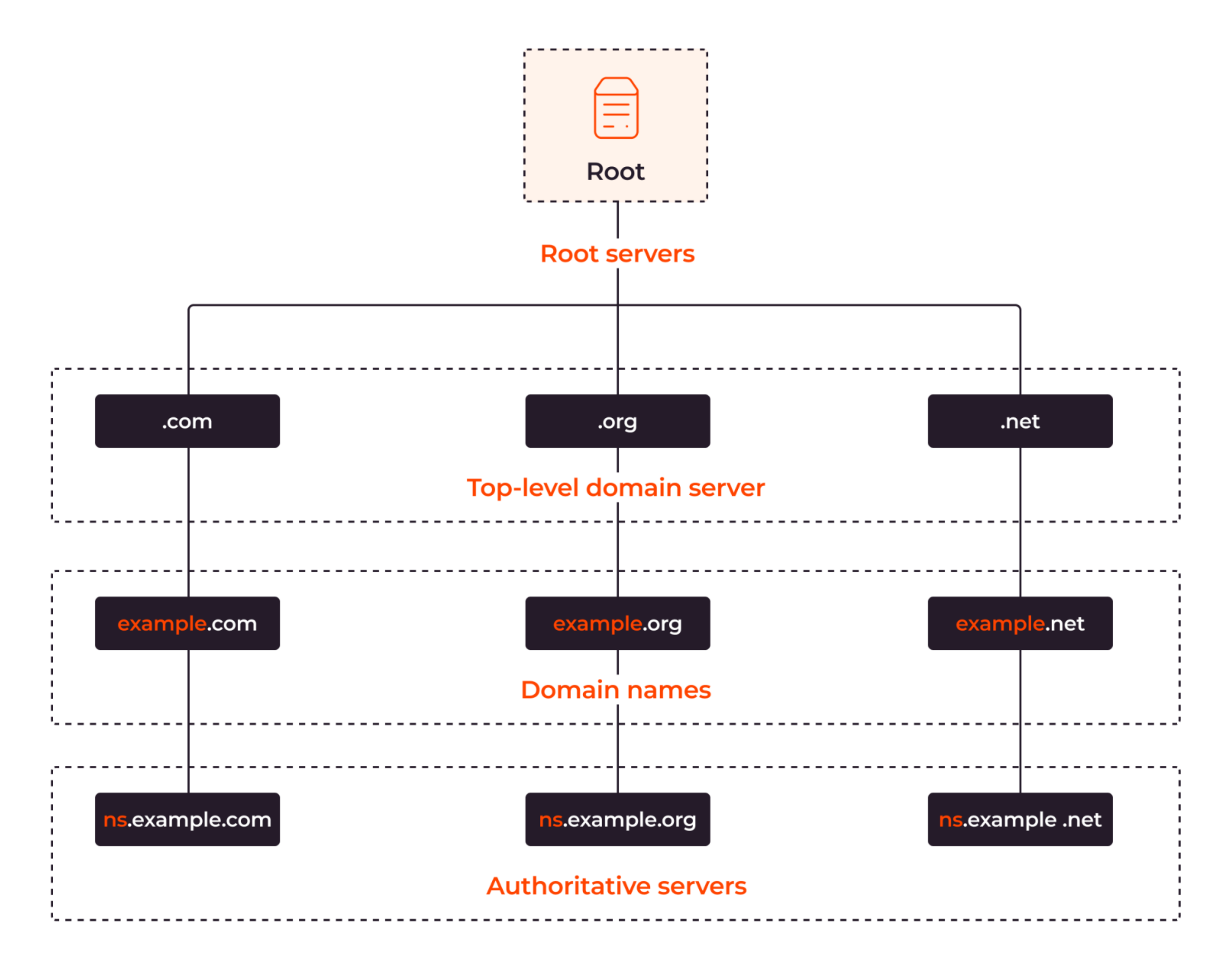
Second-level domain: A second-level domain is a part of the domain name that appears to the left of the top-level domain (TLD) and is located immediately to the left of the rightmost “dot” symbol. For instance, in the domain “gcore.com,” “gcore” is the second-level domain. Second-level domains serve as specific identifiers for websites, organizations, or individuals.

Domain Name	Second-Level Domain
gcore.com	gcore
linux.org	linux
gov.uk	gov

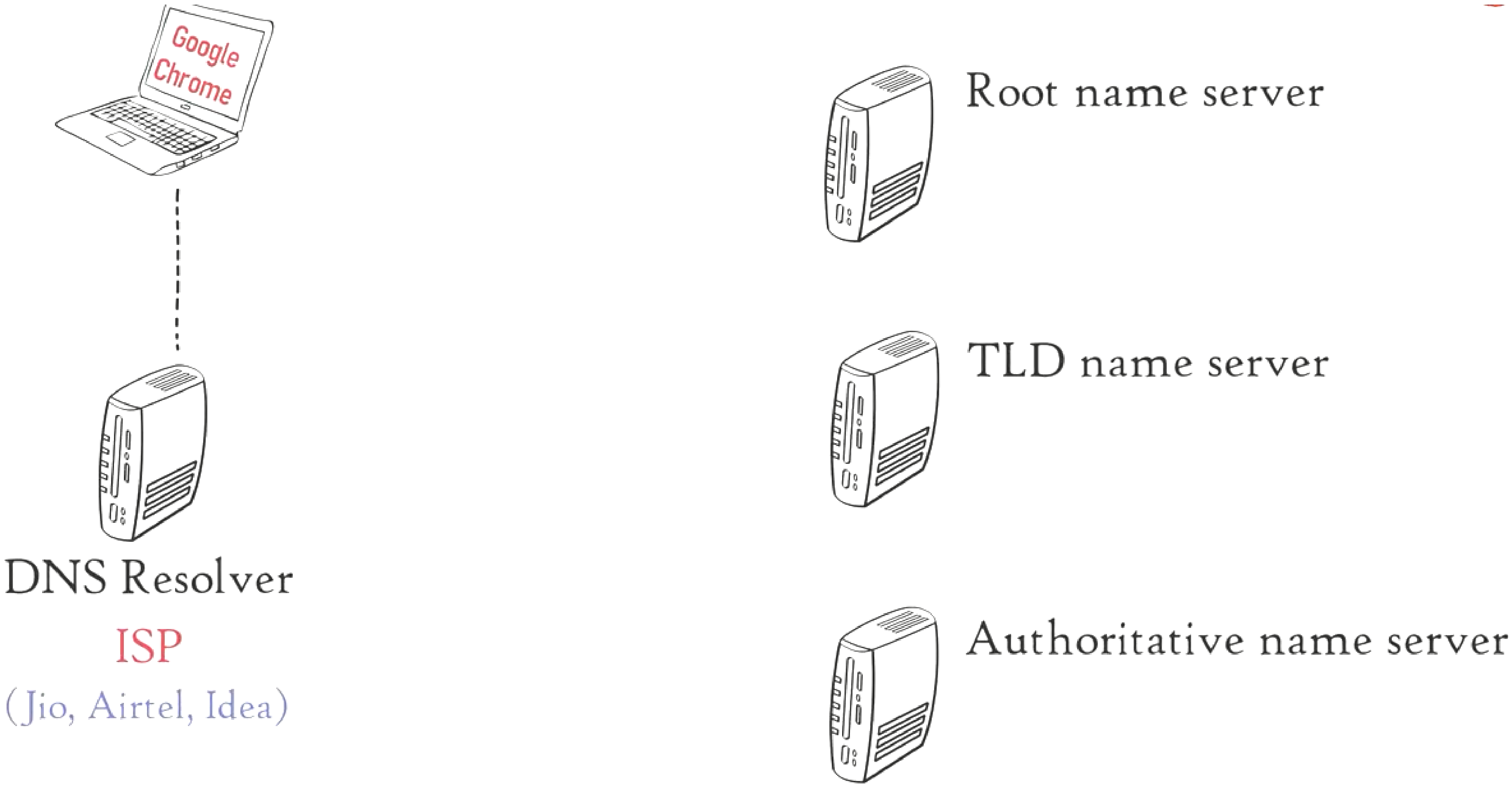
Example URL	Subdomain
www.example.com	www
support.example.net	support
forum.example.org	forum

Subdomain (third-level domain): The subdomain, also known as third-level domain, is located to the left of the main domain and separated from it by a dot. Subdomains help to organize sections of a website with distinct web addresses. They appear before the main domain in a URL, allowing site owners to keep sections connected to the main domain. For instance, in “blog.example.com,” “blog” is the subdomain, “example” is the second-level domain, and “.com” is the TLD.





Fully-qualified domain example



DNS Resolver

ISP

(Jio, Airtel, Idea)

Root name server

TLD name server

Authoritative name server

DNS RESOLVER

A DNS resolver or DNS recursor is a server which executes the process of requesting information from authoritative DNS servers to find the IP addresses for domain names. When you enter a domain name in your web browser or perform an action requiring DNS resolution, the DNS resolver first checks its local cache—a temporary storage mechanism—to see if it recently resolved the same domain name. If the information is not found in the cache, the resolver looks for the corresponding IP address by initiating a DNS lookup.

HOW A DNS RESOLVER WORKS:

Query Initiation:

- When you type a URL into your web browser, your device sends a DNS query to a DNS resolver. This resolver is usually provided by your internet service provider (ISP), but you can also use public resolvers like Google DNS (8.8.8.8) or Cloudflare DNS (1.1.1.1).

Recursive Query Process:

- **Cache Check**: The resolver first checks its local cache to see if it already has the answer to the query. If it does, it returns the cached result, speeding up the process.
- **Root Server Query**: If the resolver doesn't have the answer, it starts by querying one of the root name servers. The root server doesn't have the exact IP address but knows which authoritative servers are responsible for the top-level domain (TLD) of the query (e.g., .com, .org, .in).
- **TLD Server Query**: Next, the resolver queries the appropriate TLD server. For instance, if the domain is example.com, it will query the .com TLD servers.
- **Authoritative Server Query**: The TLD server points the resolver to the authoritative name server that holds the actual IP address for www.example.com.
- **Final Answer**: The resolver then queries the authoritative server, retrieves the IP address, and sends it back to the client (your device).

HOW A DNS RESOLVER WORKS:

Caching:

- To optimize performance and reduce load, DNS resolvers cache the responses for a certain amount of time (defined by the Time-to-Live or TTL value in the DNS records). This way, subsequent requests for the same domain can be answered more quickly from the cache.

Handling Different Types of Queries:

- **Recursive Queries**: The resolver is responsible for finding the complete answer to the query, which involves querying multiple servers until it gets the final answer.
- **Iterative Queries**: The resolver or the client receives referrals to other servers and must continue the query process itself. Recursive resolvers handle this behind the scenes for clients.

TYPES OF DNS RESOLVERS

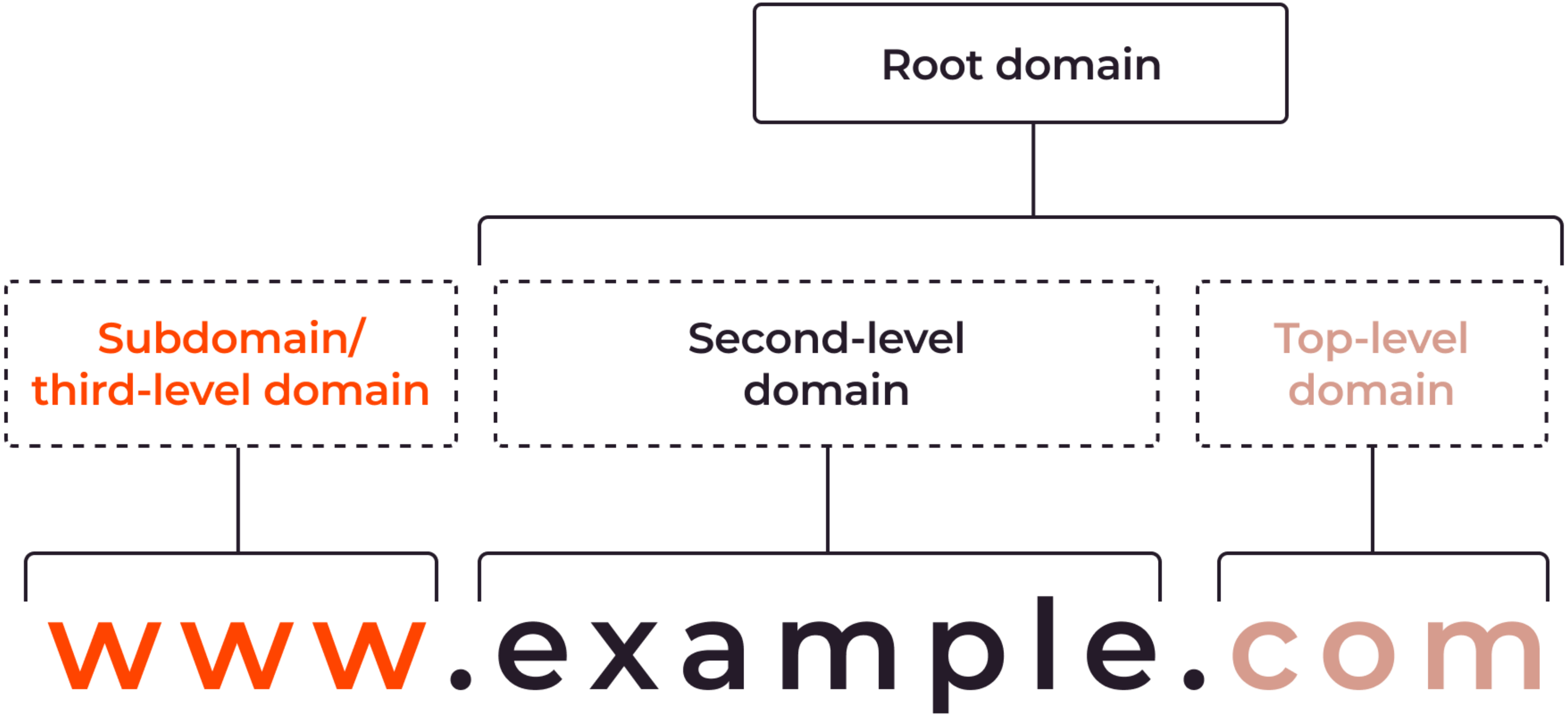
Local DNS Resolvers: Often built into operating systems, they handle initial DNS queries and typically forward requests to more powerful recursive resolvers.

Public Recursive Resolvers: Provided by companies like Google (8.8.8.8), Cloudflare (1.1.1.1), and OpenDNS, these are widely used due to their speed, security features, and privacy assurances.

Local computers do save DNS cache. This caching is part of the DNS resolution process to speed up future queries for the same domain names and reduce the load on DNS servers. Here's how DNS caching works on local computers:

- ipconfig /displaydns
- ipconfig /flushdns

ROOT NAME SERVER


Root domain
Subdomain/ third-level domain
Second-level domain
Top-level domain
www.example.com

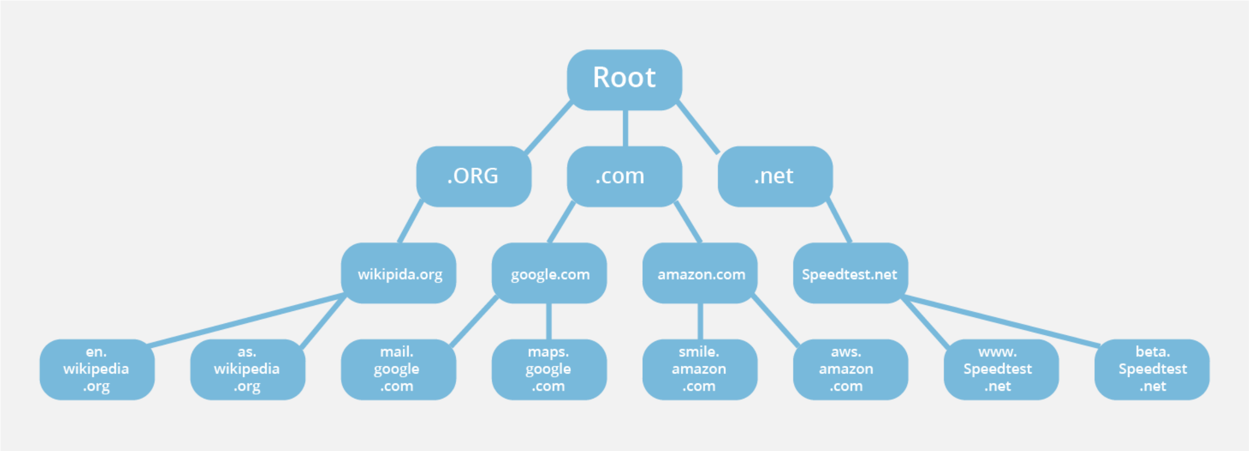
WHAT IS A DNS ROOT SERVER?

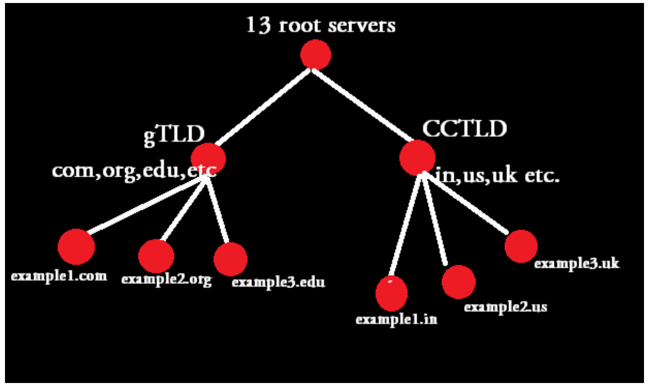
The administration of the Domain Name System (DNS) is structured in a hierarchy using different managed areas or “zones”, with the root zone at the very top of that hierarchy. Root servers are DNS nameservers that operate in the root zone. These servers can directly answer queries for records stored or cached within the root zone, and they can also refer other requests to the appropriate Top Level Domain (TLD) server. The TLD servers are the DNS server group one step below root servers in the DNS hierarchy, and they are an integral part of resolving DNS queries.

WHAT ARE ROOT NAME SERVERS?

- The administration of the Domain Name System (DNS) is structured in a hierarchy using different managed areas or “zones”, with the root zone at the very top of that hierarchy. Root servers are DNS nameservers that operate in the root zone. These servers can directly answer queries for records stored or cached within the root zone, and they can also refer other requests to the appropriate Top Level Domain (TLD) server. The TLD servers are the DNS server group one step below root servers in the DNS hierarchy, and they are an integral part of resolving DNS queries.

- There are 13 logical root name servers specified, with logical names in the form letter.root-servers.net, where letter ranges from a to m. The choice of thirteen name servers was made because of limitations in the original DNS specification, which specifies a maximum packet size of 512 bytes when using the User Datagram Protocol (UDP).Technically however, fourteen name servers fit into an IPv4 packet. The addition of IPv6 addresses for the root name servers requires more than 512 bytes, which is facilitated by the EDNS0 extension to the DNS standard.


Root
.ORG
.com
.net
wikipida.org
google.com
amazon.com
Speedtest.net
en. wikipedia .org
as. wikipedia .org
mail. google .com
maps. google .com
smile. amazon .com
aws. amazon .com
www. Speedtest .net
beta. Speedtest .net


13 root servers
gTLD
com,org,edu,etc
CCTLD
in,us,uk etc.
example1.com
example2.org
example3.edu
example1.in
example2.us
example3.uk

THE ROOT ZONE

The root servers contain the information that makes up the root zone, which is the global list of top level domains. The root zone contains:

- generic top level domains – such as .com, .net, and .org

- country code top level domains – two-letter codes for each country, such as .se for Sweden or .no for Norway

- internationalized top level domains – generally equivalents of country code top level domain names written in the countries’ local character sets

For each of those top level domains, the root zone contains the numeric addresses of name servers which serve the top level domain’s contents, and the root servers respond with these addresses when asked about a top level domain.

WHO OPERATES THEM?

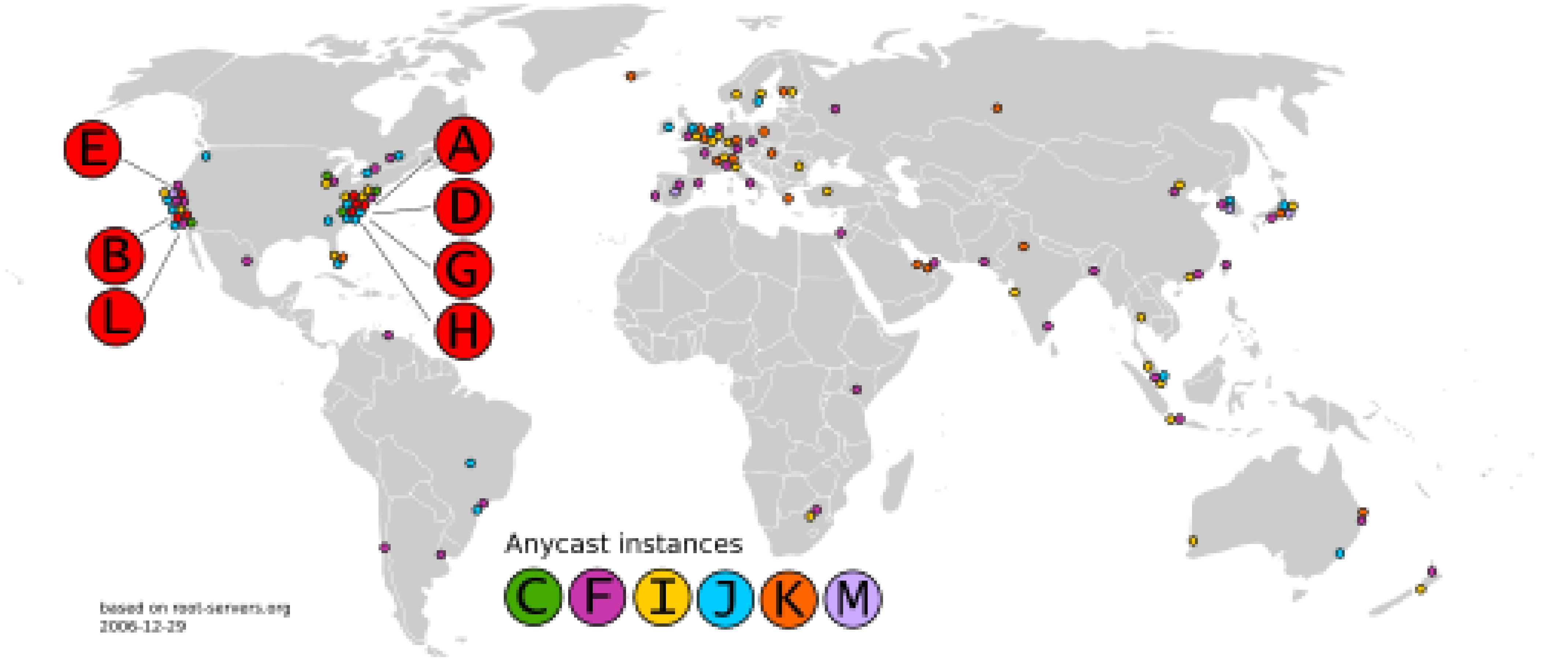
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	170.247.170.2, 2801:1b8:10::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

WHERE THEY ARE?

- Because there are 13 root servers this does not mean that there are only 13 physical servers; each operator uses redundant computer equipment to provide reliable service even if failure of hardware or software occurs. Additionally, all operate in multiple geographical locations using a routing technique called anycast addressing, providing increased performance and even more fault tolerance.
- There are more than 1,300 root server instances around the world, on all six populated continents. They are reachable using 13 numeric IP addresses – one per operating organisation, except for Verisign, which operates two root servers. Most of those addresses are assigned to multiple servers around the world, so DNS queries sent to those addresses get fast responses from local servers. This was not always the case. Before 2004, there were root server instances in only 13 locations – one per IP address – and all but three were in the United States. However, significant efforts by several of the root server operators, including Netnod, have expanded the global root server footprint since then.

- Because there are only 13 root server IP addresses, only 13 root servers can be seen from any single location at any given time. Different servers (using the same IP addresses) will be seen from different locations.
- Ten servers were originally in the United States; all are now operated using anycast addressing. Three servers were originally located in Stockholm (I-Root), Amsterdam (K-Root), and Tokyo (M-Root) respectively. Older servers had their own name before the policy of using similar names was established. With anycast, most of the physical root servers are now outside the United States, allowing for high performance worldwide.

Root Server Technical Operations Association



based on root-servers.org
2006-12-29

WHO IS RESPONSIBLE FOR THEM?

- Each operating organization is solely responsible for the root server IP address (or addresses) it operates. The operating organization determines how many locations that IP address will be served from, what those locations are, what hardware and software will be installed in each location, and how that hardware and software will be maintained. Some operators operate only a single location, while others operate many (one operator is responsible for almost 100). Each organization secures its own operating funds.

WHERE DOES THE ROOT ZONE COME FROM?

- The root zone comes from the Internet Assigned Numbers Authority (IANA), which is part of the Internet Corporation for Assigned Names and Numbers (ICANN). It is signed using DNSSEC signatures to ensure authenticity, and issued to the root server operators to publish to their root servers. The root server operators publish the root zone as written, and have no authority to alter the content.

WHAT HAPPENS IF A DNS ROOT SERVER BECOMES UNAVAILABLE?

- Thanks to the use of Anycast routing and heavy redundancy, the root servers are very reliable. But on rare occasions a root server will have to update its IP address. In this case, recursive resolvers can continue using the other 12 IP addresses in the root zone to perform DNS lookups until their software is updated with the correct addresses of all 13 servers. Since resolvers will retry until they reach a working root server, there is no disruption to the normal operations of the Internet when one root server is down.

TOP-LEVEL DOMAIN (TLD)

WHAT IS A TOP-LEVEL DOMAIN (TLD)?

- In the DNS hierarchy, a top-level domain (TLD) represents the first stop after the root zone. In simpler terms, a TLD is everything that follows the final dot of a domain name. For example, in the domain name ‘google.com’, ‘.com’ is the TLD. Some other popular TLDs include ‘.org’, ‘.uk’, and ‘.edu’.

- TLDs play an important role in the DNS lookup process. For all uncached requests, when a user enters a domain name like ‘google.com’ into their browser window, the DNS resolvers start the search by communicating with the TLD server. In this case, the TLD is ‘.com’, so the resolver will contact the TLD DNS server, which will then provide the resolver with the IP address of Google’s origin server.

WHAT IS A TOP-LEVEL DOMAIN (TLD)?

The Internet Corporation for Assigned Names and Numbers (ICANN) has authority over all TLDs used on the Internet, and it delegates the responsibility of these TLDs to various organizations. For example, a U.S. company called VeriSign operates all '.com' and '.net' TLDs.

Another purpose of TLDs is to help classify and communicate the purpose of domain names. Every TLD will tell you something about the domain that precedes it; let's look at some examples:

	Purpose
.com	commercial organizations
.edu	educational organizations
.gov	government institutions
.mil	military groups
.net	major network support centers
.org	Nonprofit organizations and others
.int	International organizations

WHAT ARE THE DIFFERENT TYPES OF TLDS?

- **Generic TLDs:** Generic TLDs (gTLDs) encompass some of the more common domain names seen on the web, such as ‘.com’, ‘.net’, and ‘.org’. The Internet Corporation for Assigned Names and Numbers (ICANN) used to heavily restrict the creation of new gTLDs, but in 2010 these restrictions were relaxed. Now there are hundreds of lesser-known gTLDs, such as ‘.top’, ‘.xyz’, and ‘.loan’.
- **Country-code TLDs:** Country-code TLDs (ccTLDs) are reserved for use by countries, sovereign states, and territories. Some examples are ‘.uk’, ‘.au’ (Australia), and ‘.jp’ (Japan). The Internet Assigned Numbers Authority (IANA), which is run by ICANN, is in charge of picking appropriate organizations in each location to manage ccTLDs

•**Sponsored TLDs:** These TLDs typically represent professional, ethnic, or geographical communities. Each sponsored TLD (sTLD) has a delegated sponsor that represents that community. For example, ‘.app’ is a TLD intended for the developer community, and it is sponsored by Google. Similarly, ‘.gov’ is intended for use by the U.S. government, and is sponsored by the General Services Administration.

•**Infrastructural TLDs:** This category only contains a single TLD: ‘.arpa’. Named for DARPA, the U.S. military research organization that helped pioneer the modern Internet, ‘.arpa’ was the first TLD ever created and is now reserved for infrastructural duties, such as facilitating reverse DNS lookups.

•**Reserved TLDs:** Some TLDs are on a reserved list, which means they are permanently unavailable for use. For example, ‘.localhost’ is reserved for local computer environments, and ‘.example’ is reserved for use in example demonstrations.

AUTHORITATIVE NAMESERVER

WHAT IS AUTHORITATIVE NAME SERVER?

- The authoritative DNS server is the final holder of the IP of the domain you are looking for.An authoritative name server provides actual answer to your DNS queries such as – mail server IP address or web site IP address (A resource record). It provides original and definitive answers to DNS queries. It does not provides just cached answers that were obtained from another name server. Therefore it only returns answers to queries about domain names that are installed in its configuration system.
- Such a server is the name server, which has the original zone records. It has been configured from the original source, and it returns answers to queries that have been predetermined by the administrator.These DNS servers are giving responses to queries just for the zones they are configured. This makes them very efficient and fast.

TWO TYPES OF AUTHORITATIVE NAME SERVERS

- **Master server (primary name server)** – A master server stores the original master copies of all zone records. A hostmaster only make changes to master server zone records. Each slave server gets updates via special automatic updating mechanism of the DNS protocol. All slave servers maintain an identical copy of the master records.
- **Slave server (secondary name server)** – A slave server is exact replica of master server. It is used to share DNS server load and to improve DNS zone availability in case master server fails. It is recommend that you should at least have 2 slave servers and one master server for each domain name.
- The authoritative servers don’t cache query results. They have data that is saved in their system. It can be master or slave. It can store the original zone records, or a secondary server which communicates directly with the primary and copies the records directly through a DNS mechanism.

HOW DO I VIEW AUTHORITATIVE NAME SERVER NAMES AND IP ADDRESS?

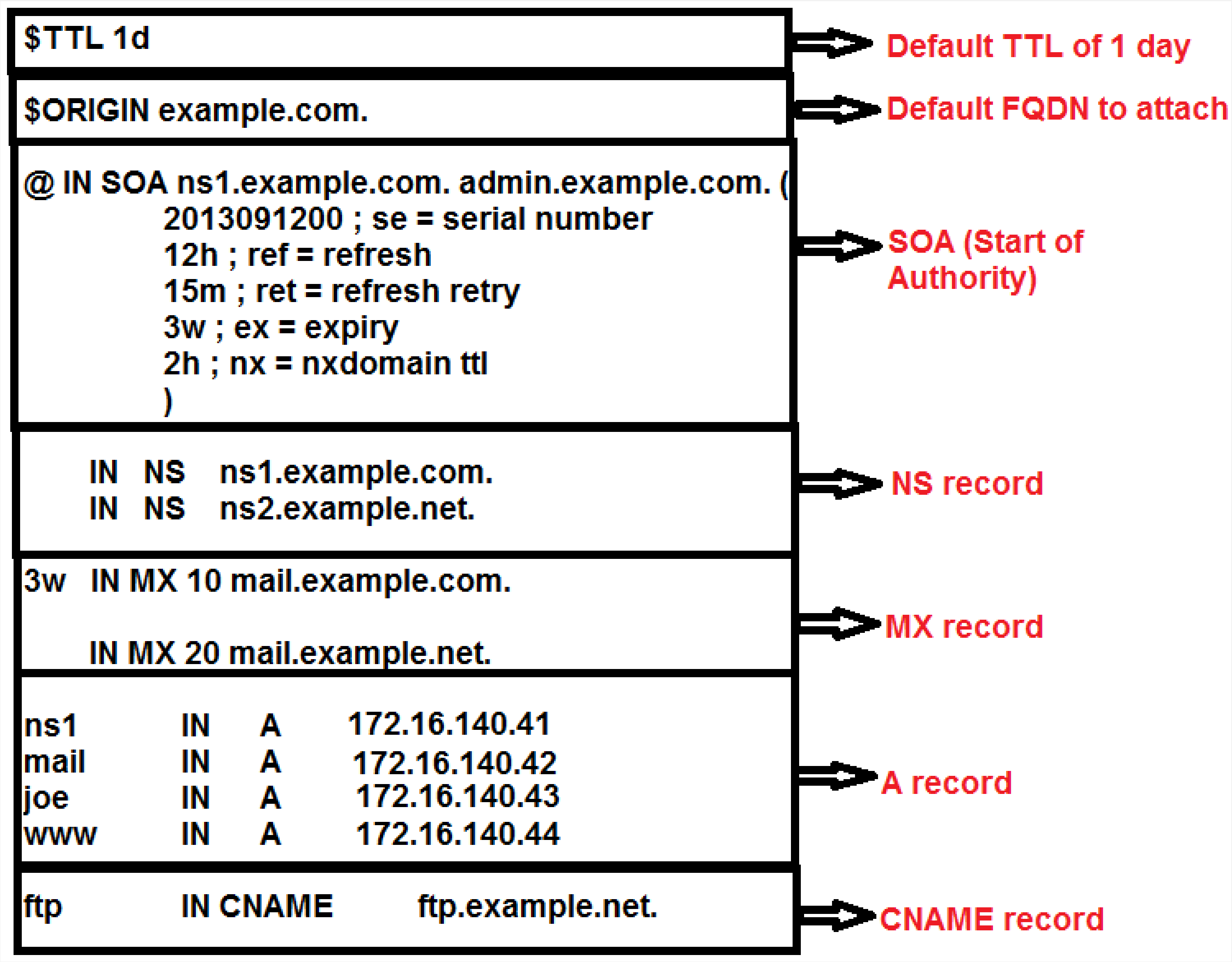
>Nslookup

>Set query=ns

>url

ZONE FILE

A **zone file** is a plain text file that contains the DNS records for a specific domain or a part of the DNS namespace, called a zone. It is used by DNS servers (specifically, authoritative name servers) to map domain names to IP addresses and other DNS data required for the functioning of the Domain Name System.



```
$TTL 1d

$ORIGIN example.com.

@ IN SOA ns1.example.com. admin.example.com. (
            2013091200 ; se = serial number
            12h ; ref = refresh
            15m ; ret = refresh retry
            3w ; ex = expiry
            2h ; nx = nxdomain ttl
            )

      IN   NS    ns1.example.com.
      IN   NS    ns2.example.net.

3w   IN MX 10 mail.example.com.

     IN MX 20 mail.example.net.

ns1         IN     A       172.16.140.41
mail        IN     A       172.16.140.42
joe         IN     A       172.16.140.43
www         IN     A       172.16.140.44

ftp         IN CNAME        ftp.example.net.
```

KEY COMPONENTS OF A ZONE FILE:

SOA Record (Start of Authority):

- Defines the primary authoritative name server for the zone.
- Contains essential information such as the administrator's email address, serial number for updates, and timing parameters (refresh, retry, expiry, and TTL).

NS Records (Name Server):

- Lists the authoritative name servers for the zone.
- These servers are responsible for answering queries about the domain and its subdomains.

A and AAAA Records (Address Records):

- **A Record**: Maps a domain name to an IPv4 address.
- **AAAA Record**: Maps a domain name to an IPv6 address.

CNAME Records (Canonical Name):

- Alias record that maps one domain name to another. Useful for pointing multiple domain names to the same IP address without creating separate A or AAAA records.

KEY COMPONENTS OF A ZONE FILE:

MX Records (Mail Exchange):

- Specifies the mail servers responsible for receiving email for the domain.
- Includes priority levels to determine the order of server use.

TXT Records:

- Allows administrators to include arbitrary text data in the DNS, often used for SPF (Sender Policy Framework), domain verification, or other security purposes.

PTR Records (Pointer Records):

- Used in reverse DNS lookups to map an IP address back to a domain name.

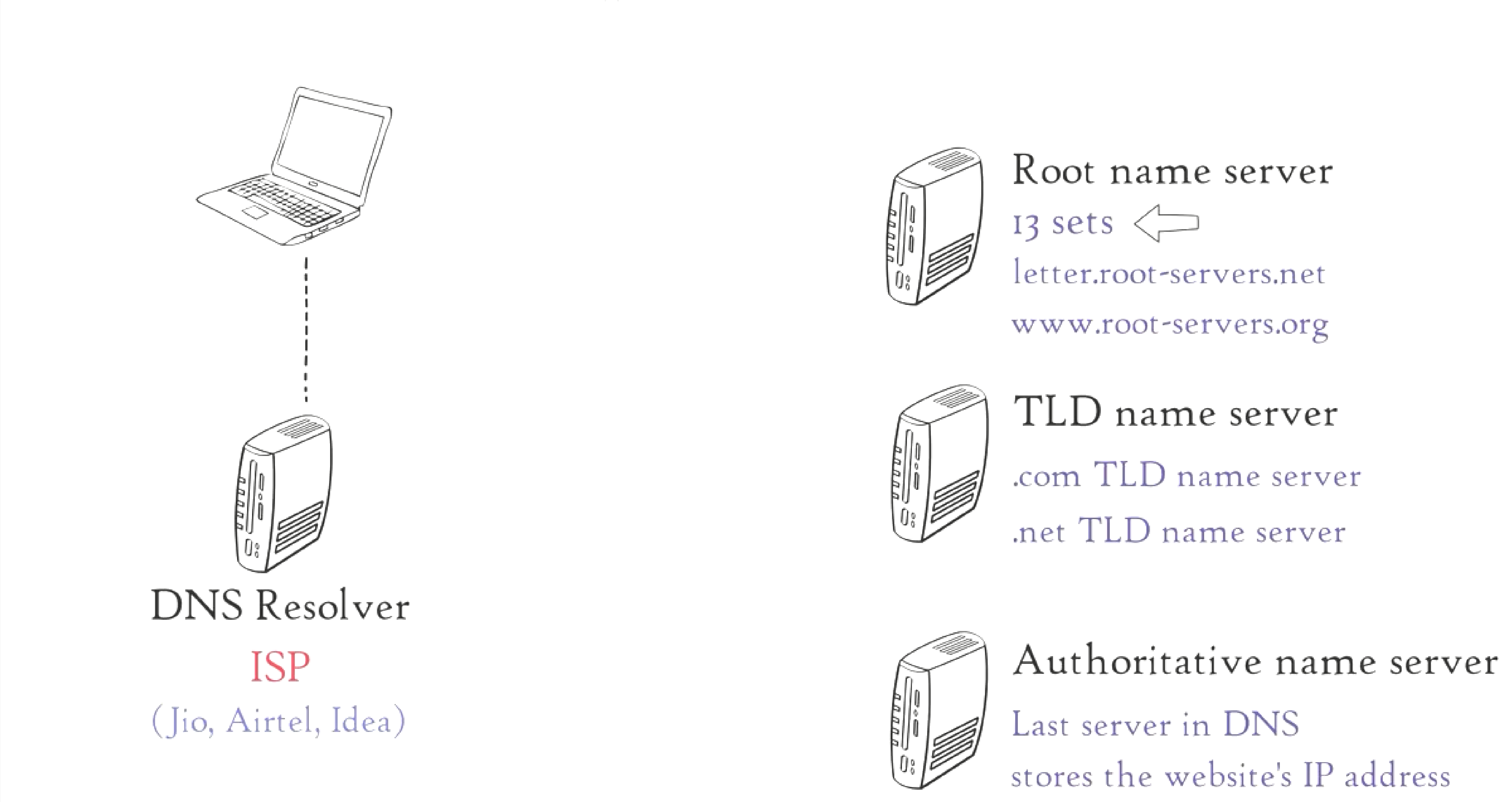
SRV Records (Service Records):

- Specifies the location (hostname and port) of servers for specific services, like VoIP or instant messaging.

Other Records:

- **SOA**: Start of Authority, marks the start of the zone.
- **SPF**: Sender Policy Framework, for email validation.

How does a computer loads a website?



DNS Resolver

ISP

(Jio, Airtel, Idea)

Root name server

13 sets ⇦

letter.root-servers.net

www.root-servers.org

TLD name server

.com TLD name server

.net TLD name server

Authoritative name server

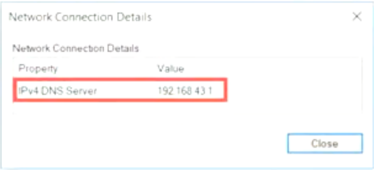
Last server in DNS

stores the website's IP address

IP address of facebook.com ?

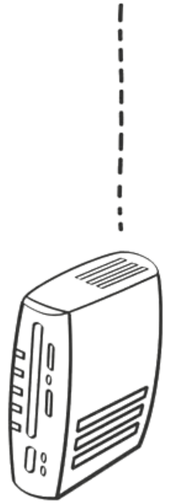
↓

Computer's OS

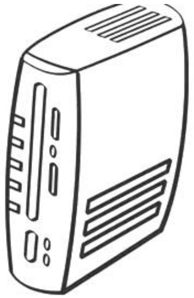

Network Connection Details

Network Connection Details

Property	Value
IPv4 DNS Server	192.168.43.1



DNS Resolver

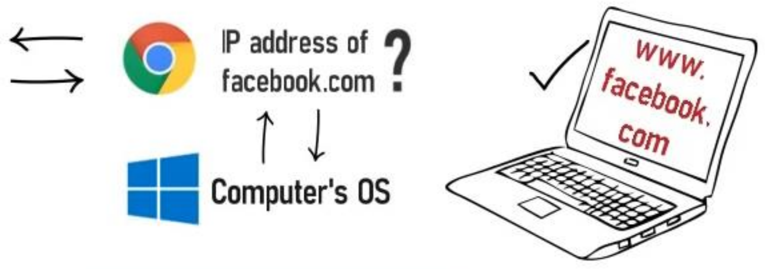


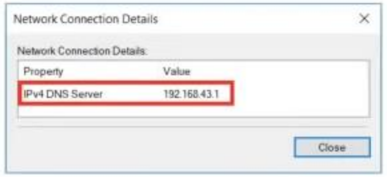
DNS Resolver

ISP

CACHE

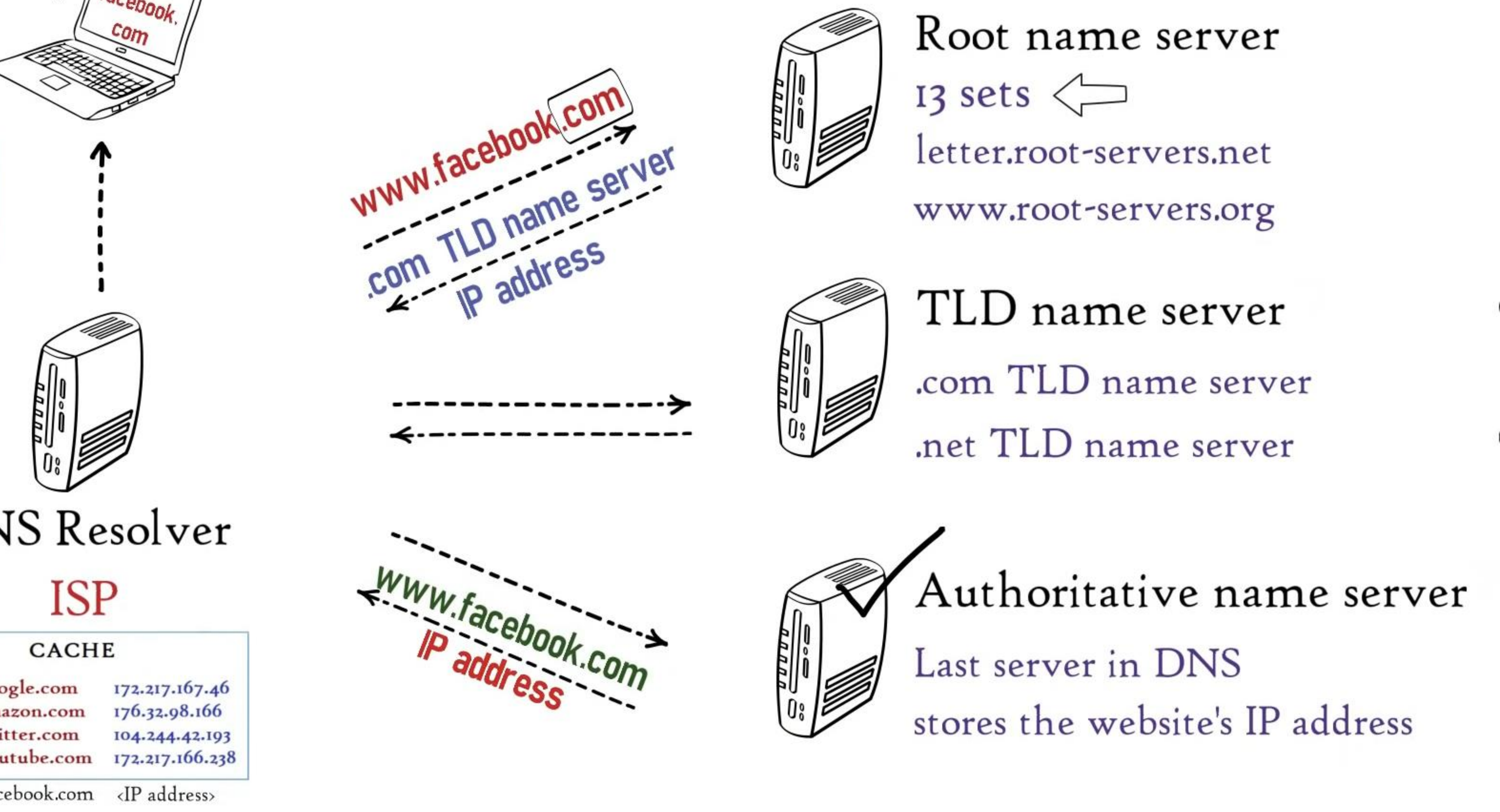
www.google.com	172.217.167.46
www.amazon.com	176.32.98.166
www.twitter.com	104.244.42.193
www.youtube.com	172.217.166.238




Network Connection Details

Network Connection Details:

Property	Value
IPv4 DNS Server	192.168.43.1



DNS Resolver

ISP

Root name server

13 sets

letter.root-servers.net

www.root-servers.org

TLD name server

.com TLD name server

.net TLD name server

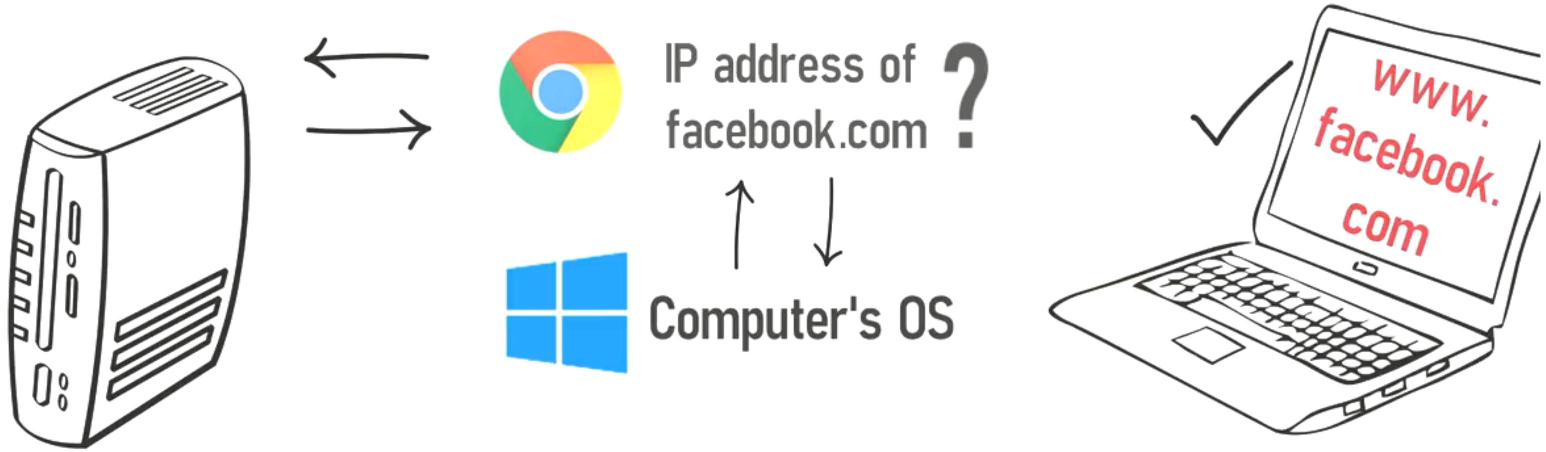
Authoritative name server

Last server in DNS

stores the website's IP address

CACHE

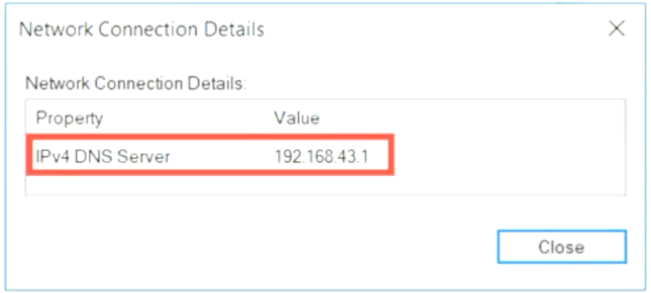
www.google.com	172.217.167.46
www.amazon.com	176.32.98.166
www.twitter.com	104.244.42.193
www.youtube.com	172.217.166.238
www.facebook.com	‹IP address›



IP address of facebook.com ?

Computer's OS

Facebook server

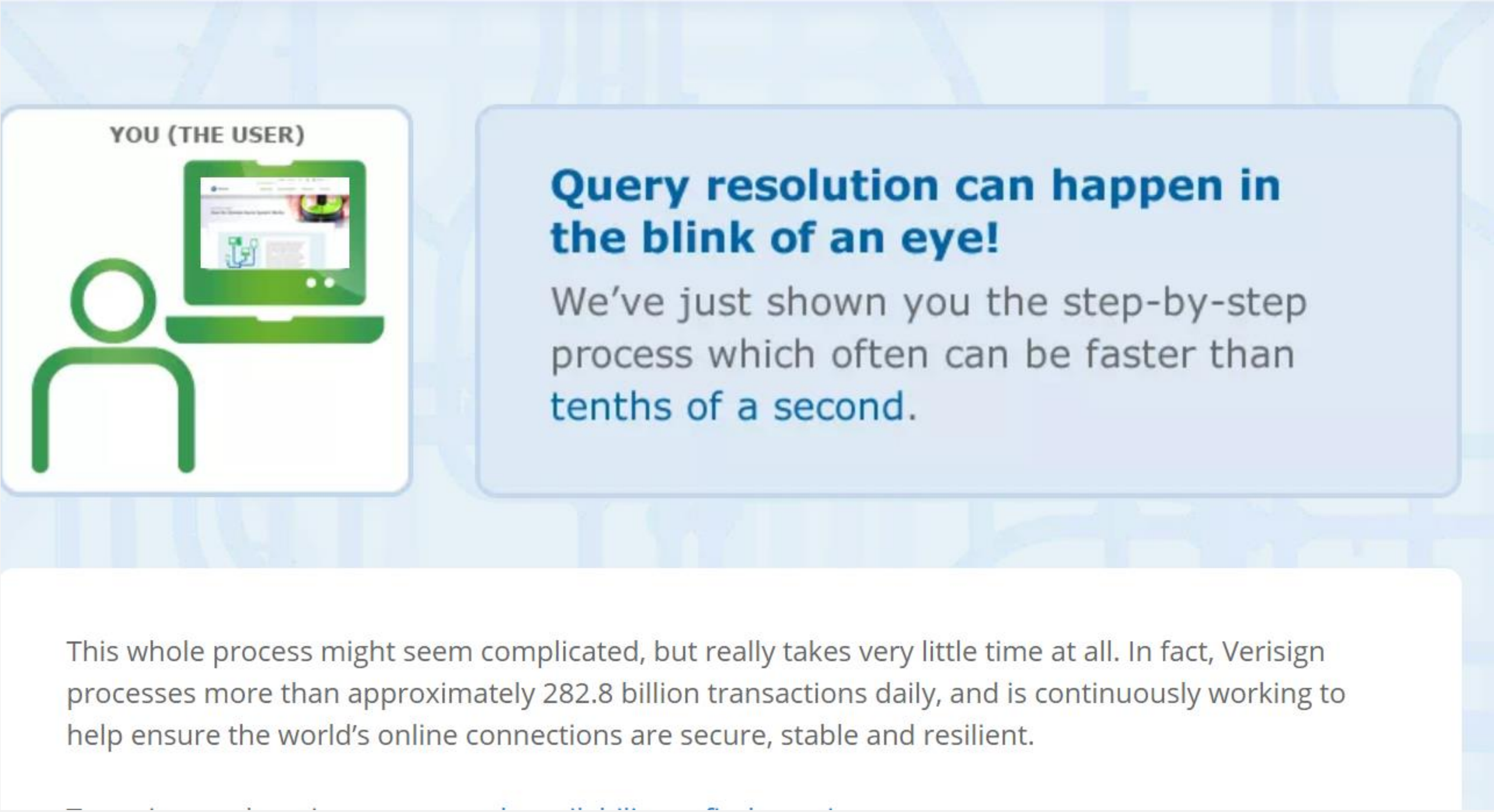


Network Connection Details

Network Connection Details:

Property	Value
IPv4 DNS Server	192.168.43.1

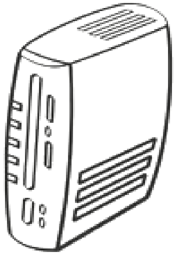
Tenths of a Second



Query resolution can happen in the blink of an eye!

We've just shown you the step-by-step process which often can be faster than tenths of a second.

This whole process might seem complicated, but really takes very little time at all. In fact, Verisign processes more than approximately 282.8 billion transactions daily, and is continuously working to help ensure the world's online connections are secure, stable and resilient.



Root name server

13 sets ⇦

letter.root-servers.net

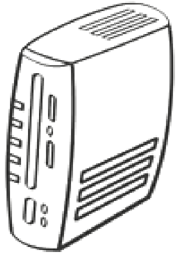
www.root-servers.org

operated by: 12 organizations

info page: letter.root-servers.org

letter: ‘a’ to ‘m’

for 'g': https://disa.mil/g-root

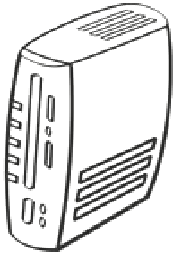


TLD name server

.com TLD name server

.net TLD name server

- domains: .com, .net, .in, .edu
- websites: .com extension
- websites: .net extension



Authoritative name server

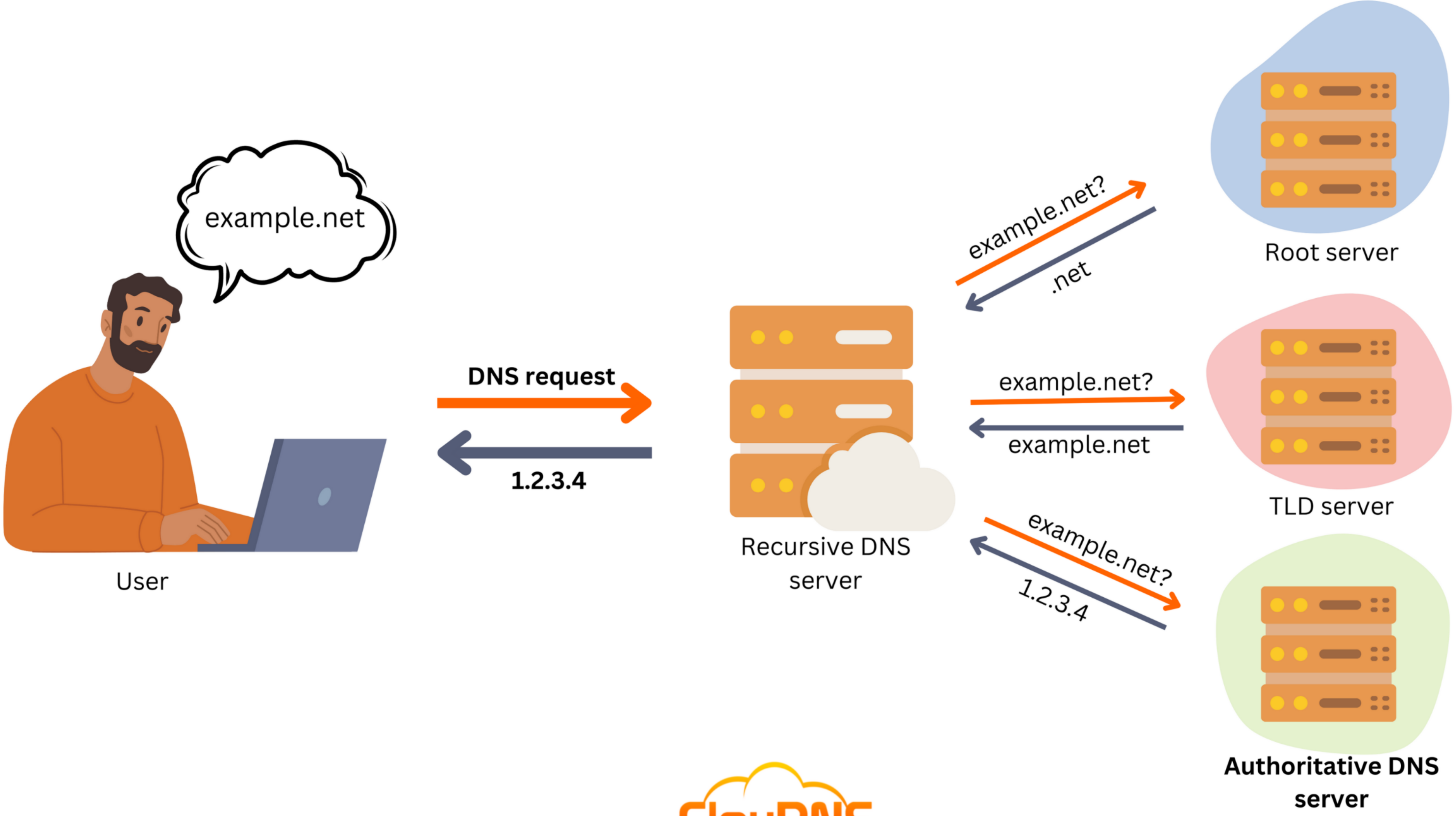
Last server in DNS

stores the website's IP address

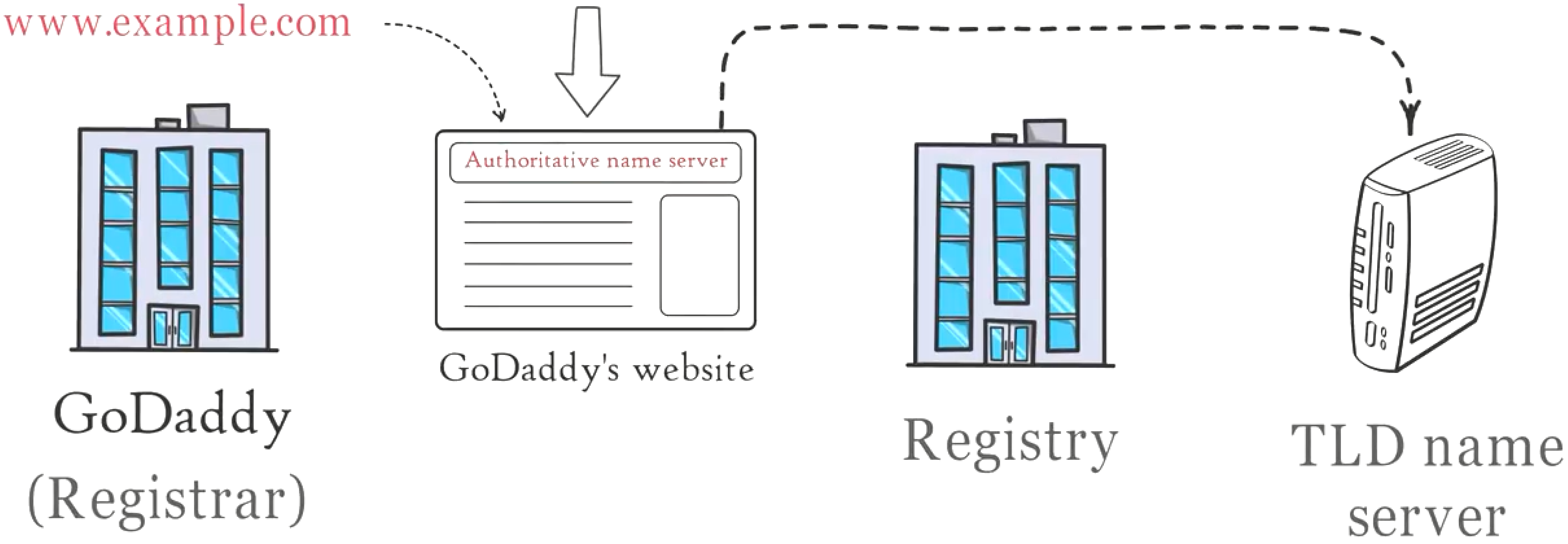
CMD Commands:

- nslookup
- set query=ns
- example.com (domain name)

Authoritative DNS server



ClouDNS



www.example.com

Authoritative name server

GoDaddy's website

GoDaddy
(Registrar)

Registry

TLD name
server

HOW DO I REGISTER AUTHORITATIVE NAME SERVER?

- First, you need to register a domain name with your domain name registrar.
- Each domain name registrar allows you to set a primary name server (master server) and at least one secondary name server (slave server).
- For example, DNSKnowledge.com domain name is registered with GoDaddy domain name registrar. GoDaddy (or any other domain name registrar) allows you to change the DNS authoritative name server at the time of registration or later any time.

AUTHORITATIVE DNS SERVER VS. RECURSIVE DNS SERVER

- Both Authoritative DNS servers and Recursive DNS servers have crucial functions, and they depend on each other to fulfill their purposes. However, there are some fundamental differences between them.
- Authoritative DNS servers store the most recent and accurate information (DNS records) for a domain and are able to provide the final answers for users’ DNS queries (DNS lookups). On the other hand, Recursive DNS servers only keep a copy of the DNS information for a particular amount of time, also known as Time to live (TTL). Additionally, they often have to obtain the answer for a DNS query from another server.
- **An Authoritative DNS server** is responsible for answering DNS queries for a particular set of DNS zones by providing information from its own data. It does not have the need to reference another source.
- **The Recursive DNS server** replies to DNS queries by asking other nameservers for the needed information (DNS records). In some cases, this server responds to DNS requests directly from its cache if the information is available there. In case it is not, the Recursive DNS server, also known as DNS resolver, is going to perform a search and ask the responsible authoritative servers until it finds the needed answer.

Is DNS necessary?

www.google.com

www.ebay.com

www.shopclues.com

.

.

.

.

www.paytm.com

~~DNS~~

172.217.167.46

Web Browser

Is DNS necessary?

www.google.com	DNS	172.217.167.46
www.ebay.com		66.211.160.86
www.shopclues.com		103.194.152.149
.		.
.		.
.		.
.		.
www.paytm.com		18.136.75.218