Miscallenous Important questions

What is nameservers, A Record , AAAA Record , MX Records , CNAME Records

What Is DNS? Often referred to as the phone book of the internet, the domain name system, or DNS, breaks
the website address (URL) into segments and queries multiple servers that contain those bits of information.
Those servers are called name servers, and they are the foundation of DNS.

What is a nameserver?

Name servers are the servers that make up DNS.
They hold the records of multiple DNS types and translate a URL into an IP address.
A nameserver is a type of DNS server. It is the server that stores all DNS records for a domain, including A records, MX records, or CNAME records.
Almost all domains rely on multiple nameservers to increase reliability:
if one nameserver goes down or is unavailable, DNS queries can go to another one.
Typically there is one primary nameserver and several secondary nameservers, which store exact copies of the DNS records in the primary server. Updating the primary nameserver will trigger an update of the secondary nameservers as well.
There are four types of name servers that make up DNS:
Recursive (also known as resolver) server
Root name server
TLD name server
Authoritative server

How DNS Works?

First, your computer will see if the website is cached in your system. If it’s not, the query will head to a DNS recursive server.

```
How we can check dns cache in our system (for windows)
open cmd run command in admin mode: ipconfig/displaydns
command to save dns cache details of your in file: ipconfig
/displaydns > dnscachecontents.txt
Samle of Info. we get in DNS Cache file :
www.serumdiagnostics.in
----------------------------------------
Record Name . . . . . : www.serumdiagnostics.in
Record Type . . . . . : 5
Time To Live . . . . : 12754
```

```
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record . . . . : serumdiagnostics.in


    Record Name . . . . . : serumdiagnostics.in
    Record Type . . . . . : 1
    Time To Live . . . . : 12754
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 45.79.125.232
```

There are many record type and they are indicated by decimal digit A Records (Code 1) , AAAA Records(Code 28), MX Records (15), CNAME Record (Code 5r), NS Records, TXT Records

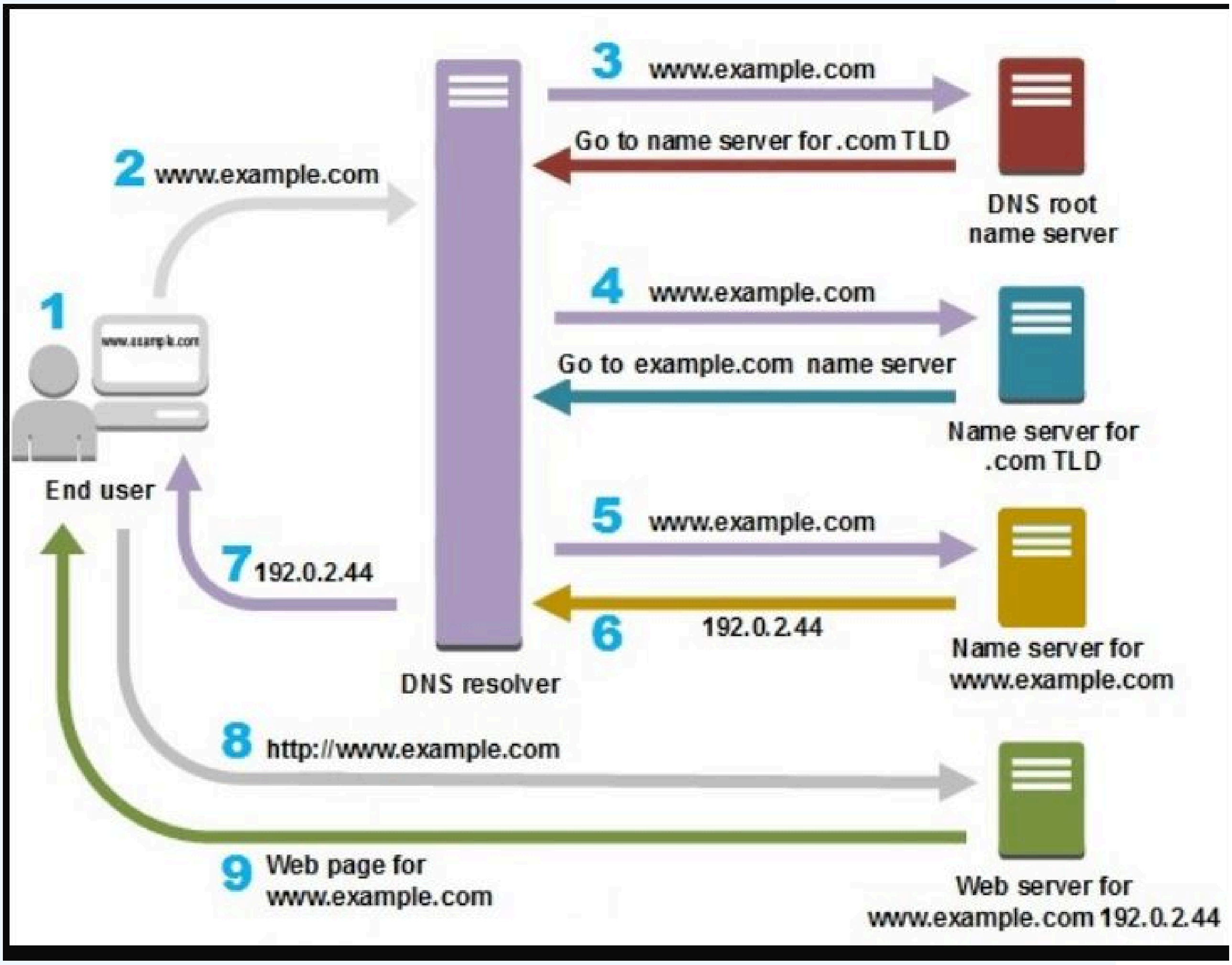
DNS Recursive Server A recursive server is usually operated by your internet service provider (ISP) or wireless carrier. If the website isn't cached in this server (usually by another user who has visited the website), then the query heads to a root server.

Root Name Server
The root server holds information about top-level domains (TLDs), including .com, .org, and .net. There are only 13 sets of root servers in the world, and they are operated by organizations like NASA and companies like Verisign.
Once the request goes to the root server, it will respond with the TLD name server.

TLD Name Server
Once your query knows which TLD name server to go to, it will visit a TLD name server
for the information in the second-level domain (the "Bluehost" in Bluehost.com).
The .com server will tell the request where to go to find the IP address for the website
you want to reach. It will point to the authoritative server, the final step in the journey.

Authoritative Server The authoritative server houses the website's IP address for the full domain. Once requested, it then sends that information back to the recursive server, which sends it to your device.
In a nutshell, your query goes back and forth between multiple servers until it has located all

the information it needs to get you to that website.



What Is DNS Cache? If there’s a website you frequent, it isn’t necessary to locate the IP address every time. DNS caching will store the data locally on your computer, or it can also be cached on the ISP’s servers.
Before it locates the IP address, your computer will check if the information is already cached. If your computer already has the data, then it doesn’t have to access a DNS server to resolve the query.

Most Common DNS type

A record

An A record (Address Record) points a domain or subdomain to an IP address. For example, you can use it for store.website.com or blog.website.com and point it to where you have your store.

CNAME Records
CNAME records, or Canonical Name, point one domain name to another. This is used for variations of your website.
If you’ve ever typed amazong.com and ended up at amazon.com, you can thank CNAME records.
These records point to www.example.com to example.com, imap.example.com to mail.example.com, and docs.example.com to ghs.google.com. The first record allows the domain to resolve to the same server with or without the www

subdomain. The second record allows you to use an alternative subdomain for email hosting and delivery. The third record allows you to use the docs.example.com subdomain with G Suite, where you can use Google's document management system.

MX Records

An MX Entry (Mail Exchanger) directs email to a particular mail server. Like a CNAME, MX Entries must point to a domain and never point directly to an IP address.

AAAA Record

The AAAA record is similar to the A record, allowing you to point the domain to an Ipv6 address. More information on IPv6 can be found at http://ipv6.com/.

What is DNS cache poisoning ?

Also called DNS spoofing
Imagine that, as a senior-year prank, high school seniors change out all the room numbers
on their high school campus, so that the new students who don't know the campus layout yet will
spend the next day getting lost and showing up in the wrong classrooms. Now imagine that the mismatched
room numbers get recorded in a campus directory, and students keep heading to the wrong rooms until
someone finally notices and corrects the directory.

DNS cache poisoning is the act of entering false information into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong websites. DNS cache poisoning is also known as 'DNS spoofing.'

IP addresses are the 'room numbers' of the Internet, enabling web traffic to arrive in the right places. DNS resolver caches are the 'campus directory,' and when they store faulty information, traffic goes to the wrong places until the cached information is corrected. (Note that this does not actually disconnect the real websites from their real IP addresses.)

The normal process:

You type a domain name into your web browser and it asks a DNS server for the IP address of the website.

The DNS server looks up the address and sends it back.
Your device stores this information in its DNS resolver cache for later use.

The attack:
An attacker puts false information into the DNS resolver cache.
They might manipulate a vulnerable DNS server or trick your device using man-in-the-middle or phishing techniques.
The incorrect information redirects you to a different website that might look the same. In reality, the attacker controls the website, putting you at risk.