DNS: 53

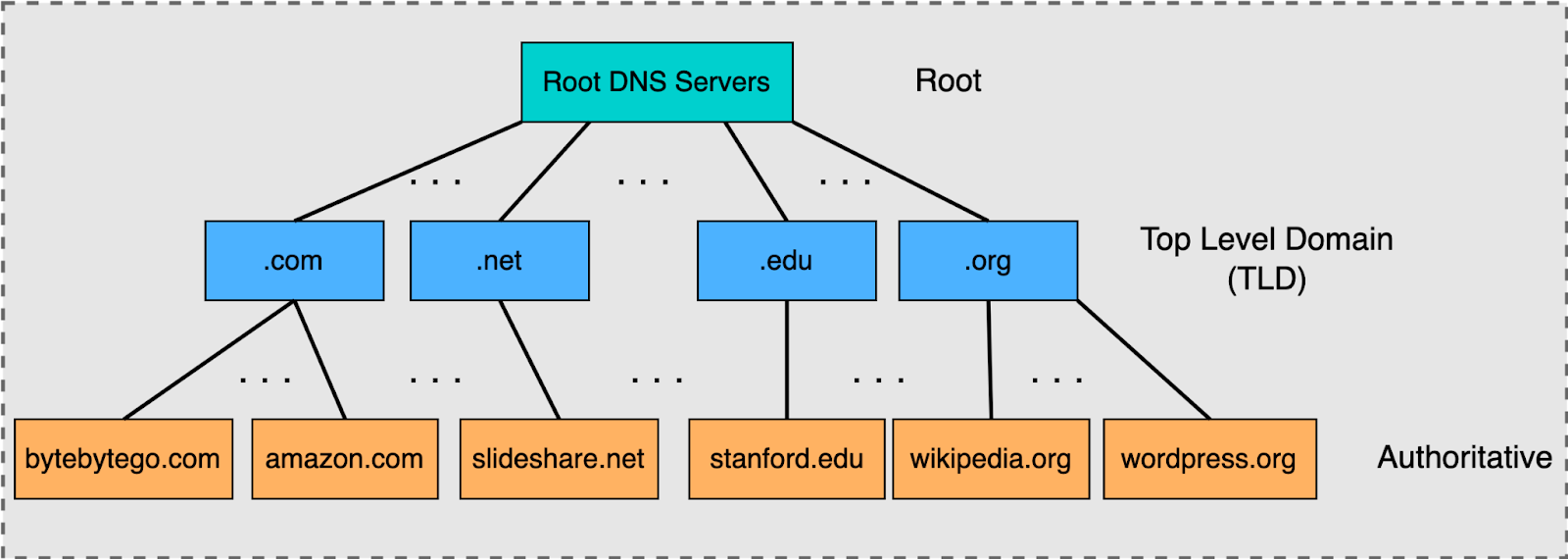
*Resources used:*

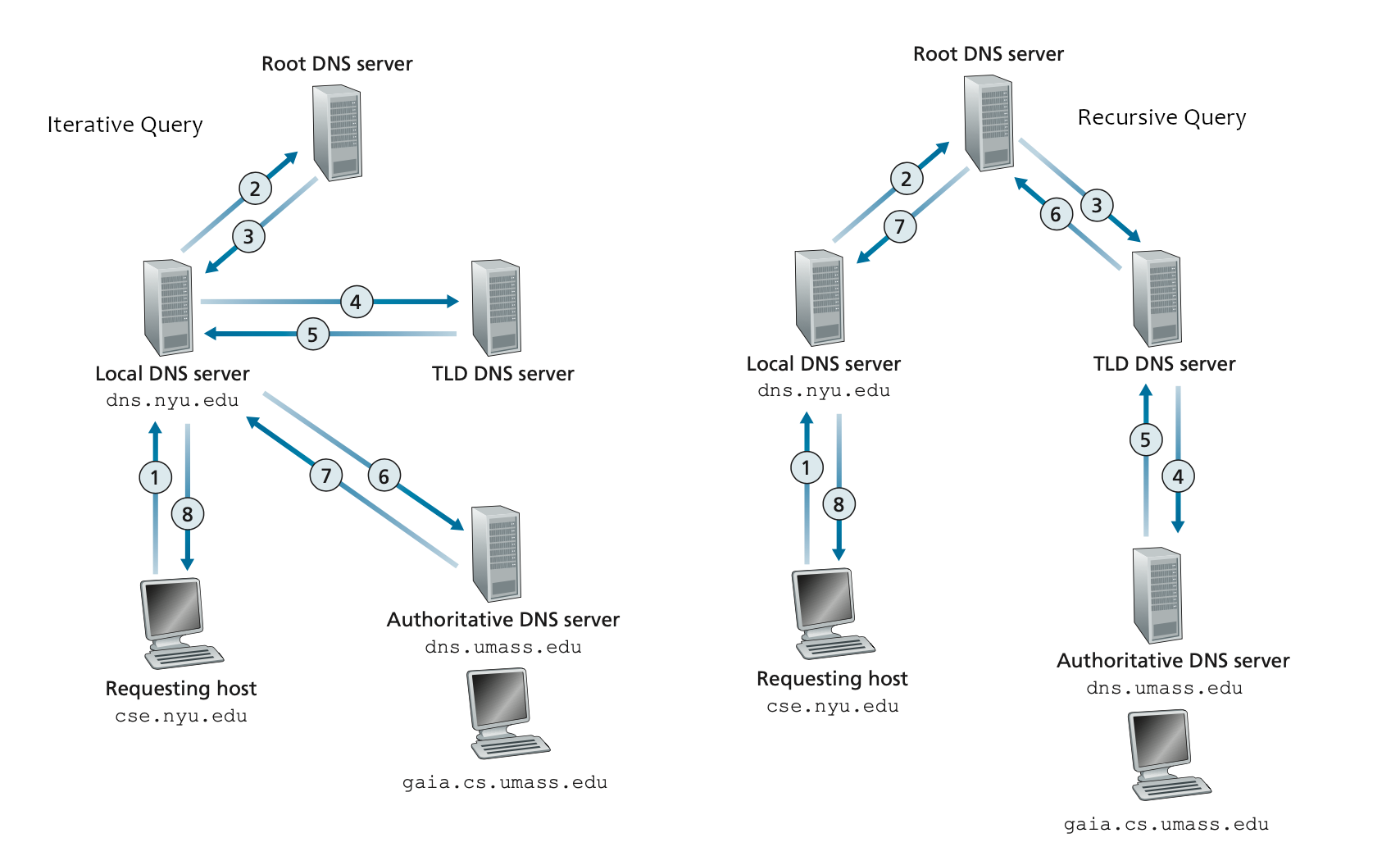
*DionTraining UDemy Course - “DNS”*

*Professor Messer on Youtube - “ An Overview of DNS, Network+”, “DNS Records”, & “DNS Configuration”*

*TechQuickie on Youtube - “DNS as Fast as Possible”*

Vocabulary:

1. Domain Name System (DNS)
   1. Helps network clients find a website using human-readable hostnames instead of numeric IP addresses. The internet’s “phone book”.
      1. Computer/workstation/device/client will reach out to a DNS server and ask, “Hey, who is neopets.com?” Then the DNS server goes, “Oh, neopets.com is XX.XX.XX.XX!” Then the client gets redirected to a web server, neopets.com!
   2. Most of us, especially home users, won’t be using our own personal DNS servers, but instead rely on our ISP’s to do this for us.
   3. Configured as a hierarchy, which makes it very easy to find things on the internet (woot-woot); there are several, SEVERAL DNS servers in the word, and hundreds of generic top-level domains and country code (geographical hierarchies) domains
   4. 
2. Fully-Qualified Domain Name (FQDN)
   1. Domain name under a top-level provider
      1. Most common top-level provider is .com
         1. Other examples: .mill, .edu, .org, .net
      2. To be fully qualified, needs “www.” in front of domain name, with top-level domain “.com”
3. Uniform Resource Locator (URL)
   1. Contains the FQDN with the method of accessing information (how do you want to access neopets.com? Securely, or insecurely?)
      1. Add HTTPS:// + neopets.com = now it’s an URL!
4. Internal DNS
   1. Allows cloud instances on the same network access each other using internal DNS names instead of having to use their IP addresses
   2. Managed on internal servers, configured and maintained by a local team, and contains DNS information about internal devices
5. External DNS
   1. Most of us are more familiar with external DNS
   2. Records created around the domain names from a central authority and used on the public Internet
   3. Often managed by a 3rd-party such as Google DNS, Quad9, etc.
6. Time to Live (TTL)
   1. Tells the DNS resolver how long to cache a query before requesting a new one
   2. Each DNS record has a TTL that’s associated with it
7. DNS Resolver/DNS Cache
   1. Basically makes a local copy of every DNS entry it “resolves” when it connects to a website; this temporary database remembers the answers it receives and stores it for about 24 hours (default time) before it runs out and searches for that information again. Once my computer searches and finds the IP for neopets.com, it will remember it for 24 hours (the IP address - no need to go searching for it again). This helps speed up the process. So if I look up neopets.com x5, I only have to find the IP address x1.
8. Recursive Lookup
   1. DNS server communicates with several other DNS servers to hunt down the IP address and return to the client
      1. BASICALLY: IF A DNS SERVER DOESN’T KNOW THE ANSWER, IT WILL ASK THE NEXT DNS SERVER, AND IF THAT DNS SERVER DOESN’T KNOW THE ANSWER, IT WILL ASK THE NEXT DNS SERVER, AND IF THAT DNS SERVER DOESN’T KNOW THE ANSWER, IT WILL ASK THE NEXT -
      2. By the way, sometimes to solve certain webpage 404 errors, you can “flush your DNS” (reset the DNS cache) command prompt, ipconfig/flushdns



DNS is set up as a hierarchy:

1. Root Level
   1. Answers requests in the root zone
2. Top-level Domain
   1. .com, .mill, .edu, .org, .net
      1. Also contains geographical hierarchy, such as .uk, .jp, .fr
3. Second-level Domain
   1. Name of the domain, usually determined by customer/enterprise/person setting up the domain
4. Sub-domain
   1. For servers, etc. like, support.neopets.com, mail.neopets.com
5. Host
   1. Lowest and most detailed level of the DNS hierarchy, refers to a specific server or machine

DNS Records

* A Record: Used to link a host name to an IPv4 address (only works for IPv4)
  + If you ever have to modify or change the IP of a device, you’re probably going to modify one of these ‘A records’
* AAAA Record: Used to link a host name to an IPv6 address
  + If you ever have to modify or change the IP of a device, you’re probably going to modify one of these ‘A records’
* CNAME Record: Points a domain to another domain or subdomain; example: I don’t use oldjudia.com anymore, but it’s all over the internet - i’ll just have oldjudia.com all redirect to my current website, newjudia.com whenever someone goes to it.CNAME records cannot be used to point to an IP address - only to point to another domain or subdomain.
  + One physical server, multiple services
* MX: “Mail exchange record”; directs emails to a mail server. Helps you figure out where a mail server; an MX record is used to direct emails to your mail server. Cannot be used to point to an IP address.
  + mail.domain.name
* TXT: Text records; adds text to the DNS. TXT used to prove domain ownership with machine-readable code for verification. You can use TXT to add SPF, DKIM, and DMARC messages.
  + Sender Policy Framework (SPF): DNS record that identifies the host authorized to send mail for the domain; only one allowed for each and every domain
    - TXT @ v=spf1 mx include:\_spf.google.com include:email.freshdesk.com - all
    - A list of all servers authorized to send emails for this domain; this prevents mail spoofing
    - Mail servers perform a check to see if incoming mail really did come from an authorized host
    - Useful public information
  + Domain Keys Identified Mail (DKIM): Provides the cryptographic authentication mechanism for mail using a public key published as a DNS record
    - Digital signature for outgoing mail; digitally sign a domain’s outgoing mail -- validated by mail servers, not usually seen by the end user - the public key is in the DKIM TXT record
  + Domain-based Message Authentication, Reporting & Conformance (DMARC): Framework that is used for proper application of SPF and DKIM, utilizing a policy that’s published as a DNS record
    - Prevent unauthorized email use (spoofing)
    - What to do with emails that aren’t validated? DMARC can be figure out/parse out these instructions…these policies are written into a DMARC TXT record
      * Accept all, send to spam, or reject the email
      * Compliance reports can be sent to the email administrator
* NS “Nameserver”: Indicates which DNS name server in the world is going to be the authoritative one for that domain.
  + I.e. cloudflare is a service provider that hosts nameserver for say…my website, neopets.com