Domain Name System (DNS)

General Overview

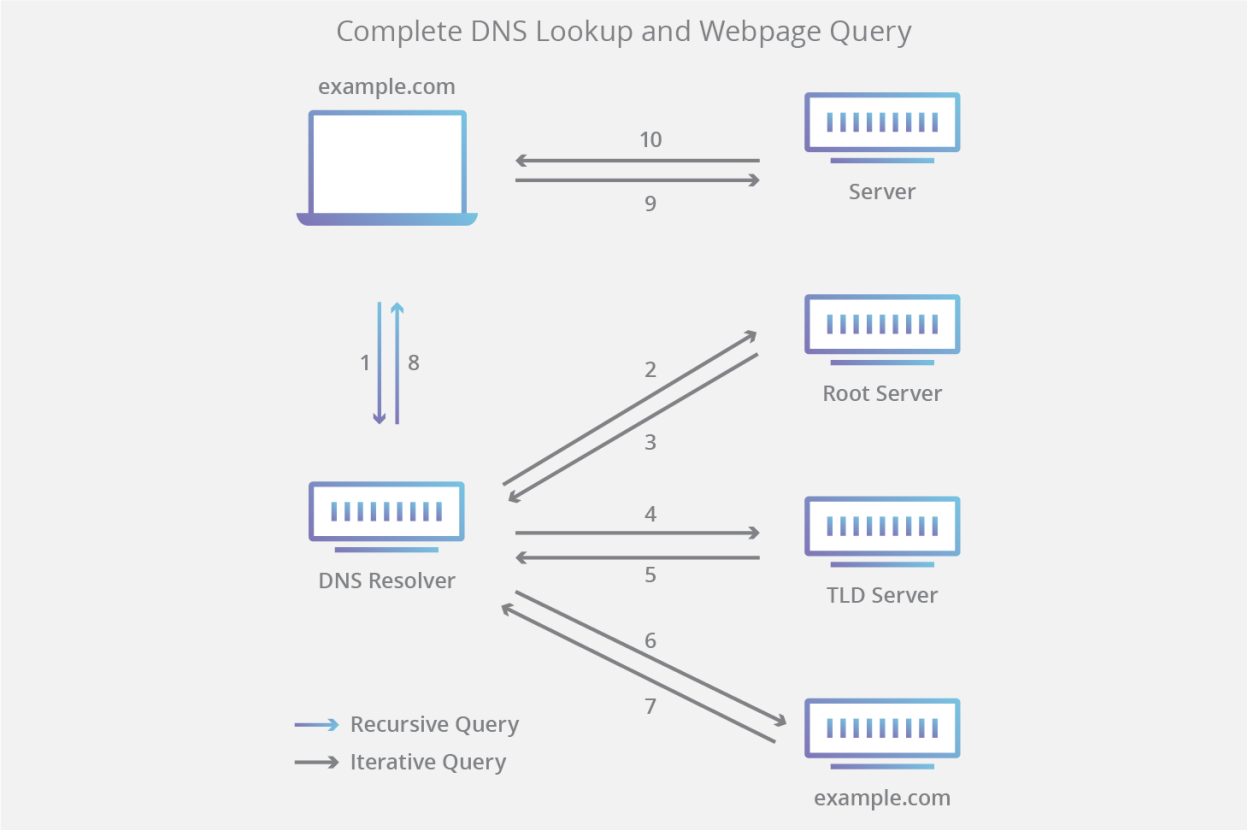
- Translates domain names to IP addresses, thus eliminating the need for humans to memorize IP addresses

DNS Servers

- DNS recursor: receives queries from client machines (through applications such as web browsers), then makes additional requests to satisfy the DNS query
    - Analogy: librarian who is asked to find a particular book
- Root nameserver: First step in resolving host names into IP addresses, pointing to more specific locations
    - Analogy: index that points to different racks of books
- TLD (top level domain) nameserver: typically resolves the last portion of a hostname (ex. “com”)
    - Analogy: specific rack of books
- Authoritative nameserver: Last stop in nameserver query, returns the IP address for the requested hostname back to DNS recursor that made the initial request
    - Analogy: dictionary on a rack of books, in which a specific name can be translated
- Note: for queries for a subdomain (ex. foo.example.com), an additional nameserver is added after the authoritative nameserver, responsible for storing the subdomain’s CNAME record.

DNS Lookup

1. A user types ‘example.com’ into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.).
3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain’s nameserver, example.com.
6. The recursive resolver sends a query to the domain’s nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially. Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:
9. The browser makes a HTTP request to the IP address.
10. The server at that IP returns the webpage to be rendered in the browser.



Note: DNS lookup info can be cached locally in the querying computer or remotely in the DNS infrastructure, thus allowing steps to be skipped in the DNS lookup process.

Types of DNS Queries:

- Recursive Query: DNS client requires that DNS server with requested resource record (or error message).
- Iterative Query: DNS client allows DNS server to return the best answer it can (ex. A referral to another DNS server for a lower level of domain namespace).
- Non-Recursive Query: DNS client queries DNS server that it already has access to because either its authoritative for the record or the record exists inside its cache.

DNS Caching: temporarily store data to improve efficiency

- Browser DNS caching
- Operating System level DNS caching
- Recursive resolver DNS caching

Sources:

- https://www.cloudflare.com/learning/dns/what-is-dns/

TCP/IP Addressing and Subnetting:

- General Overview
  - Able to connect networks of different sizes and different type systems
  - 3 main classes w/ predefined sizes, each of which can be further divided into subnetworks
- The IP Address
  - 32-bit number that unique identifies a host on TCP/IP network
  - 4 octets divided by periods, each octet is eight binary digits (so 8 bits)
  - Divided into two sections, the network address and the host address
  - When routers pass data they first pass data to the right network, then to the appropriate host
- Subnet Mask
  - Additional 32-bit number used to split the IP address into the network address and the host address
  - All 1's means network; all 0's means host
    - Ex. 11111111.11111111.11111111.00000000 means that the IP address is split as Network.Network.Network.Host
  - Other common subnets:
    - 255.255.255.192 = 11111111.11111111.11111111.11000000
    - 255.255.255.224 = 11111111.11111111.11111111.11100000
- Network Classes: 3 main classes allocated by the InterNIC (organization that administers Internet)
  - Class A:
    - 0-126 as first octet (first bit of first octet is 0)
    - 127.x.x.x is restricted for loopback IP addresses (points back to computer's TCP/IP configuration; useful when client software needs to communicate with server software on the same computer; similar to ping, allows users to test own network)
    - Default subnet mask: 255.0.0.0
    - 2^7-2 networks and 2^24-2 hosts
  - Class B:
    - 128-191 as first octet (first two bits of first octet 10)
    - Default subnet mask: 255.255.0.0
    - 2^14 network addresses and 2^16-2 host addresses
  - Class C:
    - 192-223 as first octet (first three bits of first octet set to 110)
    - Default subnet mask: 255.255.255.x
    - 2^21 network addresses and 2^8-2 host addresses
- Subnetting
  - Further dividing classes by "donating" bits from the host address to the network address

    - Ex. 255.255.255.192 “donates” 2 bits, thus splitting a single network of 254 hosts into 4 networks of 62 hosts
    - Note: The reason you subtract 2 is because binary addresses w/ host portion of all ones (broadcast address – broadcasts message to all hosts on network) and all zeros (only specify network) are invalid.
- Default Gateway
    - Router that is responsible to for transferring data between networks.
    - When a host tries to communicate with another device with TCP/IP, it first determines whether or not the destination is a local host or remote host based on its own IP address, destination IP address, and subnet mask.
- Public vs Private
    - Private IP address range:
        - 10.0.0.0 to 10.255.255.255
        - 172.16.0.0 to 172.31.255.255
        - 192.168.0.0 to 192.168.255.255
    - Computer (private IP address) -> Router (public IP address) -> ISP
- Virtual Private Networks
    - Hide IP address from the websites you visit + Encrypt data so that it cannot be accessed by ISP