Networking

Domain Name System (DNS)

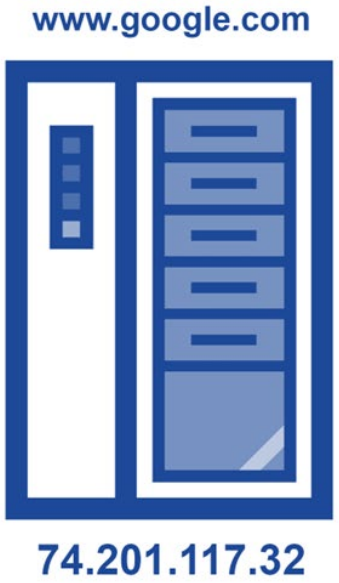
Domain Name System (DNS)

- Guiding Question: How does the Domain Name System (DNS) translate human-readable domain names into machine-friendly IP addresses, and why is this process crucial for internet functionality?

- Students will:
  - Explain the purpose of DNS and how it facilitates internet communication.
  - Describe the steps involved in the DNS name resolution process.
  - Identify and define key types of DNS records (A, AAAA, CNAME, MX, TXT, NS, PTR).
  - Differentiate between forward and reverse DNS zones and their functions.

Name Resolution

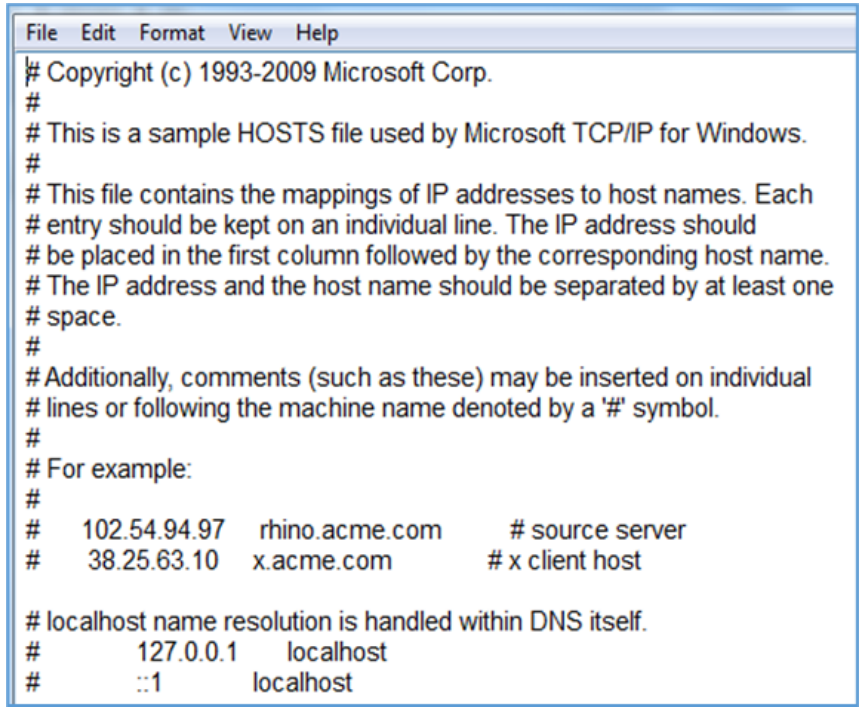
- While computers use MAC addresses and IP addresses, humans are more comfortable with text names.
- To get from a website name to an IP address, you must have someone do the translation. This is called Name Resolution.



Name Resolution

Option #1: local HOSTS file

- The HOSTS file is a listing of IPv4 addresses and matching hostnames.
- The file is stored locally on the device so it can be easily edited.
  - **Windows location:** *\Windows\system32\drivers\etc*
- Problem: Keeping all device HOSTS files up to date with Internet addresses would be impossible!



Name Resolution (cont'd)

Option #2: Domain Name System (DNS)

- DNS is a database that is used to map Internet names to their corresponding IP addresses.
- Translates names like google.com into IP addresses like 142.251.40.238
- Without DNS, we'd have to remember a bunch of numbers to visit websites, or we would have to constantly update the HOSTS file on every computer.
- DNS server address comes with DHCP lease info.

DNS & FQDN

- A **DNS** server will dynamically provide hostname to IP address resolution.
- The hostname is the name of the website server.
  - Note that the hostname must meet FQDN format.
- **Fully Qualified Domain Name** (FQDN)
  - FQDN format: `host.yourdomain.top-leveldomain`
  - Top-level domain: `.com` `.net` `.edu` `.gov` `.org` `.mil` `.int`
  - **Examples:**
    - `www.cyber.org`
    - `csaw.poly.edu`
    - `help.ubuntu.com`

DNS Steps

Step 1: Type a web address in your browser.

Step 2: The device asks a DNS server for the IP address.

Step 3: If that server doesn't know, it asks others—up to the root server.

Step 4: The IP address comes back, and the device is connected.

Step 5: The info gets saved (cached) for next time.

DNS Records

- There are several DNS records types that a domain can configure for their DNS settings.
  - **A Record:** will return info as an IPv4 address.
  - **AAAA Record:** will return info as an IPv6 address.
  - **CNAME:** Creates a nickname (aka alias) for a domain.
  - **MX:** Returns info on email servers for a domain.
  - **NS:** Shows who is the admin in charge of the domain.
  - **PTR:** Reverse lookup (IP → name).
  - **TXT:** Stores extra info, often for security.

DNS Zones

- DNS Zones must be configured to deal with the 2 types of DNS queries:
  - **Forward Zone:** translates domain names to IP addresses. (most common)
  - **Reverse Zone:** translates IP addresses to domain names.
- Zones help split up the work of DNS across multiple servers for scalability and reliability.

DNS Servers Types

- **Recursive DNS Server:** Finds IP addresses by asking other servers.
- **Authoritative DNS Server:** Gives official answers for a domain.
- **Primary Server:** Holds the original zone data.
- **Secondary Servers:** A read-only backup of the primary server.
- **Non-Authoritative Server:** Gives answers from a saved (cached) copy.

DNS Attacks

- Because DNS is a key part of how we access websites, it's a popular target for cyber attacks.
- Here are two common ways attackers try to take advantage of DNS:
  - **DNS Spoofing (Cache Poisoning):**
    - An attacker tricks a DNS server into saving a fake IP address for a real website.
    - You type in a real web address (like www.bank.com), but you get sent to a fake site that looks real—and can steal your info.
  - **Adversary-in-the-Middle (AITM) Attack:**
    - An attacker intercepts your DNS request and changes the response.
    - You think you're visiting a trusted site, but you're not.

DNS Security & Privacy

- Advanced features are available to help secure DNS.
- Security - to stop interference in the name resolution response:
  - **DNSSEC:** Adds a digital signature to make sure data is authentic, that it really comes from the indicated sender.
- Privacy - to stop anyone from viewing what websites you are visiting:
  - DoH (DNS over HTTPS): Encrypts DNS using web traffic.
  - DoT (DNS over TLS): Encrypts DNS using a secure port.