1. Define DNS (Domain Name System). What is its primary function in a network?

What is DNS (Domain Name System)?

The **Domain Name System (DNS)** is a hierarchical and decentralized naming system that translates **human-friendly domain names** (e.g., `www.google.com`) into **IP addresses** (e.g., `142.250.183.206`) that computers use to identify each other on a network.

Primary Function of DNS in a Network

The main function of DNS is **to resolve domain names into IP addresses**, allowing users to access websites and network services without memorizing numerical IP addresses.

How DNS Works (Step-by-Step Resolution Process)

1. **User Enters a Domain Name** – The user types a URL (`www.example.com`) into a browser.
2. **Browser Checks Cache** – The browser checks if it has recently resolved this domain; if not, it queries the DNS server.
3. **Query Sent to Recursive DNS Resolver** – The ISP's **recursive resolver** checks its cache or forwards the query to the next DNS server.
4. **Root Server Lookup** – If not cached, the resolver queries a **Root DNS server**, which directs it to the appropriate **Top-Level Domain (TLD) server** (e.g., `.com`, `.org`).
5. **TLD Server Lookup** – The TLD server points to the **Authoritative Name Server** for the domain (`example.com`).
6. **Authoritative Name Server Response** – This server provides the correct **IP address** for the domain.
7. **Browser Connects to the Web Server** – The browser uses the retrieved IP to load the website.

2. What are some common security threats to DNS servers?

Common DNS Security Threats

1. **Fake DNS (DNS Spoofing)** – Hackers change website addresses to trick you.

2. **Too Many Requests (DDoS Attack)** – Attackers flood the DNS server, making websites slow or crash.

3. **Hidden Malware (DNS Tunneling)** – Hackers hide viruses inside DNS requests.

4. **DNS Hijacking** – Hackers change your internet settings to take you to fake websites.

5. **Fake Website Requests (NXDOMAIN Attack)** – Attackers overload DNS by asking for websites that don't exist.

6. **Domain Theft (Registrar Hijacking)** – Hackers steal your website's domain name.

7. **Intercepting DNS Queries (MITM Attack)** – Hackers listen in and change your requests.

3. Case Study: A media company wants to serve video content using multiple geographically distributed servers. • How can they implement GeoDNS for better content delivery? • What DNS configurations should be used to direct traffic based on location?

1. Implementing GeoDNS for Better Content Delivery

How it Works:

- GeoDNS detects the user's location based on their **IP address** and directs them to the nearest server.
- This reduces **latency**, improves **load balancing**, and enhances **user experience** by serving content from the closest data center.
- Helps in managing **traffic spikes** by distributing requests efficiently.

Steps to Implement:

1. **Use a GeoDNS Service** – Cloudflare, AWS Route 53, Google Cloud DNS, or NS1.
2. **Set Up Geographically Distributed Servers** – Deploy video servers in **North America, Europe, Asia, etc.**
3. **Configure GeoDNS Rules** – Map user IP locations to the closest server.
4. **Use CDN for Caching** – Improves speed by storing video content closer to users.
5. **Monitor & Optimize** – Regularly check server loads and adjust routing.

---

2. DNS Configurations for Location-Based Traffic Routing

Key DNS Records Used:

- **A/AAAA Records** – Assigns IP addresses to domain names.
- **CNAME Record** – Points users to a CDN or regional subdomains.
- **GeoDNS Rules** – Directs traffic based on location.

Example DNS Configuration (Using AWS Route 53):

1. **Create Geolocation Routing Records:**
   - **North America → `us.example.com` → 192.168.1.1**
   - **Europe → `eu.example.com` → 192.168.2.1**
   - **Asia → `asia.example.com` → 192.168.3.1**
2. **Set Up Failover & Latency-Based Routing**
   - If a server is down, traffic is redirected to the next closest server.
3. **Use a CDN (Cloudflare, Akamai, AWS CloudFront)**
   - CDN caches video content near users, reducing load times.