Lecture Four

Domain Name System (DNS)

Understanding the Internet's Phonebook

Dr. Tarfa Yaseen Hamed

Department of Networks

College of Computer Science and Mathematics

University of Mosul

2025

Introduction to DNS

- **DNS** is a system that translates human-readable domain names (e.g., www.example.com) into machine-readable IP addresses (e.g., 192.0.2.1).
- **Purpose**: Simplifies access to websites and services by eliminating the need to memorize IP addresses.
- **Importance**: DNS is essential for the functioning of the Internet, enabling communication between devices.
- **Example**: "When you type www.google.com, DNS translates it to an IP address like 172.217.10.46."

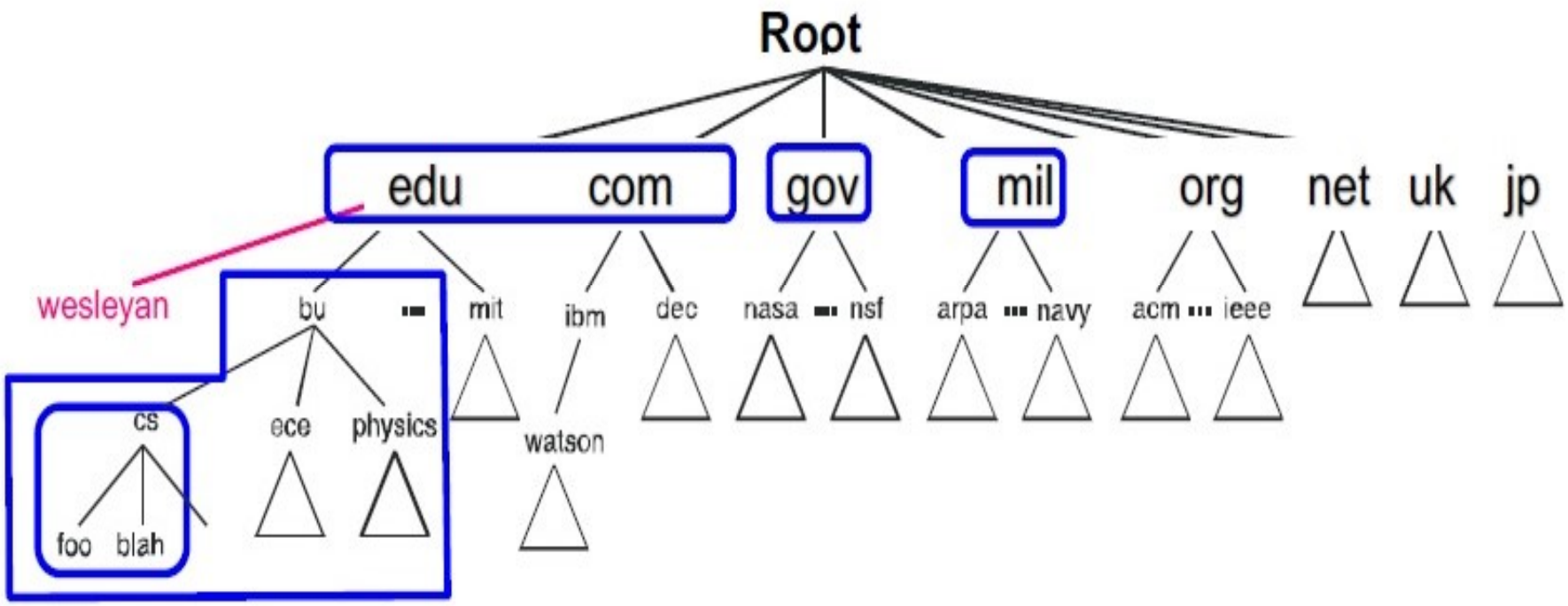
History of DNS

- **Early Internet**: Devices were identified using numeric IP addresses.
- **Problem**: IP addresses are hard to remember and not user-friendly.
- **Solution**: DNS was introduced in 1983 by Paul Mockapetris (RFC 882 and RFC 883).
- **Evolution**: DNS has evolved to support the growing complexity and scale of the Internet.

DNS Architecture

- DNS is hierarchical and decentralized.
- Components:
  1. **Root Level**: 13 root servers worldwide.
  2. **Top-Level Domains (TLDs)**: Managed by organizations like ICANN.
  3. **Second-Level Domains**: Registered by individuals or organizations.
  4. **Subdomains**: Created by domain owners (e.g., blog.example.com).

Tree structure of DNS hierarchy



DNS Components

1. **Domain Names**: Human-readable addresses (e.g., www.google.com).
2. **Name Servers**: Servers that store DNS records (e.g., authoritative servers).
3. **Resolvers**: Software that queries name servers to resolve domain names (e.g., DNS clients).
4. **Example:** "When you visit a website, your resolver queries the name server to get the IP address."

Domain Name Structure

- Example: www.example.com
  - Root: (.) [implied]
  - TLD: .com
  - Second-Level Domain: example
  - Subdomain: www
- "Each part of the domain name represents a level in the DNS hierarchy."

Types of Top-Level Domains (TLDs)

- **Generic TLDs (gTLDs)**: .com, .org, .net, etc.
- **Country Code TLDs (ccTLDs)**: .us, .uk, .in, etc.
- **Sponsored TLDs**: .edu, .gov, .mil, etc.
- **New gTLDs**: .app, .blog, .ai, etc.
- **Example**: "Google uses .com, while the UK government uses .gov.uk."

DNS Hierarchy

- **Root Level**: 13 root servers managed by organizations like ICANN.
- **TLD Level**: Managed by registries (e.g., Verisign for .com).
- **Authoritative Level**: Managed by domain owners or registrars.

DNS Resolution Process

1. User enters a domain name

   (e.g., www.example.com).

2. Resolver queries the root server.

3. Root server directs to the TLD server.

4. TLD server directs to the authoritative server.

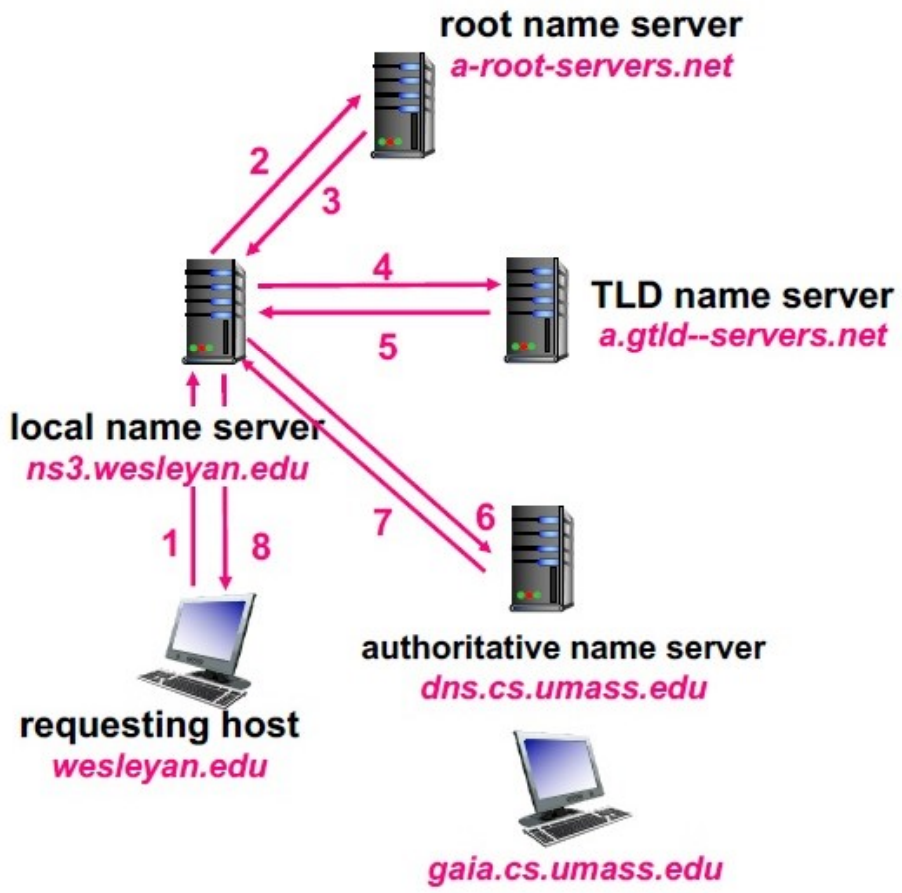
5. Authoritative server provides the IP address.

6. Resolver returns the IP address to the user.

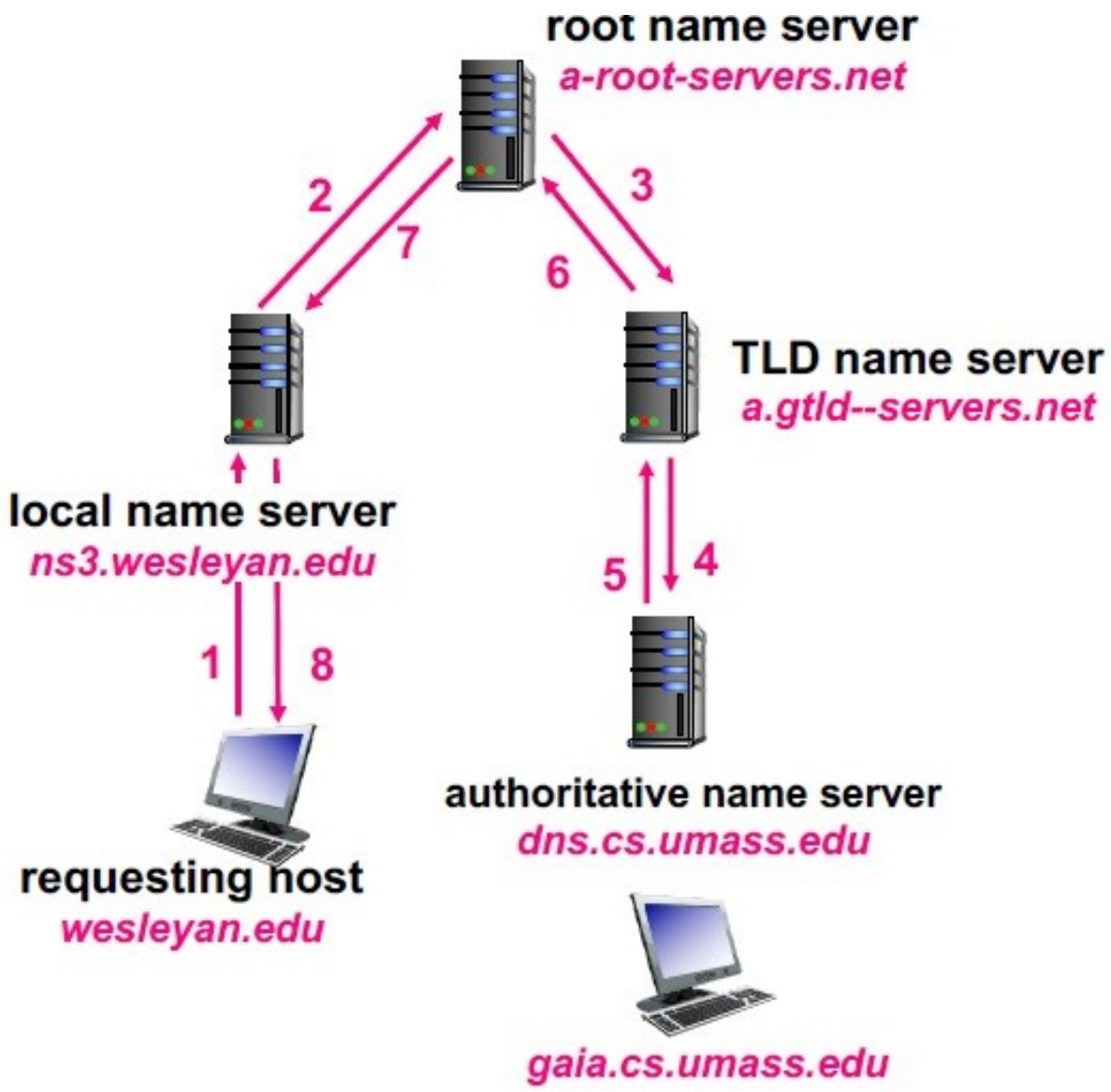
Recursive vs Iterative Queries

- **Recursive Query**: Resolver handles all steps and returns the final answer.
- **Iterative Query**: Resolver queries each server step-by-step.
- Example: "Recursive queries are used by clients, while iterative queries are used by resolvers."

Iterative Name Resolution



Recursive Name Resolution



DNS Record Types

- **A Record**: Maps a domain to an IPv4 address.
- **AAAA Record**: Maps a domain to an IPv6 address.
- **CNAME Record**: Alias for a domain name.
- **MX Record**: Mail exchange server for email.
- **NS Record**: Authoritative name server for the domain.
- **TXT Record**: Text information (e.g., SPF records).
- Example: "A CNAME record can point www.example.com to example.com."

DNS Caching

- **Purpose**: Reduces load on DNS servers and speeds up resolution.
- **TTL (Time to Live):** Determines how long a record is cached.
- **Caching Resolvers**: Store DNS responses temporarily.
- **Example**: "If you visit a website multiple times, the resolver uses the cached IP address.”

DNS Security (DNSSEC)

- **Problem**: DNS is vulnerable to spoofing and cache poisoning.
- **Solution**: DNSSEC adds cryptographic signatures to DNS records to ensure authenticity.
- **Example**: "DNSSEC prevents attackers from redirecting users to malicious websites."

DNS Over HTTPS (DoH)

- **Problem**: Traditional DNS queries are unencrypted.
- **Solution**: DoH encrypts DNS queries using HTTPS for privacy and security.
- **Example**: "DoH is used by browsers like Firefox to protect user privacy."

DNS Over TLS (DoT)

- Similar to DoH but uses TLS encryption for DNS queries.
- Provides privacy and prevents tampering.
- Example: "DoT is commonly used in mobile networks."

Public DNS Servers

- **Examples**: Google DNS (8.8.8.8), Cloudflare DNS (1.1.1.1), OpenDNS.
- Benefits: Faster resolution, improved security, and privacy.
- Example: "Google DNS is a popular alternative to ISP-provided DNS servers."

DNS Tools

- **nslookup**: Queries DNS servers for records.
- **dig**: Advanced DNS query tool.
- **whois**: Provides domain registration details.
- **Example**: "Use nslookup www.example.com to find the IP address."

DNS in Practice

- **Domain Registration**: Process of acquiring a domain name.
- **DNS Hosting**: Managing DNS records for a domain.
- **Propagation**: Time taken for DNS changes to update globally.
- **Example**: "When you register a domain, you need to configure its DNS records."

Common DNS Issues

- **Misconfigured Records**: Incorrect A, CNAME, or MX records.
- **Propagation Delays**: Changes take time to reflect globally.
- **Cache Poisoning**: Malicious alteration of DNS cache.
- **Example**: "A misconfigured MX record can cause email delivery failures."

DNS and Load Balancing

- **Load balancing** is the process of distributing incoming network traffic across multiple servers to ensure no single server is overwhelmed.
- **Purpose**: Improves performance, reliability, and scalability of applications and websites.
- **Example**: A popular website like Amazon or Netflix uses load balancing to handle millions of users simultaneously.

How DNS Enables Load Balancing

- DNS can be used as a simple yet effective method for load balancing.
- **Mechanism**: DNS servers return different IP addresses for the same domain name, distributing traffic across multiple servers.
- **Example**: When users query www.example.com, the DNS server responds with one of several IP addresses (e.g., 192.0.2.1, 192.0.2.2, 192.0.2.3).

Types of DNS Load Balancing

1. **Round Robin DNS**:
   - The DNS server cycles through a list of IP addresses for each query.
   - Example:
     - **Query 1**: www.example.com → 192.0.2.1
     - **Query 2**: www.example.com → 192.0.2.2
     - **Query 3**: www.example.com → 192.0.2.3
   - **Advantage**: Simple to implement.
   - **Limitation**: Does not account for server load or health.

Types of DNS Load Balancing (cont.)

2. **Weighted Round Robin**:
   - Assigns weights to servers based on their capacity or performance.
   - **Example**: A more powerful server may receive more traffic than a less powerful one.
   - **Advantage**: Better distribution of traffic based on server capabilities.

Types of DNS Load Balancing (cont.)

3. **Geolocation-Based DNS**:
   - Directs users to the nearest server based on their geographic location.
   - **Example**: A user in Europe is directed to a server in Europe, while a user in Asia is directed to a server in Asia.
   - **Advantage**: Reduces latency and improves user experience.

Types of DNS Load Balancing (cont.)

4. **Failover DNS**:
   - Automatically redirects traffic to a backup server if the primary server fails.
   - **Example**: If 192.0.2.1 is down, traffic is redirected to 192.0.2.2.
   - **Advantage**: Ensures high availability.

Benefits of DNS Load Balancing

1. **Improved Performance**:
   - Distributes traffic evenly, preventing server overload.
2. **High Availability**:
   - Ensures services remain available even if one server fails.
3. **Scalability**:
   - Easily add more servers to handle increased traffic.
4. **Reduced Latency**:
   - Geolocation-based DNS reduces the distance between users and servers.

DNS and Content Delivery Networks (CDNs)

- **Definition**: A CDN is a network of distributed servers that deliver web content (e.g., images, videos, scripts) to users based on their geographic location.
- **Purpose**: Reduces latency, improves load times, and ensures high availability of content.
- **Example**: Popular CDNs include Cloudflare, Akamai, and Amazon CloudFront.

How DNS Works with CDNs

- DNS plays a critical role in CDNs by directing users to the nearest or optimal server (also called an **edge server**).
- **Mechanism**:

1. A user requests content (e.g., an image or video) from a website.
2. The DNS resolver queries the CDN's authoritative DNS servers.
3. The CDN's DNS servers use geolocation and load information to determine the best edge server for the user.
4. The user is directed to the optimal edge server, which delivers the content.

Case Study: DNS Outages

- **Definition**: A DNS outage occurs when the Domain Name System fails to resolve domain names to IP addresses, making websites and services inaccessible.
- **Impact**: DNS outages can disrupt internet services, cause financial losses, and damage reputations.
- **Importance**: Understanding DNS outages helps in preventing and mitigating future incidents.

Causes of DNS Outages

1. **DDoS Attacks**:
   - Distributed Denial of Service (DDoS) attacks overwhelm DNS servers with traffic, causing them to crash.
   - Example: The 2016 Dyn DNS attack.
2. **Configuration Errors**:
   - Misconfigured DNS records or servers can lead to outages.
   - Example: Incorrect TTL settings or missing records.
3. **Hardware Failures**:
   - Server hardware failures can take DNS servers offline.
   - Example: Power outages or disk failures.

Causes of DNS Outages

4. **Software Bugs**:
   - Bugs in DNS software can cause unexpected behavior or crashes.
   - Example: A bug in BIND (a popular DNS software).
5. **Human Error**:
   - Mistakes during maintenance or updates can cause outages.
   - Example: Deleting critical DNS records accidentally.

Real-World Examples of DNS Outages

- **Example 1: The 2016 Dyn DNS Attack**
- **Cause**: A massive DDoS attack targeting Dyn, a major DNS provider.
- **Impact**:
  - Major websites like Twitter, Netflix, and GitHub were inaccessible for hours.
  - Financial losses for affected companies.
- **Lesson**: The need for robust DDoS protection and DNS redundancy.

Real-World Examples of DNS Outages (cont.)

- **Example 2: Google Outage (2020)**
- **Cause**: A configuration error in Google's DNS service.
- **Impact**:
  - Google services like Gmail, YouTube, and Google Drive were down for about an hour.
  - Millions of users affected globally.
- **Lesson**: Importance of thorough testing and validation of configuration changes.