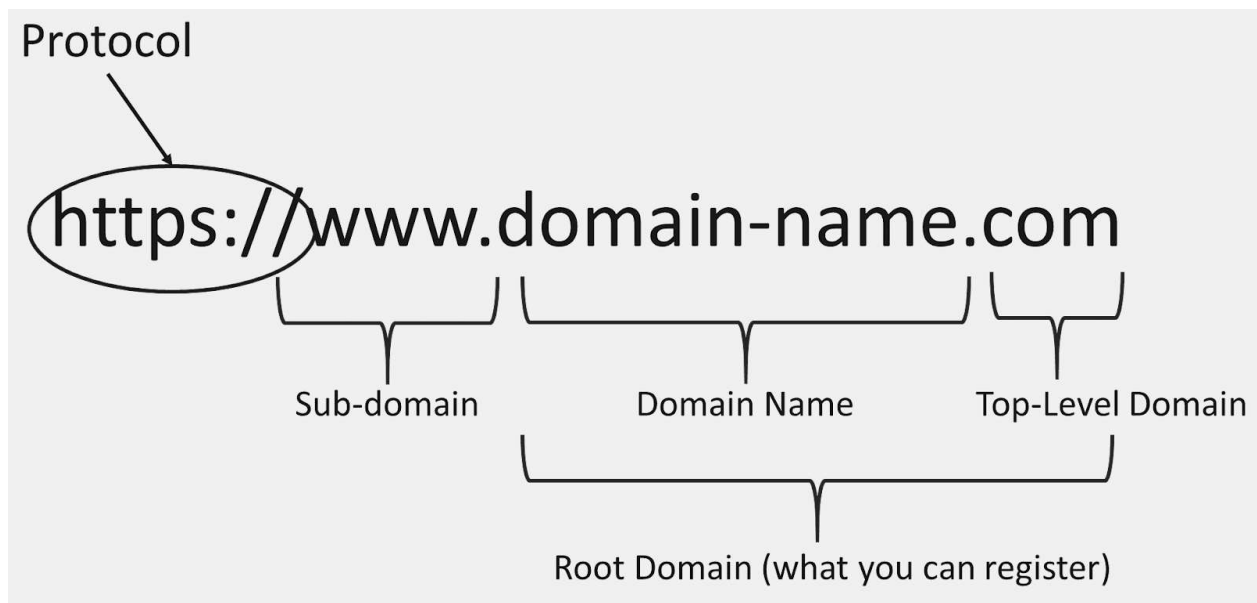


# Domain Names and DNS (Domain Name System)

## 1. Introduction to Domain Names

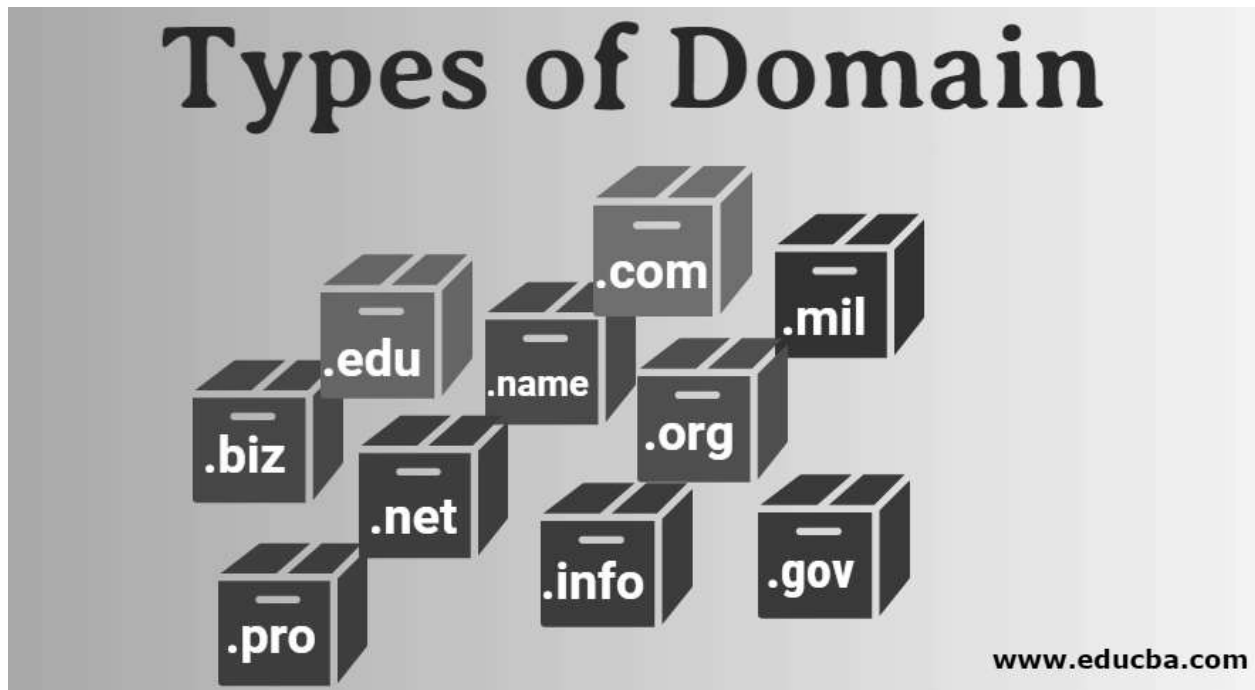
- **Definition:**
  - A domain name is a human-readable address used to access websites or other internet resources.
  - Example: `www.google.com` instead of `142.250.64.78`.
- **Purpose:**
  - Simplifies navigation on the internet.
  - Provides a memorable and user-friendly alternative to IP addresses.

## 2. Structure of a Domain Name



- Domain names are hierarchical and consist of several components separated by dots:
  - **Top-Level Domain (TLD):**
    - The highest part of a domain.
    - Examples: `.com`, `.org`, `.edu`, `.gov`.
  - **Second-Level Domain (SLD):**
    - The main part of the domain name, chosen by the owner.
    - Example: `google` in `google.com`.
  - **Subdomain:**
    - An optional prefix to the SLD.
    - Example: `mail.google.com` (where `mail` is the subdomain).

### 3. Types of Domains

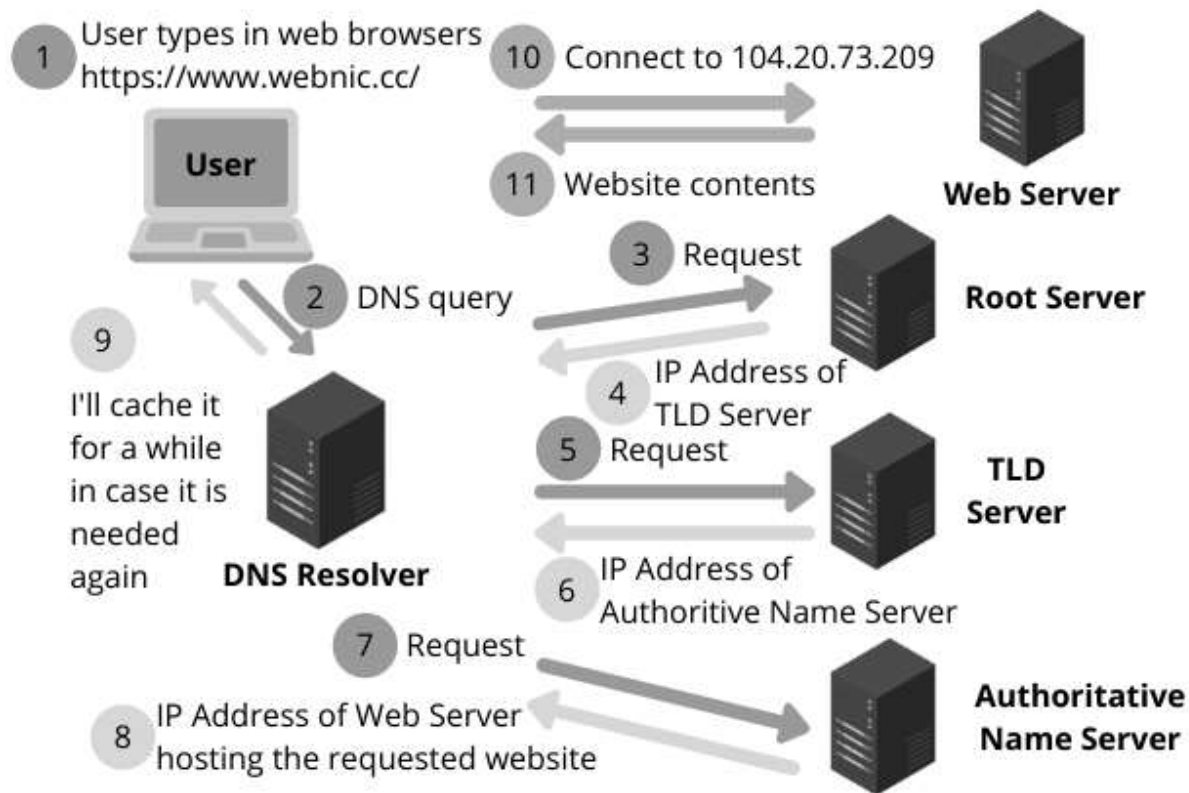


- **Generic Top-Level Domains (gTLDs):** Common and open to everyone (e.g., .com, .org, .net).
- **Country Code Top-Level Domains (ccTLDs):** Specific to a country or region (e.g., .us, .in, .uk).
- **Sponsored Top-Level Domains (sTLDs):** Restricted to specific organizations or industries (e.g., .edu, .gov).
- **Internationalized Domain Names (IDNs):** Support non-English scripts like Arabic, Chinese, or Hindi.

### 4. What is DNS (Domain Name System)?

- **Definition:**
  - DNS is a hierarchical system that translates human-readable domain names into machine-readable IP addresses.
  - Example: `www.google.com` → `142.250.64.78`.
- **Purpose:**
  - Acts as the internet's "phonebook."
  - Enables seamless navigation without needing to remember numerical IP addresses.

### 5. How DNS Works



- 1. User Request:** A user enters a domain name (e.g., `www.google.com`) into their browser.
- 2. DNS Query:** The browser sends a request to a DNS resolver to find the IP address associated with the domain.
- 3. Recursive Resolver:**
  - The resolver queries DNS servers in a hierarchical manner:
    - 1. Root DNS Server:** Directs the resolver to the appropriate TLD server (e.g., `.com`).
    - 2. TLD DNS Server:** Points to the authoritative server for the domain (e.g., `google.com`).
    - 3. Authoritative DNS Server:** Provides the IP address for the domain.
- 4. Response:** The resolver sends the IP address back to the browser.
- 5. Connection:** The browser uses the IP address to connect to the web server and retrieve the website.

## 6. Components of DNS

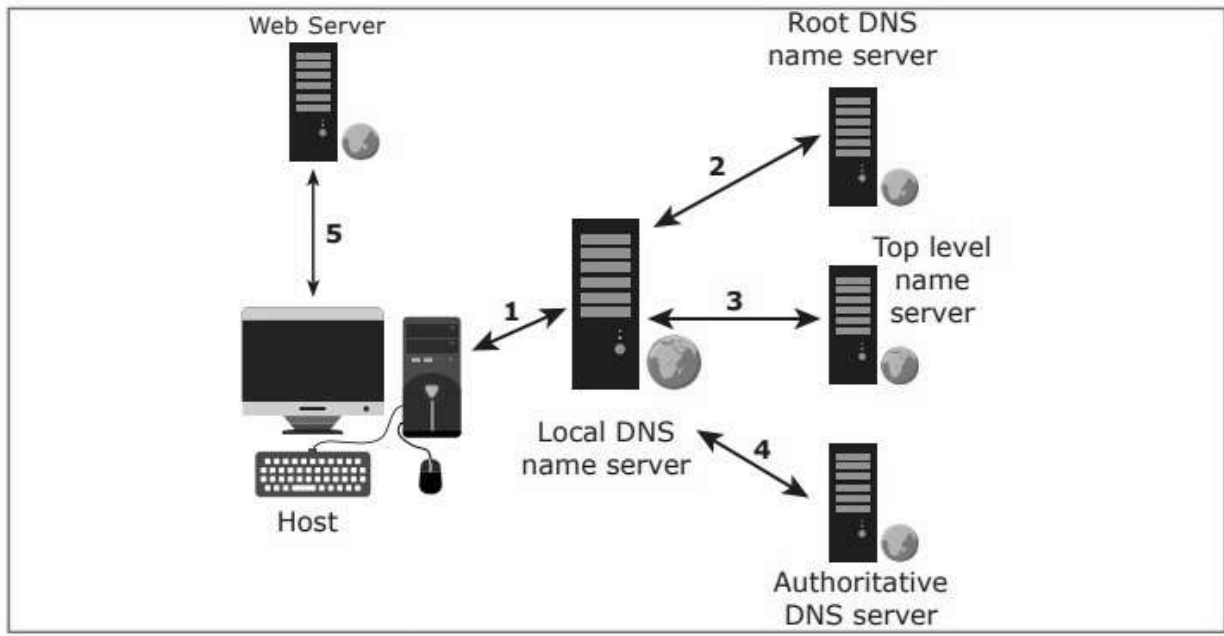


Figure 12.8 working structure of Name server

- **DNS Resolver:** The first point of contact for a DNS query, often managed by the user's ISP.
- **Root Server:** Directs queries to the appropriate TLD server; there are 13 root server clusters globally.
- **TLD Server:** Manages domains within a specific TLD (e.g., .com, .org).
- **Authoritative DNS Server:** Holds the actual mapping of domain names to IP addresses.

## 7. Types of DNS Records

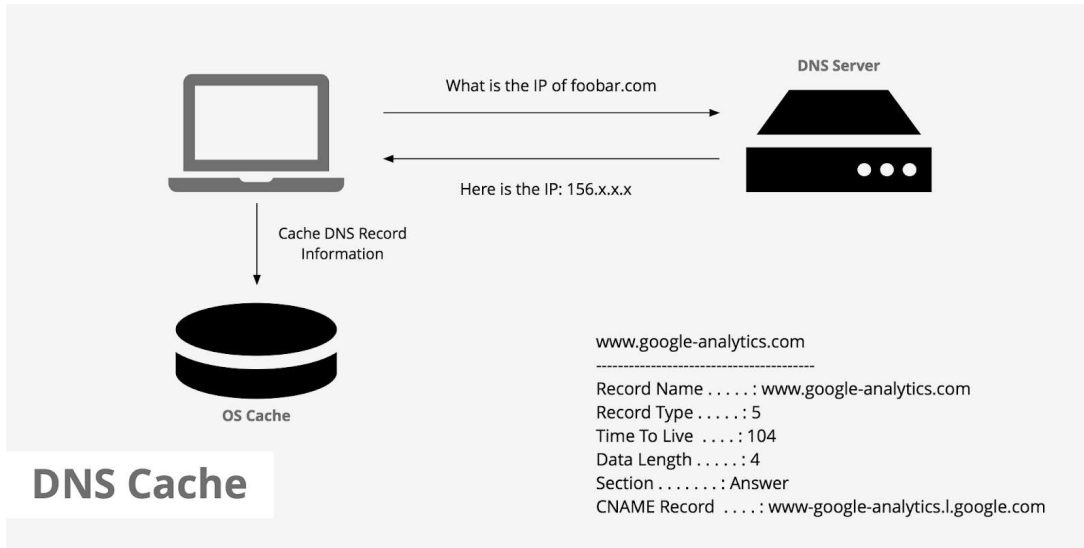
DNS RECORDS CHEAT SHEET - CONSTELLIX

<p><b>A (address)</b></p> <p><b>1</b> A (address) - Most commonly used to map a fully qualified domain name (FQDN) to an IPv4 address and acts as a translator by converting domain names to IP addresses. ✓</p>	<p><b>SOA (start of authority)</b></p> <p><b>5</b> SOA (start of Authority) - Stores information about domains and is used to direct how a DNS zone propagates to secondary name servers. ✓</p>	<p><b>SRV (service)</b></p> <p><b>9</b> SRV (service) - Allows services such as Instant messaging or VoIP to be directed to a separate host and port location. ✓</p>
<p><b>AAAA (quad A)</b></p> <p><b>2</b> AAAA (quad A) - Similar to A Records but maps to an IPv6 address (smartphones prefer IPv6, if available). ✓</p>	<p><b>NS (name server)</b></p> <p><b>6</b> NS (name server) - Specifies which name servers are authoritative for a domain or subdomains (these records should not be pointed to a CNAME). ✓</p>	<p><b>SPF (sender policy framework)</b></p> <p><b>10</b> SPF (sender policy framework) - Helps prevent email spoofing and limits spammers. ✓</p>
<p><b>ANAME</b></p> <p><b>3</b> ANAME - This record type allows you to point the root of your domain to a hostname or FQDN. ✓</p>	<p><b>MX (mail exchange)</b></p> <p><b>7</b> MX (Mail eXchange) - Uses mail servers to map where to deliver email for a domain (should point to a mail server name and not to an IP address). ✓</p>	<p><b>PTR (pointer)</b></p> <p><b>11</b> PTR (pointer) - A reverse of A and AAAA records, which maps IP addresses to domain names. These records require domain authority and can't exist in the same zone as other DNS record types (put in reverse zones). ✓</p>
<p><b>CNAME</b></p> <p><b>4</b> CNAME (Canonical Name) - An alias that points to another domain or subdomain, but never an IP address. Alias record mapping FQDN to FQDN, multiple hosts to a single location. This record is also good for when you want to change an IP address over time as it allows you to make changes without affecting user bookmarks, etc. ✓</p>	<p><b>TXT (text)</b></p> <p><b>8</b> TXT (text) - Allows administrators to add limited human and machine-readable notes and can be used for things such as email validation, site, and ownership verification, framework policies, etc. doesn't require specific formatting. ✓</p>	<p><b>QUICK TIP</b></p> <p><b>12</b> Tip: Always check for typos and mistakes when entering your DNS record information, especially your IPs. The Zone Config File is a good place to check your work and spot any mistyped information. ✓</p>

CONSTELLIX

- **A Record (Address Record):** Maps a domain to an IPv4 address.
- **AAAA Record:** Maps a domain to an IPv6 address.
- **CNAME Record (Canonical Name):** Points a domain to another domain (used for subdomains).
- **MX Record (Mail Exchange):** Directs emails to mail servers.
- **TXT Record:** Stores text information for verification purposes (e.g., SPF, DKIM for email security).

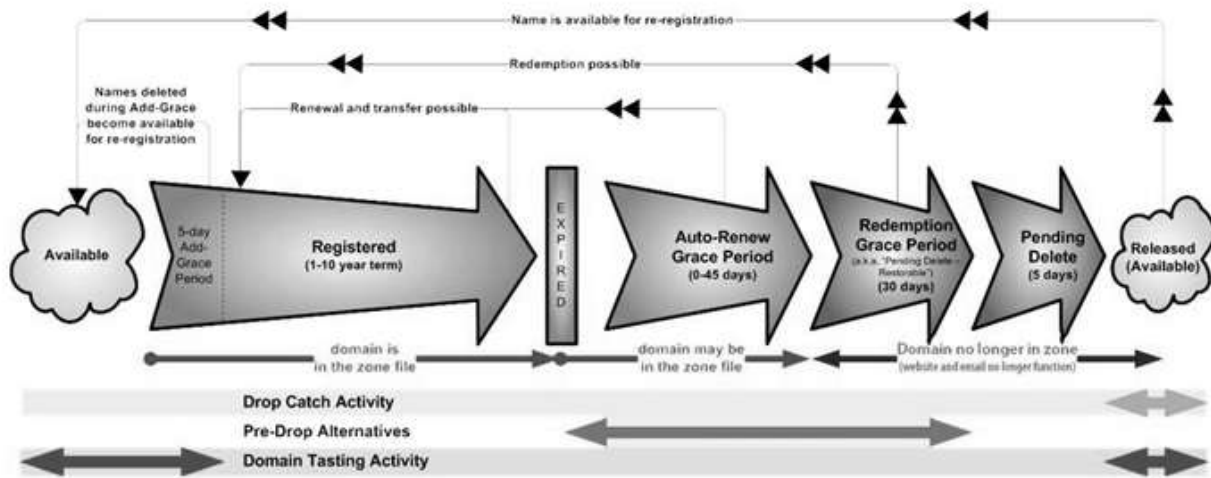
## 8. DNS Cache



- **Definition:** Temporary storage of DNS query results on devices or servers to speed up subsequent requests.
- **Benefits:**
  - Reduces query time.
  - Decreases load on DNS servers.
- **Potential Issues:** Cached data can become outdated, leading to resolution errors.

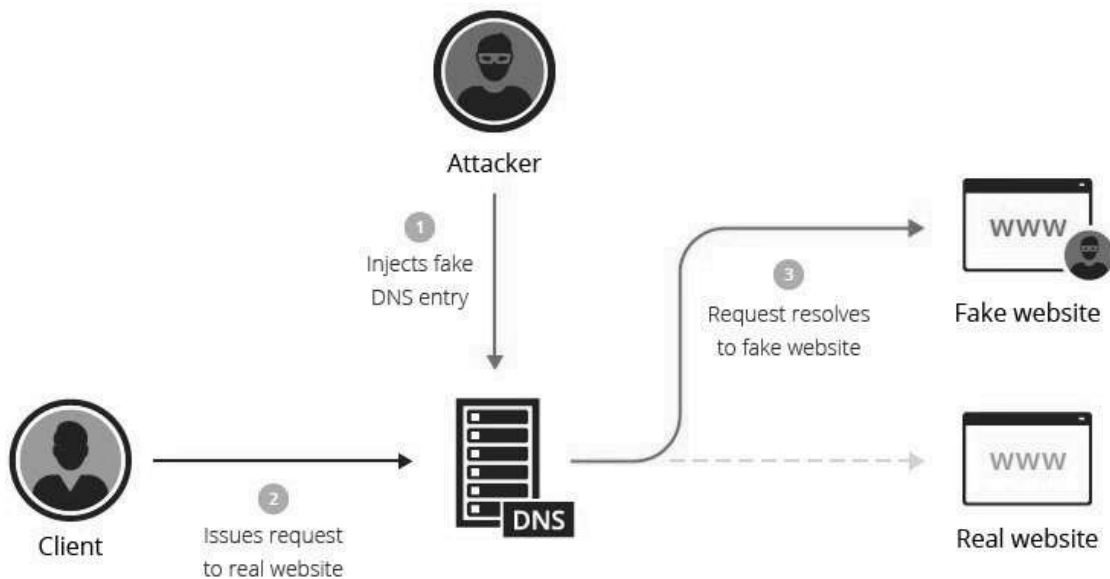
## 9. Domain Registration

- **Process:**
  - Choose a domain name.
  - Check its availability through a registrar (e.g., GoDaddy, Namecheap).
  - Register the domain and configure DNS settings.
- **Domain Lifecycle:** Available → Registered → Active → Expired → Grace Period → Deleted.

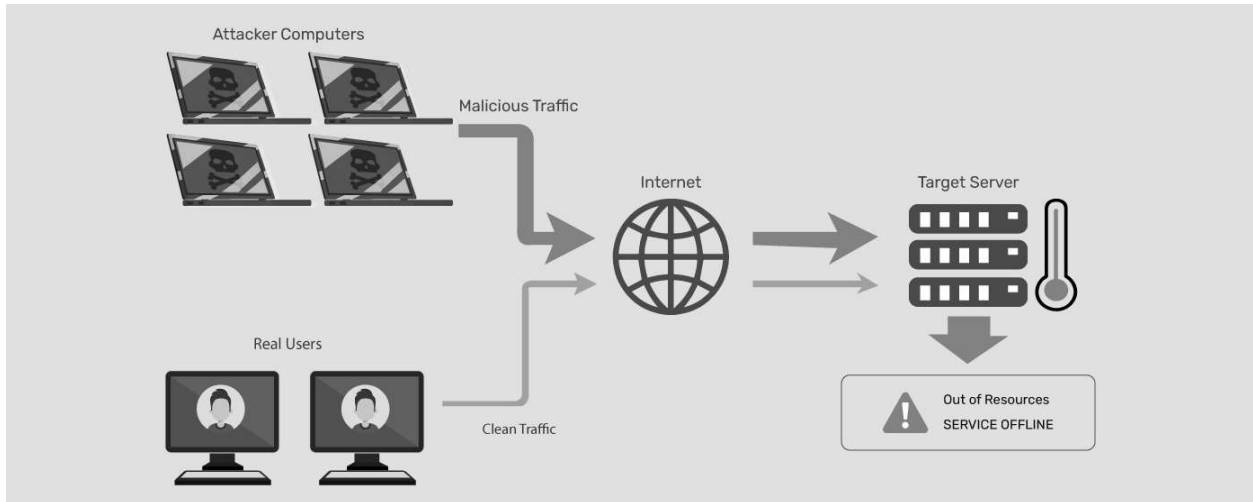


## 10. Security in DNS

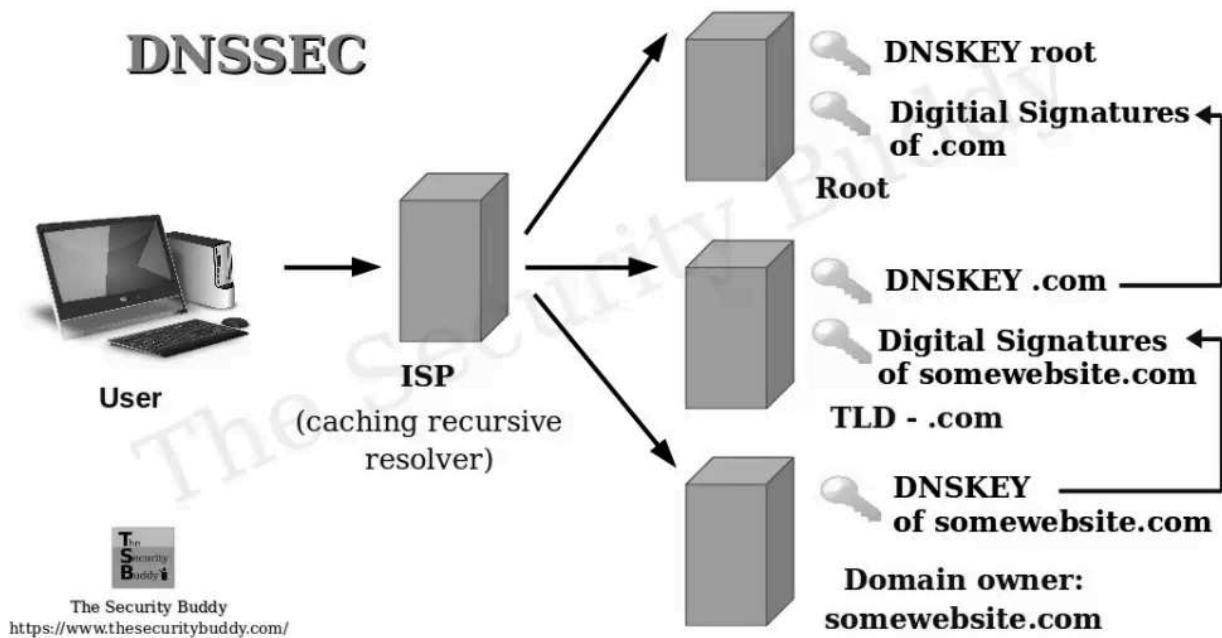
- **DNS Vulnerabilities:**



- **DNS Spoofing/Cache Poisoning:** Attackers provide false DNS responses to redirect users to malicious sites.



- **DDoS Attacks:** Overwhelming DNS servers with traffic to disrupt service.
- **Mitigation Techniques:**



- **DNSSEC (Domain Name System Security Extensions):** Adds authentication to DNS responses using digital signatures.

## DNS-over-HTTPS

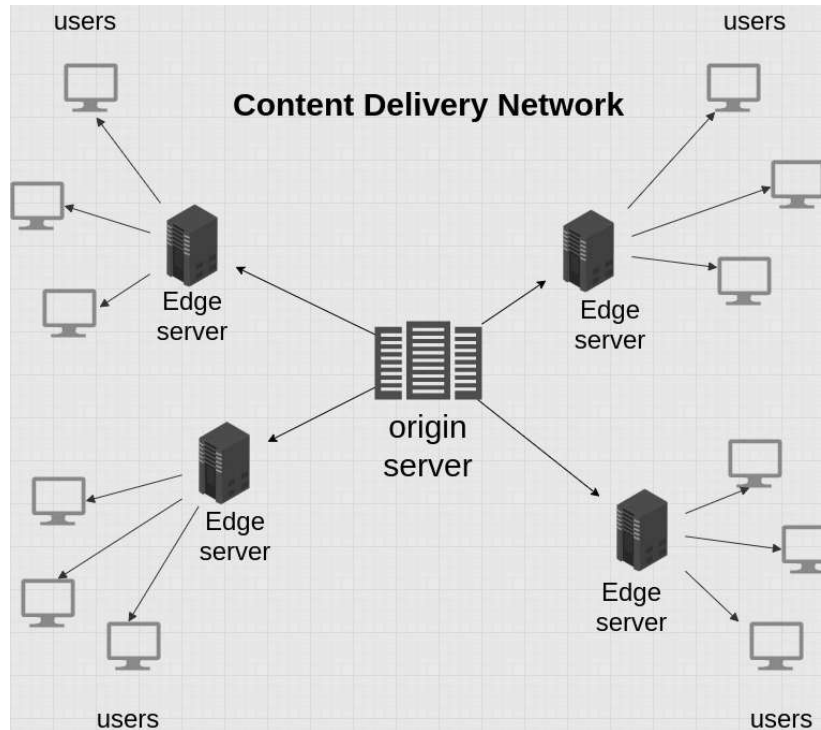


## DNS-over-HTTPS

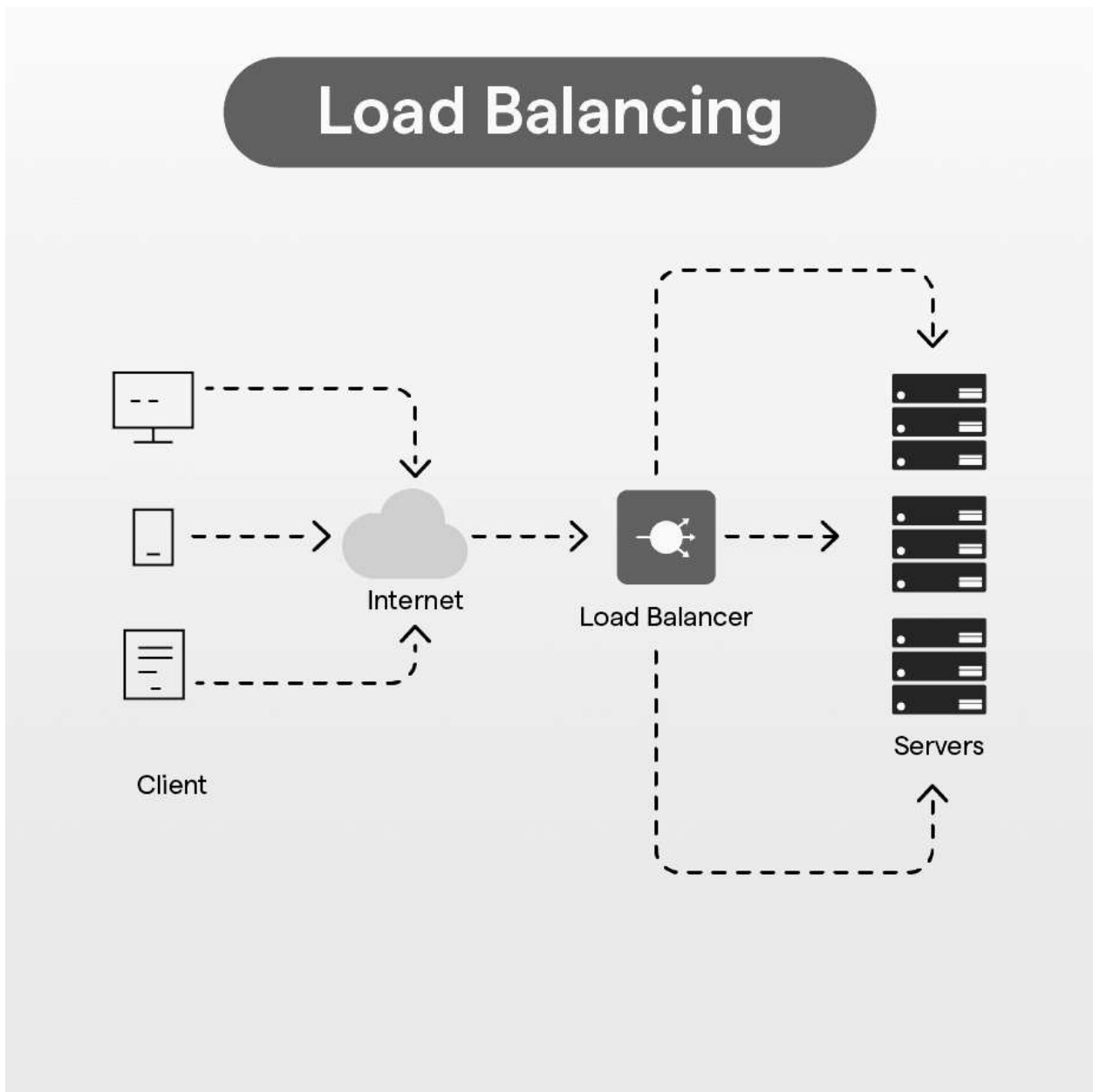


- **HTTPS DNS (DoH):** Encrypts DNS queries for privacy.

## 11. DNS in Modern Applications



- **Content Delivery Networks (CDNs):** Use DNS to route users to the nearest server for faster content delivery.



- **Load Balancing:** DNS helps distribute traffic among multiple servers to ensure reliability.
- **Cloud Computing:** Domain names map to virtual resources in cloud environments.