

DNS and CDN

ELEC-C7420 Basic Principles in Networking



Aalto-yliopisto
Sähkötekniikan
korkeakoulu

Yu Xiao

2022.02.08

Learning Outcomes

After this lecture, you should be able to

- **Describe how DNS query works**
- **Describe the basics of Content Delivery Network (CDN)**

Domain Names

www.aalto.fi

Mobilecloud.aalto.fi

Research.comnet.aalto.fi

www.youtube.com

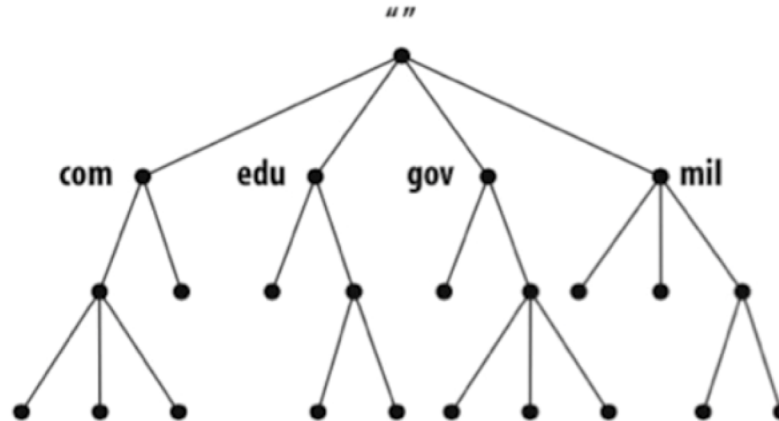
icann.org

...

An important function of domain names is to provide easily recognizable and memorable names to numerically addressed Internet resources.

Domain Names

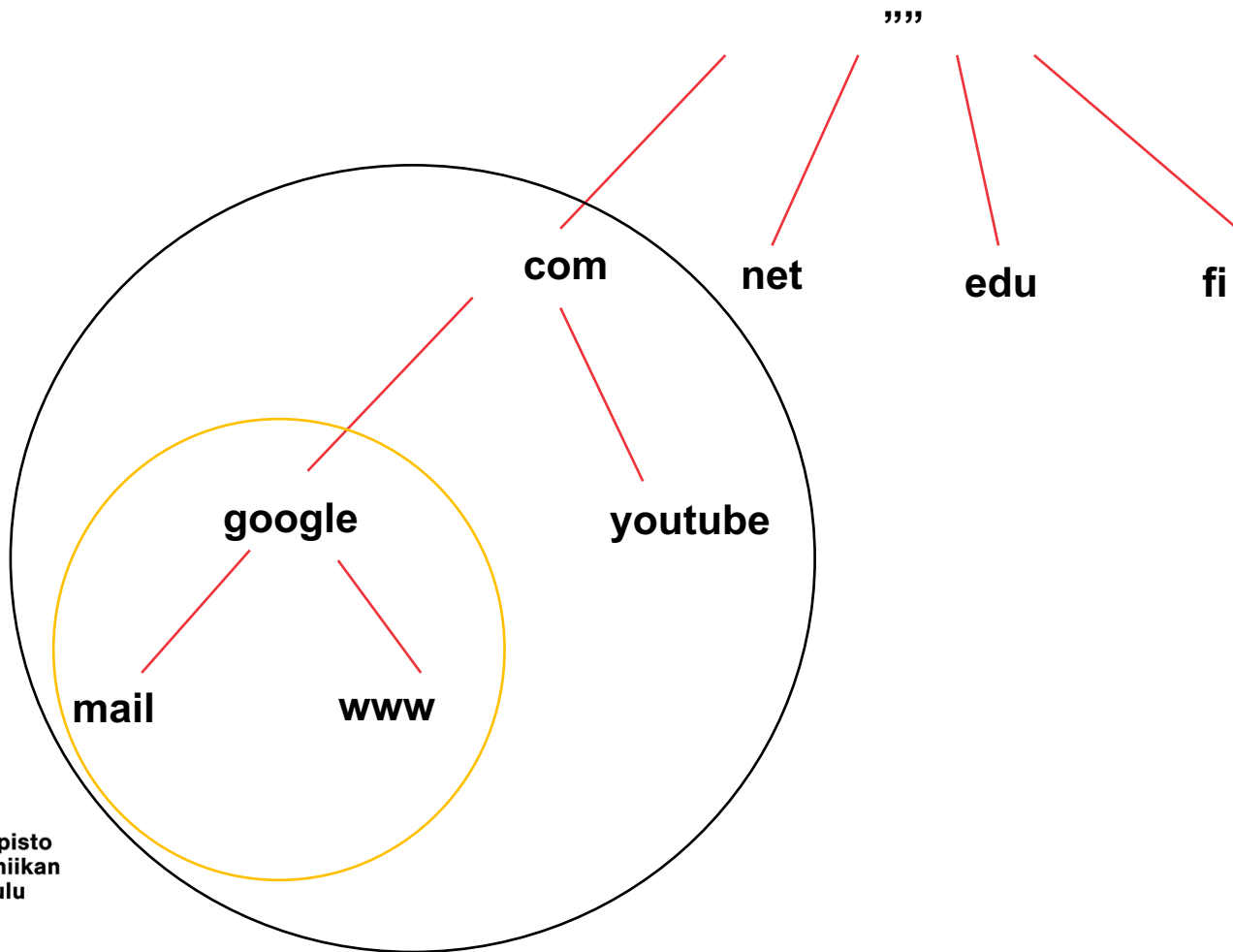
- Domain names → resources (e.g., computers, websites)
- Paths in an inverted tree
 - An inverted tree is made up of nodes and links between nodes
 - Each node is connected to its parent by a single link
 - One node can be parent to arbitrarily many children



Labels

- Each node has a label, between 0 and 63 bytes in length
- The root node (at the top) has a special, reserved label, written “” (for a zero-length label)
- Otherwise, the main restriction is that all of the children of a node have different labels
- **Domain name: the series of labels from the node to the root, read with dots separating the labels**

Domain

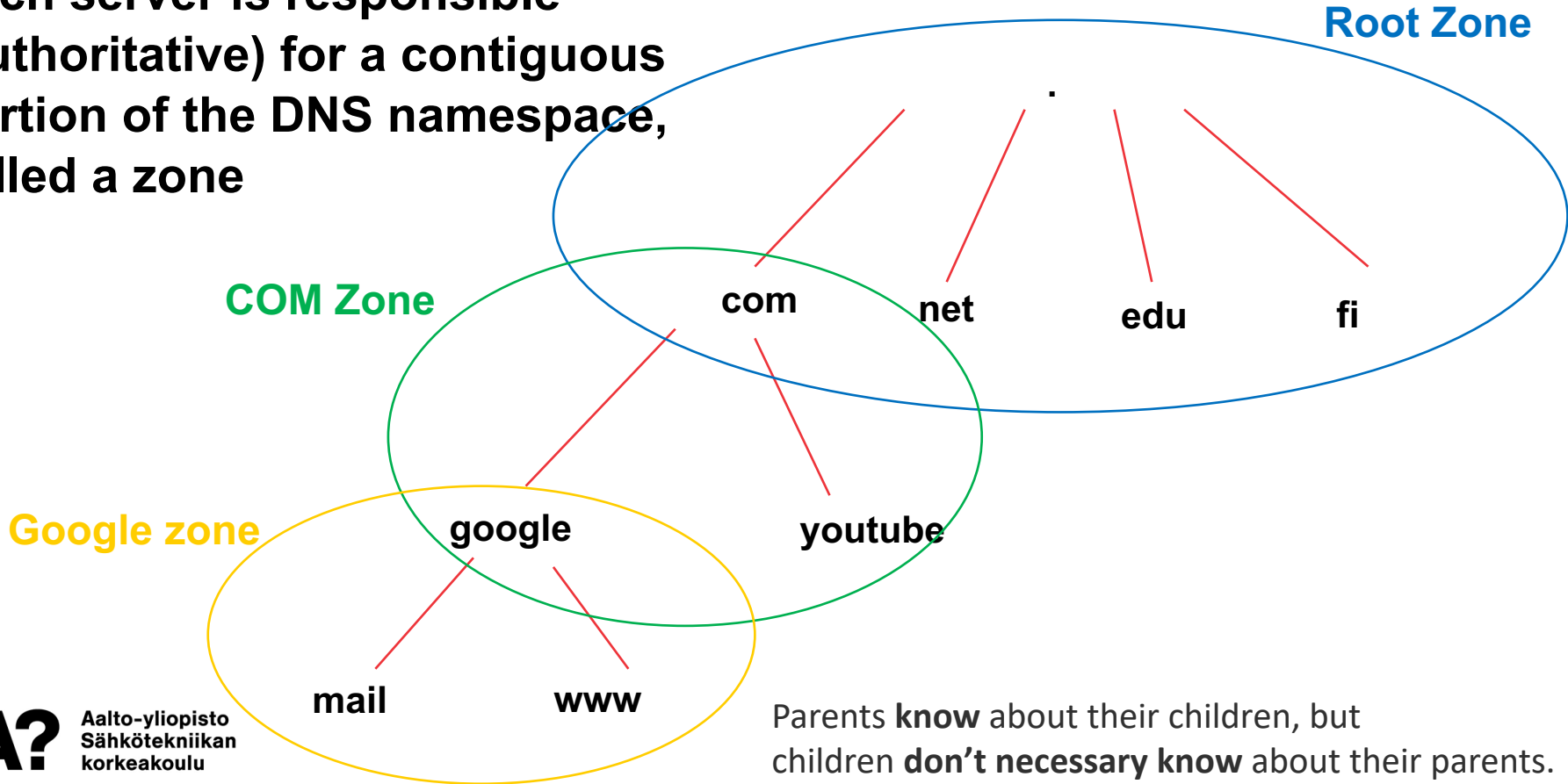


Domain Name System (DNS)

- **Application layer protocol, responsible for mapping domain names into IP addresses**
- DNS protocol relies on UDP by default, but can also work over TCP as a fallback when firewalls block UDP.
- **DNS is a distributed database**
- **Resolver:** A DNS client that sends DNS messages to obtain information about the requested domain name space
- **A DNS name server** is a server that stores the DNS records for a domain; A DNS name server responds with answers to queries against its database.

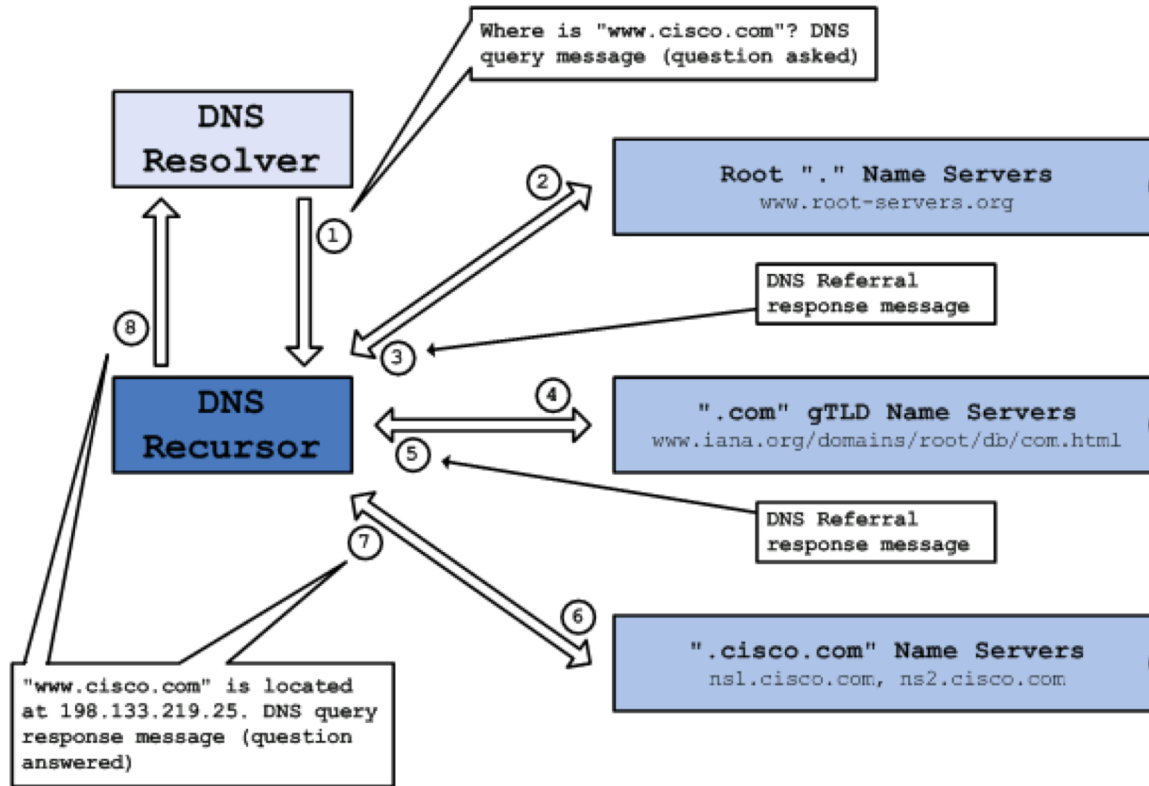
DNS Zones

Each server is responsible (authoritative) for a contiguous portion of the DNS namespace, called a zone



Parents **know** about their children, but children **don't necessary know** about their parents.

Recursive Query



- **Authoritative Server:** A DNS server that responds to query messages with information stored in resource records for a domain name space stored on the server.
- **Recursive Resolver:** A DNS server that recursively queries for the information asked in the DNS query.

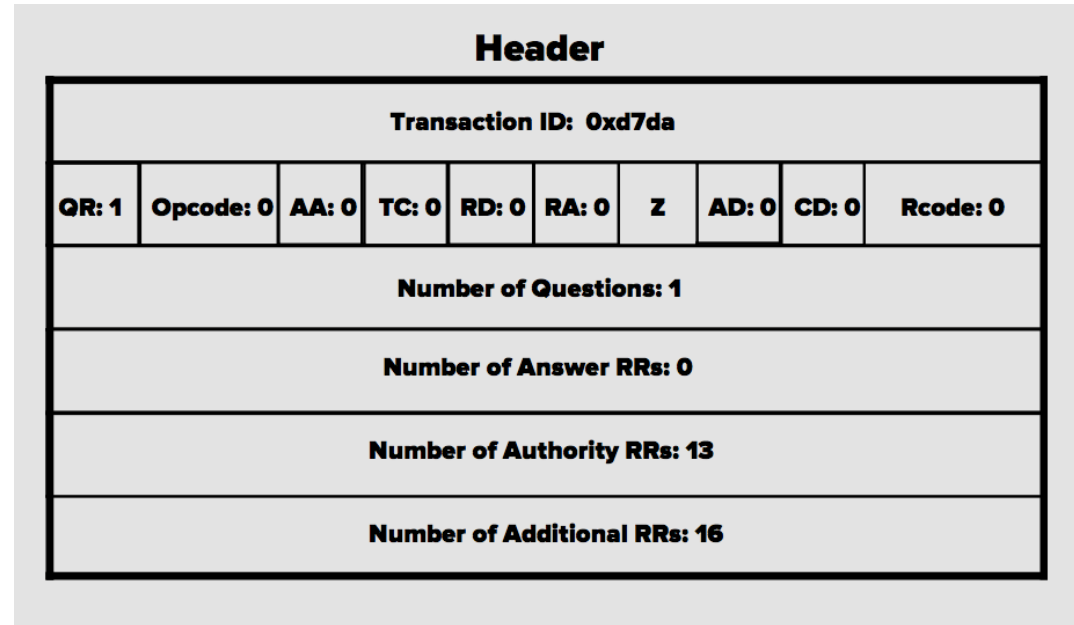
gTLD: generic top-level domain
Source: Cisco

DNS Messages

DNS protocol is composed of three types of messages: **queries**, **responses**, and updates.

The first sixteen bits are for the **Transaction ID**, used to match the response to the query, and is created by the client on the query message and returned by the server in the response.

The **question** is present in both the query and the response, and should be identical.



Example of Query and Answer

Queries

www.google.com: type A, class IN
Name: www.google.com
Type: A (Host address)
Class: IN (0x0001)

Answers

www.google.com: type A, class IN, addr 74.125.131.147
Name: www.google.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 5 minutes
Data length: 4
Addr: 74.125.131.147 (74.125.131.147)
+ www.google.com: type A, class IN, addr 74.125.131.103
+ www.google.com: type A, class IN, addr 74.125.131.104
+ www.google.com: type A, class IN, addr 74.125.131.106
+ www.google.com: type A, class IN, addr 74.125.131.99
+ www.google.com: type A, class IN, addr 74.125.131.105

Answer: in the response from recursive resolver to an end user's computer, or in the response from the authoritative name server of the domain to the recursive resolver.

Answer RR



Aalto-yliopisto
Sähkötekniikan
korkeakoulu

Source: <http://blog.catchpoint.com/2014/07/09/dissecting-dns-communications/>

```

[-] Domain Name System (response)
    [Request In: 3]
    [Time: 0.014981000 seconds]
    Transaction ID: 0xccf9
    [-] Flags: 0x8000 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 4
    Additional RRs: 4
    [-] Queries
    [-] Authoritative nameservers
        [-] google.com: type NS, class IN, ns ns2.google.com
            Name: google.com
            Type: NS (Authoritative name server)
            Class: IN (0x0001)
            Time to live: 2 days
            Data length: 6
            Name Server: ns2.google.com
        [-] google.com: type NS, class IN, ns ns1.google.com
        [-] google.com: type NS, class IN, ns ns3.google.com
        [-] google.com: type NS, class IN, ns ns4.google.com
    [-] Additional records
  
```

```

[-] Additional records
    [-] ns2.google.com: type A, class IN, addr 216.239.34.10
        Name: ns2.google.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 2 days
        Data length: 4
        Addr: 216.239.34.10 (216.239.34.10)
    [-] ns1.google.com: type A, class IN, addr 216.239.32.10
    [-] ns3.google.com: type A, class IN, addr 216.239.36.10
    [-] ns4.google.com: type A, class IN, addr 216.239.38.10
  
```

Additional records

Domain name in both the RR name and RR data fields

Authority RR

When a name server does not have the answer to the query (as is not authoritative), it will not send answer records.

Resource Record (RR)

- A **resource record** is a format used in DNS message that is composed of NAME, TYPE, CLASS, TTL, RDLENGTH, and RDATA.

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

AAAA, IPv6 address record

DNS Caching

- Temporarily storing the results of recently browsed websites' DNS queries on a local file for faster retrieval
- **DNS clients and DNS server both use caching to speed up the domain name lookup process and to ease traffic on the root servers**
- In the context of a DNS record, **Time to Live (TTL)** is a numerical value that determines how long a DNS cache server can serve a DNS record before reaching out to the authoritative DNS server and getting a new copy of the record.

Host Names

- A hostname is a domain name that has at least one associate IP address. (e.g. www.aalto.fi)
- A valid domain name may not necessarily be valid as a hostname

IPv6 addresses

- **Unicast:** one to one
- **Multicast:** one to many
- **Anycast: One-to-one-of-many association** where datagrams are routed to any single member of a group of potential receivers that are all identified by the same destination address

Anycast Addressing

- Anycast addresses are allocated from the unicast address space. Assigning a unicast address to more than one interface makes a unicast address an anycast address. Example:

ipv6 address 2002:0db8:6301::/128 anycast

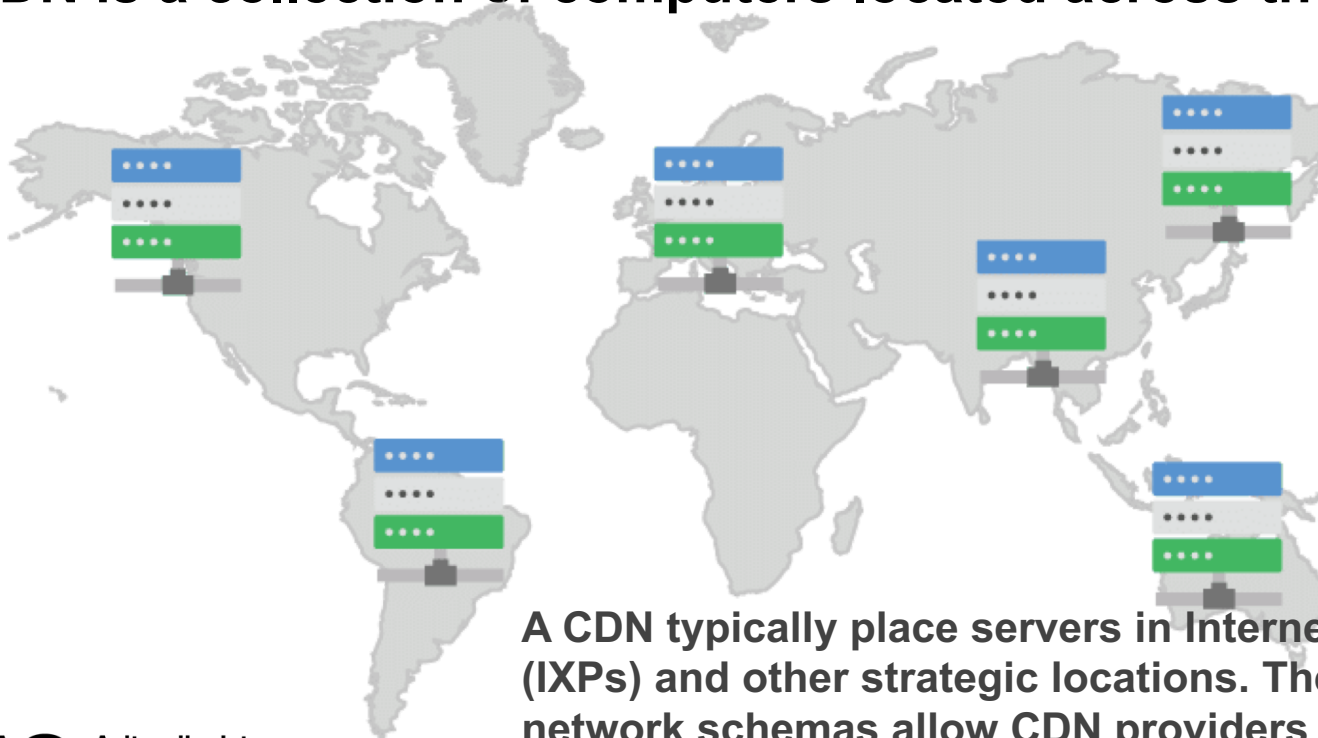
- **Anycast Address can not be used as source address of IPv6 packet**
- **The routing algorithm selects the single receiver from the group based on least-expensive routing metric (e.g. #hops, distance, latency, efficiency, cost)**

Content Delivery Network(CDN)

- **CDN makes your website load fast all around the world**

Web Hosting + CDN

CDN is a collection of computers located across the earth

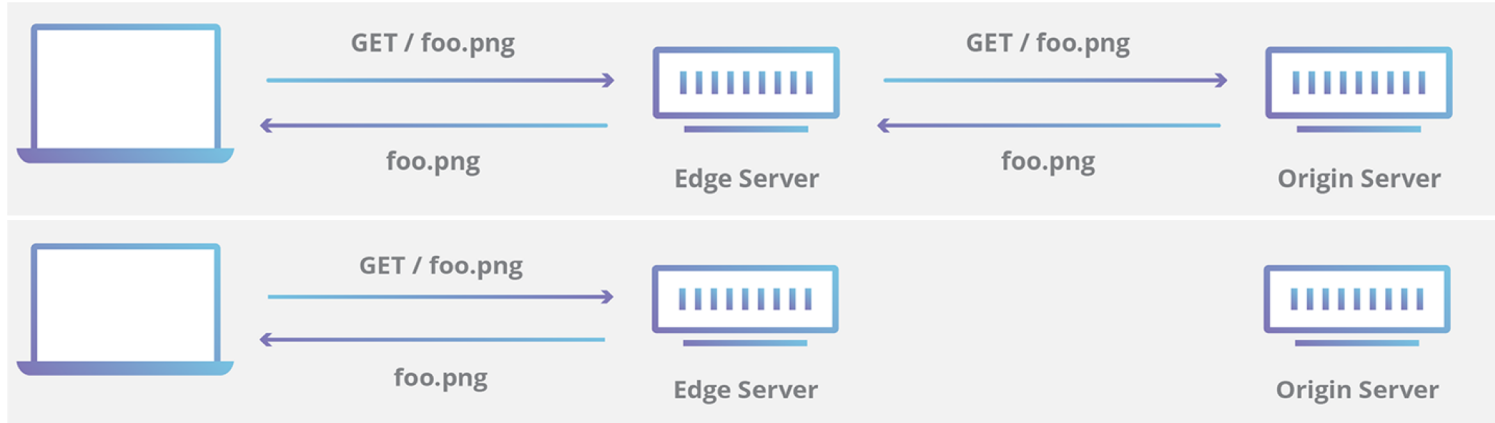


A CDN typically place servers in Internet exchange points (IXPs) and other strategic locations. These optimized network schemas allow CDN providers to optimize the route and reduce latency.

Source: <https://woorkup.com/cdn-for-dummies/>

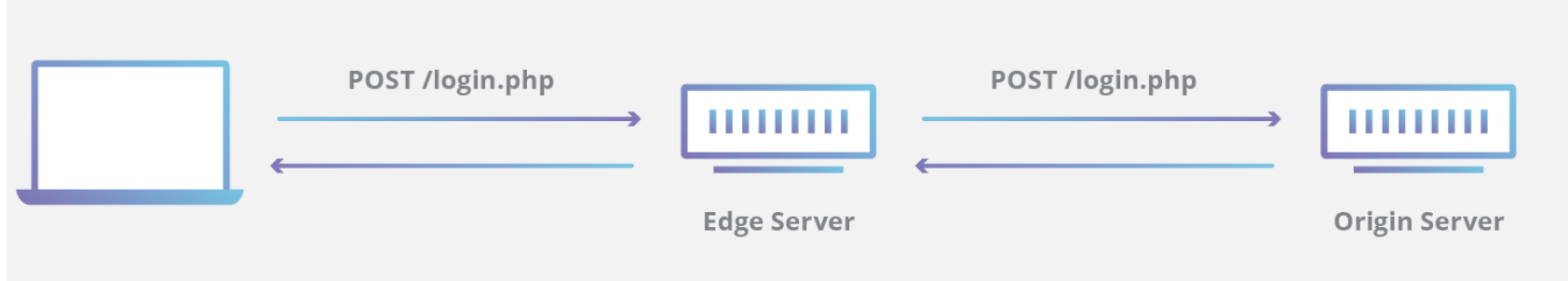
Benefits of CDN

- With a CDN requests to your website are always routed to the nearest available server.
 - A CDN improves the latency by pulling static content files from the origin server into the distributed CDN network in a process called **caching**.



Edge Server vs. Original Server

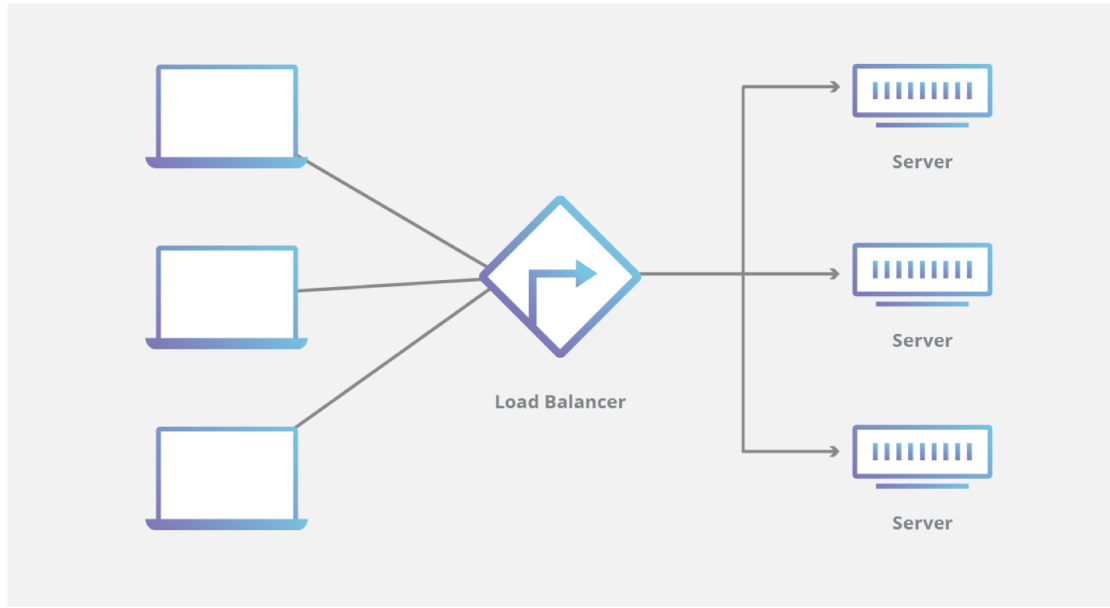
- This interplay between edge servers handling static content and origin servers serving up dynamic content is a typical separation of concerns when using a CDN.



Important server-side code such as the database of hashed client credentials used for authentication is typically maintained inside an origin server.

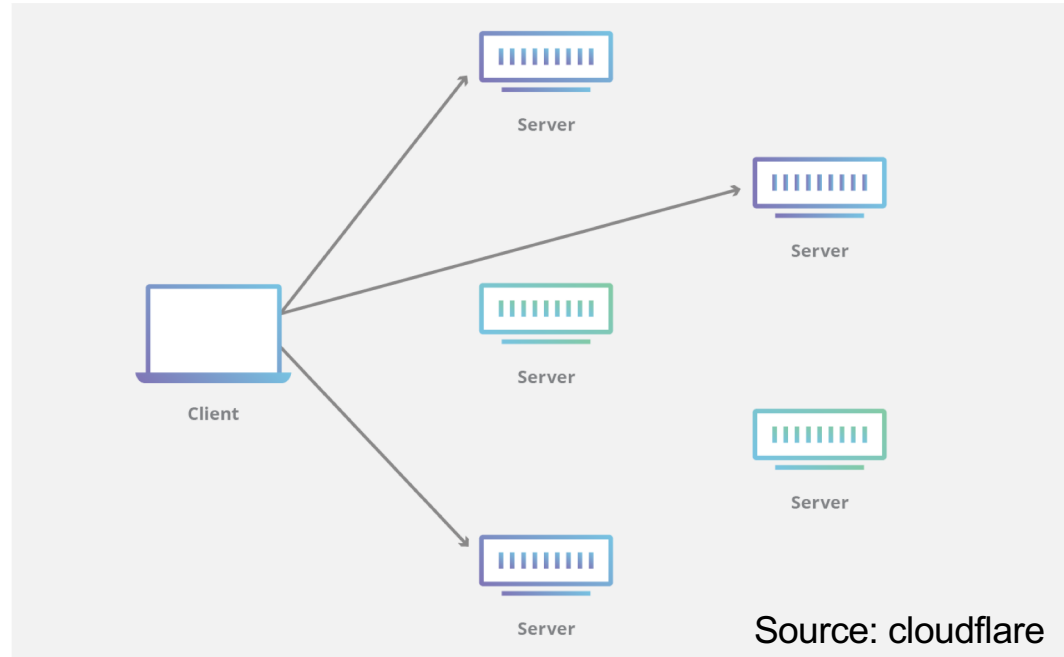
Benefits of CDN

- Load balancing distributes network traffic evenly across several servers, making it easier to scale rapid boosts in traffic.



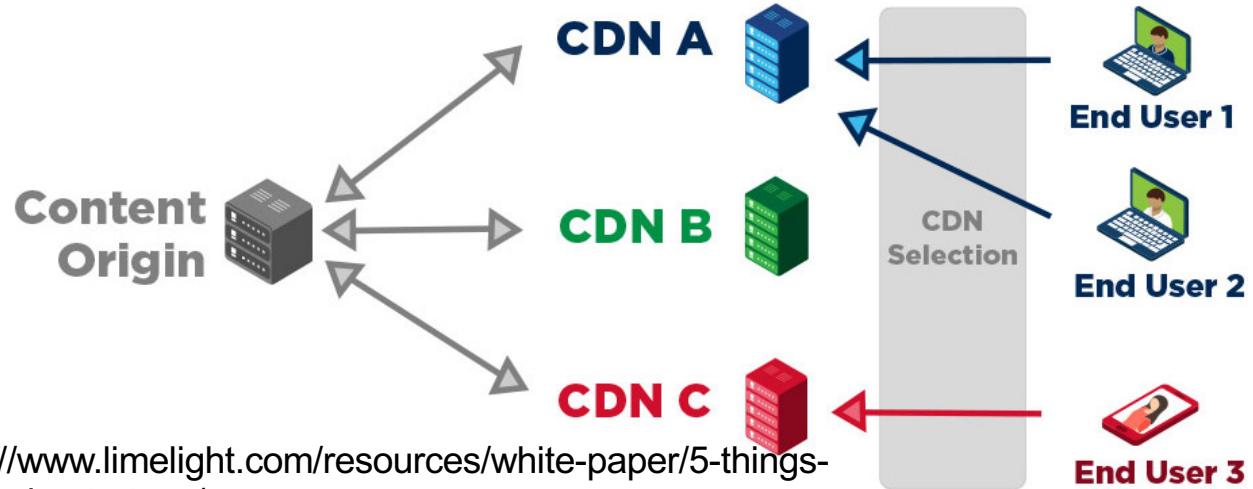
Benefits of CDN

- In the event that an entire data center is having technical issues, Anycast routing transfers the traffic to another available data center, ensuring that no users lose access to the website.



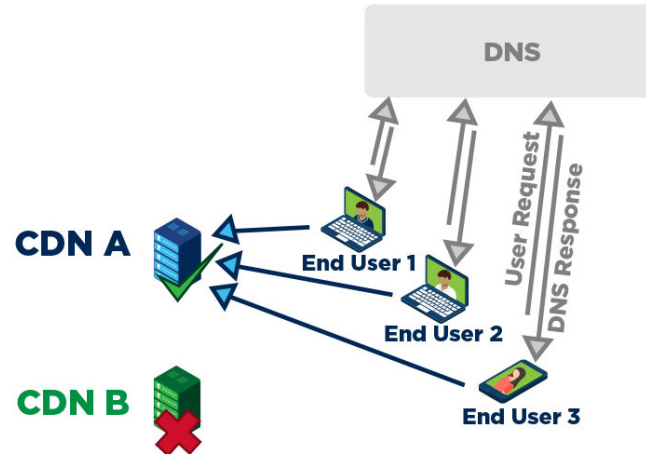
Multi-CDN

- The goal of deploying multiple CDNs is to distribute load among two or more CDNs
- Multi-CDN can minimize single points of failure by providing alternate delivery options in the event of a CDN outage.



Selection of CDN

- Selecting an optimal CDN could be based on a number of criteria – availability, geographic location, traffic type, capacity, cost, performance or combinations of the above.
- CDN selection may be carried out manually, or it may be automated using techniques like DNS or commercial decision engines.



Self-test

- **What is DNS responsible for?**
- **Can you describe the process of recursive query?**
- **What are the benefits of CDN?**
- **What is anycast?**