

# DNS(Domain Name Server)

Dns'i en basit seviyede telefon numarası rehberi gibi düşünelim,(sıra kesin değil) .Uçtan uca dns'in çalışmasını inceleyelim.

## DNS RESOLVİNG OLARAK ARAŞTIR

- 1.domaini tarayıcıya gir
- 2.cache host(browser cache – O.S cache)
- 3.Etc host'taki karşılaştırma yap “sudo nano /etc/hosts/ “dosyasına oluştıır (arada bir adım var)
- 52.94 bir ip adresini yaz etc/hosta kaydet ping at.Alan adına erişemez çünkü ssl engeller
- 4.os:dns adresini kontrol et (windowstaki 8.8.8 muhabbeti) (ISP'ye ,Udp 53 üzerinden bağlanır)

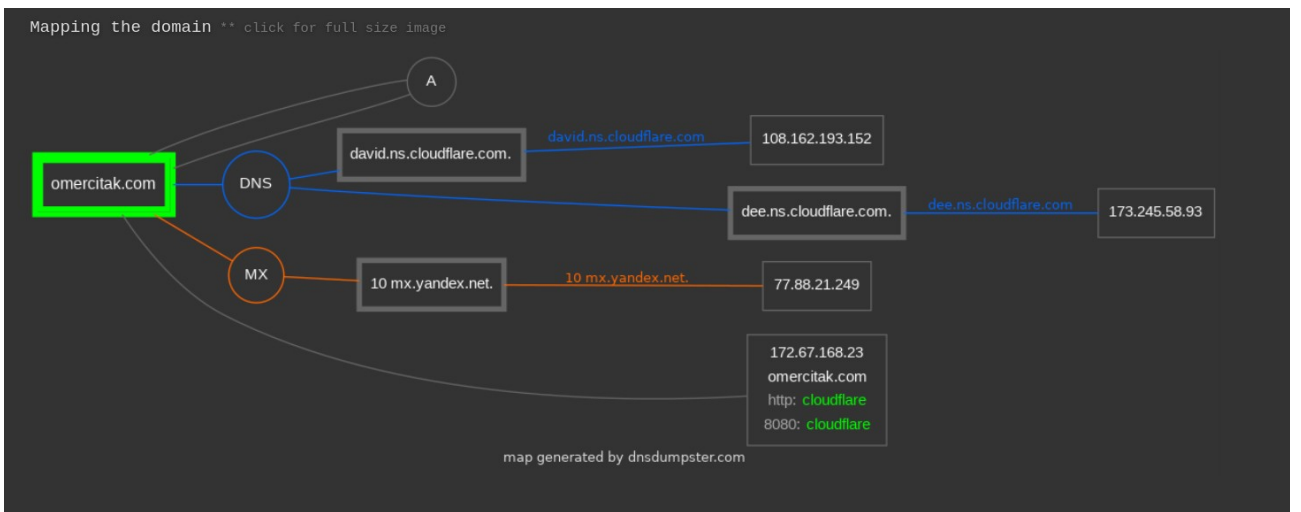
## (ZONE TRANSFER)

### ----MODEM

- 5.modemde root dns,cache (domainde sağdan sola okunur)
- 6.abc.asd.com.tr → ilk olarak tr domainine bilen servislere gider.[Nic.tr'ye gider] cache domainde yoksa asd.tr için [Nic.tr'ye gider]
- 7.abc.asd.com.tr → ilk olarak asd.tr domainine bilen servislere gider.[Nic.tr'ye gider]

### ----MODEM

## DNS DUMPTER İLE BAŞTAN UCA SÜRECİ GÖRSELLEŞTİREBİLİRİZ.



Aşağıdaki kelimeleri detaylı araştırabilerseniz iyi olur.

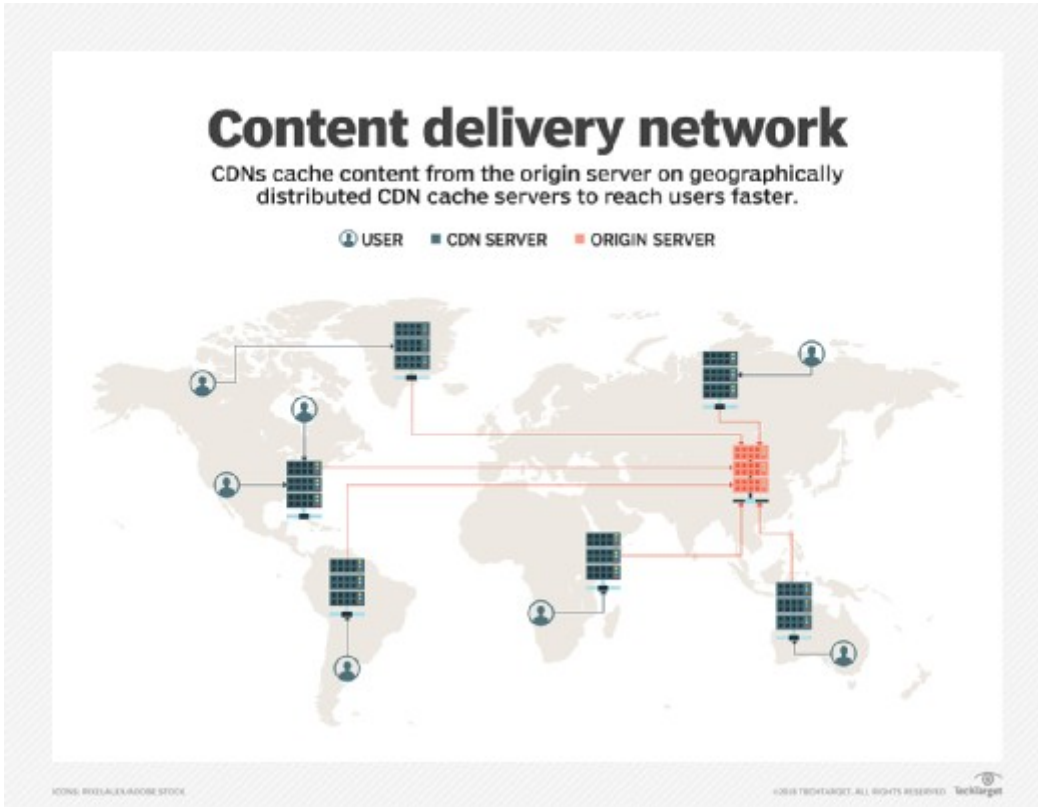
ANAME

AAAAName (IPv6)

CNAME

NS :Başka bir alt alanlarını bağlamak için kullanılır.

## CDN(Content Delivery Network)

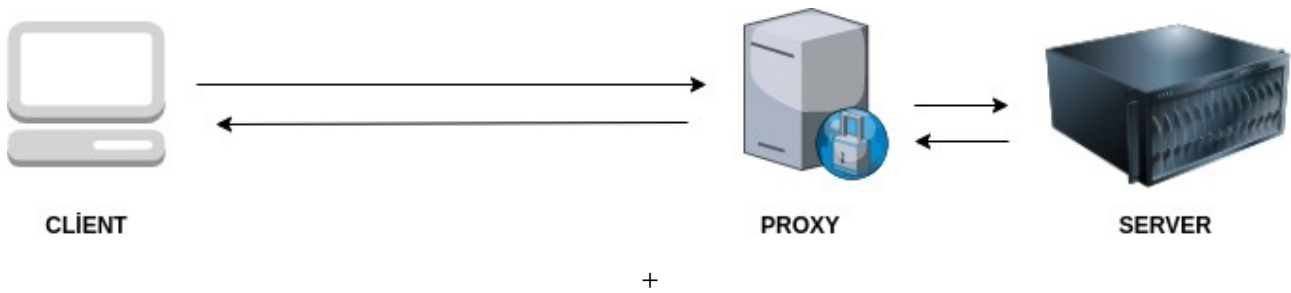


Büyük firmaların ,farklı lokasyonlarda bulunan sunuculara dağıtılıyor.(Load balancer işine benzer)

Bu yapının kullanılmasındaki en büyük amaç ise şudur .O bölgedeki kullanıcıların daha hızlı bir şekilde içeriğe ulaşması veya bir veri göndermesini sağlamaktır.

Geliştirici kısmında ise çeşitli css ve js dosyalarını cdn yayınlayarak daha hızlı sayfanın render edilmesi sağlanır.

## Cloudflare(Reverse Proxy)



Reverse proxy’de ise en büyük avantajı dışarıdan gelecek ddos ataklarını veya istekleri ilk olarak proxy server’a yönlendirerek ,websitenin kimliğini bu sayedegizleyebiliyoruz.

## HTTPS UYGULAMA

**GET / HTTP/1.1**(proxy line) method / path protokol ,version

**(header)**

**Host(keyword):** agaclar.net(value)

**User-Agent:** Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/109.0

**Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

**Accept-Language:** en-US,en;q=0.5

**Accept-Encoding:** gzip, deflate

**Connection:** close

**Upgrade-Insecure-Requests:** 1

**(header)**

asdsadsa=asdasdsa&asdas=asd (request body) +

Content-Type=application/x-www-form-urlencoded

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers>

headerler ek bilgi taşır.

### Access-Control-Allow-Credentials

- [Access-Control-Allow-Headers](#)
- [Access-Control-Allow-Methods](#)
- [Access-Control-Allow-Origin](#)
- [Access-Control-Expose-Headers](#)
- [Access-Control-Max-Age](#)

- [Access-Control-Request-Headers](#)
- [Access-Control-Request-Method](#)

authorization yetkilendirme ,auth doğrulama

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Authorization>

[Authorization](#) : Basic credentials (username,password)

swagger auth örneğine bak,haslı metni bash64'e çevir

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Disposition>

## SPA

Arkada api olup ,front end ise http methodları alıp verir bunada spa denir.

## tarayıcıdaki bellekler

LocalStorage:tema ile ilgili bilgiler

session :oturum için bilgileri ekler

cookie:bizim kim olduğumuzu servera söyleyen yapıdır.

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie>

setcookie,belleğe yazılacak verileri yazdırmayı sağlayan cookie.

Phpssıd

Cookieelerde Domaini kendimiz belirleyemeyiz.Cookie her istekte yazılıyor.

## FLAGS

**Httponly** :cookie javascript tarafından okunmasın istiyorsak  
httponly:true diyoruz.

**Secure:true** ,https ile request başladığında cookie yollasın dersin  
true yap

jsleri localStorage

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite>

**SameSite:**



Bu sessionda ise tokenları kullanarak kullanıcının bilgilerini tarayıcıda tutarak sürekli veritabanı ile haberleşmesi yerine daha hızlı çözümler üretiyoruz.

## X-Forwarded-Host .

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Forwarded-Host>

## X-Forwarded-FOR

Sunucu clientten gelen sunucunun x-forwarded-for üzerinden proxy'den geçip geçmediğini anlar.

## X-XSS-Protection

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection>

X-XSS-Protection: 0 koruma kapalı  
X-XSS-Protection: 1 koruma açık

## LOCATION

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Location>

## SERVER

**Server: Apache/2.4.1**

## ÖDEV

Aşağıdaki özellikleri sağlayan raw request yazınız.

**Method:** patch

**path:** /upload

**header name:** x-platform\_name

**header value:** android\_app

**body-type :** multipart/form data

-----  
**1.body element name:** name

**1.body element value:** name

-----  
**2.body element name:** profile\_picture.png

**2.body element value:** 1x1.png

## YANIT

PATCH /upload HTTP/1.1

Host: www.google.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120

Safari/537.36

Content-Type: multipart/formdata;

headers: {'x-platform-name': 'android-app'}

-----338219200525315680161545846948

Content-Disposition: form-data; name="text"

denemespn

-----338219200525315680161545846948

Content-Disposition: form-data; name="file1"; filename="cdn.png"

Content-Type: image/png

»PNG