(Writer: @HalilGÖKSEL)

# Domain Name System

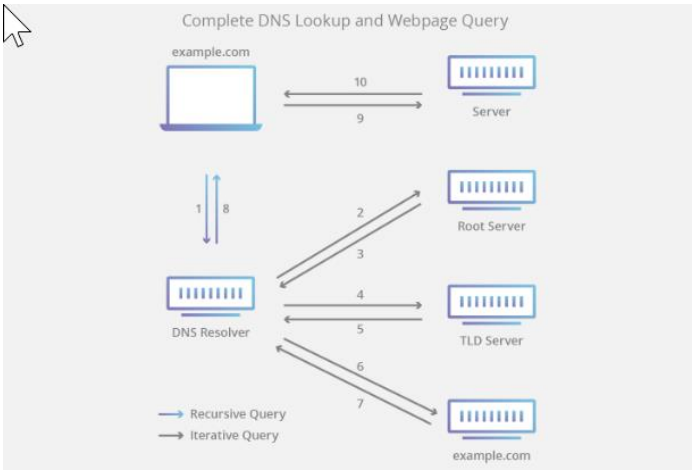
## İçerik

## DNS Nedir

DNS sorusuna en kısa cevap “internetin rehberi” en güzel tabir olur. En basit Teknik cevap verecek olursakta Alan adlarını IP’ye çeviren servis yada protokol diyerek DNS nedir sorunu sonlandırmak isterim.

## DNS Nasıl Çalışır

Bir istemci üzerinden gelen DNS istekleri üzerine 4 farklı DNS sunucusu role oynamaktadır. Bunlar (**DNS Resolver, TLD, Root, Authoritative Name Server)**
Oturduğumuz yerde google’a feysbuk yazması kolay arka planda işler nasıl dönüyor bir bakalım
Hiyerarşik olarak bir örnek ile inceleme yapalım
Evimdeki bilgisayarımdan halilgoksel.com web sitesinde gitmeye çalışayım.
Daha önce alan adımı search etmedim, DNS önbelleğimde tutulmuyor, hiç biryerden erişilmemiş var sayıyorum.




1-Evimdeki istemcimden ben web tarayıcımda halilgoksel.com arattığımda ilk istek (OS üzerinde farklı bir yapılandırma olmadığını var sayıyorum) benim DNS Resolver karşılar (DNS Resolver DNS isteklerindeki ilk duraktır yani istemci üzerimde benim dns kayıtlarımı manuel olarak tanımladığım 8.8.8.8 (google)’dır

2-DNS Resolver üzerinde DNS kaydının olmadığını farkeder, DNS’in daha önce hiç istek almadığını var saydık, Root DNS kadar bu istek ulaşır ve oradan ilgili çözümlemeyi yapar.

3- Root DNS, Resolver DNS’e etki alanları için bilgi toplayan TLD DNS’e yönlendir (Top Level Domain daha sonra bahsedicez .com .biz .co TLD’dir)

4-Resolver daha sonra .com TLD’ye istekte bulunur.

5-TLD sunucusu etki alanının NS bilgilerini yani NS IP’si ile cevap verir. (NS bizim DNS kayıtlarınımzdan sorumlu ad sunucusudur.)

6-Son olarak, Resolver NS alanına tekrar bir sorgu gönderir

7-Daha sonrası zaten bildiğn gibi NS üzerinden var olan istek kaydını bulur ve çözer en istedği DNS kaydını cevap döndürür.

8-DNS Resolver web browser'a etki alanın IP adresi ile yanıt verir halilgokselcom arka planda (212.12.12.12 ör.) çalıştırır.

9-Tarayıcı IP adresine bir HTTP isteğinde bulunur.

10-Artık amacımıza ulaşmış bulunmaktayız hayırlı olsun

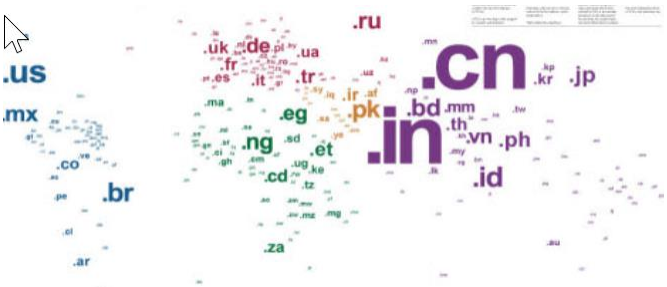
# DNS Hiyerarşisi

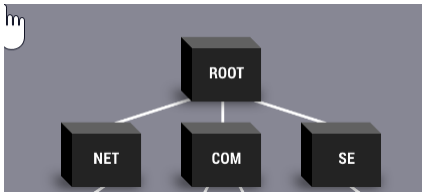
## Recursive DNS

İstemciden gelen DNS isteğini ilk karşılayan DNS sunucusudur. DNS istemcilerinin isteklerini ön belleğe alarak en kısa sürede DNS çözümlemesini yapan servislerdir.

## TLD

Top Level domain yani (.com / .biz / .uz / .co) gibi alan adımızın bir üst düzey etki alanına (TLD) adı veririz. Tüm TLD'ler tek bir DNS sunucusunda birleşir, Bunada Root DNS diyoruz.




## Root DNS

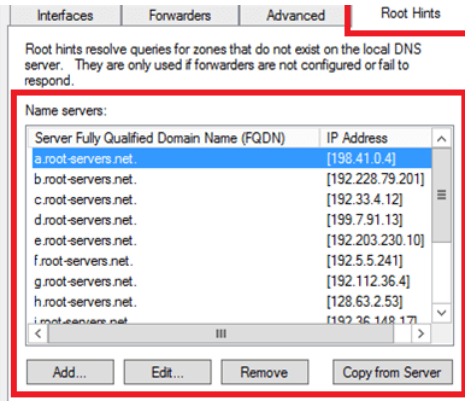
Alan adı sistemi hiyerarşisinde bulunan en üsttünde bulunan DNS sunucusuna Root DNS diyoruz.

13 Farklı Root DNS olduğu bilinmektedir. (windows server DNS mamangement üzerindede görebiliriz.)

Bu hiyerarşi mimarisinde gösterilendir, Elbette bir çok root DNS vardır. Dünya üzerinde 600'den fazla root DNS olduğu kaynaklarda yazmakta.

13 Root DNS'den birini ICANN (İnternet Tahsisli Sayılar ve İsimler Kurumu (diğerlerini ise NASA, verisign gibi kuruluşlar yönetir.

ICANN ozel bir kuruluştur, utemel gorevi İnternet alan adları sisteminin teknik yönetimini, IP adres alanlarının tahsisini ve root dns yönetmekle görevli olan bir kuruluştur.




Önbelleğe alınmamış bir DNS sorgusu yaptığımızda, Evimizden çıkan arama root DNS'lere kadar ulaşır, TLD, sonra recursive diyerek çözümleme tarafımıza ulaşır. Cache bellekte tutulduğundan 2. Bir aramada root'a gerek kalmadan DNS cache'inde ilk bulduğu DNS sunucusundan yanıt alarak çözümleme devam eder. İstemcimiz üzerinde ve web tarayıcılarımızdada DNS cache tutulduğunu unutmayalım.

### Authoritative DNS

DNS kayıtlarını üzerinde tutan ve bunlardan sorumlu olan DNS sunucularıdır diyebilirim özetçe, NS sunucularında Authoritative Zone'lar oluşturulmakta, Zone'lar içerisinde DNS kayıtlarınız bulunmakta.

## DNS Kayıtları

### SOA Record

SOA Kaydı bir DNS kaydı değildir desek yanlış olmaz, SOA Kaydı, DNS Zone'unuzun ilk oluşturulmasıyla birlikte oluşturulan bir kayıttır.

Her zone ait SOA değerlerini DNS adminlerince değiştirilebilmektedir.

SOA kaydı Zone hakkında aşağıdaki gibi idari bilgileri içermektedir.

**Primary Name Server:** Zone'unuza ait birincil NS sunucusunu işaret etmektedir.

**Serial:** Bu bölgedeki zone ait seri numarasını içermektedir, Seri NO SOA tarafından otomatik oluşturmaktadır.

**Refresh:** İkincil bir DNS sunucusunun, değişiklikleri kontrol etmek için birincil DNS sunucusunun SOA kaydını sorgulamadan önce beklediği süre.

**Rerty:** İkincil sunucunun başarısız bir bölge aktarımını yeniden denemeden önce beklediği saniye cinsinden süre. Genellikle, yeniden deneme hızı yenileme hızından daha düşüktür. Varsayılan değer 1800 saniyedir. Yeniden deneme hızı 180 ila 2419200 saniye arasında değişir.

**Expire:** İkincil bir sunucunun bir bölge aktarımını tamamlamaya çalışacağı saniye cinsinden süre. Bu süre başarılı bir bölge aktarımından önce sona ererse, ikincil sunucunun bölge dosyasının süresi dolar. İkincil, verilerinin güvenilir olamayacak kadar eski olduğunu düşündüğü için sorguları yanıtlamayı bırakacaktır.

**TTL:** Minimum  yaşam süresi değeri, zone üzerindeki tüm kaynak kayıtları için geçerlidir. Bu değer, Client üzerinde gelen isteklerde, DNS sunuculara verileri önbellekte ne kadar tutmaları gerektiğini bildirmek için sorgu yanıtlarında sağlanır. Basitçe burada girdiğiniz değer TTL değeri kadar Client cache'inde DNS kaydını tutar. Varsayılan değer 3600 saniyedir (1 Saat).

| | | | |
|---|---|---|---|
| halilgoksel.com | SOA | 6 hours | ns-cloud-e1.googledomains.com. cloud-dns-hostmaster.google.com. 30 21600 3600 259200 300 |

```
Non-authoritative answer:
halilgoksel.com
        primary name server = ns-cloud-e1.googledomains.com
        responsible mail addr = cloud-dns-hostmaster.google.com
        serial  = 30
        refresh = 21600 (6 hours)
        retry   = 3600 (1 hour)
        expire  = 259200 (3 days)
        default TTL = 300 (5 mins)
```

>nslookup

>set type=SOA

>halilgoksel.com

## A Record

En sık kullandığımız A kaydı en basit ifadeyle etki alanımızı ve alt etki alanlarımızı bir IP adresine yönlendirir, Domain ile IP arasında bir eşleme yapar.

Web sites yönlendirmelerden biride  A kaydı ile çözüm üretmektedir.

DNS sağlayıcınızda aşağıdaki örnekteki gibidi A kaydı girebilirsiniz.

| hostname | Type | TTL | Data |
|---|---|---|---|
| halilgoksel.com | A | 1 hour | 212.12.12.12 |
| linkedin.halilgoksel.com | A | 1 hour | 212.12.12.12 |
| www.halilgoksel.com | A | 1 hour | 212.12.12.12 |

```
Non-authoritative answer:
Name:    www.halilgoksel.com
Address:  212.12.12.12

> linkedin.halilgoksel.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    linkedin.halilgoksel.com
Address:  212.12.12.12
```

Command Prompt üzerinden sorgulamak için

>nslookup

>set type=A

>halilgoksel.com

★ Eğer kaydı var olmayan tüm alt alan adlarınız belirlediğiniz sunucuya yönlendirmek isterseniz Hotname "*" type "A" "IP" bilgisi girerek bu işlemi gerçekleştirebilirsiniz.

## MX Record

MX kaydı, Mail exchange anlamına gelmektedir. Bir mail altyapınızda e-posta alışverişi için kullanılır. İnternet üzerinden domaininize herhangibir e-posta göndermek istediğinde, e-posta iletimi için domaininize ait MX kayıtlarınıza sorgulamaktadır.

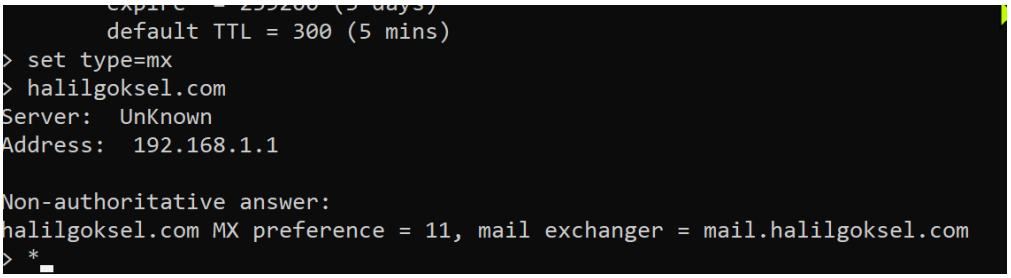
Yani MX kaydının e-mailleşmedeki yeri posta göndermek değil posta almak, yani adreslemek içindir.

DNS Kayıtlarına gelip kayıt türüne MX seçerek yönlendirilecek sunucunun kaydını (IP olarak değil önceden tanımlanmış A kaydı ) olarak girebilirsiniz.

MX kaydı girerken başındaki 10 (Priority değeri olarak geçmekte) değeri öncelik ifader eder, Yani öncelik değeri, Birden fazla Mail sunucunuz var ise Priority değeri ile öncelik verebilirsiniz

Priority değeri yüksek öncelik kayıt döndürür.

| Ana makine adı | Tür | TTL | Veriler |
|---|---|---|---|
| halilgoksel.com | MX | 1 saat | 10 mail.halilgoksel.com. |
| mail.halilgoksel.com | A | 1 saat | 212.12.12.12 |




>nslookup

>set type=mx

>halilgoksel.com

## CNAME Record

Cname Kaydı kısaca bir alt etki alanınıza yada farklı yada farklı bir etki alanının birden fazla host tarafından bilinmesini olanak sağlamaktadır. CNAME oluşturmanın amacı yönetimde kolaylık ve yönlendirmedir.

Özetle alt alan adlandırınız, farklı alan adlarına yada kendi alan adınızayönlendirmektedir.

Cname kaydı için hedef bir A kaydın olması gerekmektedir. Örnek olarak

ftp.halilgoksel.com

www.halilgoksel.com A record (halilgoksel.com 212.12.12.12)

docs.halilgoksel.com

Olarak cname tanımladığımızda tüm cname'ler A kaydını çözecektir. Herhangi bir değişiklikte A kaydını değiştirmek yeterli olacaktır.

Web site yönlendirme çözümlerinden biride cname'dir.

| Ana makine adı | Tür | TTL | Veriler |
|---|---|---|---|
| halilgoksel.com | A | 1 saat | 212.12.12.12 |
| ftp.halilgoksel.com | CNAME | 1 saat | halilgoksel.com. |
| hg.halilgoksel.com | CNAME | 1 saat | vodafone.com. |
| www.halilgoksel.com | CNAME | 1 saat | halilgoksel.com. |

```
www.halilgoksel.com     canonical name = halilgoksel.com
> hg.halilgoksel.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
hg.halilgoksel.com      canonical name = vodafone.com
>
```

>nslookup

>set type=cname

>www.halilgoksel.com

★ Cname ile web site yönlendirmeleri tavsiye edilmemekte, Nedeni çift çözümleme yaptığı içindir. Bu durumda erişimde gecikme yaşanabilir.

## TXT Record

Domaininize bir metin bilgisi girmek isterseniz TXT kaydıyla bunu yapabilirsiniz. DNS sorgularına text olarak cevap verir.

Daha çok DKIM, DMARC, SPF gibi güçlendirilmiş e-postalar için girilen kayıtlar içermektedir. Bu tür kayıtları TXT olarak girmeniz gerekmektedir.

| Ana makine adı | Tür | TTL | Veriler |
|---|---|---|---|
| halilgoksel.com | A | 1 saat | 212.12.12.12 |
| halilgoksel.com | TXT | 1 saat | "Seni seviyorum" |

```
> set type=txt
> halilgoksel.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
halilgoksel.com text =

        "I Love You"
>
```

>nslookup

>set type=txt

>halilgoksel.com

⭐ DKIM, DMARC, SPF kayıtları güçlendirilmiş e-posta güvenliği için kullanılmaktadır, Zorunlu kayıtlar değildir ama e-postanızın alıcılara ulaşmasını istiyorsanız olmazsa olmazdır. TXT Record ile oluşturulur. Biraz detaydan bahsedicek olursa;

## DKIM

(DomainKeus Identified Mail)

E-Posta gönderen alan adının e-posta mesajla ilişkinlendirilmesimi sağlar. Basitçe şöyle olarak DKIM kaydı ile siz bir public key'I domaininize tanımlarsınız.

Siz e-posta gönderdiğinizde alıcı taraf DKIM sorgulama politikası yapıyor ise ki büyük kuruluşlar bankalar vs. yapar,Gönderdiğiniz e-posta ile DKIM kaydınızı mailinide imzalarsınız, Sizin ilettiğin e-posta kontrolünde DKIM kaydı sorgular, ve girdiğiniz key ile eşleşirse DKIM sorgusundan geçersiniz, Sizin domaininizden geldiğinin göstergesi olarak Kabul edilir.

Örnek bir DKIM kaydı aşağıdaki gibidir. (Key oluşturmak için birçok tool kullanabilirsiniz.)

⭐ Eğer DKIM kaydı girerken value limit hatası alıranız 255 limiti vardır, değer arasında "" (boşluksuz çift tırnak) ile tüm kaydı girebilirsiniz.

| Ana makine adı | Tür | TTL | Veriler |
|---|---|---|---|
| s1.halilgoksel.com | TXT | 1 saat | "v=DKIM1;t=s;p=MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAxlA7SuODnNPOhYdE4RkMl/WzVuMffQUwaOxClyDFegNkvsvw8mH4txg6c9rIxFkI8jI36cTjopS6JgppGuFGjeJFBj2tXmaeWKBoWsKXLF5kbc/Em/KAFSvHXoIFm9tSdaMX7AYBAc8YLYN/x1vA12/SRrRDFt0ygWuowSH6sMB3WDjspAhxWTSbE4IxNyzE84NO" "Qma8vHnBCa5sQqrrPWPYcYeCFAL3JWH4x/5rBy4Lkym08cSlS00qSu77+RUpCE/1jKSiTC5ttFIlgPfRnMVJlzKPltXo1LTBybM5yBZnwLWDeGIDvHAuuQ22S8iQjESXmg8AZJCr6gRjY3+JYaaJpds30lLYSneFzFQt6+mabBMptQKgwREp1oZhujzVBU98YHDbrpihtkpujJCAY1N4pvBcCkzeGH/XUCu7JP34U+TPRQcLCi/frJdEKatDhPV" "taZyDzCpgHMqkiV+ib1x/7jTI9+V/j2BLWZhxVUUKSzcYglbW99pci5vUZkHeDqz5ajiJp/TxzgL9br3lwQBt05oWYRAkHt2+mTnOlP2JOcAiUjJ3wCjoVOLIE+G5wxyMkJSiqd1JgeOiyvpKZZFEtp6H9ry/5EOWP/pHqp+JVNygd/1FO4s6YIHLVCSay9d1n7Gnfnnhjrulaf TjNvpOMPoMjmAbTcOPDz8ae9kCAwEAAQ==" |

## DMARC

Domain-Base Message Authentication Reporting and Conformance

DMARC'I en basit haliyle bir e-posta firewall'I olarak düşünebiliriz. DMARC oluşturduğumuz takdirde domainimize iletilen e-postalar bizim oluşturduğumuz dmarc kaydı çerçevesinde gelen e-postaları sorgulama yapar, ve karantinaya aldırabiliriz.

Kısaca domainimize pishing, spam gönderilerini önlemek amacıyla kullanabiliriz.

Oluşturabileceğimiz etiketler aşağıdaki gibidir.

**v** Etiketi: Kullanımı zorunludur. Protokol sürümünü belirtir. Bu değer DMARC1 olmalıdır.
Örnek kullanım: v=DMARC1

**p** Etiketi: Kullanımı zorunludur. Şüpheli E-postalar için hangi protokolün işleneceği tanımlar: none: İletiyle ilgili hiçbir işlem yapılmaz. Şüpheli iletiler günlük rapora kaydedilir. quarantine: İletiler Spam olarak işaretlenir ve diğer işlemler için saklanır.

**reject:** İleti, alıcıya gönderilmemesi için iptal edilir. Örnek kullanım : p=quarantine.

**pct** Etiketi: Kullanımı isteğe bağlıdır. DMARC politikasının uyguladığı şüpheli iletilerin yüzdesini belirler. Şüpheli iletiler, DMARC kontrolünden geçemeyen iletilerdir. Varsayılan değer 100'dür. Örnek kullanım: pct=100

**rua** Etiketi:Kullanımı isteğe bağlıdır. Alanınızla ilişkili DMARC etkinliği hakkında rapor almak için, bu seçeneği kendi E-posta adresinizi ekleyerek kullanın. Örnek kullanım: rua=mailto:bilgi@domaininiz.com

**sp** Etiketi:Kullanımı isteğe bağlıdır. Alt alan adlarınız için farklı bir DMARC politikası uygulanmasını istiyorsanız bu seçeneği kullanın. Kullanılabilecek değerler p etiketinin değerleriyle aynıdır. Örnek kullanım : sp=reject

**aspf** Etiketi:Kullanımı isteğe bağlıdır. SPF (ASPF) için kullanılacak modu belirler. Bu mod, ileti bilgilerinin SPF imzalarıyla tam olarak nasıl eşleşmesi gerektiğini tanımlar. Varsayılan, Relaxed değeridir.

**r**:Relaxed (Esnek) değeri kısmi eşleşmelere, örneğin bir alan içindeki alt alanlara izin verir.

**s:**Strict (Katı) değeri, tam eşleşme olmasını gerektirir. Örnek kullanım: aspf=r

Örnek bir DMARC kaydı aşağıdaki gibidir.

| Ana makine adı | Tür | TTL | Veriler |
|---|---|---|---|
| _dmarc.halilgoksel.com | TXT | 1 saat | "v=DMARC1; p=karantina; rua=mailto:mail@halilgoksel.com,mailto:1e2c04ac@mxtoolbox.dmarc-report.com; ruf=mailto:mail@halilgoksel.com,mailto:1e2c04ac@forensics.dmarc-report.com; fo=1; pct=100" |

## SPF

Sender Polisy Framework

En basit anlamıyla alan adınızın hangi e-posta sunucularından göndermenize izin verdiğiniz tanım türü olarak diyebiliriz.

SPF Kayıtları eğer Office365 kullanıyorsanız Office365 panelinde verilen SPF tanımını girmelisiniz, Eğer Local exchange yada farklı SMTP sunucularını kullanıyorsanız SMTP IP bilgisini girmelisiniz, Eğer Mail reklam hizmeti alıyorsanız domaininiz iletilen farklı sunucular tarafından e-posta gönderim hizmeti varsa SPF tanımını girmelisiniz, SPF tanımı yapılmazsa yüksek ihtimal alıcı tarafta karantina düşer, yada DROP edilebilir
DMARC'da olduğu gibi SPF kaydı oluştururkende belirlediğimiz mekanizlar çerçevesinde halinde oluşturmak gerekir. Aşağıdaki mekanizma açıklamaları yer verilmiştir.
SPF örnek tanımı aşağıdaki gibidir.

| Ana makine adı | Tür | TTL | Veriler |
|---|---|---|---|
| halilgoksel.com | TXT | 1 saat | "v=spf1 a mx a: ip4:212.12.12.12 -all" |

| Niteleyici | Eşleşme durumunda alıcı sunucunun gerçekleştireceği işlem |
|---|---|
| + | Kimlik doğrulamasından geçer. Eşleşen IP adresine sahip sunucu, alanınız için ileti göndermeye yetkilendirilir. İletilerin kimliği doğrulanır. Mekanizmada bir niteleyici kullanılmadığında bu, varsayılan işlemdir. |
| - | Kimlik doğrulaması başarısız olur. Eşleşen IP adresine sahip sunucunun alan için ileti göndermesine yetki verilmez. SPF kaydı, gönderen sunucunun IP adresini veya alanını içermediğinden ileti, kimlik doğrulamasından geçemez. |
| ~ | Kimlik doğrulaması başarısız olabilir. Eşleşen IP adresine sahip sunucunun alan için ileti göndermesine büyük ihtimalle yetki verilmez. Alıcı sunucu genelde iletiyi kabul eder ancak aynı zamanda şüpheli olarak işaretler. |
| ? | Nötr. Kimlik doğrulamasında ne başarılı ne de başarısız olur. SPF kaydı, alan için ilgili IP adresinin ileti göndermesine yetki verildiğini açıkça belirtmez. Nötr sonuç içeren SPF kayıtları genellikle `?all` kullanır |

| Mekanizma | Açıklama ve izin verilen değerler |
|---|---|
| v | SPF sürümü. Bu etiket gereklidir ve bunun kayıttaki ilk etiket olması gerekir. Bu mekanizma şu şekilde olmalıdır:<br>`v=spf1` |
| ip4 | Posta sunucularını IPv4 adresi veya adres aralığına göre yetkilendirin. Bu değerin bir IPv4 adresi ya da standart biçimde bir aralık olması gerekir. Örneğin:<br>`ip4:192.168.0.1`<br>veya<br>`ip4:192.0.2.0/24` |
| ip6 | Posta sunucularını IPv6 adresi ya da adres aralığına göre yetkilendirin. Bu değerin bir IPv6 adresi ya da standart biçimde bir aralık olması gerekir. Örneğin:<br>`ip6:3FFE:0000:0000:0001:0200:F8FF:FE75:50DF`<br>veya<br>`ip6:2001:db8:1234::/48` |
| a | Posta sunucularını alan adına göre yetkilendirin. Örneğin:<br>`a:solarmora.com` |
| mx | Bir veya daha fazla posta sunucusunu MX kaydına göre yetkilendirin. Örneğin:<br>`mx:mail.solarmora.com`<br>Bu mekanizma SPF kaydınızda yoksa varsayılan değer, SPF kaydının kullanıldığı alanın MX kayıtlarıdır. |
| include | Üçüncü taraf e-posta göndericilerini alana göre yetkilendirin. Örneğin:<br>`include:servers.mail.net` |
| all | Gelen tüm iletilerin eşleştiğini belirtir. Bu mekanizmayı SPF kaydınıza her zaman eklemenizi öneririz.<br>Bu, SPF kaydındaki en son mekanizma olmalıdır. SPF kaydında `all` mekanizmasından sonra gelen tüm mekanizmalar yoksayılır. |

## NS Record

Name Server kaydı, Alan adınızın yönetiminiden sorumlu olan sunucuların bilgisini yer verir.

Name Server değişiklikleri alan adı register ettiğiniz servis üzerinden yapılmaktadır.

Örnek bir hikaye ile, Godady üzerinden bir alan adı satin aldınız, Siz DNS kayıtlarınızı on-prime ortamınızda yönetmek istiyorsunuz, Bir Windows DNS servisi kurdunuz ve dışarıya açık şekilde yapılandırdınız ve DNS kayıtlarını alan adınıza eşliyecek şekilde girdiniz.

Bu durumda DNS çözümlemesini bekleyemezsiniz, Register ettiğiniz platform üzerinden yapılandırdığınız NS bilgilerini kendi DNS sunucunuza yönlendirmelisiniz.

Bu sayede domaininize gelen istekler kendi DNS sunucunuz üzerinden çözümlemeye başlayacaktır.

İşlem sonrasında artık DNS kayıtlarınızı kendi on-prime üzerinden register etmeye başlayabilirsiniz.

Örnek NS kayıtları

| Ad sunucusu |
| --- |
| ns-cloud-e1.googledomains.com |
| ns-cloud-e2.googledomains.com |
| ns-cloud-e3.googledomains.com |
| ns-cloud-e4.googledomains.com |

NS sorgulama

```
set type=ns
> halilgoksel.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
halilgoksel.com nameserver = ns-cloud-e4.googledomains.com
halilgoksel.com nameserver = ns-cloud-e3.googledomains.com
halilgoksel.com nameserver = ns-cloud-e1.googledomains.com
halilgoksel.com nameserver = ns-cloud-e2.googledomains.com
> 0
```

>nslookup

>set type=ns

>halilgoksel.com

## SRV Record

SRV kaydı, IP üzerinden VoIP, anlık mesajlaşma, outlook üzerinde on-prime sunucunuzu bulması hizmetler için ana bilgisayar ve bağlantı noktasını belirtir. SRV kayıtlarının diğer kayıtlardan farkı port , servis, bilgisi içermesidir. Yani arka planda bir servise değiniyor diyebiliriz.

SRV kayıtları, listeledikleri çeşitli sunucuların "önceliğini" ve "ağırlığını" gösterir. Bir SRV kaydındaki "öncelik" değeri, yöneticilerin verilen hizmeti destekleyen bir sunucuyu diğerine göre önceliklendirmesini sağlar. Daha düşük öncelik değerine sahip bir sunucu, diğer sunuculardan daha fazla trafik alacaktır. Ancak, "ağırlık" değeri benzerdir: daha yüksek ağırlığa sahip bir sunucu, aynı önceliğe sahip diğer sunuculardan daha fazla trafik alacaktır.

Aralarındaki temel fark, önceliğe bakılmasıdır. Sunucu A, Sunucu B ve Sunucu C olmak üzere üç sunucu varsa ve bunların sırasıyla 10, 20 ve 30 öncelikleri varsa, "ağırlıkları" önemli değildir. Hizmet her zaman önce Sunucu A'yı sorgulayacaktır.

Ancak A, B ve C Sunucularının hepsinin 10 önceliğe sahip olduğunu varsayalım - bir hizmet aralarında nasıl seçim yapacak? Ağırlığın bir faktör haline geldiği yer burasıdır: Sunucu A'nın "ağırlık" değeri 5 ise ve Sunucu B ve C'nin "ağırlık" değeri 3 ve 2 ise, Sunucu A en fazla trafiği alacak, Sunucu B ikinciyi alacaktır. en çok trafik ve Sunucu C en çok üçüncü sırada yer alır.

Örnek bir SRV kaydı aşağıdaki gibidir.

| Ana makine adı | Tür | TTL | Veriler |
|---|---|---|---|
| _autodiscover.halilgoksel.com | SRV | 1 saat | 0 0 443 mail.exchange.local. |

## RDNS

Reverse DNS zone IP’den domain doğrulamak için oluşturduğumuz etki alanlarımızdır.

Reverse DNS Zone yönetmek için internet servis sağlayacınızdan,  Ripe talebinde bulunmalısınız, Ripe kayıtlarınız on-prime kullanacaksanız DNS sunucunuzu göstermelidir.

Basit anlamda DNS zone için NS tanımı yapıyor şeklinde düşünebiliriz.

Ripe tarafından kaydınız yok ise PTR’larınız yanıt vermez.

Ripe veri tabanı üzerinden kaydınızı sorgulamak için ripe.net üzerinden bakabilirsiniz

⭐DNS sunucunuz üzerinde RDNS zone oluşturduğunuzda girdiğiniz IP'nin kayıt sonrasında 1. Oktek ile 3. oktet yer değiştirmektedir. RDNS zone aratırken bu şekilde aratmalısınız.

Ör:

212.12.32.0 > halilgoksel.com

Kayıt: 32.12.212.0.in-addr.arpa


## PTR

Pointer Record ters DNS araması için, IP'den domain sorgular. RDNS zone altında kayıt girilir.

A kaydının tam tersi'dir. PTR Kayıtları RDNS Zone üzerinde girilmelidir.

| Host: | Type: | Points to: | TTL |
|---|---|---|---|
| 1.0.168.192.in-addr.arpa | PTR | hostname1.example.com | 1 Hour |
| 2.0.168.192.in-addr.arpa | PTR | hostname2.example.com | 1 Hour |

PTR kaydı e-posta sunucunuz için zorunluluk kılmaktadır. Eğer girilmez ise e-postalarınız reject alabilir yada karantinaya düşer.

## ALIAS Record (ANAME)

ALIAS kaydı benzeri şekilde Cname olarak görebiliriz, çok daha kullanışlı olduğunu söyleyebilirim.

ALIAS bazen ANAME olarak'da forumlarda yada altyapılarda karşınıza cıkabilir, ikisinin aynı şey olduğunu belirtmek isterim.

Alıas en basitle domain'den domaine yönlendirmektedir.

Cname'den farkı sadece subdomain olarak değil domain olarak'da yönlendirme yapabilmenizdir.
Web site yönlendirme taleplerinde diğer bir seçeneğinde bu oldunu söyleyebilirim.

### DNAME Record

Dname kaydından kısaca bahsetmek isterim.

Çalışma şekli Aname ve Cname ile benzerdir.

Aname ile domain bazında yönlendirme yapabilirken, Dname'de subdomain bazında yönlendirme yapılabilir.

Cname kaydından farkı, Tüm subdomain'leri (kaydı olan olmayan) belirlediğiniz etki alanına yönlendirir.

### CERT Record

CERT kaynak kayıtları, sertifikaları DNS'de depolamak için kullanılır. Hassas içeriği şifrelemenin bir kısmı, gönderen ve alan tarafların gerçekliğinin doğrulanmasını içerir. DNS CERT kayıtları bu bilgileri depolar ve sağlar.

### CAA Record

CAA kaydı, alan sahiplerinin belirli üçüncü taraf satıcıları, alanları adına SSL sertifikaları verme yetkisi vermelerine olanak tanıyan özel bir DNS kaydı türüdür (TXT veya CERT'yi düşünün). Bu, CA'ların bir CAA kaydının varlığını kontrol etmesini ve bulunursa, bu etki alanı için sertifika vermeden önce yetkilendirildiklerini doğrulamasını gerektirir. Detay için **bakabilirsiniz**

### NAPTR Record

NAPTR kayıtları Daha önce pek duymadığımız yada, benimde pek karşılaşmadığım bir kayıt türü, Yinede makalede yer verme gereksinimi duydum.

NAPTR Kayıtları SRV kayıtları ile birlikte çalışır, Daha cok mobil app'lerde SIP sunucuların kullanıcı adresleri ile eşleşmesinde, İnternet üzerinden VoIP telefonlara erişebilme gibi imkanlar sunar. Basitçe arka planda bir hizmete yönlendirildiğini düşünebiliriz.

## Daha Az Kullanılan DNS Kayıt Türleri

- **AFSDB** kaydı - Bu kayıt, Carnegie Melon tarafından geliştirilen Andrew Dosya Sisteminin (AFS) istemcileri için kullanılır. AFSDB kaydı, diğer AFS hücrelerini bulmak için işlev görür.
- **APL** kaydı - 'Adres önek listesi', adres aralıklarının listelerini belirten bir deneme kaydıdır.
- **DNSKEY** kaydı - ' DNS Anahtar Kaydı ', Etki Alanı Adı Sistemi Güvenlik Uzantısı (DNSSEC) imzalarını doğrulamak için kullanılan bir genel anahtar içerir.

- **CDNSKEY** kaydı - Bu, bir ebeveyne aktarılması amaçlanan DNSKEY kaydının bir alt kopyasıdır.
- **DCHID** kaydı - 'DHCP Tanımlayıcı', IP ağlarında kullanılan standartlaştırılmış bir ağ protokolü olan Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) için bilgi depolar.
- **HIP kaydı** - Bu kayıt, bir IP adresinin rollerini ayırmanın bir yolu olan 'Ana bilgisayar kimlik protokolünü' kullanır; bu kayıt en sık mobil bilgi işlemde kullanılır.
- **IPSECKEY** kaydı - 'IPSEC anahtarı' kaydı , uçtan uca bir güvenlik protokolü çerçevesi ve İnternet Protokol Paketi'nin (TCP/IP) bir parçası olan İnternet Protokol Güvenliği (IPSEC) ile çalışır .
- **LOC** kaydı - 'Konum' kaydı, bir alan için boylam ve enlem koordinatları biçimindeki coğrafi bilgileri içerir.
- **NSEC** kaydı - 'Sonraki güvenli kayıt', DNSSEC'nin bir parçasıdır ve istenen bir DNS kaynak kaydının mevcut olmadığını kanıtlamak için kullanılır.
- **RRSIG** kaydı - 'Kaynak kaydı imzası', DNSSEC'ye göre kayıtların kimliğini doğrulamak için kullanılan dijital imzaları depolamak için bir kayıttır.
- **RP** kaydı - Bu, 'sorumlu kişi' kaydıdır ve alan adından sorumlu kişinin e-posta adresini saklar.
- **SSHFP** kaydı - Bu kayıt, 'SSH ortak anahtar parmak izlerini' saklar; SSH, Secure Shell anlamına gelir ve güvenli olmayan bir ağ üzerinden güvenli iletişim için bir kriptografik ağ protokolüdür.

Daha önce tecrübe etmediğim kayıt türleridir, Detaylar Google'da

Kaynak

# NEDİR

## TTL Nedir ?

Time To Live kayıtlarınızın ne kadar süreyle önbelleğe alınacağını belirler.

Yani siz TTL değerini belirlediğinizde dünya çapındaki dns sunucularında belirlediğiniz zaman dilimine kadar eski değeri gösterecek demektir.

TTL 3600 = 1 Saat demektir.

Web sunucu yada mail sunucu gibi kritik dns kayıtlarının adreslerini değiştirirken TTL değerleri kısaltmanız, kesinti süresini minimuma indirmeniz demektir.

Aşağıda yer verilen DNS'in gelişmiş özellikleri DNS sunucularına göre farklılık gösterebilir, Ama işlevsel özelliği aynıdır. Yer alan görüntüde Windows Server DNS Management üzerinden inceledik.

### DNSSEC Nedir ?

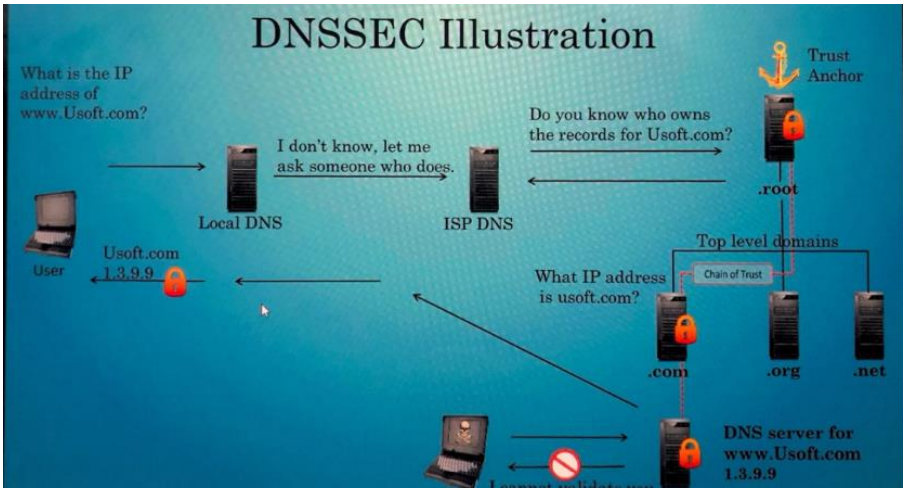
DNS kendi başına bir güvenlik sağlamaz, Ben bir istemci üzerinden web tarayıcısında linkedin.com yazdığında, linkenin ardında bulunan servislerine değilde kendi sunucularıma yönlendirmem oldukça mümkündür.

DNS Security amacı DNS önbellek zehirlenmeleri, ortadaki adam saldırılarını önlemek amacıyla sunduğu güvenlik servisidir.

Burada DNSSEC devreye girmektedir. Zone ait DNS kayıtlarını imzalayarak, DNS zone ortamında bir güven zinciri oluşturur. DNS yanıtlarını DNS key ile digital imzalar kullanarak verir.

### DC Record Nedir ?

DS kaydı, DNSSEC bölgelerinin alt bölgelerinin** orijinalliğini doğrulamak için kullanılır. Üst bölgedeki DS anahtar kaydı, alt bölgedeki KSK karmasını içerir. DNSSEC çözümleyicisi bu nedenle, KSK kaydını karma hale getirerek ve bunu üst bölgenin DS kaydındakilerle karşılaştırarak alt bölgenin orijinalliğini doğrulayabilirsiniz. DS Kaydı ile DNSSEC etkin domaininizin public key'ini DC sunununuzda tanımlayabilirsiniz. DNSSEC çalışma şekli aşağıdaki gibidir.




DNSSEC sorgusu yapabileceğiniz bir tool linkini buradan erişebilirsiniz

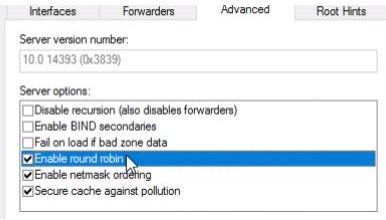
## Round-Robin Nedir ?

Birden fazla A kaydı olan DNS kayıtlarında yük dengeleme sağlar. Örnek olarak Birden fazla node olan aynı servis üzerinde(Web sunucusu olabilir, RDP terminaleri olabilir vs.) dns isteklerinin isteklerin sırayla dağıtmak için round-robin dns servisini kullanabiliriz

(A record)

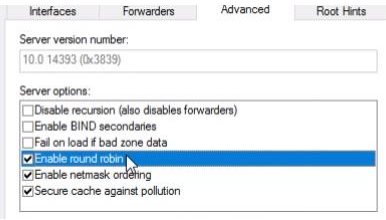
Halilgoksel.com 212.12.12.12
Haligoksel.com 212.12.12.11

Halilgoksel.com 212.12.12.10
İstemci üzerinde gelen istekler sırayla dağıtacaktır 12-11-10 Sunucuların DNS isteklerini round-robin ile çözecektir.



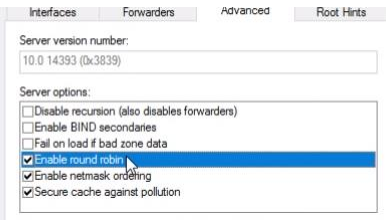

## Recursion Nedir ?

DNS Sunucusunun diğer DNS sunucularına sorgu atabilmesini sağlar, DNS'in var olan sorguları forwarding DNS sunucularına (Manuel olarak girdiğiniz dns kayıtları), ROOT DNS sunucularına yönlendirir, DNS sorgusunu bu şekilde yeniler. (Eğer bunu devre dışı bırakırsanız google giremiyorum diye arama almanız muhtemeldir.)



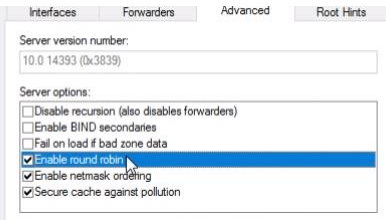

## BIND Secondary Nedir

Zone'ların diğer DNS sunucularına taşınmasını olanak sağlar




## Fail on Load Nedir

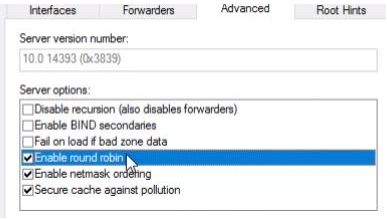
Zone'lar üzerindeki verilerin hatalarının algılanıp kullanılmamasını sağlar




## Netmask Ordering Nedir?

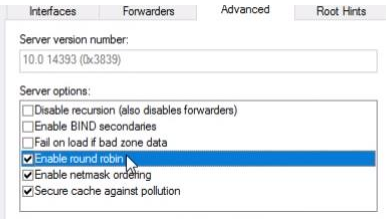
Sorgu gönderen network'ün DNS sorgusuna uygun şekilde cevap verir. Örnek olarak local dns sunucumuzda bir servis üzerinde birden fazla A kaydı olduğunu var sayarsak, 10.10.10.1 vlanından gelen

bir isteğe kayıt var ise 10.10.10.1 aynı blok'tan giril A kaydından DNS sorgusuna cevap verir.



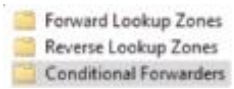

## Cache Pollution Nedir ?

DNS Sunucuda önbelleğin kirlenmesini önlemek amacıyla belirli sürelerde temizlenmesidir. Cache üzerinde temizlik yapar.




## Conditional Forwarder Nedir ?

Forward ve Reverse Zone'ları zaten biliyorsunuz, Conditional Forwarders ise, Koşullu yönlendirme işlemi recursion'da bahsettiğimiz gibi, Local DNS üzerinde var olmayan kayıtları yönlendirir demiştik. Conditional kayıt girersek arada bir gecikme olmadan dns üzerinde sorgu aramadan belirlediğimiz dns sunucularına yönlendirme işlemi yapar. Aradaki sorgu süresini local'de aramadığından en aza indirir Domain bazında kayıt girilir.




## DNS Delegation Nedir ?

DNS Delegation işlemi, Alt etki alanlarında  delegasyon yani yetkilendirme işlemi sağar. Domain farklı bir Authoritative DNS, Subdomain farklı bir Authoritative DNS üzerinden yönetilir. Bir örnekten yola çıkacak olursak

Halilgoksel.com Zone kayıtlarım / ns.haligoksel.com üzerinde var sayalım, ben subdomain oluşturup, alt alan adlarımın farklı bir zone'da bağımsız bir şekilde yönetilmesini istediğimde delegation işleti yaparak bu elde edebilirim.

Halilgoksel.com / ns.halilgoksel.com name server'larımı gösterirken.

HG.haligoksel.com / ns-cloud-e1.googledomains.com Name server'ları gösterebilirim, Böylede supzone'u farklı bir DNS sunucusunda tamamen izole ve bağımsız bir şekilde yönetebilirim.

## RIR Nedir ?

DNS konusundan biraz daha bağımsız ama bilmemiz gerektiğini düşündüğüm bir konu.

Regional internet registry (bölgesel kayıt defteri), Dünya üzerindeki var olan bölgeler, kıta veya ülke üzerinde IP adreslerini yöneten bir kuruluştur diyebiliriz.

5 Farklı kuruluş vardır, Türkiye için RIPE NCC yönetmektedir.

Ripelerin bir sonraki tahsis alanı ise ISS'ler (internet servis sağlayıcılarıdır "Vodafone, turkcel, turknet vs"), Hükümetler, Büyük kuruluşlar vs olabilir.

RIPE bu sağlayıcılara bir blok verir, bu blogu kullanarak her bir kullanıcıya yada modeme diyim basitçe dağıtımını sağlar.

Statik bir IP'adresininizin var olduğunu ve exchange sunucusu kaldırmak istediğinizi var sayalım, Bunun için bir RDS Zone , zone altında PTR kaydı gereklidir. Eğer siz static IP'nizi RDS zone oluşturup tanımlamasanız çalışmasını beklemeyin, İnterner servis sağlayıcınıza RIPE formu ileterek, ripe ileterek, RIR üzerinde kayıt oluşturulması gerekmektedir, Ardından RDNS Zone'unuzu yönetebilirsiniz.