

# DNS Nedir?

14545568 – HIKMET TÜYSÜZ

# DNS

- ▶ DNS, Domain Name System'in kısaltılmış şeklidir. Türkçe karşılığı ise Alan İsimlendirme Sistemi olarak bilinir.
- ▶ DNS, 256 karaktere kadar büyüeyebilen host isimlerini IP'ye çevirmek için kullanılan bir sistemdir.
- ▶ İnternet ağını oluşturan her birim sadece kendine ait bir IP adresine sahiptir. Bu IP adresleri kullanıcıların kullanımı için `www.site_ismi.com` gibi kolay hatırlanır adreslere karşılık düşürülür. DNS sunucuları, internet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır.
- ▶ Host ismi, tümüyle tanımlanmış isim (full qualified name) olarak da bilinir ve hem bilgisayarın ismini hem de bilgisayarın bulunduğu internet domainini gösterir.
- ▶ DNS, verilen bir makina adının IP adresini çözerek makinaların internet üzerinde host isimleri ile haberleşmelerine olanak tanır.

# DNS'in Amacı Nedir?

- ▶ DNS, kolay anlaşılabilir ve kullanılabilir makine ve alan isimleri ile makine IP adresleri arasında çift taraflı dönüşümü sağlar.
- ▶ IP adreslerinin gündelik hayatta kullanımı ve hatırlanması pek pratik olmadığı için domain isimlendirme sistemi kullanılır.
- ▶ Ana amacı, ağ üzerinden gelen alan adı veya IP numarası ile ilgili sorgulamalara yanıt vermektir. Bu amaç için çok yaygın olarak "Berkeley Internet Name Domain (BIND)" yazılımı kullanılmaktadır. Siz bir siteye erişmek istediğinizde, DNS sayesinde hangi site nerede, hangi IP hangi bilgisayara ait olduğu belirlenir ve istediğiniz yere erişirsiniz.

# DNS Tarihçesi

- ▶ 1984 yılına kadar DNS diye bir şey yoktu. O yıla kadar isim-IP çözümlenmesi HOSTS adında bir metin dosyası ile yapılmaktaydı. İnternetteki bilgisayarların isimleri ve IP adresleri bu dosyaya elle kaydediliyordu. İnternetteki bilgisayarların her birinde bu dosyanın bir kopyası bulunmaktaydı. Bir bilgisayar bir başka bilgisayara ulaşmak istediğinde bu dosyayı inceliyor eğer dosyada o bilgisayarın kaydı bulunuyorsa IP adresini alıyor ve iletişime geçiyordu.

# DNS'in Yapısı

- ▶ DNS sistemi isim **sunucuları** ve **özümleyicilerinden** oluşur. İsim sunucuları olarak düzenlenen bilgisayarlar host isimlerine karşılık gelen IP adresi bilgilerini tutarlar.
- ▶ özümleyiciler ise DNS istemcilerdir. DNS istemcilerde, DNS sunucu ya da sunucuların adresleri bulunur.
- ▶ Bir DNS istemci bir bilgisayarın ismine karşılık IP adresini bulmak istediđi zaman isim sunucuya başvurur. İsim sunucu, yani DNS sunucu da eđer kendi veri tabanında öyle bir isim varsa, bu isme karşılık gelen IP adresini istemciye gönderir. DNS veri tabanına kayıtların manuel girilmesi gerekir.

- ▶ DNS sistemi, isim sunucuları ve çözümleyicilerinden oluşur. İsim sunucuları olarak düzenlenen bilgisayarlar, host isimlerine karşılık gelen IP adresi bilgilerini tutarlar. Çözümleyiciler ise DNS istemcilerdir. DNS istemcilerde, DNS sunucu ya da sunucuların adresleri bulunur.
- ▶ Bir DNS istemci bir bilgisayarın ismine karşılık IP adresini bulmak istediği zaman isim sunucuya başvurur. İsim sunucu, yani DNS sunucu da eğer kendi veritabanında öyle bir isim varsa, bu isme karşılık gelen IP adresini istemciye gönderir. DNS veritabanına kayıtların elle, tek tek girilmesi gerekir.

► **Resolving (Çözümleme) - Aranılan bir kaydı bulma işlemi:**

- Mesela <http://google.com.tr> adresine karşılık gelen IPv4 adresinin olmasının bulunması. Çözümleme yapan yazılımlar iki çeşit işlem yaparlar; özyineli çözümleme ve özyineli olmayan çözümleme. Sorgularda gönderilen RD (recursion required - özyineli gerekli) bitlerine göre sorgunun türü belirlenir. Özyineli olmayan sorgulara cevap veren sunucular cevap olarak ardışık isim sunucuları verirler. Sonuç olarak yapılan bir sorgu özyineli değil ise <http://google.com.tr> için doğrudan 8.8.8.8 IP'si ya da "makina bulunamadı" cevabı verilebilir. Fakat özyineli bir sorguda cevabı bulmak için başka bir isim sunucusunun IP'sini verebilir.

► **Authoritative Nameserving (Yetkili İsim Sunumu):**

- Bir alan hakkında bilgi bulunduran sunucudur. Mesela yildiz.edu.tr alanının MX (Mail eXchanger), NS (Name Server), A (Address)(Bunlar - Resource Record - Özkaynak Kaydı olarak bilinir) kayıtlarının tutulduğu isim sunucusudur



# DNS Sorgulama

- ▶ DNS; mail sunucuları, domain isimleri ve IP adresleri gibi bilgileri tutan hiyerarşik bir yapıdır. Bir DNS istemcisi, ad çözümlemesi yapmak için DNS sunucularını sorgular. DNS hizmetleri; kullanıcının girdiği bir DNS adını çözüp, IP adresi gibi o ad ile ilişkili bilgileri oluşturur.
- ▶ DNS sorgulaması yapmadan önce yapılan bir tarama sonucunda, DNS bilgileri 'name servers(NS)' ya da 'domain servers' olarak görülür. Bu bilgilerin erişiminden sonra DNS sorgulamasıyla daha fazla bilgiye ulaşılır.
- ▶ Yanlış yapılandırılmış bir DNS sunucusu sonucunda 'Bölge Transferi(Zone Transfer)' olarak bilinen atak yapılabilir. Bölge transferi ile DNS sorgusu yapılan hedefle ilgili birçok bilgiye ulaşılabilir. Bölge transferi; DNS sunucusunun çalıştığı domain ile ilgili bütün verileri içerir. Bu önemli bilgilerin içinde e-posta sunucusunun ismi, IP adresi, kullanılan işletim sistemi ile ilgili bilgiler vardır.

- ▶ Bölge transferlerine karşı bir önlem olarak güvenlik duvarında (firewall) veya ağ geçitlerindeki yönlendiricilerde 53 numaralı TCP portu gelen tüm yetkisiz bağlantılara karşı kapalı tutulmalıdır.
- ▶ DNS sorgulasından bir korunma yöntemi olarak alan adı bir domain değilse, -.tr uzantı ile sonlanmıyorsa 'private domain' haline getirmek bazı tehlikelerden korur. Private domain olan alan adlarında kişisel bilgiler 'Private' halini alır. Yani gerçek bilgiler gizlenir. Ama, private domain her domain sağlayıcıda yoktur.

- ▶ İnternet adresleri ilk önce ülkelere göre ayrılır. Adreslerin sonundaki tr, de, uk gibi ifadeler adresin bulunduğu ülkeyi gösterir. Örneğin tr Türkiye'yi, de Almanya'yı, uk İngiltere'yi gösterir. ABD adresleri için bir ülke takısı kullanılmaz çünkü DNS ve benzeri uygulamaları yaratan ülke ABD'dir.
- ▶ İnternet adresleri ülkelere ayrıldıktan sonra com, edu, gov gibi daha alt bölümlere ayrılır. Bu ifadeler DNS'de üst düzey (top-level) domainlere karşılık gelir. Üst düzey domainler aşağıdaki gibidir:
- ▶ **Com** : Ticari kuruluşları gösterir.
- ▶ **Edu** : Eğitim kurumlarını gösterir.
- ▶ **Org** : Ticari olmayan, hükümete de bağlı bulunmayan kurumları gösterir.
- ▶ **Net** : İnternet omurgası işlevini üstlenen ağları gösterir.
- ▶ **Gov** : Hükümete bağlı kurumları gösterir.
- ▶ **Mil** : Askeri kurumları gösterir.
- ▶ **Num** : Telefon numaralarını bulabileceğiniz yerleri gösterir.
- ▶ **Arpa** : Ters DNS sorgulaması yapılabilecek yerleri gösterir.