

CUMHURİYET ÜNİVERSİTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

DNS ve DHCP

(İşletim Sistemleri Ödevi - No : 2014123007)

1. GİRİŞ

Ağ sunucusu, bir ağ veya internet üzerinden gönderilen istekleri değerlendirip gerekli verileri istemcilere gönderen bilgisayar veya cihaza verilen isimdir. Sunucular genellikle belirli bir görev ve işleyişe sahip özel bilgisayarlardır. Günümüzde çeşitli amaçlarla kullanılan ağ sunucuları bulunmaktadır.

2. DHCP (Dynamic Host Configuration Protocol)

Dinamik istemci ayarlama protokolü, basit olarak sistemdeki bilgisayarlara IP adresi ve buna bağlı olarak çeşitli parametreleri otomatik olarak atamak için kullanılan servistir. Ağa bağlı olan ve bağlanacak olan her bilgisayar için manuel olarak atanması gereken parametreleri otomatik olarak atayarak sistem yöneticisinin işini kolaylaştırır.

2.1. Ağa bağlı bilgisayarların kimliklendirilmesi

- 1) IP Adresi : Ağa bağlanan her bilgisayarın bir IP adresine sahip olması gerekir. DHCP sunucusu ağa bağlanan her bilgisayarın farklı ve özgün bir IP adresine sahip olmasını sağlar.
 - 2) Ağ Alt Maskesi (IP maskesi): İki cihaz veya bilgisayarın aynı ağda olup olmadıklarını kullandıkları ağ alt maskeleri belirler. Ağ alt maskesi IP adresinin ilk 24 bitine karşı gelen kısımdır. Ağa bağlı her ethernet kartı için bir ağ alt maskesi bulunmalıdır.
 - 3) Gateway IP Adresi : Eğer bilgisayarların bağlı bulunduğu ağın internet bağlantısı var ise ağda bulunup internete bağlanacak olan bilgisayarların bir gateway(geçit) IP adresine sahip olması gerekir.
 - 4) DNS IP Adresi : Bir ağ için en az bir, tercihen iki adet DNS IP adresinin önceden belirlenmiş olması gerekir. DNS IP adresi , ağdaki bir bilgisayar için name resolving işlemi yapacak olan sunucunun IP adresidir.
-

2.2 DHCP Sunucusu

DHCP sunucusu bir ağdaki bilgisayarları kimliklendirme işlemini otomatik olarak gerçekleştiren bir bilgisayardır. Ağa bağlanan bir bilgisayar için bu kimliklendirme işlemini adım adım şu şekilde sıralayabiliriz.

DHCP discover : Bir bilgisayar ağa ilk defa bağlandığında veya ağa bağlı bir bilgisayar ilk defa açıldığında, tüm ağa DHCPDISCOVER mesajını broadcast eder. Bu mesaj bilgisayarın, ağa bağlı bulunan herhangi bir DHCP sunucusunun olup olmadığını anlama şeklindedir. DHCPDISCOVER mesajının içeriği;

- Hedef IP Adresi : Bilinmemektedir. 255.255.255.255 IP adresi ile broadcast edilir.
- Hedef MAC adresi : Bilinmemektedir. FF.FF.FF.FF.FF.FF adresi ile broadcast edilir.
- Kaynak IP adresi : Mesajı gönderen bilgisayarın(istemci) IP adresi daha atanmadığı için 0.0.0.0 değerine sahiptir.
- Kaynak MAC adresi : Mesajı gönderen bilgisayarın MAC adresidir. Ethernet kartının adresi olduğundan bellidir. Örneğin : 01:23:45:67:89:AB

DHCP offer : DHCP sunucusu, istemci tarafından ağa broadcast edilen discover mesajını alır. Kendi IP veritabanını sorgulayarak istemciye verilecek olan IP adresini belirleyerek DHCPOFFER mesajı ile istemciye bildirir. Ağa bağlı bulunan birden fazla DHCP server bulunabilir. İstemci bu durumda gönderdiği discover mesajına en hızlı cevap veren DHCP sunucusunun IP bilgilerini benimseyecektir. DHCPOFFER mesajının içeriği;

- Hedef IP Adresi : Onaylanmadığı için halen 0.0.0.0 adresidir.
- Hedef MAC Adresi : İstemci bilgisayarın MAC adresidir. 01:23:45:67:89:AB
- Kaynak IP adresi : DHCP sunucusunun IP adresi. 10.0.0.1
- Kaynak MAC adresi : DHCP sunucusunun MAC adresi. 0F:44:56:76:90:FC

DHCP request : İstemci kendisine tahsis edilen IP adresinin kiralandığına dair DHCP sunucuya bir broadcast mesajı yollar. Eğer istemci birden fazla DHCPOFFER mesajı aldıysa ikinci bir broadcast mesajı ile diğer DHCP sunucularına artık bir IP adresi olduğunu bildirir.

DHCP acknowledgement : DHCP request mesajını alan DHCP sunucusu artık istemci ile ilgili gerekli kayıtları yaparak gerekli olan ağ alt maskesi,DNS adres veya adresleri gibi diğer parametreleri istemciye gönderir.

DHCP sunucusu istemciye bildirdiği IP adresini, istemciye belirli bir süreliğine tahsis eder. Bu yüzden bu işleme IP kiralama(leasing) işlemi adı verilmektedir. Bu kiralama süresini DHCP sunucusunu kuran ağ yöneticisi belirler.

2.3 DHCP Relay

Farklı LAN ya da WAN'lar için DHCP sunucusunun IP atama işleminin gerçekleştirebilmesi için ağları birbirine bağlayan router'ların ayarlanması işlemidir. Bir yerel ağda bulunan DHCP sunucusun başka bir yerel ağdaki bilgisayara IP atayabilmesini sağlar.

DHCP relay için IP atamasının yapılması istenen ağdaki gateway(router)'ın dışarıdan

gelen DHCP mesajlarını ağı iletmesi gerekir. Bunun için gerekli ayarlamalar aşağıdaki gibi yapılabilir.

1. enable (Bu komut routera user modunda komutlar girebilmemizi sağlar.)
2. configure terminal (bu komut ile terminali konfigure edeceğimizi belirtiyoruz.)
3. int fa0/0 (Yerel ağın bağılı bulunduğu arayüzü konfigure ediyoruz. Belirtilen fast ethernet arayüzü farklı bir numarada ise komut ona göre tekrar düzenlenmelidir.)
4. ip helper-address <DHCP server address> (IP ataması yapmasını istediğimiz DHCP sunucusunu ayarlıyoruz.)

Belirtilen ağlar farklı yerel ağlar olduğundan sahip oldukları yerel IP adresleri de farklılık gösterebilmektedir. Bu yüzden DHCP sunucusun 2 farklı ağı IP adresi atamasını sağlamak için birden fazla IP havuzu tanımlanmalıdır.

2.4 Routerların DHCP sunucusu olarak ayarlanması

Büyük yerel ağlar ya da geniş alan ağları için DHCP sunucusu kritik bir önem arz etmektedir. Bunun için kullanılacak olan sunucunun hatasız çalışması ve bütün bilgisayarlara takılmadan IP adresi atayabilmesi gereklidir. Bu yüzden DHCP sunucuları seçilirken kullanılacak olan bilgisayarın, ağın potansiyel durumuna göre seçilmesi ve ihtiyaçları karşılayabilmesi istenir. Fakat ev veya küçük ofisler gibi bilgisayar sayısı birlirli bir limiti geçmeyen ağlar için DHCP sunucusu kullanmak gerekmebilir. Bu tür ağlar için routerlar DHCP sunucusu olarak görev yapabilmekte ve ufak çaplı IP atama işlemlerini gerçekleştirebilmektedirler. Bunun için gereken komutlar aşağıdaki gibidir.

1. enable
2. configure terminal
3. ip dhcp pool <pool_name>
4. network <ip_address> <subnet_mask>
5. dns-server <ip_address>
6. ip dhcp excluded-address <starting_ip_address> <end_ip_address>
7. copy run start (belirliten ayarlar router başlatıldığında otomatik olarak ayarlanacaktır.)

3. DNS (Domain Name System)

Alan adı sistemi, host isimleri ile IP adresleri arasında çift taraflı dönüşüm sağlayan dağıtık bir veritabanıdır. Bu sistem dünyanın en geniş ve en aktif dağıtılmış veritabanını oluşturarak internetin devamlılığını sağlar. Aynı zamanda da, internetteki alan adlarının tutulduğu ve e-posta alma-gönderme sağlayıcılarına ait bilgilerin de saklandığı yerdir.

3.1 DNS Hiyerarşisi

DNS sisteminin en üstünde bulunan root sunucuları internet ortamında kritik bir rol üstlenmektedirler. Çünkü host isimleri-ip dönüşümü ilk olarak root sunucularında başlar. Root sunucuları Top-Level Domain(Üst Düzey Alan) sunucularının adresini bilirler ve gelen

istekleri gerekli TLD sunucularına yönlendirirler.

DNS veritabanı sistemi en tepede root sunucularının yer aldığı ağaç yapısındadır. Ağaç yapısındaki dallanma maksimum 127 basamaktır. Her nokta maksimum 63 karakterden oluşabilmektedir. DNS sisteminde root nokta (.) ile gösterilir. Veritabanı üzerindeki her bir alt nokta “domain”; bu domainden kollara ayrılan her bir parça ise “subdomain” olarak adlandırılır. Bir adres en alttan root’a gelecek şekilde gösterilir. Aynı düğüm (parent node) altındaki düğümlerin (children node) farklı isimde olması gerekir. Böylelikle domain adları tek olması sağlanmış ve olası çakışmalar önlenmiş olur.

İsim çözümleme işleminde sorgulama sağdan sola doğru gerçekleştiğinden en üst düzeydeki yetkili kısım en sağdaki kısım olmaktadır. ceng.ktu.edu.tr adresinde bu kısım “.tr” dir. Daha sonra edu.tr à ktu.edu.tr alt alan adları gelmektedir. Buradaki sıralama genelden özele doğrudur. Sağdan sola gidildikçe alt alan adlarının barındırdıkları IP adresi sayıları azalır.

3.2 DNS Mimarisi

DNS sistemi isim sunucuları (name server) ve özümleyicilerden (resolver) oluşur. İsim sunucuları host isimlerine karşılık gelen IP adres bilgilerini tutarlar. Çözümleyiciler ise DNS istemcileridir(client), bilgisayarlara yüklü TCP/IP protokolünün bir bileşenidir ve DNS sunucu yada sunucularının adreslerini içerir.

DNS serverları herhangi bir domain/zone için yetkili olup olmamalarına göre ikiye ayrılır.

- Authoritative DNS Name Server : Bu sunucular yetkilendirilmiş sunuculardır. Bir zone veya domain için yapılan tüm DNS sorgularından sorumludur. Birincil Sunucu (Master Server) ve İkincil Sunucu (Slave Server) olmak üzere iki farklı türü bulunmaktadır.
- Non-Authoritative DNS Name Caching Server : Bir zone veya domain için yetkilendirilmemiş sunucular da bulunmaktadır. İlk sorgulamada gereken veriyi yetkilendirilmiş sunuculardan aldıktan sonra TTL süresince öne belleklerinde tutarlar. Böylelikle zamandan kazanç sağlamaklarlar.

3.3 DNS Sunucuları

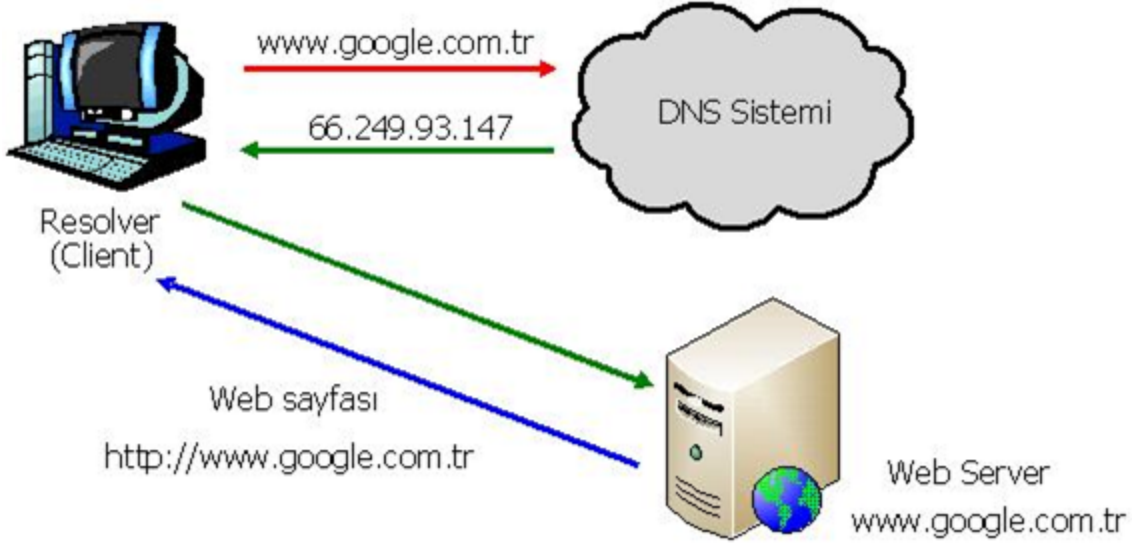
DNS sunucuları, URL (Uniform Resource Locator) ya da FQDN(Fully Qualified Domain Name) olarak adlandırılan adreslerin IP'lere çözümlenmesini sağlarlar. Bu işlem, hatırlaması zor olan IP adreslerini kullanmak yerine, hatırlaması daha kolay olan host isimlerinin kullanımına izin verir.

3.3.1 DNS İsim Çözümlemesi

DNS sunucuları sorumlu olduğu ve de başka yollara ile öğrendiği bütün FQDN'leri ve IP adreslerinin listesini belleğinde saklar. İstemcilerin öğrenmek istediği IP ve FQDN'leri öğrenebilmesi için sorgusunda FQDN/IP, sorgu çeşidini (Kaynak Kaydı(Resource Record)) belirtmesi gerekir.

İstemci tarafından yapılan bir DNS sorgusunun işleyişi şu şekilde gerçekleşir:

1. İstemci öncelikle kendi belleğinde kayıtlı adresleri tarar.
2. İstemci tarafından cache'lenmiş kayıtlara bakar.
3. İstemci kendisinde aradığı cevabı, sorguyu belleğinde kayıtlı DNS sunucularına gönderir.
4. DNS sunucuları gelen sorgunun yetkili olduğu kısımda olup olmadığına bakar
5. Değilse cevabın önbelleğinde olup olmadığını kontrol eder.
6. Eğer DNS sunucusu sorguya cevap bulamazsa, belleğinde kayıtlı Root(Kök) sunucularına sorguyu yönlendirir.
7. Kök sunucuları sorguyu ilgili TLD(Top Level Domain) sunucularına yönlendirir.
8. TLD sunucuları sorguyu ilgili sunuculara yönlendirerek istemciye cevabın iletilmesi sağlanır.



Şekil 1 : DNS İsim Çözümlemesi

Caching : Caching işlemi DNS sorgularını hızlandıran en önemli özelliklerden biridir. DNS sunucuları ve istemciler bir kere öğrendikleri bilgiyi belli bir TTL(Time-To-Live) değeri süresince belleklerinde tutarlar. Böylece yapılacak sonraki aynı sorgular için işlem süresi azalır. Caching ile Root sunucuların sürekli sorgulanması önlenir aynı zamanda da veri trafiğinden tasarruf edilmiş olur.

Çok fazla istek alan alanların (google.com, yahoo.com gibi) tutulduğu sunucularda aşırı trafik meydana gelir. Yük dağılımının yapılması ve yedekleme amacıyla bu alanlar birden fazla sunucuda tutulur. Yani aynı host ismine birden fazla IP adresi atanır.

Ters DNS Çözümlemesi : IP adresinden isim çözümlemesi yapılmasıdır. Ters sorgulama için “in-addr.arpa” adında özel bir domain bulunmaktadır. Örneğin, 160.75.99.72 adresine karşılık gelen bilgisayar ismini bulmak için DNS sunucuya “72.99.75.160.in-addr.arpa” kaydı sorulur.

3.3.1.1 DNS Kaynak Kayıtları (Resource Records)

DNS sunucularının asıl görevi olan isim-ip dönüşümleri Kaynak Kayıtları aracılığıyla yapılır. Kaynak kayıtları formatı RFC¹ 1035 3.2.1. de belirtilmiştir. Kaynak kayıtları genel olarak ;

“ALAN_ADİ-----TTL-----SINIF-----KAYNAK_KAYDI----KAYNAĞA_AİT_VERİ”
şeklindedir.

ALAN_ADİ : Kaynak kaydı yapılacak adresi belirtir.

TTL (Time To Live): Diğer DNS sunucuları/istemcileri tarafından bilginin ne kadar süre ile önbellekte (cache) tutulacağını belirtir.

SINIF : Kaynak kaydın sınıfını belirten anımsatıcı bir değer içerir.

0→Rezerve

1→İnternet (IN)

2→Atanmamış

3→Chaos (CH)

4→Hesiod (HS)

5-65534→Atanmamış

65535→Rezerve

KAYNAK_KAYDI (Resource Record) :

A Kaydı : Adres kaydıdır. 32 bitlik IPV4 adresini DNS domain ismine eşler.

AAA Kaydı : IPV6 için adres kaydıdır. 128 bitlik IPV6 adresini DNS domain ismine eşler.

CNAME (Canonical Name) : Alias yani takma isim yoluyla başka bir DNS sunucuda bulunan kaydın yolunu belirler yani başka bir DNS sunucuda bulunan kaydın farklı bir isimle de kayıt altına alınmasını sağlar. Ancak kullanıcılar aranılan hostun gerçekte nerede olduğunu göremezler.

MX (Mail Exchanger) : Sistemde bulunan mail serverları tanımlamak için kullanılır. Bu kayıt sayesinde mail server'ın bilgileri DNS tarafından bilinmektedir.

TXT (Text) : Belirli bir kaynak hakkında, nerde bulunduğu ve sahipliği gibi açıklayıcı bilgileri içeren bir kayıttır. Bir text dosyadan ibarettir.

NS (Name Server): Ağ üzerinde bulunan ve kullanım da olan DNS sunucuları tanımlar.

¹ *Request For Comments (RFC) : İnternet standartları ve belgelerinin genel adı

3.3.1.2 DNS Sorguları

Ağımızda bulunan istemciler ve DNS sunucular arasında isim çözebilmek için bir sorgu trafiği oluşur. DNS sorguları ağda istemci bir makineden DNS sunucusuna veya DNS sunucusundan başka bir DNS sunucusuna yapılabilir. Bu şekilde rekürsif sorgu ve iteratif sorgu olmak üzere iki çeşit sorgu tipi vardır.

Rekürsif Sorgulama (Recursive Query) : İstemci tarafından DNS sunucusuna yapılan sorgu rekürsif olarak adlandırılır. İstemcinin ağdaki bir kaynağa yada internetteki herhangi bir siteye bağlanmak için IP adresini DNS sunucusuna sorarken yaptığı sorgu tipidir. Bu sorguya DNS sunucusu olumlu yada olumsuz cevap vermek zorundadır. İstemci sorgusunu DNS sunucusuna rekürsif sorgu olarak yapar, DNS sunucusu istemcinin yaptığı sorguyu alır ve üzerindeki kayıtlara bakarak veya diğer DNS sunuculara sorarak cevabı iletir.

İteratif Sorgulama (Iterative Query) : DNS sunucuların kendi aralarında yaptıkları sorgulara denir. Ağda bulunan bir istemci DNS sunucusuna ulaşmak istediği IP adresini sorduğunda DNS sunucusu bu IP adresini biliyorsa istemciye cevap verir. Eğer DNS sunucusu istemcinin istediği isim çözümlemesini kendi veritabanına bakarak yanıtlayamıyorsa internete yada localde bulunan diğer DNS sunucudan sorgular. Bu işlemi istenilen IP adresini bulana kadar sürdürür. İteratif sorguyu alan DNS sunucusu kendi veritabanına ve ön belleğine bakar ve sorguyu yapan DNS sunucusuna IP adresi yada aradığı IP adresini bulabileceği DNS sunucusunun ip adresini bildirir. DNS sunucusunun diğer DNS sunucu yada sunucularla yaptığı sorgulama tipi iteratif sorgulama olarak adlandırılır.
