

A to

Z

*Tarayıcıda Enter'a
Basmak*

Y A V U Z Ç İ Ç E K

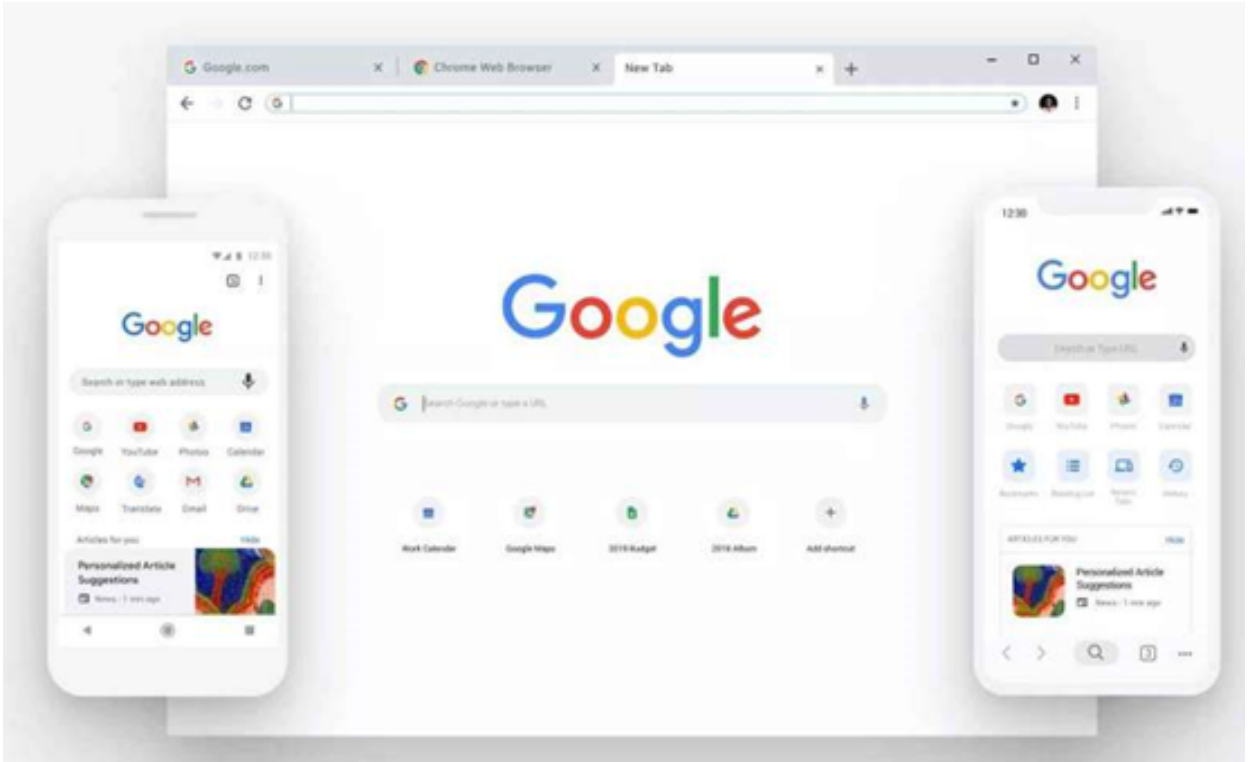
211110024



KUGUVEGA
TECHNOLOGY

Tarayıcıyı Açtık

- **Uygulama imajı RAM'e aktarılır.**
- **Çekirdek, gerekli olan DLL kütüphanelerini tespit eder ve yükler.**
- **Her DLL kütüphanesinin DllMain() fonksiyonu, kendi içerisindeki bağımlılık sırasına göre çalıştırılır.**
- **Yukarıda Bahsedilenleri biraz açmamız gerekirse;**





KUGUVEGA
TECHNOLOGY

Tarayıcın İmajını Almak Nedir ?

- **İmaj Neden Alınır ?**

Bu Sorunun cevabını şu şekilde verebiliriz;

Kullandığımız programlar diskteki verilerin bilgilerinin tutulduğu metadata bilgilerini değiştirir. Bir programla kurtaramayacağımız verileri başka bir programla kurtarmak bazen mümkün olabiliyor. Bunun için orjinal diskin metadatalarını değiştirmemek zarar vermemek için imaj alıp imaj üzerinden işlem yaparız.

Yani burda kastedilen uygulamada direkt değişiklik yaptığımızda metadatalara zarar vermemek için uygulamanın kopyasını alıyormuşuz gibi düşünün. Bunun hakkında bir örnek vermek gerekirse;

Bunun için polisler bir yere baskın yaptığında açık bilgisayar kapatılmaz ve hemen ram imajı alınır. Disk imajı alınırken kapatılması sorun yaratmamaktadır. Fakat RAM bilgisayar kapatıldığında temizlenmektedir.

```
Computer name: WIN-QMKG8MP05G3

--> Proceed with the acquisition ? [y/n] y

[+] Information:
Dump Type: Microsoft Crash Dump

[+] Machine Information:
Windows version: 6.1.7600
MachineId: ED354D56-B100-4285-98ED-C37AE78D0F
TimeStamp: 131548315304852350
Cr3: 0x185000
KdDebuggerData: 0x82b7abe8

Current date/time: [2017-11-10 <YYYY-MM-DD> 23:52:10 <
```



KUGUVEGA
TECHNOLOGY

• **Dynamic Link Library(DLL) Nedir ?**

DLL İngilizce Dynamic Link Library, Türkçe anlamı Dinamik Bağlantı Kütüphanesi'dir. Adı Dynamic Link Library baş harfleri alınarak kısaltılmıştır.

DLL dosyaları görevi çalışan programların ortaklaşa yapmış olduğu işlemleri tek bir dosya içinde yapmak, program çalışma esnasında gerekli olan fonksiyonları kendi içerisinde bulunmaz ise bunu dinamik link kütüphanesi'nde yani DLL dosyasında aramaktadır. Bu şekilde programlar tek bir dosya üzerinden çalışarak bellek kullanımını minimum seviyeye düşürerek hem program hızını ve bilgisayar hızını artıracak, birçok DLL dosyasını yerine tek bir DLL dosyası kullandığından hard disk üzerinde fazla yer kaplamayacaktır.

Programlar işlevlerini devam ettirmek için DLL dosyaları içerisinde bulunan işlemlerden yardım alarak çalıştırma bütünlüğü sağlamaktadır. Bir exe dosyası nasıl programın çalışmasında gerekli ise DLL dosyasında aynı şekilde programın çalışmasında gerekli sistem dosyalarıdır.

DLL dosyaları çalıştırmış olduğu programların ayrılmaz bir bütündür ve tek başına çalışmazlar. Eğer ilgili DLL dosyası bulunamaz, ismi veya içeriği hatalı bir şekilde değişirse DLL dosyası eksikliği veya hatalı DLL dosyası nedeni ile programlar işlevini devam hale getiremezler.

Programların ihtiyaç duydukları DLL dosyalarının her biri farklı isimde olabilir ama uzantıları tüm DLL dosyaları için .dll olmak zorundadır. Bir DLL dosyası ses ile alakalı işlemlerini yerine getirirken diğer DLL dosyaları görüntü ile alakalı işlevleri yerine getiriyor olabilir, her DLL dosyasının farklı, farklı işlevleri bulunmaktadır.

Özetlemek gerekirse DLL threadlere bölünmüş dosyaları bütünleyerek fazla yer kaplamadan programların işlevini yerine getirir





KUGUVEGA
TECHNOLOGY

- **DLLMain() Nedir ?**

Dinamik bağlantı kitaplığına (DLL) isteğe bağlı bir giriş noktası. Sistem bir işlemi veya iş parçacığını başlattığında veya sonlandırdığında, işlemin ilk iş parçacığını kullanarak yüklenen her DLL için giriş noktası işlevini çağırır. Sistem ayrıca LoadLibrary ve FreeLibrary işlevleri kullanılarak yüklendiğinde veya kaldırıldığında bir DLL için giriş noktası işlevini de çağırır . Aşağıdaki örnekte daha detaylı bir şekilde görebilirsiniz

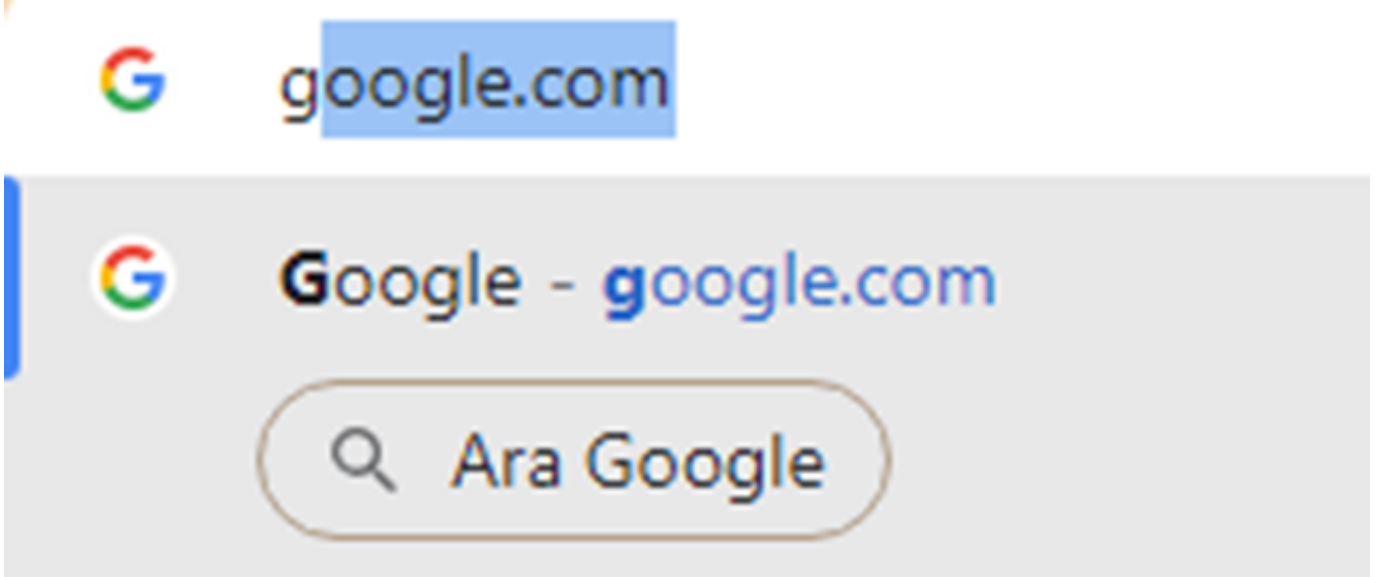
```
BOOL WINAPI DllMain(  
    HINSTANCE hinstDLL,    // handle to DLL module  
    DWORD fdwReason,       // reason for calling function  
    LPVOID lpReserved )    // reserved  
{  
    // Perform actions based on the reason for calling.  
    switch( fdwReason )  
    {  
        case DLL_PROCESS_ATTACH:  
            // Initialize once for each new process.  
            // Return FALSE to fail DLL load.  
            break;  
  
        case DLL_THREAD_ATTACH:  
            // Do thread-specific initialization.  
            break;  
  
        case DLL_THREAD_DETACH:  
            // Do thread-specific cleanup.  
            break;  
  
        case DLL_PROCESS_DETACH:  
            // Perform any necessary cleanup.  
            break;  
    }  
    return TRUE;    // Successful DLL_PROCESS_ATTACH.  
}
```



KUGUVEGA
TECHNOLOGY

- **Tarayıcıda Basılan Tuş**

Kullandığınız tarayıcının çalışma prensibine ve ayarlarına bağlı olarak, “g” tuşuna bastığınızda tarayıcı otomatik doldurma fonksiyonu ile size önerileri getirir. Buradaki fonksiyon genellikle cache ve cookie prensibi üzerinden çalışır..



Yukarıda anlatılan terimlere biraz detaylı şekilde incelemek gerekirse



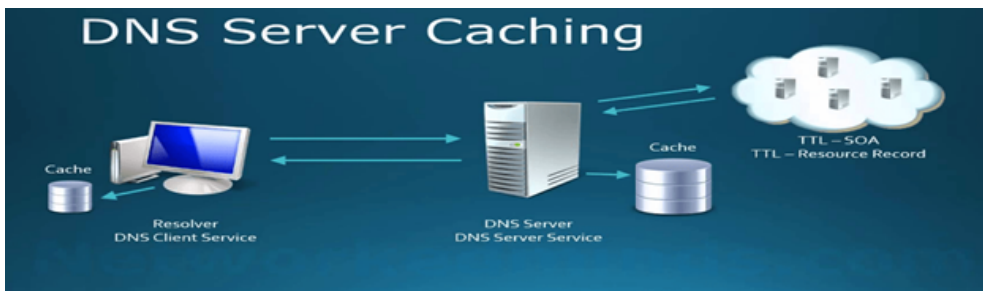
KUGUVEGA
TECHNOLOGY

• Cache Nedir ?

Daha fazla hız isteyen günümüz internet kullanıcısının en büyük problemlerinden biri de, girmek istediği web sitesinin geç açılmasıdır. Eğer internet kullanıyorsanız, bu durum her internet kullanıcısı gibi sizin de başına mutlaka gelmiştir.

Örneğin, büyük görüntüler içeren bir web sayfası düşünün. Bu sitenin açılmasını beklemek, belirli bir sürenin üzerine çıkınca çok sıkıcı bir hal alır. Bu yüzden, aynı siteye girerken her seferinde beklemeyin diye tarayıcının önbelleği bazı bölümleri saklar. Aynı sayfaya tekrar erişmek isterseniz, yazılım önbelleğinde depolanan içeriğe (geçici dosyalar biçiminde), internet üzerinden indirmeye gerek kalmadan doğrudan erişebilirsiniz. Bu da tarama hızını artırır. Yani bir web sitesini ilk kez ziyaret ediyorsanız, tarayıcınız sonraki ziyaretlerinizde bu web sitesine daha verimli şekilde erişmenizi sağlayacak bilgileri tutar.

Önbellekleme web’de gezinme performansınızı artırırken, web sayfalarının tarayıcıda önbelleğe alınması nedeniyle gizli ve hassas bilgiler içerdiği için sizi bilgisayar korsanlarına karşı savunmasız bırakabilir. Bu, teorik olarak kimlik doğrulama verilerinizi, oturum bilgilerinizi veya gizli müşteri bilgilerinizin görünür olmasını sağlayabilir. Tarayıcı gözetimsiz bırakılırsa ve başka bir kullanıcının buna erişimi varsa, örneğin işyerinde paylaşılan bir bilgisayarda, bir sonraki kullanıcı tarayıcı önbelleğinden önceki kullanıcının geçmişine erişebilir ve gizli olabilecek verileri görebilir.





KUGUVEGA
TECHNOLOGY

• **Cookie Nedir ?**

Çerezler: bir web sayfası ziyaret edildiği zaman tarayıcılardaki kullanıcıların depolandığı küçük dosyalardır. Kişilerin web siteleri üzerinde aradıklarını tarayıcı geçmişinde kayıt tutar. Site üzerindeki hareketleri tarayıcı kayıtlarında tutarak bir web sitesine izin verir.

Cookies 1994 yılında Netscape firması tarafından kullanılmaya başlanmıştır. İlk kullanım amacı bir kullanıcının girdiği siteye, tekrar girip girmediğini kontrol etmek içindi. Günümüzde cookies esas amacından fazla sapmadan fakat çok daha fazla bilgi almak için kullanılmaktadır.

Hatırlanmamızı sağlayan cookies yani çerez yada kurabiye dediğimiz text dosyalarıdır. Bilgilerimiz bu dosyalara yazıldığında aynı sitelere girdiğimizde bizi tanıyarak tekrar bilgilerimizi yazmaya gerek kalmaz.

İnternette çeşitli web sitelerinde dolaşır, bazılarına üye oluruz. Üye olduğumuz bu sitelere girerken her seferinde kullanıcı adı ve şifremizi girmemek için beni hatırla ikonuna tıklarız. Bu ikona tıkladığımız andan itibaren çerezler devreye girer. Bize özel text dosyasına bilgilerimiz kaydedilir. Cookies’lerden okunan bilgiler sayesinde, siteyi açtığımız andan itibaren bilgilerimiz siteye ulaşır ve bizi tanır.



Yukarıdaki Resime baktığımızda Dallandığını görmekteyiz



KUGUVEGA
TECHNOLOGY

- **Cache Ve Cookie Arasındaki Farkı**

Önbellek ve çerez arasındaki fark, önbellek, müşterinin makinesinde web sayfalarını hızlı bir şekilde yüklemek için web kaynaklarını saklamak için geçici bir bellektir ve bir çerez, kullanıcının tercihlerini ve gezinme etkinliklerini sürdürmek için müşterinin makinesinde depolanan küçük bir bilgi parçasıdır.

Cyber Technophile

Cache



Vs

Cookies





KUGUVEGA
TECHNOLOGY

- **Enter Tuşuna Bastığımızda**

Klavyenin USB veya sanal olması buradaki akışı biraz değiştirse de, genel olarak:

- Klavyenin mantıksal devresine elektrik akımı gider.
- Bu akım, keyCode değerine dönüştürülür ki “Enter” tuşuna ait değer 13’tür.
(Burda eklememiz gerekirse KeyCode’dan kastedilen şey binary sistemidir)
- Klavye, sinyali IRQ’ye gönderir.
- IRQ, klavye tuşlarına basılması, mouse hareketleri gibi donanımsal eylemlerde işlemciye sinyal gönderir ve işlemci eylemin kimliğini belirten ve çekirdek tarafından sağlanan IDT’ye göre bu sinyali işler.





KUGUVEGA
TECHNOLOGY

• IRQ Nedir ?

"Interrupt Request" ifadesinin harflerinden kısaltılarak oluşturulmuştur. Bir süre bilgisayar kullanan herkes su ünlü "IRQ çakışması" tabirini duyar. IRQ 'nun Türkçesi "kesme" dir. Yani işlemci bir işle meşgulken, bilgisayarın bir yerinden baska bir donanımdan işlemciye söyle bir emir geliyor: "Benimle de ilgilen!" Bu istek işlemcinin işini böler. Tabii işlemci aynı anda çok sayıda işi birden yapabilir.

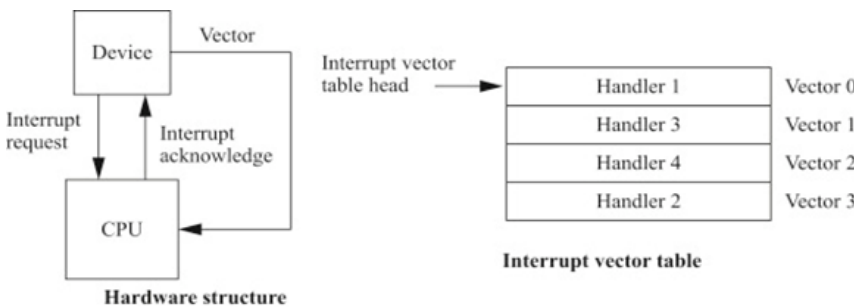
Klavye ve fare kullanırken bir yandan ekrana gönderilen verileri işler, sabit diskten okuma yapar, modemini indirdiği dosyalara bakar...

IRQ çakışması

İşlemciye işini görmesi için ihtiyaç duyan bir aygıtın ona sinyal gönderebilmesi için özel bir hatta ihtiyacı vardır. Buna "IRQ hattı" adı verilir. Bilgisayarımızda 0'dan 15'e kadar numaralanan 16 IRQ hattı vardır. İki aygıt aynı IRQ hattını kullanmaya kalkarsa çakışma meydana gelir ve o aygıtlar kullanılamaz. Aygıtın birinin ayarlanarak boş olan bir hatta yönlendirilmesi gerekir.

IRQ hatları

- IRQ 0: Sistem saati.
- IRQ 1: Klavye
- IRQ 2: Programlanabilir IRQ denetçisi. (Modemler, COM3 ve COM 4 portları)
- IRQ 3: COM 2 portu (modemler, COM 4, ses ve ağ kartları, teyp yedekleme birimlerini hızlandıran kartlar)
- IRQ 4: COM 1 portu (modemler, COM 4, ses ve ağ kartları, teyp yedekleme birimlerini hızlandıran kartlar)
- IRQ 5: Ses kartı (LPT2, LPT3 - yani ikinci ve üçüncü paralel portlar - COM 3, COM 4, modemler, ağ kartları, MPEG kartları, teyp yedekleme birimlerini hızlandıran kartlar)
- IRQ 6: Disket sürücü denetleyicisi (teyp yedekleme birimlerini hızlandıran kartlar)
- IRQ 7: LPT1, yani ilk paralel port (LPT2, COM 3, COM 4, modemler, ağ kartları, ses kartları, teyp yedekleme birimlerini hızlandıran kartlar)
- IRQ 8: Gerçek zamanlı saat.
- IRQ 9: (Ağ kartları, ses kartları, SCSI kartları, PCI aygıtlar, yeniden yönlendirilen IRQ2 aygıtları)
- IRQ 10: (Ağ kartları, ses kartları, SCSI kartları, PCI aygıtlar, ikinci ve dördüncü IDE kanalları)
- IRQ 11: (Görüntü kartları, ağ kartları, ses kartları, SCSI kartları, PCI aygıtlar, üçüncü ve dördüncü IDE kanalları)
- IRQ 12: PS/2 fare (Görüntü kartları, ağ kartları, ses kartları, SCSI kartları, PCI aygıtlar, üçüncü IDE kanalı)
- IRQ 13: FPU, yani matematik işlemci.
- IRQ 14: Birinci IDE kanalı (SCSI kartlar)
- IRQ 15: İkinci IDE kanalı (Ağ ve SCSI kartlar)



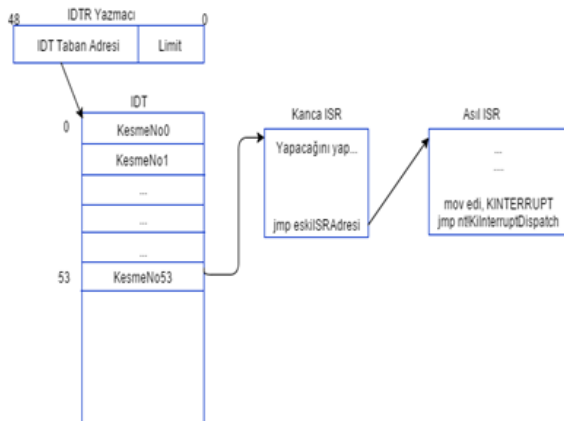


KUGUVEGA
TECHNOLOGY

- **IDT Nedir ?**

IDT tabloları işletim sistemi tarafından gerçek moddan korumalı moda geçerken IVT'ye karşılık olarak yaratılır. Her işlemcinin kendi IDT adresini gösteren ayrı bir IDTR yazmacı bulunmaktadır, yani her işlemcinin kendi IDT tablosu var. Bunu bilmek önemli çünkü IDT kancalama yaptığınızda diğer işlemcileri unutmamalısınız. Basit olarak IDT tablosu ISR2(Interrupt Service Routines - Kesme Servisi Rutinleri)'lara erişmemizi sağlayan 8 bayt boyutunda (Interrupt Gate-Kesme Kapısı) yapılar içermektedir. Bu rutinler bahsi geçen kesme oluştuğunda yapılacak olan işlemleri içeriyor isminden anlaşılacağı gibi. İşletim sistemi kesme her çalıştığında ona ait olan ISR'yi çalıştırarak gerekli işlemlerin gerçekleşmesini sağlıyor. Son olarak ilk 32 girdimiz CPU için ayrılmış olup, geri kalanlar sistem ve kullanıcının kullanımına bırakılmıştır.

IDT kancalama ise, basitçe IDT içerisinde bir girdideki ISR adresini bizim oluşturduğumuz ISR ile değiştirmek demek. (Ya da dilerseniz komple IDT girdisini de değiştirebilirsiniz tabi..) Yani kısaca asıl kesme rutinini, bizim belirlediğimiz rutin ile değiştirmek demek. Yani aşağı yukarı aşağıdakine benzer bir şey:



Kesme (Interrupt)

ISR (Interrupt Service Routine) nedir?

- ISR, mikroişlemcide yapılan kesmelerin yönetilmesinden sorumlu olan bir programdır.



KUGUVEGA
TECHNOLOGY

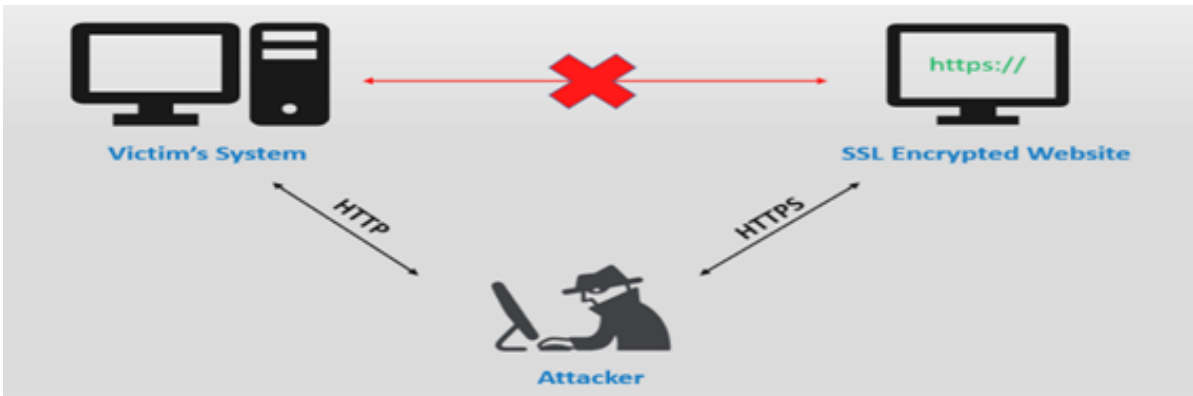
• HSTS Kontrolü Nedir ?

HTTP Strict Transport Security (HSTS), User-Agentlara ve web tarayıcılarına en baştan ve tarayıcıya geri gönderilen bir yanıt başlığı üzerinden bağlantılarını nasıl kullanacaklarını bildiren bir web sunucusu yönergesidir.

Kısaca HSTS, web sunucunuz veya web barındırma hizmetiniz için güvenlik ayarları ile ilgili tam güvenliğı sağlayabilecek yoldur.

Web sitenizde bulunan SSL sertifikası kapıyı kapatmak olabilir ve bilirsiniz ki bazen sadece kapıyı kapatmak yetmez. Web siteleriniz için de bazen SSL yeterli olmayacaktır çünkü insanlar web sitenize "http://" üzerinden erişmenin bir yolunu bulabilir. HSTS (HTTP Strict-Transport-Security), tarayıcıları ve uygulama bağlantılarını varsa HTTPS kullanmaya zorlar. Böylece birisi sadece http://www veya http:// yazsa bile, http:// olarak gelen istekler, HSTS protokolüne göre direkt olarak HTTPS olarak alınır.

Tarayıcı, sadece HTTPS üzerinden gelen istekleri işleyen web sitelerin listesini HSTS üzerinden denetler. Söz konusu website listede bulunuyorsa, HTTP protokolü yerine HTTPS üzerinden istek gönderilir.



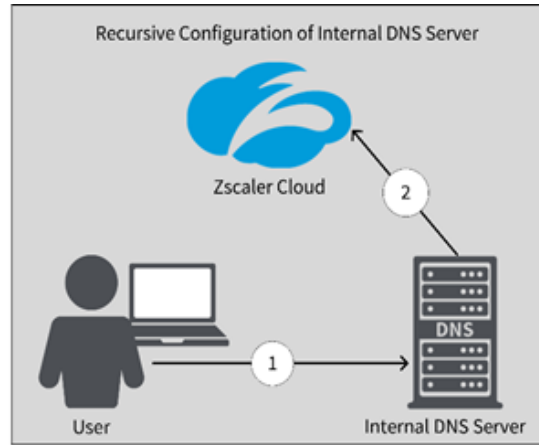
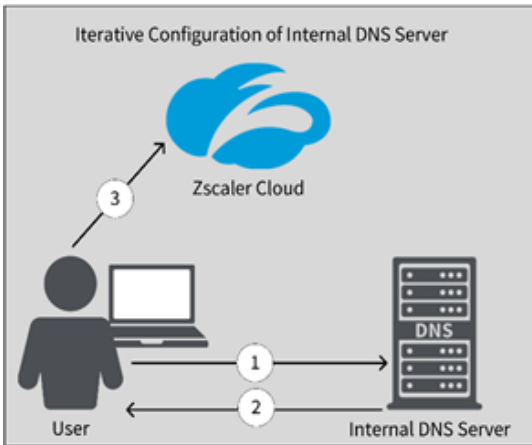


KUGUVEGA
TECHNOLOGY

• DNS Kontrolü Nedir ?

- Tarayıcı, adresin cache’de olup olmadığını denetler, şayet bulunmuyorsa birçok majör işletim sisteminde “gethostbyname” fonksiyonu tetiklenir.
- gethostbyname fonksiyonu, DNS üzerinden kontrol etmeden önce yerel dosya sistemindeki “hosts” dosyasının ilgili host adını çözümleyip çözümlemediğini kontrol eder.
- Bu aşamada eğer cache üzerinde ve hosts dosyası üzerinde çözümleme yapılamazsa, ISP veya router düzeyinde DNS sunucusuna istek yapılır.

DNS sunucusunun bulunduğu subnet’e göre ARP süreci başlatılır





KUGUVEGA
TECHNOLOGY

- **Hosts Dosyası Nedir ?**

Hosts ya da yaygın kullanımıyla host dosyası, bir internet sitesine girebilmek için ihtiyaç duyulan Internet Protocol olarak bilinen IP adreslerinin yazılı olduğu dosyadır. Kullanıcının istediği internet sitesine girmek için, İnternet tarayıcı satırına sitenin adresini yazmasıyla birlikte, bilgisayarınızın işletim sistemi öncelikle kendi dosyaları arasında bulunan hosts dosyalarında bu internet sitesinin adresini arar.

Ad	Değiştirme tarihi	Tür	Boyut
hosts	14.02.2020 15:42	Dosya	2 KB
hosts.ics	14.08.2019 23:02	iCalendar File	1 KB
lmhosts.sam	19.03.2019 07:49	SAM Dosyası	4 KB
networks	30.10.2015 10:21	Dosya	1 KB
protocol	30.10.2015 10:21	Dosya	2 KB
services	30.10.2015 10:21	Dosya	18 KB



KUGUVEGA
TECHNOLOGY

- **ISP Nedir ?**

internet çözüm bulmak, çalışmak, ulaşmak ve çok daha fazlası için hayatın her alanına dokunan bir kılavuздur.

Bu nedenle hızlı ve güvenilir bir internet bağlantısına duyulan ihtiyaç gün geçtikçe artmaktadır. İhtiyaçlar arttıkça sunulan internet hizmetleri ve sağlayıcıları da aynı doğrultuda farklılaşabilir. ISP (Internet Service Provider) olarak bilinen internet servis sağlayıcı, farklı abonelik türleri ile internete bulunduğunuz yerden erişmenizi sağlayan bir araçtır. Hizmet verilen coğrafyaya göre değişen ISP'ler arasında yaygın olarak kullanılan bazı firmalar bulunur. Türkiye'de bulunan ISP firmaları arasında BİMcell, Millenicom, Pttcell, TTNET, TTNET Mobil, Turk.net, Turkcell, Turkcell Superonline, Uydunet, Vodafone bulunur. Kullandığınız servisin hangi firma tarafından verildiğini öğrenmek için modem arayüzüne giriş yaptıktan sonra çıkan bağlantı bilgileri kısmından "kullanıcıadi@firmaadi" şeklinde verilen bilgiye ulaşmak yeterlidir. ISP firmaları kullanıcı ile internet arasındaki trafiği bir bütün halinde sunmayı amaçlayan erişim sağlayıcılarıdır. Ancak kullanıcının konumuna ve kullanımına bağlı olarak paketlenmiş bazı hizmetleri de sunabilir. Alan adı tescili, tarayıcı ve yazılım paketleri, web barındırma ve e-posta hizmetleri bu bilişim kaynakları arasında yer alır.





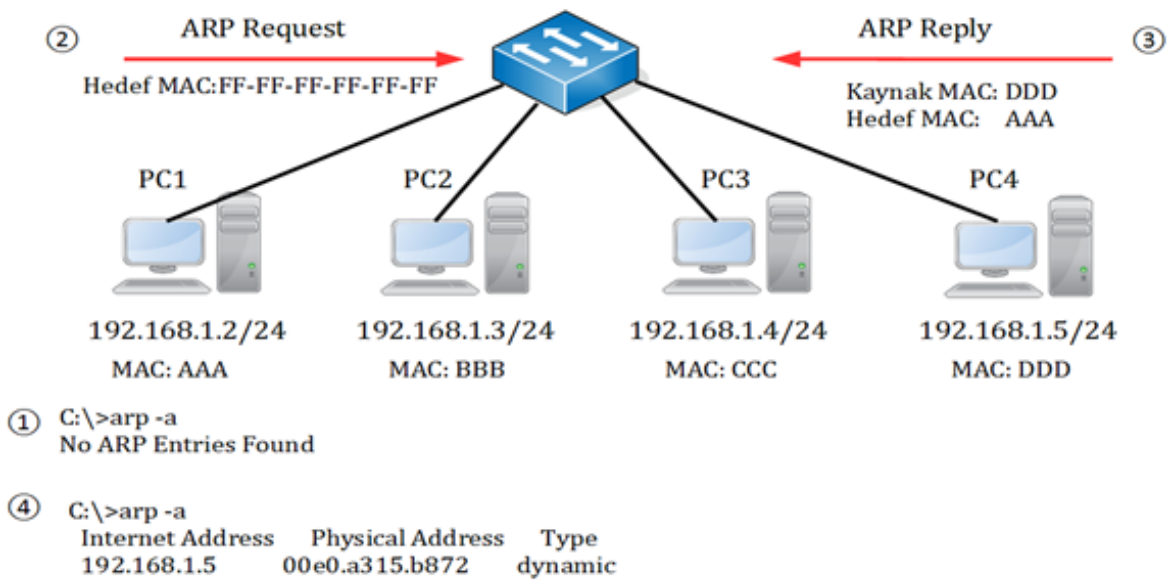
KUGUVEGA
TECHNOLOGY

- **ARP Nedir ?**

Adres Çözümleme Protokolü (ARP), Internet Protokolü adresinin (IP adresi) yerel ağda tanınan fiziksel makine adresine eşlenmesi için kullanılan bir protokoldür. Örneğin, günümüzde kullanımda olan en yaygın IP seviyesi olan IP Sürüm 4'te bir adres 32 bit uzunluğundadır. Ancak bir Ethernet yerel alan ağında bağlı cihazların adresleri 48 bit uzunluğundadır. (Fiziksel makine adresi, Medya Erişim Denetimi veya MAC adresi olarak da bilinir.)

Genelde ARP önbellege olarak adlandırılan bir tablo, her MAC adresi ile karşılık gelen IP adresi arasında bir ilişkiyi sürdürmek için kullanılır.

ARP, bu korelasyonu yapmak ve her iki yönde adres dönüşümü sağlamak için protokol kurallarını sağlar.





KUGUVEGA
TECHNOLOGY

- **ARP**

- Ağ katmanına ARP broadcast'i gönderilmeden önce IP adresi ve MAC adresi kontrol edilir.
- ARP'nin cache mekanizması hedef IP adresini bulduğunda ilgili kütüphane fonksiyonunu çalıştırır.
- Bu noktada adres cache içerisinde bulunmuyorsa, yerel Route tablosundaki subnet'ler kontrol edilir.
- OSI modelinin ikinci katmanı olan "Data Link"e ARP isteği gönderilir.
- Burada donanım farklılığına göre farklı aşamalar devreye girer, direkt bağlantıda Router "ARP Reply" yanıtını gönderir. 6. Switch bağlantısı varsa, CAM tablosu kontrol edilerek MAC adresi ve port eşlemesi yapılır.

Ağ katmanı, varsayılan gateway veya DNS sunucusu üzerinden IP adresine eriştikten sonra UDP isteği yapılmak üzere 53. port aktif olur.

IP adresi alındıktan sonra, tarayıcı TCP socket stream'i iletmek üzere "socket" isimli sistem fonksiyonunu çağırır. Bu stream isteği ilk olarak 4. katmanda (Transport) işlenir ve bir TCP segmenti hazırlanır.

Segment, ağ katmanına iletilir. IP header bilgisi paket formatına dönüştürülür ve bu paket Link katmanına gönderilir.

Bu aşamadan sonra paketler, 0 ve 1 sinyallerinin analog sinyale dönüştürülmesi üzere modeme iletilir ve yerel subnet'i yöneten Router'a ulaştırılır. İletim boyunca her Router, IP header bölümünden sonraki varış adresi bilgisini alır uygun olan bir sonraki Router'a iletir. Burada TTL devreye girer ve her geçen Router üzerinden TTL azaltılır. Son varılan Router kuyruğunda yer yoksa veya sıfır değerine ulaşırsa, paket drop edilir.

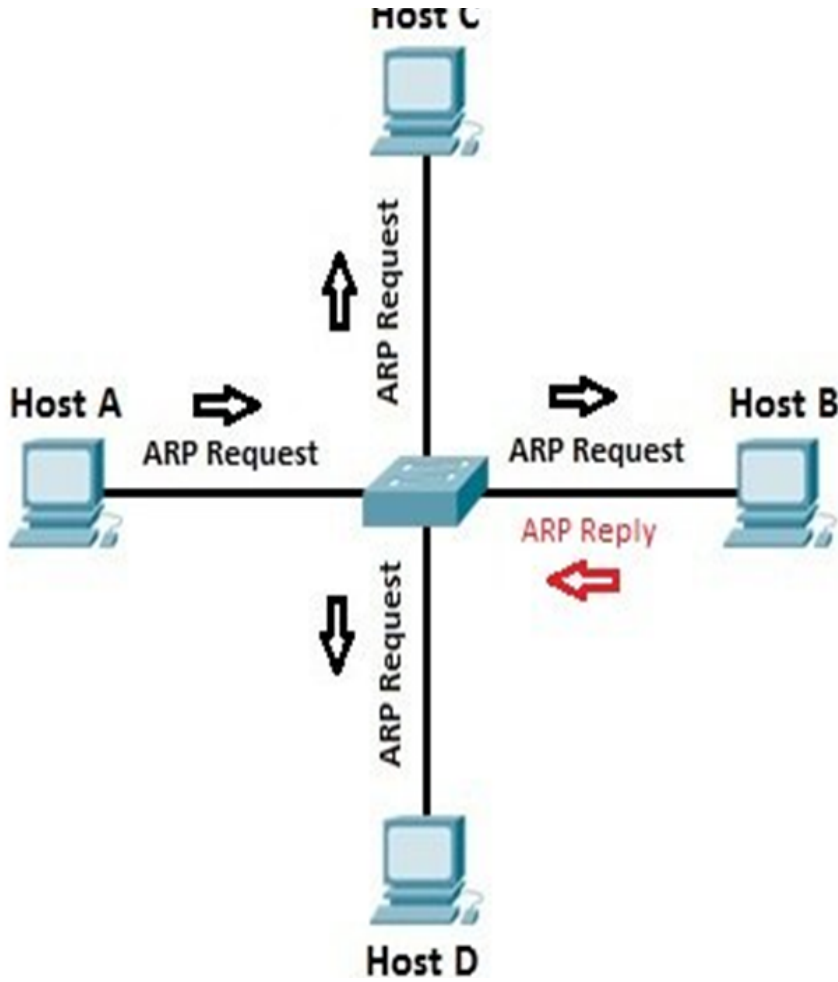


KUGUVEGA
TECHNOLOGY

Bu aşamadaki TCP akışı birden çok gerçekleşir ve Handshake aşaması başlatılır.

- **Sunucu, SYN paketini oluşturmak üzere ISN'i belirler.**
- **İstemci ISN'si + 1 formülü ile ACK paketini ekler.**

İstemci, kendi tarafındaki ISN'yi artırır ve ACK'yi belirler

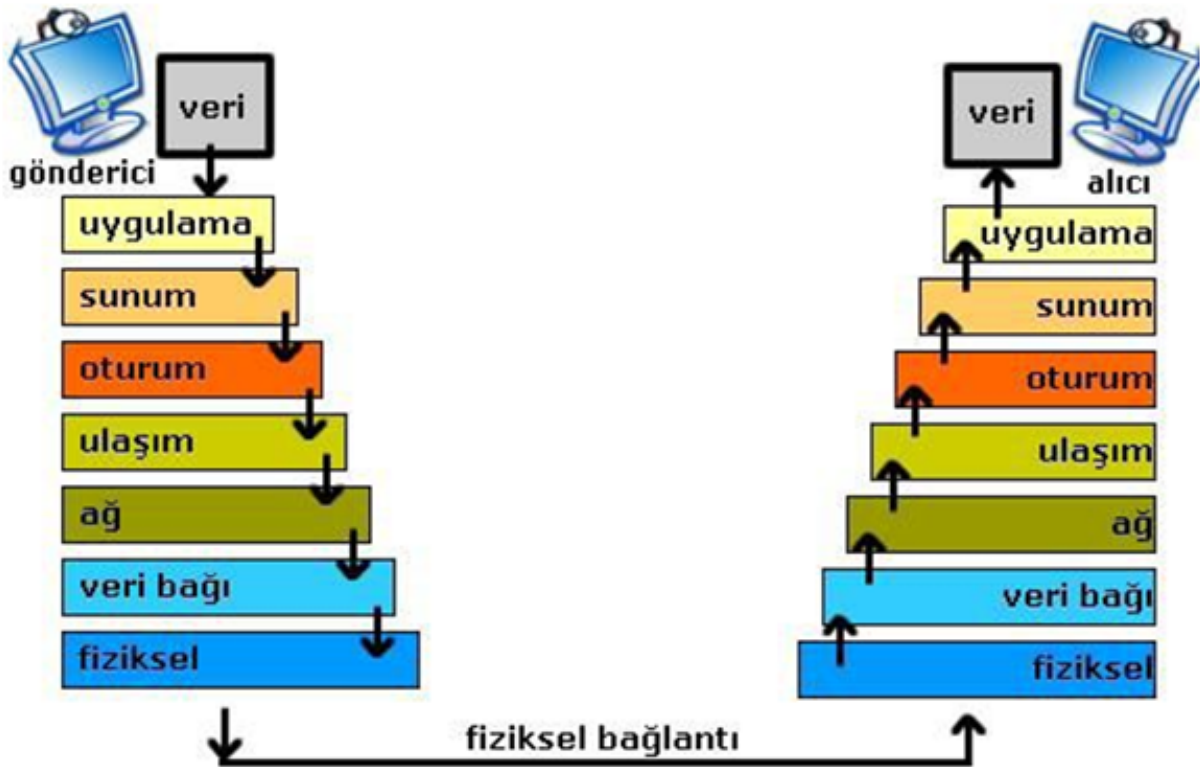




KUGUVEGA
TECHNOLOGY

- **OSİ Modeli Nedir ?**

OSI modeli (Open System Interconnection) yedi katmandaki protokolleri uygulamak için bir bilgisayar ağı çerçevesi tanımlar. Ağ oluşturma terimlerindeki bir protokol, bir tür müzakere ve iki ağ kurulumu arasında kuraldır. OSI modelini ISO (International Organization for Standardization) geliştirmiştir. Amaç aslında iki bilgisayar arasındaki iletişimin nasıl olacağını tanımlamaktan başka bir şey değildir.





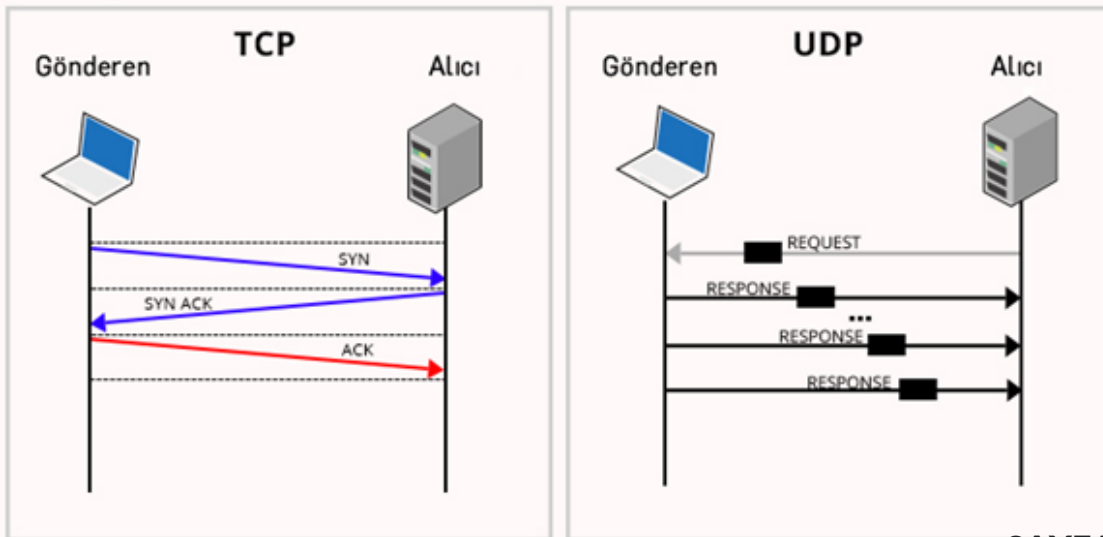
KUGUVEGA
TECHNOLOGY

- **UDP Nedir ?**

UDP (User Datagram Protocol) Türkçesi ile Kullanıcı Veribloğu İletişim Kuralları, TCP/IP protokol takımındaki iki aktarım katmanı protokolünden bir tanesidir ve verilerin bağlantı kurmadan yolanmasını sağlamaktadır.

Gelişmiş bilgisayar ağlarında, paket anahtarlı bilgisayar iletişimde datagram modu oluşturabilmek adına UDP protokolü geliştirilmiştir. Söz konusu protokol minimum protokol mekanizması ile bir uygulama programından başka bir programa mesaj göndermek için bir prosedür içermektedir. Paketin garantisini isteyen uygulamalar da TCP protokolünü kullanmaktadır.

TCP ve UDP İletişim



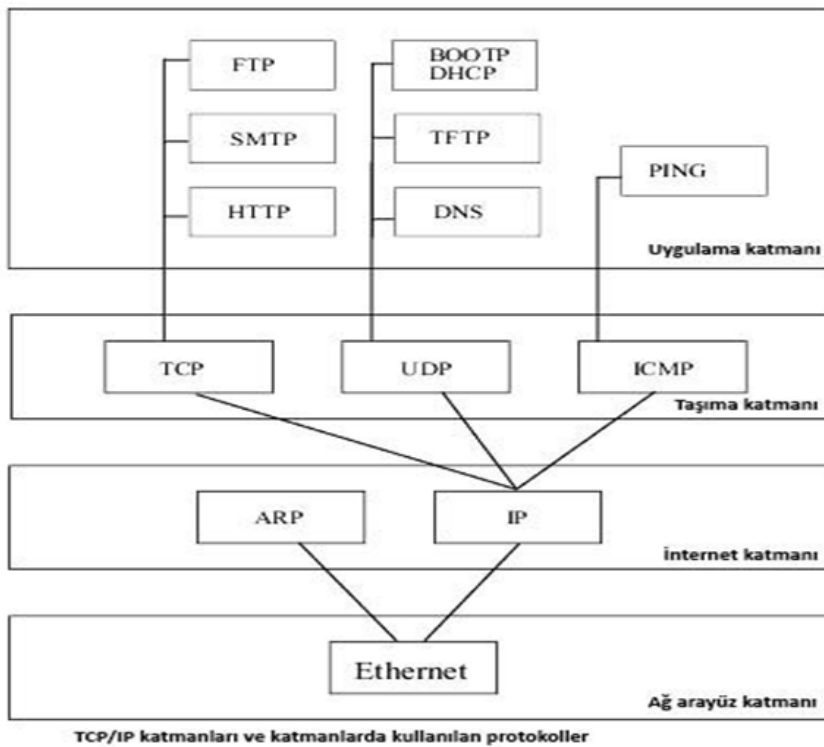


KUGUVEGA
TECHNOLOGY

- **TCP Nedir ?**

TCP (Transmission Control Protocol) bilgisayarlar arasındaki iletişimin, küçük paketler hâlinde ve kayıpsız olarak gerçekleştirilmesini sağlayan bir protokoldür. Aslında TCP (Transmission Control Protocol) protokolünün en önemli özelliği kimlik doğrulaması yapması ve veriyi karşı tarafa gönderirken veya alırken verinin bütünlüğünü sağlamasıdır. Gelişmiş bilgisayar ağlarında ortaya çıkan kayıpları önlemek için TCP protokolü yazılmıştır. HTTP, HTTPS, POP3, SSH, SMTP, TELNET ve FTP gibi günlük hayatta sıkça kullandığımız protokollerin veri iletimi TCP vasıtasıyla yapılır.

UDP protokolüne göre yavaş ancak güvenli bir veri iletişimi sağlar. UDP (User Datagram Protocol) protokolünde ise verinin karşı bilgisayar tarafından alınıp alınmadığı kontrol edilmez ve veri iletişimi çok hızlı bir şekilde gönderilir





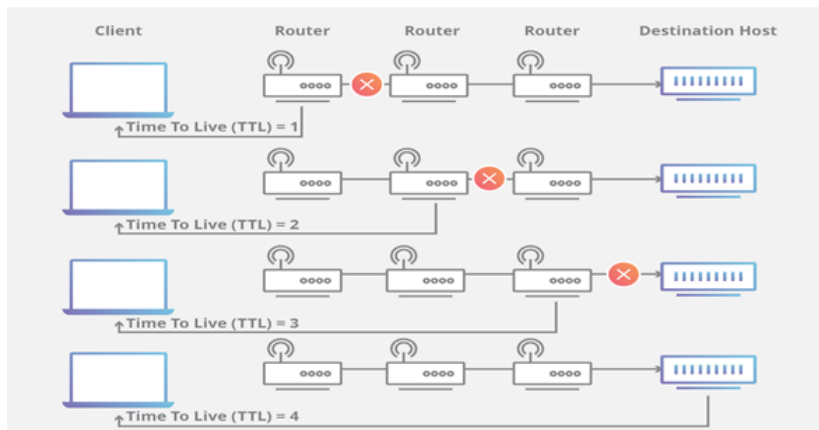
KUGUVEGA
TECHNOLOGY

- **TTL Nedir ?**

TTL (Transistor-Transistor Logic) anlamına gelir. Entegre devrelerin bir sınıflandırmasıdır.

Mantık kapıları devrelerinde sadece iki tip sinyal işlenir: “1” yüksek(high) ve “0” düşük(low). Yüksek sinyal voltaj seviyesi entegrenin besleme gerilimi kadar olur. yani 5V ile entegreyi besliyorsanız girişteki veya çıkıştaki yüksek(high) durum 5V olur. düşük(low) durumu ise 0 voltu(ground) temsil eder.

TTL geçitleri 5 voltluk nominal güç kaynağı voltajı +/- 0,25 volt seviyesinde çalışır. İdeal olarak, bir TTL “yüksek” sinyali tam olarak 5,00 volt ve TTL “düşük” sinyali 0,00 volt tam olarak olmalıdır. Bununla birlikte, gerçek TTL geçit devreleri böyle mükemmel voltaj seviyelerini üretmez ve bu ideal değerlerden önemli ölçüde sapan “yüksek” ve “düşük” sinyalleri kabul edecek şekilde tasarlanmıştır. “Kabul edilebilir” giriş sinyali voltajları “düşük” lojik durum için 0 volt’tan 0.8 volt’a ve “yüksek” mantıksal durum için 2 volt ila 5 volt arasında değişir. “Kabul edilebilir” çıkış sinyali voltajları (belirli bir yük koşuluyla kapı üreticisi tarafından garanti edilen voltaj seviyeleri) “düşük” mantık durumu için 0 volt ila 0,5 volt arasında ve “yüksek” lojik durum için 2,7 volt ila 5 volt arasında değişir.





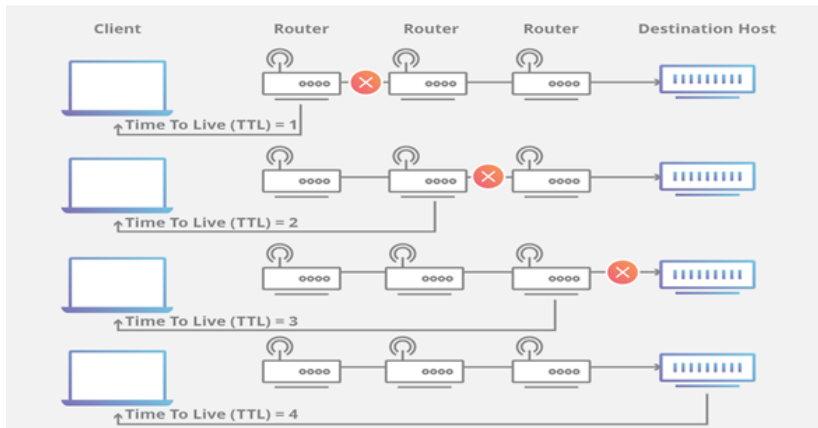
KUGUVEGA
TECHNOLOGY

- **TTL Nedir ?**

TTL (Transistor-Transistor Logic) anlamına gelir. Entegre devrelerin bir sınıflandırmasıdır.

Mantık kapıları devrelerinde sadece iki tip sinyal işlenir: “1” yüksek(high) ve “0” düşük(low). Yüksek sinyal voltaj seviyesi entegrenin besleme gerilimi kadar olur. yani 5V ile entegreyi besliyorsanız girişteki veya çıkıştaki yüksek(high) durum 5V olur. düşük(low) durumu ise 0 voltu(ground) temsil eder.

TTL geçitleri 5 voltluk nominal güç kaynağı voltajı +/- 0,25 volt seviyesinde çalışır. İdeal olarak, bir TTL “yüksek” sinyali tam olarak 5,00 volt ve TTL “düşük” sinyali 0,00 volt tam olarak olmalıdır. Bununla birlikte, gerçek TTL geçit devreleri böyle mükemmel voltaj seviyelerini üretmez ve bu ideal değerlerden önemli ölçüde sapan “yüksek” ve “düşük” sinyalleri kabul edecek şekilde tasarlanmıştır. “Kabul edilebilir” giriş sinyali voltajları “düşük” lojik durum için 0 volt’tan 0.8 volt’a ve “yüksek” mantıksal durum için 2 volt ila 5 volt arasında değişir. “Kabul edilebilir” çıkış sinyali voltajları (belirli bir yük koşuluyla kapı üreticisi tarafından garanti edilen voltaj seviyeleri) “düşük” mantık durumu için 0 volt ila 0,5 volt arasında ve “yüksek” lojik durum için 2,7 volt ila 5 volt arasında değişir.





KUGUVEGA
TECHNOLOGY

• TLS Handshake Nedir?

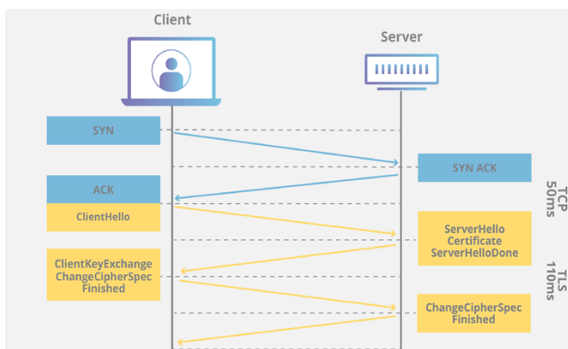
- mesaj, istemcinin hangi TLS sürümünü desteklediğini, desteklenen şifreleme yöntemlerini de kapsayan bir byte dizisini içerecektir.
- Sunucu, cevap olarak SSL sertifikasını, seçtiği şifreleme yöntemini ve sunucu tarafından oluşturulan başka bir rastgele byte dizisini içeren mesajı geri gönderir.
- İstemci, sunucunun SSL sertifikasını "sertifika yetkilisiyle" (Certificate Authority) doğrular. Bu kontrol, sunucunun söylediği "kişi" olduğunu ve istemcinin etki alanının da gerçek sahibi ile etkileşime girdiğini doğrular.
- İstemci, rastgele bir byte dizisi gönderir. Bu dizi, ortak anahtarla şifrelenmiştir ve sadece sunucu tarafından özel anahtarla şifresi çözülebilir.
- Sunucu bu diziye çözer.
- Hem istemci hem de sunucu, oluşturulan bu dizilerden oturum anahtarları oluşturur.
- İstemci, bir oturum anahtarıyla şifrelenmiş "tamamlandı" mesajı gönderir.
- Sunucu, bir oturum anahtarıyla şifrelenmiş "tamamlandı" mesajı gönderir.
- İstemci ve sunucu arasındaki iletişim, oturum anahtarları üzerinden devam eder ve Handshake süreci tamamlanır.

Eğer istemci HTTP protokolünü ve tarayıcı da HTTP/1.1 kullanıyorsa, Host adının yer aldığı bir bilgi ile GET isteği gönderilir.

Sunucu, gelen HTTP isteğini metoda göre tanımlar ki bu örnekte GET olarak belirtilmiştir. Host adını tanımladıktan sonra dizin yolunu belirler, aksi belirtilmediği sürece "/" üzerinden çalışır.

Web sunucusu, hedef sunucuda google.com adına bağlı bir sanal host konfigürasyonunun doğruluğunu denetler. Şayet web sunucusu tarafında bir "rewrite" modülü kullanılıyorsa, istemciden gelen istek bu kuralı işleyecek şekilde çalıştırılır. Hedef sitenin kullandığı yorumlayıcıya göre (PHP, ASP.NET vs.) ana sayfayı yorumlar.

Sunucu, web sitesine ait kaynakları oluşturduktan sonra Parse ve Render süreci başlar.





KUGUVEGA
TECHNOLOGY

- **Rewrite Nedir?**

URL Rewrite, çeşitli amaçlar için URL'leri değiştirme, yeniden yazma işlemidir. "Web adresi" olarak URL, tarayıcı çubuğu alanına girildiğinde tarayıcıyı belirli bir siteye ve sayfaya taşınmaya yönlendiren bir dizedir. Web sitenizde yer alan karmaşık URL'leri basit şekilde yeniden yazarak kullanıcı erişimi ve site görünürlüğünü düzenleyebilirsiniz.





KUGUVEGA
TECHNOLOGY

- **Parse Nedir ?**

Parse, bilgisayar biliminde bileşenlerin daha kolay işlenmesi ve söz diziminin doğruluğunun kontrol edip etiketlenmesine yardımcı olan dönüşüm yöntemidir. Parse sayesinde bilgisayarlar her bir bileşene işleme alabilir ve zahmetsizce makine diline dönüştürebilirler.

Parse'i kullanarak bileşenler içindeki cümleler ayrıştırılabilir ve kelimeler her birinin ayrı bileşenlere dağıtılabilirler. Parse yöntemi, yüksek seviyeli programlama dillerinin (high-level programming language) tümünde kullanılmaktadır. C++ ve Java gibi dillerde kodlar çalıştırılabilir makine diline dönüştürülmeden önce Parse yöntemiyle ayrıştırılır. Yüksek seviyeli programlama dillerinin haricinde Parse'i görebileceğimiz başka örnekler yok değil. PHP ve Perl gibi betik dilleri HTML'e doğru verinin aktarılmasını sağlamak için web sunucusu tarafından parse edilerek ayrıştırılırlar.

