



# TCP/IP PROTOKOLÜ

---

**Mustafa NUMANOĞLU**

# TCP/IP Protokolü Nedir?

- TCP/IP (Transmission Control Protocol / Internet Protocol) bilgisayarlar ile veri iletme / alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır.
- Kısaca, TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını ortaya koyar.

# TCP/IP Protokol Kümesi

- TCP/IP protokol kümesi İnternet networkünün oluşmasını sağlar. TCP/IP protokol kümesi altı çekirdek protokol ve bir dizi yardımcı program (utility) içerir.
- Altı çekirdek ve beş temel protokolden oluşur. Bunlar:
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)
  - IP (Internet Protocol)
  - ICMP (Internet Control Message Protocol)
  - IGMP (Internet Group Management Protocol)
  - ARP (Address Resolution Protocol)

# Temel TCP/IP Protokolleri

- Beş temel protokolden oluşur:
  - FTP (File Transfer Protocol)
  - TFTP (Trivial File Transfer Protocol)
  - HTTP (Hypertext Transfer Protocol)
  - HTTPS (Secure Hypertext Transfer Protocol)
  - SMTP (Simple Mail Transfer Protocol)

# Yardımcı Programlar / Protokoller

## Program

## İşlevi

- Ping Konfigürasyonu kontrol eder ve bağlantıyı test eder. Ping 131.140.1.1 şeklinde kullanılır.
- FTP Windows bilgisayarlar ile TCP/IP hostları arasında tek yönlü dosya transferini sağlar.
- TFTP (Trivial File Transfer Protocol) Windows bilgisayarlar ile TCP/IP hostları arasında UDP kullanarak tek yönlü dosya transferini sağlar.
- Telnet Terminal öykünümü sağlar.
- RPC (Remote Copy Protocol) UNIX host bilgisayar ile Windows bilgisayar arasında dosya kopyalar.
- RSH (Remote Shell) UNIX hostundaki komutları çalıştırır.
- Finger Uzak bilgisayar hakkında bilgi sağlar.

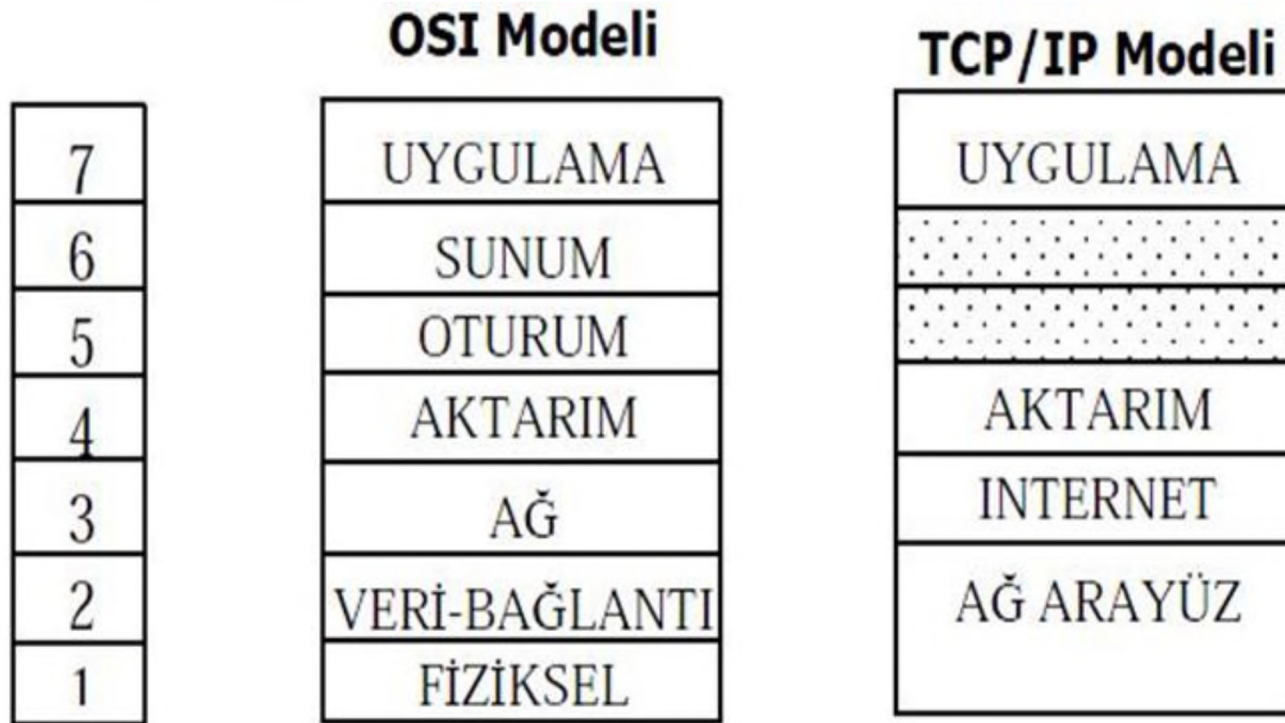
# Yardımcı Programlar / Protokoller

- REXEC (Remote Execution) Uzak bir bilgisayardaki bir işlemi çalıştırır.
- ARP Yerel olarak düzenlenmiş IP adreslerinin ön belleğini hazırlar.
- IPCONFIG Mevcut TCP/IP konfigürasyonunu gösterir.
- NBTSTAT IP adresleriyle düzenlenmiş NetBIOS bilgisayar adlarını görüntüler.
- Netstat TCP/IP protokolünün çalışması ilgili bilgileri görüntüler.
- Route Yerel yönlendirme tablosunu gösterir ve değiştirilmesini sağlar.
- Hostname RCP, RSH ve REXEC programlarının kimlik denetimini yaparak yerel bilgisayarın adını döndürür.

# TCP (Transmission Control Protocol)

- TCP/IP, OSI (Open System Interconnection) gibi üst üste sıralanmış katmanlardan oluşur. Fakat TCP/IP protokol grubu DOD (Department Of Defense) modelini referans almıştır.
- TCP/IP OSI modelinden önce geliştirilmiştir ve OSI modelinin yedi katmanına karşılık TCP/IP dört katmana sahiptir.

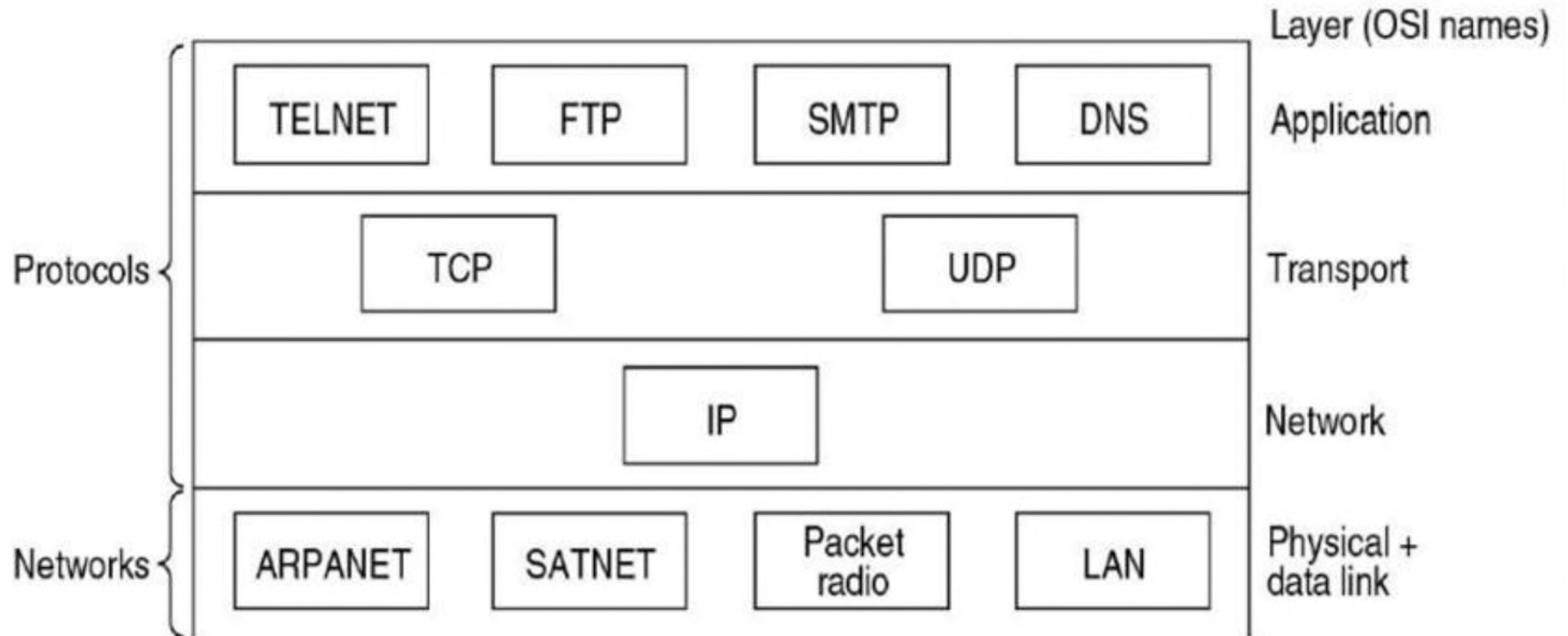
# TCP (Transmission Control Protocol)



OSI ve TCP/IP Referans modeli



# TCP (Transmission Control Protocol)



**TCP/IP Katmanları**

# TCP (Transmission Control Protocol)

- **İşleyişi:** TCP/IP'de, yollanan veriler katmanlara göre paketlenerek yollanır ve alıcıda bu paketler teker teker açılıp veri ulaştırılır. Her katmanda yollanan verinin türüne göre (e-posta, dosya aktarımı) belirli protokoller görev yapar.
- OSI referans modelindeki 7 katmana karşılık TCP/IP'de 4 katman mevcuttur; **Application (Uygulama)**, **Transport (Taşıma)**, **Internet**, **Network Interface (Ağ Arayüzü)** .

# TCP Katmanları

- **4. Application Layer (Uygulama Katmanı):** Bu katmanda veriyi göndermek isteyen uygulama ve kullandığı dosya biçimi bulunarak gönderilen verinin türüne göre farklı protokoller çalıştırılır (HTTP, SMTP, FTP, Telnet, vs.) ve programlarla Taşıma protokollerinin haberleşmesi sağlanır.
- Uygulama Katmanı Taşıma Katmanı ile portlar aracılığıyla haberleşir. Portlar numaralandırılmış standart uygulamalardır (HTTP:80, FTP:21, vs.) ve Taşıma Katmanında gelen paket içeriğinin türünün anlaşılmasında rol oynar.

# TCP Katmanları

- **3. Transport Layer (Taşıma Katmanı):** Bu katman verinin ne şekilde gönderildiğini gösterir. **TCP (Transmission Control Protocol)** ve **UDP (User Datagram Protocol)** protokolleri bu katmanda çalışır. TCP ve UDP iletim esnasında veriye içinde bazı kontrol bilgilerinin bulunduğu bir **başlık (header)** ekler.
- TCP, kayıpsız veri gönderimi sağlayabilmek için kullanılan protokoldür. Gönderilen veriler için özel bir **TCP kabul paketi (TCP ACK)** gönderilir ve gelmiş olan paketlerin doğruluğu kontrol edilir. Gönderen taraf, kabul gelmediği sürece paketi tekrar gönderir, böylece gönderim sağlanmış olur.
- TCP'de veri iletimi için iki bilgisayar arasında **Three-Way Handshake (Üç Zamanlı El Sıkışma)** bağlantısı kurulur.

# TCP Katmanları

- HTTP, HTTPS, POP3, SMTP, FTP, SFTP gibi protokollerdeki veri iletimi TCP aracılığıyla yapılır. UDP'de ise gönderilen paketin ulaşp ulaşmadığı kontrol edilmez. Bağlantı kurulum işlemleri, veri akış kontrolü ve tekrar iletim işlemleri yapmayarak iletim süresini azaltır ve ağ üzerinde TCP'ye oranda daha az bant genişliği kaplar. TFTP, SNMP gibi protokoller UDP aracılığıyla çalışır.

# TCP Katmanları

- **2. Internet Layer (İnternet Katmanı):** Bu katmanda hedef veya kaynak IP adresleri veriye eklenerek verinin hangi bilgisayara gönderileceği belirlenir ve gönderilen paket **Veri Bloğu (Datagram)** halini alır.
- Datagram maksimum 65,535 bayt boyutunda olabilir, daha fazla boyutlardaki paketleri IP protokolü yeteri kadar Datagram'a ayırır. IP, ICMP, IGMP, ARP gibi protokoller bu katmanda çalışır.

# TCP Katmanları

- **1. Network Interface Layer (Ağ Arayüzü Katmanı):** Bu katmanda verinin kablo üzerinde alacağı yapıyı tanımlayarak bir ve sıfırların fiziksel olarak görüntülenmesi sağlanır. Ethernet Ağ Arayüzü Katmanında kullanılan ve veri iletiminin fiziksel görünümünü sağlayan en yaygın kablolu yerel ağ teknolojisidir.
- Ethernet üç alt katmana sahiptir; **LLC (Logic Link Control Layer- Mantıksal Bağlantı Kontrolü)**, **MAC (Media Access Control-Ortam Erişim Kontrolü)** ve **Physical (Fiziksel)**.

# TCP Katmanları

- LLC alt katmanında, İnternet Katmanı'ndaki **frame (çerçeve)**'in hangi protokolle geldiğini belirleyerek iletimin MAC'a geçişini sağlar. MAC alt katmanında, hedef ve kaynak mac adresleri eklenir. LLC ve MAC, veri bloğuna kendi başlıklarını ekleyerek tam "frame" yapısını oluştururlar. Fiziksel alt katman ise bu "frame"i elektrik sinyaline (kablolu ağda) ya da elektromanyetik dalgalara (kablosuz ağda) dönüştürür.



# UDP (User Datagram Protocol)

- UDP TCP/IP protokol takımının iki aktarım katmanı protokolünden birisidir.
- Verileri herhangi bir bağlantı kurmadan karşı tarafa göndermeyi sağlamaktadır.
- Geniş alan ağlarında ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında kullanılır. UDP, oyunlar için oldukça kullanışlıdır.
- UDP bağlantı kurulum işlemlerini, akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir.
- UDP ve TCP aynı iletişim yolunu kullandıklarında UDP ile yapılan gerçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır.

# UDP (User Datagram Protocol)

- UDP güvenilir olmayan bir aktarım protokolüdür. Ağ üzerinden paketi gönderir ama gidip gitmediğini takip etmez ve paketin yerine ulaşip ulaşmayacağına onay verme yetkisi yoktur. UDP üzerinden güvenilir şekilde veri göndermek isteyen bir uygulama bunu kendi yöntemleriyle yapmak zorundadır.
- UDP, mümkün olduğu kadar az sayıda mesaj alış-verişine odaklı, Ulaşım katmanı'nda faaliyet gösteren bir protokoldür. Verilerin doğru ya da yanlış şekilde iletilip iletilmediğini garanti etmez.
- TCP'ye göre daha hızlıdır fakat güvenli değildir. Veri ismine datagram adı verilir. Datagramın segmentten farkı ise içerisinde sıra numarasının bulunmamasıdır. Kaybolan verinin tekrar gönderilmesi, akış kontrolü gibi konularla ilgilenmez.

# UDP (User Datagram Protocol)

- IP'nin kullanımı için bir arayüz oluşturur. Basitliği nedeniyle gerçek zamanlı uygulamalarda tercih edilir. Kısa istek ve cevapların taşındığı uygulamalarda da UDP kullanılabilir. UDP bağlantılarının kurulması (setup) gerekmediği gibi sonlandırılması (release) da gerekmez. Kaybolan UDP segmentleri için birşey yapılmaz.
- UDP'yi kullanan protokollerden bazıları DNS, TFTP, ve SNMP protokolleridir. Uygulama programcıları birçok zaman UDP'yi TCP'ye tercih eder, zira UDP ağ üzerinde fazla bant genişliği kaplamaz.

# UDP (User Datagram Protocol)



# FTP (File Transfer Protocol)

- FTP (File Transfer Protocol) İnternete bağlı bir bilgisayardan diğerine (her iki yönde de) dosya aktarımı yapmak için geliştirilen bir internet protokolü ve bu işi yapan uygulama programlarına verilen genel addır.
- İlk geliştirilen internet protokollerinden biridir. FTP protokolü ile bir bilgisayardan bir başka bilgisayara dosya aktarımı yapılırken, o bilgisayar ile etkileşimli-aynı anda (on-line) bağlantı kurulur ve protokol ile sağlanan bir dizi komutlar yardımıyla iki bilgisayar arasında dosya alma/gönderme işlemleri yapılır.

# FTP Gereklilikleri

FTP bağlantısı için;

- Bağlanacak bilgisayarın internet adresi (nümerik ya da sembolik formatta),
- Bağlanacak bilgisayarda dosyalarına ulaşmak istenilen hesapla ilgili kullanıcı numarası ve şifresi,
- İnternet erişimi olan, üzerinde FTP yazılımı bulunan bir bilgisayar,
- Bağlanacak bilgisayarda, FTP protokol komutlarını yorumlayacak çalışır durumda bir FTP Servis programı (FTP Sitesi) gereklidir.

# FTP Gereklilikleri

- Genel kullanım: ftp <ftp yapılacak makinanın adresi> şeklindedir.
- Bundan sonra, ilgili bilgisayara bağlanıldığında, kullanıcı numarası ve parola (password) sorulur. Daha sonra da, o kullanıcının makinasına bağlanılmış olur. Bu şekilde, etkileşimli bir ortamda, bazı komutlar verilerek iki makina arasında dosya işlemleri, ayrıca bağlanılan makinada bazı temel dosya / disk işlemleri (dizin açma, dosya silme vb) yapılabilir.

# Standart FTP Komutları

**cd:** Dizin değiştirme (cd <dizin adı>) (cd .. : bulunulan dizinden bir öndekine geçme)

**pwd:** Bulunulan dizinin ismini verir

**dir:** Bulunulan dizindeki dosyaları listeleme

**ls:** Bulunulan dizindeki dosyaları kısa olarak listeleme (Örnek kullanımlar: ls -lr: ayrıntılı, tersten alfabetik listeleme; ls -lr |more: sayfa sayfa listeleme (dizin içinde çok fazla sayıda dosya varsa bu kullanım oldukça yararlıdır))

**get:** Dosya alma (get <dosya\_adi> (<alındıktan\_sonraki\_adi>). (<alındıktan\_sonraki\_adi> seçimlidir, kullanılmayabilir. Bu durumda dosya\_adi aynen kullanılacaktır.

**put:** Dosya gönderme

(put <dosya\_adi> <göndereceğimiz\_yerdeki\_adi>)



# Standart FTP Komutları

**mget:** Birden fazla dosya almak istendiğinde kullanılır. Örnek kullanımlar: `mget *.zip`, `mget a*.*` vb..

**mput:** Birden fazla dosya göndermek istendiğinde kullanılır.

**ascii:** Dosya aktarımlarında, aktarım modu olarak ASCII kullanılacağını belirtme.

**binary:** Dosya aktarımlarında aktarım modu olarak BINARY kullanılacağını belirtme. Arşiv dosyaları (zip, arj, z, zoo, hqx vb), çalıştırılabilir programlar (.exe, .com), resim formatlı programlar (gif, jpeg vb) FTP ile alınmadan/ya da gönderilmeden önce mutlaka bu komut verilmelidir.

**delete:** FTP yapılan yerde bir dosyayı silme (`delete <dosya adı>`, eğer yetkiniz varsa kullanabileceğiniz bir komuttur) **mkdir:** FTP yapılan yerde yeni bir dizin oluşturma (`mkdir <dizin adı>`, eğer yetkiniz varsa kullanabileceğiniz bir komuttur)

# Standart FTP Komutları

**rmdir**: FTP yapılan yerde boş bir dizini silme (`rmdir <dizin adı>`, eğer yetkiniz varsa kullanabileceğiniz bir komuttur) **help**: Kullanılabilecek komutlar ile ilgili bir yardım ekranı açar.

**lcd**: FTP ortamından çıkmadan, kendi makinanızda dizin değiştirmeyi olanaklı kılar.

**close**: FTP ortamından çıkmadan, sadece ilgili bağlantıyı kapatmak için kullanılır.

**quit**: FTP ortamından çıkmak ve bağlantıyı kapatmak için kullanılır (`bye` komutu da aynı işi görür).

Bazı FTP merkezleri, tüm bir dizini sıkıştırarak gönderme özelliğine sahiptir. Örnek: `GET linux linux.zip` şeklinde sıkıştırılmış olarak alabiliriz.

# Anonymous FTP

- FTP işlemi sırasında, güvenlik olarak, bağlanacağımız makinadaki kullanıcı numarası (User Name) ve parola (Password) bilgilerini bilmemiz gerekir (Program, bunları bize sorar). Bağlanılan makina, kişiye özel ve parolasını sadece bizim bildiğimiz bir makina olabileceği gibi, herkese açık bir arşiv merkezi de olabilir. Böyle merkezlere herkesin kolayca erişip dosya almasını sağlamak için tek tip bir kullanıcı numarası tanımlanmıştır.

# Anonymous FTP

- Bu merkezlere ftp yapıldığında kullanıcı ismi olarak anonymous (ya da ftp) girildiğinde, bizden parola olarak kendi e-posta adresimizi girmemiz istenir. Parola yazılırken görünmez. Örnek olarak;  
ftp; [ftp.ank.edu.tr](ftp://ftp.ank.edu.tr)  
user ftp password; mnuman@ankara.edu.tr
- Burada, şifre olarak e-mail adresinin girilmesi genellikle istatistiksel amaçlar içindir. Web üzerinden yapılan anonymous FTP'lerde şifre girilmesine gerek kalmaz.

# Web Üzerinden FTP Nasıl Yapılır?

- Günümüzde bilişim hizmetleri tüm Internet servislerine daha becerikli ve etkileşimli ortamlardan erişilmesi ve farklı servislerin etkileşimli olarak kullanılması şeklinde kendini göstermektedir.
- Bu ortamlardan en popülerleri Web (World Wide Web)'dir. FTP de dahil olmak üzere pek çok internet servisi ve ilave pek çok özellik bu ortamlar üzerinden yaygın olarak kullanılmaktadır. Dolayısıyla, FTP yapmanın bir diğer yolu da, Web üzerinden FTP yapmaktır.
- Bu yöntem hem kullanım açısından daha kolaydır (komutları ezberlemek / bilmek zorunluluğu da yoktur) hem de daha etkili sonuçlar alınmaktadır. Örneğin; binary bir dosyayı yanlışlıkla, standart FTP programları ile kolayca ASCII modda almak mümkündür.

# Web Üzerinden FTP Nasıl Yapılır?

- Bu gibi sakıncalar Web üzerinden yapılan FTP'lerde ortadan kalkmaktadır. Ayrıca, Bookmark ve cache gibi faydalı özelliklerinden dolayı da bu ortamların sağladıkları bazı kolaylıklar vardır. Çoğu Web istemcisinin sağladığı grafik ara birim özelliğini de unutmamak gerekir. Böylelikle, örneğin standart resim formatlarında olan bir resim dosyasını aldığı anda görüntüsü ekrana da görülebilmektedir.

# TFTP (Trivial File Transfer Protocol)

- TFTP 1980 yılında tanımlanmış, FTP'nin temel fonksiyonel şekli olarak ifade edilen basit bir dosya transfer protokolüdür.
- Basit yapısından dolayı kullanılması esnasında çok az bellek tüketilmektedir. Bu özelliğinden dolayı, yeterli yığın bellek cihazı (mass storage device) olmayan yönlendirici (router) bilgisayarların önyüklemesinde kullanılırdı. Halen ağ üzerinde bulunan host makinalar arasında küçük dosyaların transferi için kullanılmaktadır.

# HTTP (Hypertext Transfer Protocol)

- **HTTP** (Hypertext Transfer Protocol, Hipermetin Aktarma İletişim Kuralı) bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiperortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır.
- Web'in en ilginç yönlerinden biri de çok basit olmasıdır. Bir Web dokümanına ulaştığımızda her şey 4 ana fazda gerçekleşir:
  - Bağlantı
  - Ne istediğimizin web servisine iletilmesi
  - Cevap
  - İlgili sayfaya yapılan bağlantının kesilmesi.

Bu ana safhalar, web üzerinde iletişimin kurallarını tanımlayan bir protokolü oluştururlar.



# HTTPS (Secure Hypertext Transfer Protocol)

- HTTPS (Secure Hypertext Transfer Protocol, Türkçe güvenli hiper metin aktarım iletişim kuralı) hiper metin aktarım iletişim kuralının (HTTP) güvenli ağ protokolü ile birleştirilmiş olanıdır.
- Klasik HTTP protokolüne SSL protokolünün eklenmesi ile elde edilir. İnternette sunucular ve son kullanıcılar arasında bilgilerin "başkaları tarafından" okunamayacak şekilde nasıl aktarılacağına dair kurallar ve yöntemleri düzenleyen bir protokoldür.

# HTTPS (Secure Hypertext Transfer Protocol)

- Başında "https" yazılan adreslerle bağlantı kurduğunuzda, bilgiler sadece karşı taraf ve sizin tarafınızdan okunabilecek şekilde şifrelenir. http ile yapılan bilgi alışverişinde ise bir şifreleme yoktur, başka kişiler de sizin aldığınız ve verdiğiniz bilgilere ulaşabilir. https, bilgi güvenliği gereken zamanlarda uygulanan bir güvenli iletişim protokolüdür.
- Özellikle internet üzerinden yürütülen bankacılık işlemleri için banka siteleriyle bağlantı kurulduğunda ya da kredi kartıyla ödeme yapılan sistemlerde kredi kartı bilgileriniz doğrulanırken, adres çubuğunun başında "http" yerine "https" yazdığına dikkat edilmelidir.

# HTTPS (Secure Hypertext Transfer Protocol)

- Sosyal ağların popüler hale gelmesiyle daha çok kişisel bilgi, web üzerinden şifresiz olarak gönderilmeye başlanmıştır. Bu ağlarda profilinizi özel yaparak gizliliğinizi artırmanız mümkün olsa da, veriler hala şifresiz olarak aktarılmaya devam edecektir.
- Şifresiz veriler ise araya girecek herhangi biri tarafından kolaylıkla elde edilebilir. Twitter ve Facebook gibi bazı hizmetler, buna yönelik HTTPS bağlantısı sunmaya başlamışlardır.

# HTTPS (Secure Hypertext Transfer Protocol)

- **HTTPS'in anlamı:** "HyperText Transfer Protocol Secure" teriminin kısaltması olan HTTPS'i parçalarına ayırarak tanımlamaya çalışalım:
- **Hypertext**, bir web sitesinin kod veya eklenti gerektirmeyen, metin, tablo veya resim gibi içeriklerini açıklar. Aynı kelime HTML'de de bulunmaktadır (HyperText Markup Language).
- **"Secure"**, HTTP ve SSL/TLS protokollerinin birleşimini temsil eder. Bu protokoller web'de gezinme dışında e-postalar, anında mesajlaşma ve voip gibi içeriğin de şifrelenmesinde kullanılır.
- Yani HTTPS, web sitelerinin "**düz metin**" ile kurduğu iletişimin güvenliği artırmak amacıyla **şifrelenmesi** demektir.

# HTTPS'nin HTTP'den farkları

- Öncelikle HTTP ön tanımlı olarak 80. portu kullanır. HTTPS'in kullandığı ön tanımlı port ise 443'tür.
- HTTP man-in-the-middle attack, yani ortadaki kişi saldırılarına ve dinlemelere karşı korumasızdır. Ağı dinleyerek verileri toplayan bir saldırgan kolaylıkla bilgileri okuyabilir ve gizli kalması gereken parolaları, kullanıcı hesaplarını ele geçirebilir.
- HTTPS ise bu tür saldırılardan korunmak amacıyla tasarlanmıştır. Bu nedenle HTTPS, çoğunlukla parola ve kullanıcı adlarının gönderildiği form sayfalarında tercih edilir. Tamamen HTTPS ile yayın yapan web siteleri de mevcuttur.

# SMTP (Simple Mail Transfer Protocol)

- Elektronik posta gönderme protokolü (Simple Mail Transfer Protocol), bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür.
- Sadece e-posta yollamak için kullanılan bu protokolde, basitçe, istemci bilgisayar SMTP sunucusuna bağlanarak gerekli kimlik bilgilerini gönderir, sunucunun onay vermesi halinde gerekli e-postayı sunucuya iletir ve bağlantıyı sonlandırır.

# SMTP (Simple Mail Transfer Protocol)

- Mesaj, bir hedefe gönderilince, mesaj bir cihazda (genelde bir diskte) bekleme listesine yerleştirilir. Hedefteki sunucu yazılımı, mesajlar için kuyruğu düzenli olarak kontrol ederek bir uyarı postalar. Onları fark ettiğinde, hedeflerine teslim etmeye başlar. SMTP mail göndermek, POP3 mail almak için kullanılır.

# SMTP (Simple Mail Transfer Protocol)

