COMPUTER NETWORK

ARPANET

1969'da ABD Savunma Bakanlığı tarafından geliştirilen ilk geniş alan ağıdır. Paket anahtarlama teknolojisini kullanarak bilgisayarlar arasında veri iletimini sağlamış ve internetin temelini oluşturmuştur.

World Wide Web (www)

İnternet üzerindeki bilgilere erişimi sağlayan sistemdir. HTML, URL ve HTTP protokollerini kullanarak web sitelerini görüntülemeye olanak tanır.
İnternet ve WWW farklı kavramlardır; internet fiziksel altyapıyı temsil ederken, WWW bu altyapı üzerinde çalışan bir servis olarak düşünülebilir.

Search Engines

İnternet üzerindeki bilgileri tarayıp indeksleyen ve sıralayarak kullanıcıya sunan sistemlerdir. Google, Bing gibi arama motorları, arama algoritmalarıyla en uygun sonuçları gösterir.

ISOC (Internet Society)

1992’de kurulan, internetin açık, güvenli ve erişilebilir olması için çalışan uluslararası bir organizasyondur. IETF gibi kuruluşlarla birlikte internet standartlarını geliştirmeye katkıda bulunur.

IETF

IETF, internetin teknik standartlarını geliştiren ve yöneten bir organizasyondur. TCP/IP, HTTP, DNS, IPv6 gibi protokollerin tasarlanması ve iyileştirilmesi için çalışmalar yapar. Açık bir topluluk olup, gönüllü mühendisler ve uzmanlar tarafından yönetilir.

Protokol

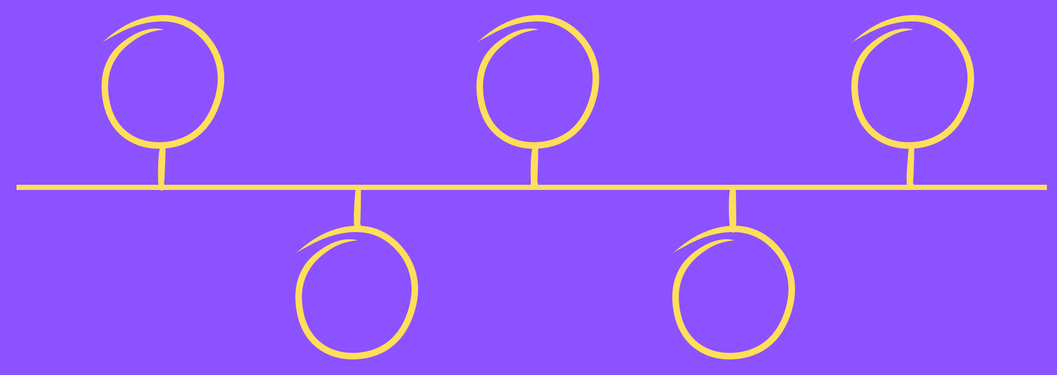
Protokol, ağ üzerindeki cihazların iletişim kurmasını sağlayan kurallar ve standartlar bütünüdür.

Topoloji

Bir networkteki cihazların birbiriyle nasıl bağlandığını ve verilerin nasıl iletildiğini belirleyen yapıdır.Türleri:

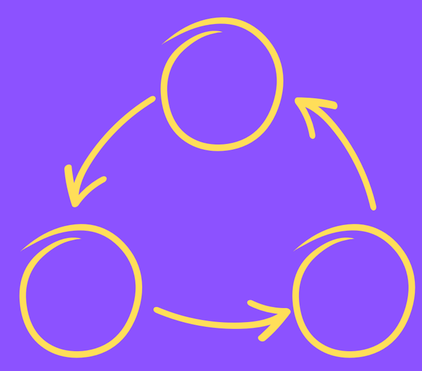
Bus

Tüm cihazlar tek bir hat üzerinden birbirine bağlanır ve veriler bu hat üzerinden iletilir. Hata oluşursa tüm network etkilenebilir.



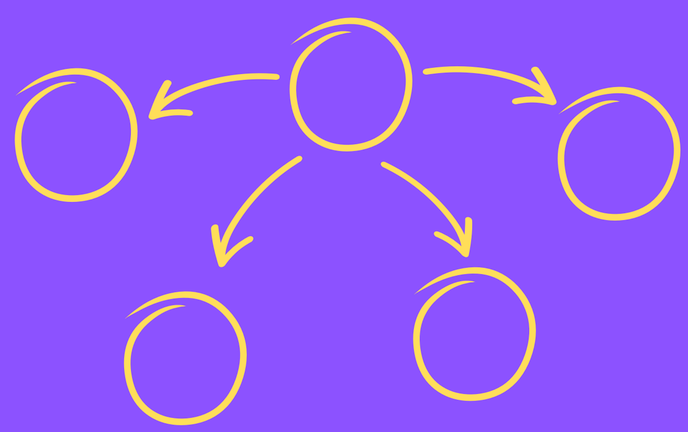
Ring

Cihazlar birbirine döngüsel olarak bağlanır. Veri, sadece bir yön üzerinden akar ve bir cihazın ağrızalanması sonucunda tüm network etkilenebilir.



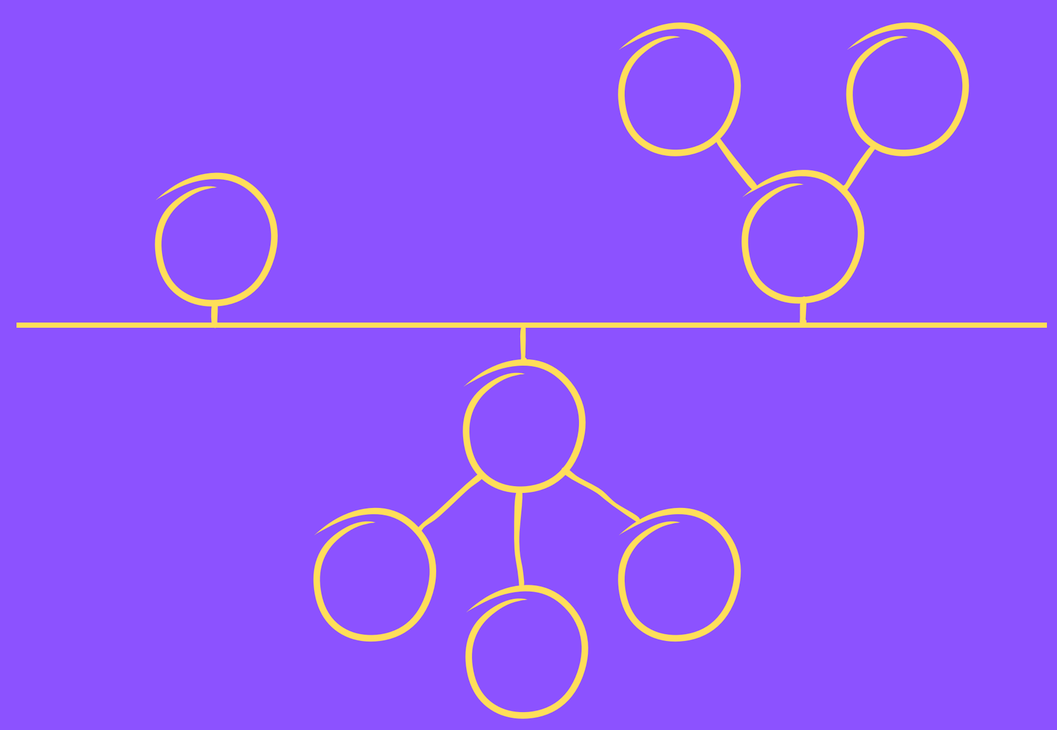
Star

Tüm cihazlar merkezi bir cihaz üzerinden bağlanır.Merkezi cihaz arızalanırsa tüm network kesilir, ancak diğer cihazlar bağımsız olarak çalışabilir.



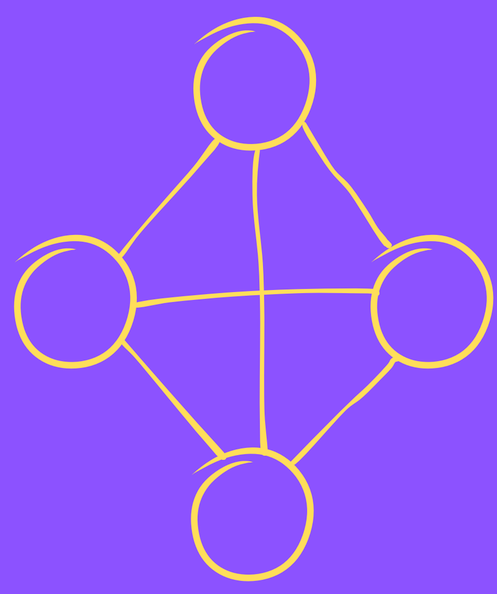
Tree

Star topolojisinin genişletilmiş bir şekildir; network, ana bir root cihazdan branşlar şeklinde daha küçük ağlara bağlanır.



Mesh

Her cihaz, diğer cihazlarla doğrudan bağlatıya sahiptir.Yüksek güvenlilik ve verimlilik sağlar ancak yüksek maliyetlidir.



OSI (Open Systems Interconnection)

Network iletişimini katmanlara ayıran teorik bir modeldir.

Physical Layer

Bu katman bit olarak iletilen verilerin nasıl elektirik, ışık veya radyo sinyallerine çevirileceğini ve aktarılacağını tanımlar. Kablolar, network kartları , router'lar gibi fiziksel cihazlarla ilgilidir.

Data Link Layer

Fiziksel katmanla iletişimi sağlayan ve veri iletimini düzenleyen katmandır.Ethernet veya Token Ring gibi erişim yöntemlerini kullanır. Veriler bu katmandan fiziksel katmana iletilmeden önce framelere bölünür

Network Layer

Verinin kaynak cihazdan hedef cihaza nasıl yönlendireleceğini belirler.Veriler bu katmanda paket olarak taşınır. IP adresleme sistemi bu katmanda kullanılır ve router'lar paketleri en uygun yollarla hedefe yönlendirir.Ayrıca trafik yönetimi sağlayarak farklı segmentler arasındaki paket iletimini kontrol eder.

Session Layer

İki cihaz arasındaki bağlatıyı yönetir, bağlantının ne zaman kurulacağını ve sonlandırılacağını belirler. Bu katman, veri alışverişinin kesintisiz devam etmesini sağlamak için mekanizmalar içerir. Uzak masaüstü ve VPN gibi uygulamalar bu katmanda çalışır.

Presentation Layer

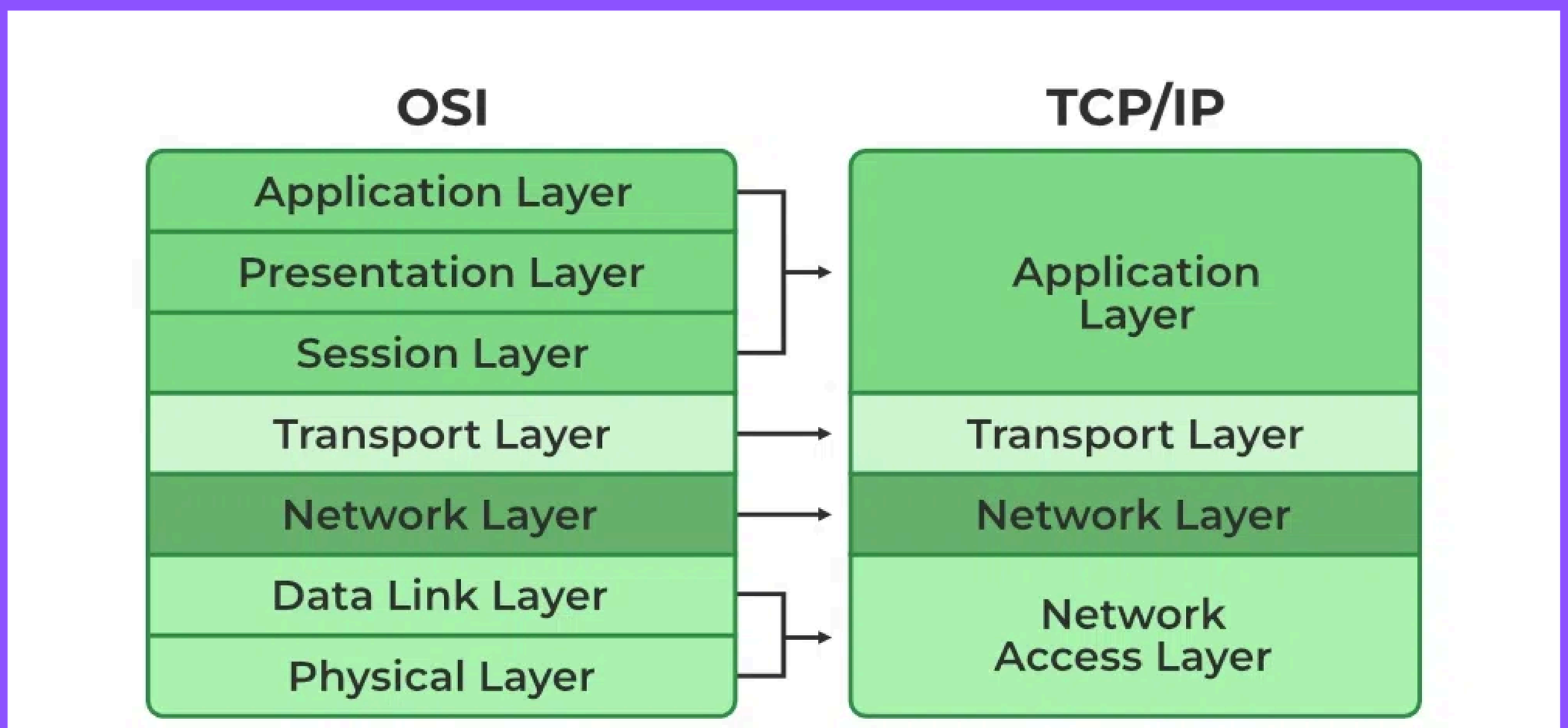
Verinin uygulama katmanı tarafından anlaşılabilir hale getirilmesini sağlar.Bu katmanda veri sıkıştırma, şifreleme dönüşümleri gerçekleştirilir.Ayrıca JPEG, MP3 gibi medya formatları da bu katmanda işlenir

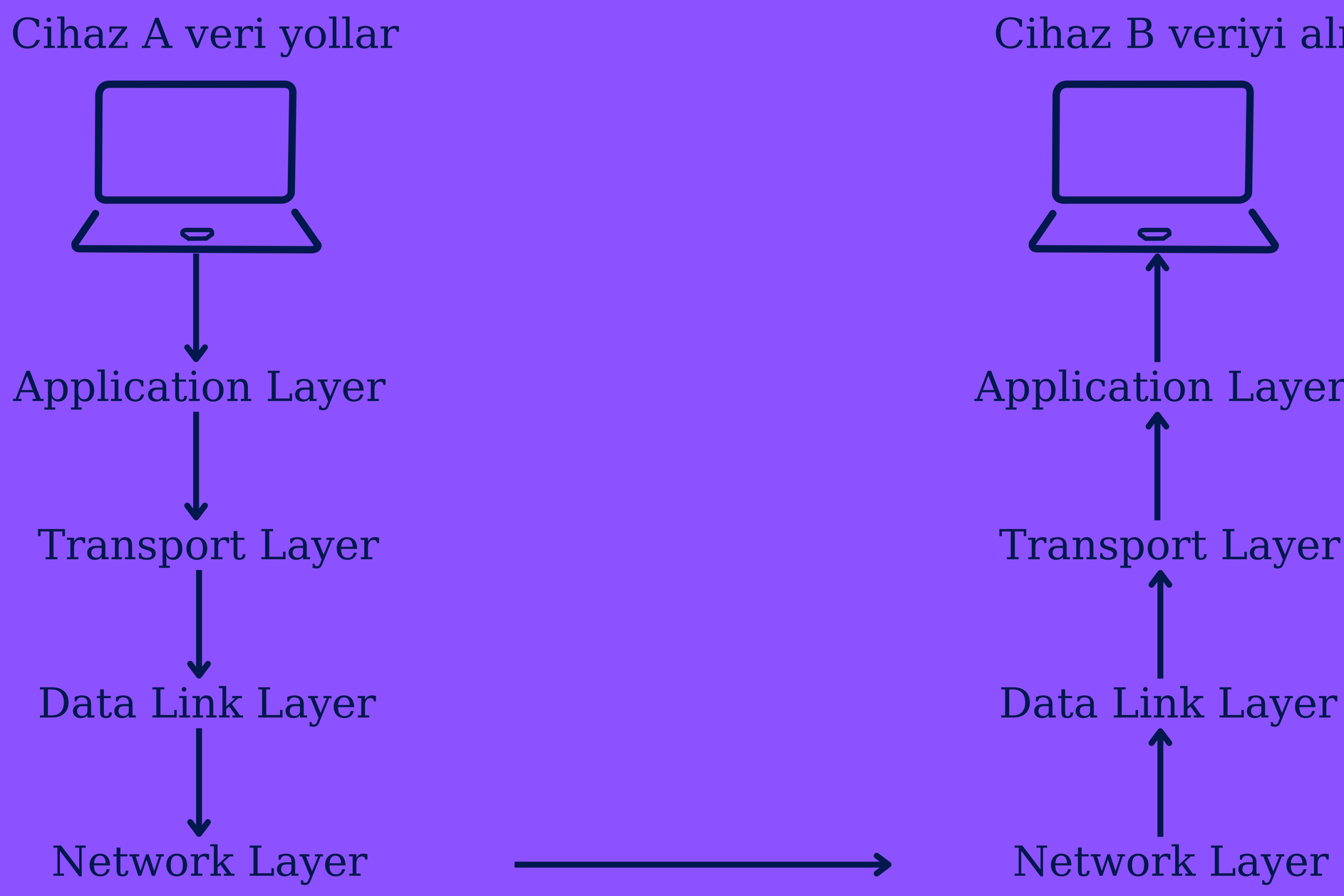
Application Layer

Kullanıcı doğrudan etkileşimde bulunfuğu katmandır. Web tarayıcıları (HTTP, HTTPS), e-posta servisleri ve dosya transfer protokolleri gibi network hizmetleri burada çalışır.Veriyi işler, alt katmanlara iletir veya alınan veriyi anlaşılır hale getirerek kullanıcaya sunar.

TCP/IP (Transmission Control Protocol, Internet Protocol)

OSI modeli 7 katmandan oluşurken, TCP/IP modeli 4 katmandan oluşur. Bu model daha pratik ve günümüz internetinde kullanılan modeldir.





Client-Server Architecture

Bir networkte istemcilerin (client) merkezi bir sunucuya (server) bağlanarak veri ialışverişi yaptığı mimaridir.Web siteleri, e-posta servisleri ve bulut tabanlı uygulamalar bu mimariyi kullanır.

Data Center (Veri Merkezi)

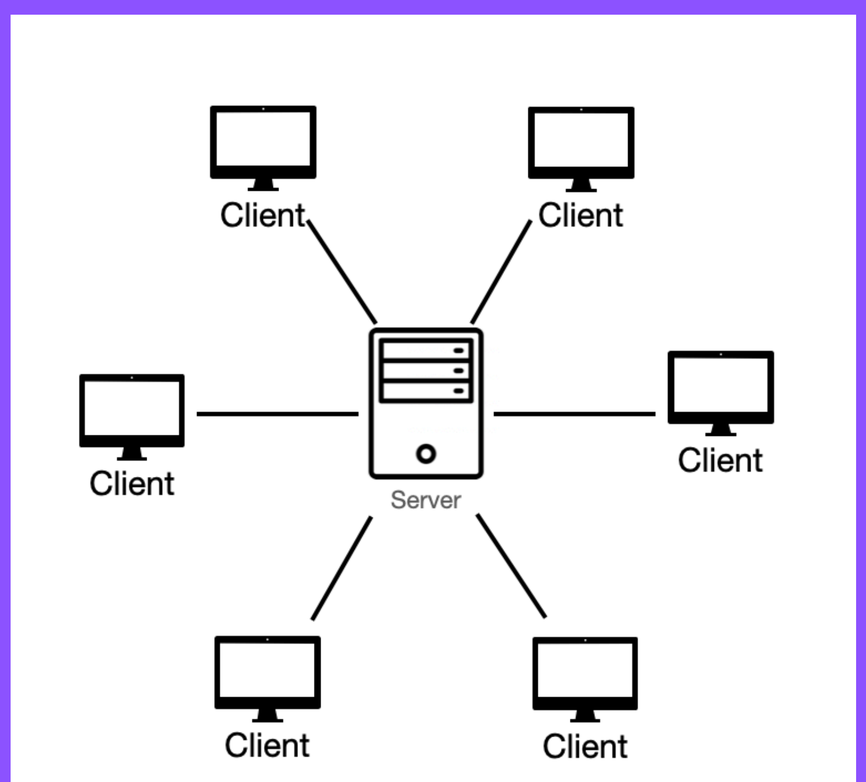
Büyük miktarda verinin depolandığı, işlendiği ve yönetildiği, birçok sunucunun bulunduğu fiziksel bir tesistir. İstemcilerin bağlandığı sunucular genellikle veri merkezlerinde yer alır ve web hizmetleri, uygulamalar, veritabanları burada çalıştırılır.

P2P Architecture

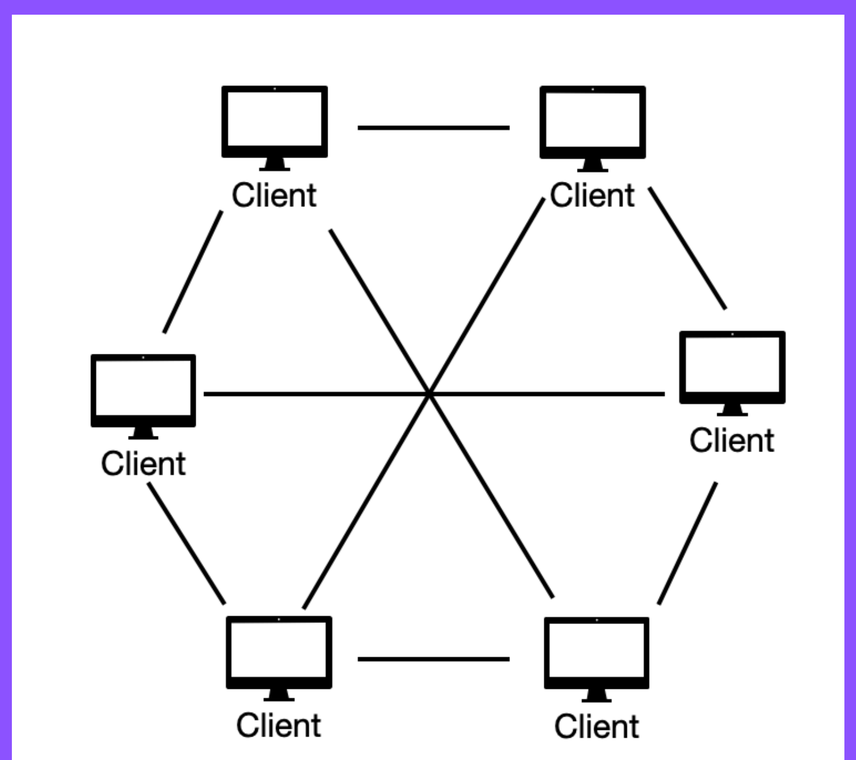
Merkezi bir sunucuya (server) bağlı kalmaksızın, ağdaki cihazların doğrudan birbirleriyle veri alışverişi yapmasını sağlayan mimaridir.Dosya paylaşım ağlarında ve blockchain teknolojilerinde yaygın olarak kullanılır.

BitTorrent

P2P mimarisini kullanan popüler bir dosya paylaşım protokolüdür. Büyük dosyaların daha verimli şekilde indirilmesini sağlamak için, dosyalar küçük parçalara bölünerek ağdaki diğer kullanıcılarla paylaşılır. Kullanıcılar, dosyayı hem indirir hem de aynı anda başkalarına yükleyerek ağın performansını artırır.

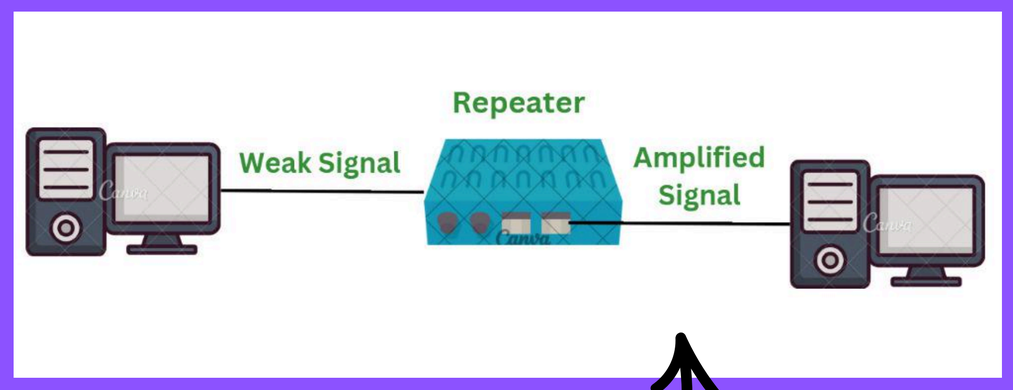


Client Server Architecture



P2P Architecture

Network Cihazları

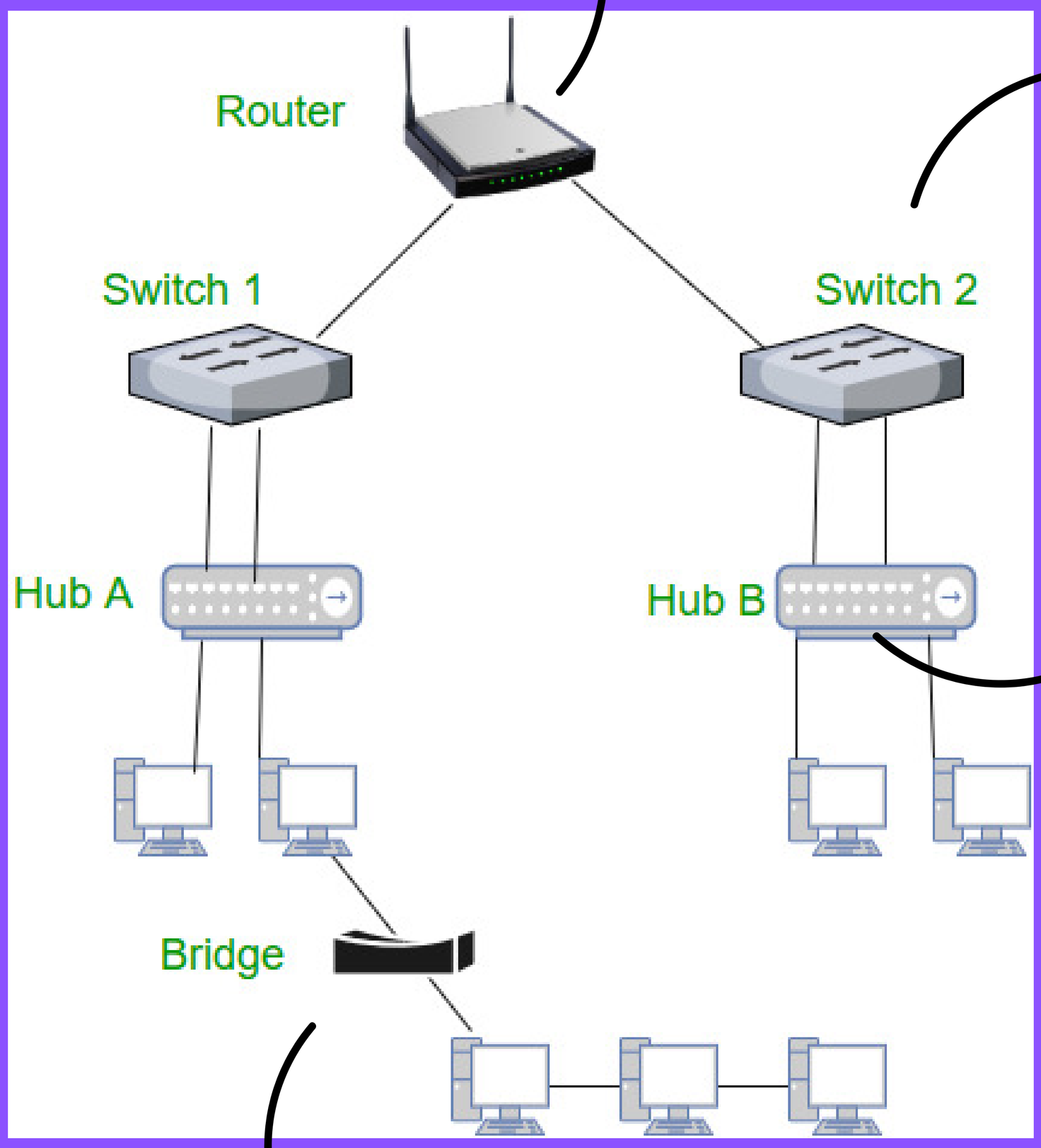


Router

Ağlar arasında veri iletimini yapan cihazdır.IP adresi üzerinden yönlendirme yaparak en uygun yolu seçer.

Repeater

Bir ağda veri iletim mesafesini artırmak için kullanılan cihazdır. Zayıflayan sinyalleri alır, yeniden güçlendirir ve iletim mesafesini uzatır. Genellikle kablolu ağlarda kullanılır



Switch

Hub’a benzer ancak daha verimli bir cihazdır. Veriyi yalnızca hedef cihazlara iletir, bu da ağ trafiğini optimize eder. Daha akıllıdır çünkü veri paketlerinin hedef adreslerine göre iletim yapar.

Hub

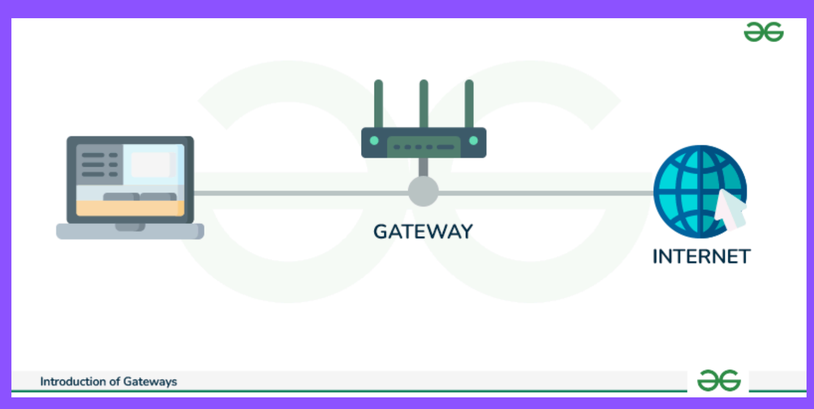
Bir ağdaki tüm cihazlar arasındaki iletişimi sağlayan cihazdır. Verilen veriyi tüm bağlı cihazlara iletir (broadcast). Ancak verimlilik açısından zayıf olduğu için genellikle daha modern ağlarda kullanılmaz

Bridge

Ağlar arasında veri iletimi yapan cihazdır. İki farklı ağ segmentini birbirine bağlar ve veri trafiğini yönetir. Düşük seviyedeki veri çakışmalarını önler.

Gateway

Farklı ağ protokollerini birbirine bağlayan cihazdır. Örneğin, bir yerel ağ ile internet arasında veri iletimi yapan bir cihaz olabilir. Genellikle ağlar arasındaki protokol dönüşümünü yapar.



Network İletişim Protokolleri

TCP (Transmission Control Protocol) → Güvenilir, bağlantı tabanlı veri iletimi sağlar. Veri kaybını önlemek için hata kontrolü ve sıralama yapar.

UDP (User Datagram Protocol) → Bağlantısız, hızlı ama güvenilir olmayan veri iletimi yapar. Sesli ve görüntülü görüşmeler gibi gecikme hassasiyeti olan uygulamalarda kullanılır.

IP (Internet Protocol) → Cihazların ağ üzerinden adreslenmesini ve yönlendirilmesini sağlar. IPv4 ve IPv6 olmak üzere iki versiyonu vardır.

Application Layer Protokolleri

HTTP (HyperText Transfer Protocol) → Web sayfalarının tarayıcılar tarafından alınmasını sağlar.

HTTPS (HTTP Secure) → Şifrelenmiş güvenli web iletişimi sağlar.

FTP (File Transfer Protocol) → Dosya transferi için kullanılır.

SMTP (Simple Mail Transfer Protocol) → E-posta gönderimi için kullanılır.

POP3 (Post Office Protocol v3) / IMAP (Internet Message Access Protocol) → E-postaların alınmasını sağlar.

Network Yönetim Protokolleri

DNS (Domain Name System) → Alan adlarını IP adreslerine çevirir.

DHCP (Dynamic Host Configuration Protocol) → Cihazlara otomatik IP adresi atar.

Kablosuz (Wireless) ve Yerel Ağ (LAN) Protokolleri

Ethernet (IEEE 802.3) → Kablolu ağ iletişim standardıdır.

Wi-Fi (IEEE 802.11) → Kablosuz ağ iletişimi sağlar.

Bluetooth → Kısa mesafede cihazlar arası veri iletimi sağlar.

Network Güvenliği Protokolleri

TLS (Transport Layer Security) / SSL (Secure Sockets Layer) → Web siteleri ve uygulamalar için şifreli veri iletişimi sağlar.

IPSec (Internet Protocol Security) → IP tabanlı güvenli veri iletimi sağlar.

SSH (Secure Shell) → Güvenli uzak bağlantılar için kullanılır.

Bazı Terimler

Proces

Proces, bilgisayarın üzerinde çalıştırdığı her programdır. Örneğin, bilgisayarınızda Web tarayıcınızı açtığınızda, bu bir proces olarak başlar. Tarayıcı, kendi belleğini ve kaynaklarını kullanarak çalışır.

Örnek: Google Chrome açtığınızda, Chrome bir işlem başlatır ve tüm çalışma işlemleri (sayfaları yüklemek, sekmeler arasında geçiş yapmak) bu işlem içinde yönetilir.

Thread

Thread, processin alt birimidir. Yani, bir işlemde birden fazla thread olabilir. Örneğin, Google Chrome'u açarken aynı anda bir sayfa yükleniyor, bir yanda da arka planda başka işler yapılıyor (güncellemeleri kontrol etmek). Bu procesler farklı thread'ler tarafından paralel olarak yapılır.

Örnek: Google Chrome'da bir sayfa yüklenirken, diğer bir thread de arka planda belgeyi kaydetmek gibi başka bir işlemi yapabilir.

Socket

Socket, ağ üzerindeki iki cihaz arasında veri iletimi yapmak için kullanılan bir yazılım arabirimidir. Her socket, bir IP adresi ve port numarasına sahiptir ve istemci ile sunucu arasındaki bağlantıyı sağlar. TCP veya UDP protokolleri ile çalışabilir.Bilgisayarlar arasındaki ağ bağlantısını sağlayan bir "kapı" gibidir.

Örnek: Google Chrome'da bir web sitesine gitmek istediğinizde, bu isteği internet üzerinden göndermek için socket kullanılır. Tarayıcınızın soketi, sunucudan veri alır (örneğin, bir web sayfası).

Ephemeral Port

Ephemeral port, istemciler (client) tarafından bağlantı kurarken geçici olarak kullanılan port numaralarıdır. Genellikle 1024 ile 65535 arasında bir numara alır ve bağlantı sona erdiğinde serbest bırakılır. Sunucu yerine istemci tarafında kullanılır.

Örnek: Google Chrome'u açtığınızda, bağlantı kurmak için bir geçici port numarası kullanılır (mesela 1025), bu port numarası web sayfası yüklendikten sonra serbest bırakılır.

1) Application Layer

Kullanıcı ile ağ arasındaki etkileşimi sağlayan katmandır. Bu katmanda, HTTP, FTP, SMTP, DNS gibi protokoller çalışır ve veriyi kullanıcı dostu hale getirir. Web tarayıcıları, e-posta istemcileri ve dosya transfer uygulamaları bu katmanda çalışır, böylece kullanıcının internet servisleriyle doğrudan etkileşime girmesi sağlanır.

HTTP

HTTP, World Wide Web'de (WWW) tarayıcılar ve sunucular arasında veri iletmek için kullanılan bir protokoldür. Web sayfaları ve diğer medya öğeleri HTTP protokolü ile iletilir. Her web sayfasına erişim, HTTP üzerinden yapılır.

Worl Wide Web

WWW, dünya çapında farklı sunucular (veya bilgisayarlar) aracılığıyla paylaşılan farklı bilgileri içeren web sitelerinin koleksiyonu olarak tanımlanır.

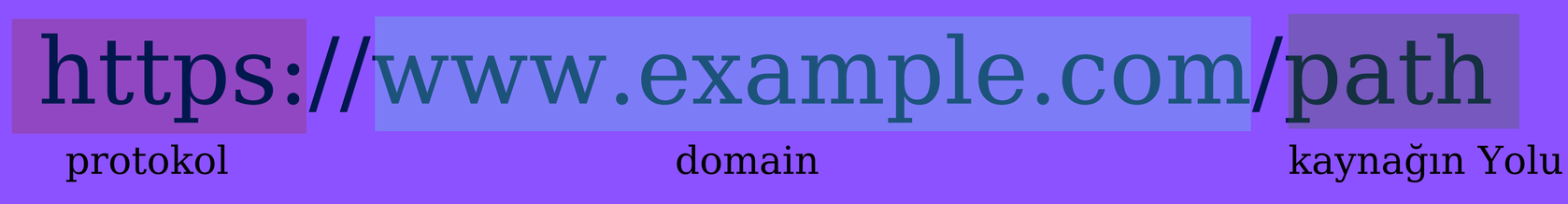
Web sayfaları, hiperlinkler aracılığıyla birbirine bağlanır ve bu bağlantılar HTML formatında yazılır. Hiperlinkler, kullanıcıların ilgili bilgilere kolayca erişmesini sağlar. HTTP protokolü üzerinden bu sayfalara ulaşılır ve hipermetin sayesinde kullanıcılar tıklayarak daha fazla bilgi edinebilir. Veriler, metin, resim, ses veya video formatlarında sunulabilir.

Hiperlink

Hiperlink, bir web sayfasında bulunan ve kullanıcıyı başka bir sayfaya, kaynağa veya aynı sayfada başka bir bölüme yönlendiren bir bağlantıdır. Hiperlinkler genellikle metin (örneğin, tıklanabilir kelimeler) veya görseller (örneğin, resimler) şeklinde olabilir ve tıklandığında başka bir web sayfasına ya da bir dosyaya yönlendirir.

URL (Uniform Resource Locator)

URL, internet üzerindeki bir kaynağın (web sayfası, dosya vb.) adresini belirtir. URL, protokol (http), domain (www.example.com) ve kaynağın yolunu (örneğin /path/to/resource) içerir.



Domain

internet üzerindeki bir kaynağın tanımlayıcı adresidir. Web sitelerinin internet üzerindeki "adresleri" olarak düşünülebilir. Bir domain adı, genellikle bir web sitesine erişmek için kullanılan IP adresinin daha okunabilir bir versiyonudur.

Örnek: www.example.com bir domain adıdır. Bu domain, IP adresi gibi teknik bir adresi (örneğin, 192.168.1.1) daha kullanıcı dostu bir hale getirir.

HTTP METHODS

HTTP, istemcinin sunucuya nasıl istek göndereceğini belirleyen bazı yöntemlere sahiptir

GET → Sunucudan veri almak için kullanılır. Örneğin, bir web sayfası yüklendiğinde kullanılan yöntem.

POST → Sunucuya veri göndermek için kullanılır, örneğin bir formu gönderirken.

DELETE → Sunucudan belirli bir kaynağı silmek için kullanılır.

PUT → Sunucudaki bir kaynağı güncellemek veya yeni bir kaynak eklemek için kullanılır.

HTTP Request Headers

HTTP request headers, istemcinin (tarayıcı) sunucuya gönderdiği ek bilgileri içerir.

Accept-Language → İstemcinin tercih ettiği dili belirtir. Örneğin, en-US (İngilizce - ABD) veya tr (Türkçe).

User-Agent → Tarayıcı ve işletim sistemi hakkında bilgi verir. Web sunucuları, gelen isteğin türünü anlayabilir.

HTTP Status Code (Durum Kodu)

HTTP yanıtları, istemcinin yaptığı isteğin sonucunu belirtmek için durum kodları kullanır.

1xx (Bilgilendirme) → İstek alındı, ancak işleme devam ediyor. Örnek:
100 Continue - İstek alınmaya devam edebilir.

2xx (Başarı) → İstek başarıyla işleme alındı. Örnek:
200 OK - İstek başarıyla tamamlandı.

3xx (Yönlendirme) → İstemci başka bir URL'ye yönlendirilmelidir. Örnek:
301 Moved Permanently - Kaynak kalıcı olarak taşındı.

4xx (İstemci Hatası) → İstemci hatalı istek yaptı. Örnek:
404 Not Found - Kaynak bulunamadı.

5xx (Sunucu Hatası) → Sunucu isteği işlerken hata meydana geldi. Örnek:
500 Internal Server Error - Sunucu hatası oluştu.

Cookies

Cookies, web siteleri tarafından kullanıcıların tarayıcılarında saklanan küçük veri dosyalarıdır. Bu dosyalar, kullanıcıların siteye olan önceki ziyaretlerini hatırlayarak, deneyimlerini kişiselleştirmek ve kullanıcı tercihlerini kaydetmek amacıyla kullanılır.

Cookies'in Kullanım Alanları:

1) Kullanıcı oturumunu yönetmek (örneğin, giriş yapmış bir kullanıcının tekrar giriş yapmaması).
2) Kullanıcı tercihlerini hatırlamak (örneğin, dil veya tema tercihi).
3) Web sitesinin performansını izlemek (örneğin, ziyaretçi sayısı, popüler sayfalar).

Third Party Cookies

Bir web sitesinin ziyaretçisi tarafından doğrudan değil, o site dışında başka bir domain (örneğin bir reklam ağı) tarafından yerleştirilen çerezlerdir. Bu tür çerezler, genellikle kullanıcıyı takip etmek ve reklam hedeflemesi yapmak için kullanılır.

E-Posta

E-posta iletişimi, e-postaların nasıl gönderileceğini, alınacağını ve saklanacağını belirleyen bir dizi protokole dayanır.

SMTP

E-posta gönderdiğinizde, ilk olarak SMTP (Simple Mail Transfer Protocol) sunucusu tarafından işlenir. SMTP, e-postayı e-posta istemcinizden (Outlook, Gmail vb.) alıcıların mail sunucusuna göndermek için kullanılır.Ancak, e-posta depolanmaz, yalnızca iletilir.

Port: SMTP genellikle 25 numaralı portu kullanır, ancak modern e-posta sunucuları güvenli e-posta göndermek için 587 veya 465 portlarını da kullanabilir.

E-posta gönderildikten ve alıcının mail sunucusunda saklandıktan sonra, alıcı bu e-postayı almalıdır. Bu işlemde POP3 (Post Office Protocol 3) veya IMAP (Internet Message Access Protocol) protokolleri kullanılır.

POP3

E-posta istemcilerinin sunucudan e-posta alıp yerel cihaza indirmesine olanak tanır. OP3 kullanıldığında, e-posta sunucudan cihazınıza indirilir ve genellikle indirildikten sonra sunucudan silinir. Bu durum, e-postaların yalnızca indirilen cihazdan erişilebileceği anlamına gelir. Ancak POP3, e-postaların birden fazla cihazda senkronize edilmesine imkan tanımaz; yani bir cihazda indirilen e-posta, diğer cihazlardan erişilemez.

Port: Varsayılan olarak 110 numaralı portu kullanır. Güvenli bağlantılar için 995 numaralı port kullanılabilir.

IMAP

Kullanıcıların e-postalarına doğrudan sunucudan erişmesini ve yönetmesini sağlar. IMAP, kullanıcıların e-postalarını sunucudan görüntülemesine ve düzenlemesine olanak tanır. E-postalar sunucuda kaldığı için, bir cihazda yapılan değişiklikler (örneğin, e-postaların okunması) tüm cihazlarda senkronize olur. Bu, IMAP'ı birden fazla cihazdan e-posta erişimi için ideal hale getirir ve e-posta yönetimini daha esnek bir hale getirir.

Port: IMAP, güvenli bağlantılar için 993 numaralı portu, güvensiz bağlantılar için ise 143 numaralı portu kullanır.

DNS Domain Name System

İnternetteki alan adlarını IP adreslerine çevirmek için kullanılan bir sistemdir. DNS, internetin "telefon rehberi" gibi çalışarak kullanıcıların alan adları ile IP adresleri arasında bağlantı kurmasını sağlar.

Root DNS Server

Root DNS sunucusu, internetin Domain Name System (DNS) hiyerarşisinin en üst seviyesinde bulunan kritik bir bileşendir. Kullanıcıların alan adlarını (örneğin, example.com) IP adreslerine çevirmek için başlattığı sorguların ilk durağıdır. Alan adlarının en üst düzeyinde bulunur ve ".com", ".org", ".net" gibi üst düzey alan adı sunucularına yönlendirme yapar.Doğrudan alan adlarını çözümlemez; bunun yerine, ilgili TLD (Top-Level Domain) sunucularına yönlendirir.

TLD (Top-Level Domain)

TLD, bir alan adının en üst seviyesini temsil eden uzantıdır.

SLD (Second-Level Domain)

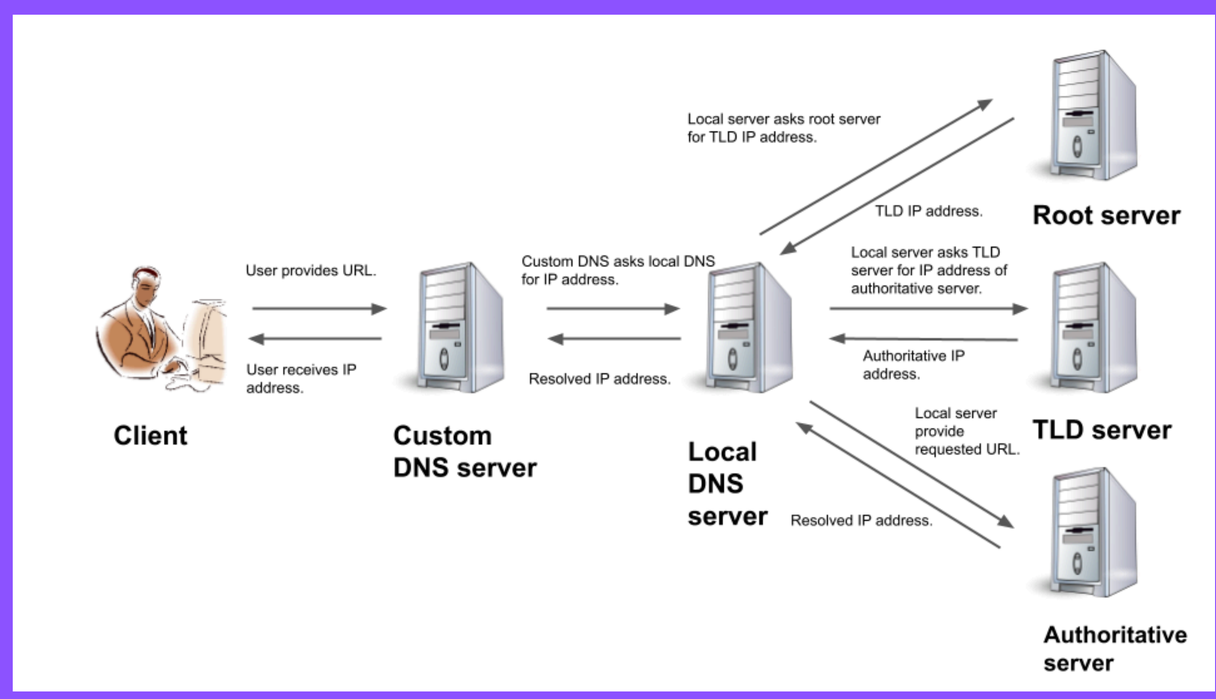
SLD, bir alan adının TLD’den önce gelen kısmıdır.

university.edu.tr alan adında SLD = university, TLD = .edu.tr

example.com alan adında SLD = example, TLD = .com

DNS Hiyerarşisi

1. Root DNS Server (En üst seviye)
2. TLD DNS Server (.com, .org, .tr gibi uzantıları yönetir)
3. SLD DNS Server (Alan adlarını IP adreslerine çeviren sunucular)
4. Recursive DNS Resolver (İnternet servis sağlayıcısı tarafından sağlanan, sorguları root ve TLD sunucularına yönlendiren sistem)



ICANN ve Root DNS Server

ICANN (Internet Corporation for Assigned Names and Numbers), internet üzerindeki IP adresleri, alan adları ve root DNS sistemlerini yönetmekten sorumlu küresel bir organizasyondur. ICANN, root DNS sunucularının çalışmasını denetler ancak bu sunucular farklı organizasyonlar tarafından işletilir.

2) Transport Layer

Cihazlar arasında güvenilir veya güvenilir olmayan veri aktarımını yöneten TCP/IP modelinin ikinci katmanıdır. Bu katman, veri akışını yönetir, paketleri doğru sırayla iletir ve ağ üzerindeki farklı uygulamaların birbirleriyle güvenli veya güvenli olmayan şekilde iletişim kurmasını sağlar. TCP ve UDP gibi protokoller bu katmanda çalışır.
Veriler, kaynaktan hedefe gönderilirken segment veya datagram adı verilen küçük veri bloklarına ayrılır. Bu süreç, büyük veri dosyalarının güvenli ve verimli bir şekilde iletilmesine yardımcı olur.

Trafik Kontrolü

Network trafiğinin dengeli bir şekilde yönetilmesi, transport katmanının önemli görevlerinden biridir. Bu katman, veri akışını düzenleyerek ağda tıkanıklık yaşanmasını önler. TCP, pencere boyutu (window size) mekanizmasını kullanarak karşı tarafın veri alım hızına göre gönderilen veri miktarını

Window Size: TCP akış kontrolü sırasında veri iletimini denetleyen bir parametredir ve alıcı tarafın bir anda alabileceği maksimum veri miktarını belirtir.

Checksums

Veri iletimi sırasında oluşabilecek hataları tespit etmek için taşıma katmanı checksum adı verilen hata kontrol mekanizmasını kullanır. Bu yöntemle, her paket belirli bir doğrulama değeri ile birlikte gönderilir ve alıcı bu değeri kontrol ederek verinin bozulup bozulmadığını tespit eder. Hatalı paketler tespit edildiğinde TCP, eksik veya hatalı verileri yeniden göndererek bütünlüğü sağlar.

Timers

Veri paketlerinin zamanında ve eksiksiz ulaşmasını sağlamak için zamanlayıcılar kullanır. Bir veri paketi belirli bir süre içinde alıcıdan onay mesajı (ACK) almazsa, zamanlayıcı tetiklenir ve paket tekrar gönderilir. Bu mekanizma, ağda veri kaybını önlemeye ve iletişim güvenilirliğini artırmaya yardımcı olur.

ACK (Acknowledgment): TCP protokolünde "onay" anlamına gelen bir mesaj türüdür ve güvenilir veri iletimisağlamak için kullanılır.

Reserved Address

Reserved IP adresleri, belirli ağ hizmetleri veya özel kullanımlar için ayrılmış IP bloklarıdır. Genel internette yönlendirilmezler, belirli amaçlarla kullanılırlar.
Örnekler:
Özel Ağlar (Private IPs) → 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12 (LAN içinde kullanılır, internete çıkmaz)
Loopback Adresi (127.0.0.0/8) → Cihazın kendisini test etmesi için kullanılır.
Link-Local Adresleri (169.254.0.0/16) → DHCP sunucusu yoksa cihazlar otomatik IP alır.

LocalHost

Cihazın kendi kendisine erişimini ifade eden sanal adrestir. Genellikle "127.0.0.1" IP adresiyle eşleştirilir.

Loopback Host

Ağ arayüzünü kullanmadan kendi bilgisayarında testler yapmak için kullanılır.

IP Paketi

Ağ üzerinden veri iletmek için kullanılan temel yapıdır. İki ana bileşeni vardır:

Header:
Başlık kısmı, paketin **nasıl iletileceğini** belirleyen bilgileri içerir.

Alan	Açıklama
Source IP	Paketi gönderen cihazın IP adresi
Destination IP	Paketin ulaşması gereken hedef IP adresi
Version	IPv4 mü, IPv6 mı olduğunu belirler
TTL (Time To Live)	Paketin maksimum kaç yönlendirici geçebileceğini belirler
Protocol	Üst katmandaki protokolü (TCP, UDP, ICMP vb.) belirtir
Header Checksum	Hata kontrolü için kullanılır

Payload (Veri Bölümü):
Web sayfası verisi, e-posta içeriği, ses/görüntü verisi vb. burada taşınır.

TTL (Time To Live)

TTL, paketin yönlendiriciler arasında kaç kez taşınabileceğini belirleyen bir sayaçtır.Her yönlendirici paketin TTL değerini 1 azaltır.TTL sıfıra ulaşırsa, paket atılır ve göndericiye bir ICMP "Time Exceeded" hatası döner.
Sonsuz döngüye giren paketleri önlemek için kullanılır

Middleboxes (Ara Cihazlar)

Ağ trafiğini denetleyen ve değiştiren ara cihazlar olarak tanımlanır. Bunlar, veri paketlerinin doğrudan hedefe ulaşmadan önce farklı kurallara göre işlenmesini sağlar. Güvenlik duvarları (firewall), NAT cihazları, yük dengeleyiciler (load balancer) ve proxy sunucuları bu kategoriye girer. Middlebox'lar güvenliği artırma, trafik yönetimi ve ağ performansını iyileştirme amacıyla kullanılır.

Firewall

Firewall, ağ trafiğini filtreleyerek yetkisiz erişimleri engelleyen ve güvenliği artıran bir ağ cihazı veya yazılımıdır. Paket filtreleme yapan basit firewall'lar Network Layer (Katman 3) ve Transport Layer (Katman 4) seviyesinde çalışır, IP adresleri ve port numaralarına göre izin veya engelleme işlemi yapar. Daha gelişmiş stateful firewall'larbağlantı durumunu takip eder ve uygulama katmanı seviyesinde (Katman 7) çalışan firewall'lar, belirli protokolleri derinlemesine analiz ederek zararlı trafiği engelleyebilir.

NAT (Network Address Translation)

NAT, bir özel ağ içindeki cihazların internete tek bir genel IP adresi üzerinden çıkmasını sağlayan bir mekanizmadır. Örneğin, evdeki veya iş yerindeki tüm cihazlar yerel ağda 192.168.x.x gibi özel IP adresleri kullanırken, NAT sayesinde internete çıkarken tek bir genel IP adresi ile görünürler. NAT, IPv4 adreslerinin yetersizliği nedeniyle yaygın olarak kullanılmıştır. NAT’ın farklı türleri vardır:

- Static NAT: İç IP adreslerini belirli bir dış IP adresiyle eşleştirir.
- Dynamic NAT: İç IP adreslerini rastgele bir dış IP adresiyle eşleştirir.
- PAT (Port Address Translation – NAT Overload): Birden fazla cihazın tek bir genel IP adresini kullanmasını sağlar ve port numaralarını kullanarak bağlantıları ayırt eder.

3) Data Link Layer

Data Link Layer, OSI modelinin 2. katmanıdır ve cihazların aynı ağ içinde (LAN – Local Area Network) nasıl iletişim kuracağını belirler. Bu katman, veriyi "frame" (çerçeve) adı verilen yapılar halinde işler ve fiziksel bağlantılar üzerinden iletilmesini sağlar. Hata tespiti, erişim kontrolü ve adresleme gibi işlemler bu katmanda gerçekleştirilir. Ethernet, Wi-Fi ve PPP (Point-to-Point Protocol) gibi protokoller Data Link Layer’da çalışır. Bu katmanda IP adresleri değil, fiziksel donanım adresleri (MAC adresleri) kullanılır, böylece cihazlar aynı ağ içinde doğrudan haberleşebilir.

DHCP (Dynamic Host Configuration Protocol)

DHCP, cihazlara otomatik olarak IP adresi, ağ geçidi (gateway) ve DNS sunucusu gibi bilgileri atayan bir protokoldür. Bir cihaz ağa bağlandığında, DHCP sunucusuna bir istek (DISCOVER) gönderir ve sunucu uygun bir IP adresi atar. Bu, manuel IP yapılandırmasını gereksiz hale getirir ve ağ yönetimini kolaylaştırır. DHCP, ağdaki IP adreslerini dinamik olarak tahsis edebilir, böylece bir cihaz bağlantısını kestiğinde, onun IP adresi başka bir cihaza atanabilir.

MAC

MAC (Media Access Control) adresi, her ağ arayüzüne üretim sırasında atanan, 48-bit uzunluğunda benzersiz bir fiziksel adresdir. Bu adres, bir cihazın aynı ağ içindeki diğer cihazlarla doğrudan iletişim kurmasını sağlar. Bir MAC adresi, altı çift onaltılık sayıdan (hex) oluşur (örn. 00:1A:2B:3C:4D:5E). IP adreslerinden farklı olarak, MAC adresleri değişmez ve cihazın donanımına gömülüdür. Ancak, bazı işletim sistemlerinde MAC adresi değiştirilebilir (MAC spoofing).

ARP

ARP, IP adreslerini MAC adreslerine çevirmek için kullanılan bir protokoldür. Bir cihaz, aynı ağda haberleşmek istediği bir IP adresinin MAC adresini bilmiyorsa, ARP isteği (ARP Request) gönderir. Hedef cihaz, kendi MAC adresini içeren ARP yanıtı (ARP Reply) ile geri döner.

Cihazlar, ARP isteklerine sık sık ihtiyaç duymamak için ARP Cache adı verilen bir tablo kullanır. Bu tablo, IP adresi ve ona karşılık gelen MAC adresini belirli bir süreliğine saklar, böylece ağ trafiği azaltılmış olur. Ancak, yanlış ARP girişleri (ARP spoofing gibi saldırılar) ağ güvenliği açısından risk oluşturabilir.

Frame

Frame, Data Link Layer’da kullanılan veri paketinin adıdır. Bir frame, veriyi alıcıya iletmek için kaynak MAC adresi, hedef MAC adresi, hata kontrol bilgileri (CRC – Cyclic Redundancy Check) ve asıl veri içeren bir yapıdadır. Ethernet ve Wi-Fi gibi protokoller, farklı çerçeve formatları kullanır. Frame yapısı, ağda iletilen verinin doğru şekilde alıcıya ulaşmasını sağlar ve hata kontrolü yaparak bozuk verilerin tespit edilmesine yardımcı olur.

TCP ve Application Layer ilişkisi

Application Layer, büyük miktarda ham veri (raw data) gönderdiğinde, TCP bu veriyi uygun boyutlardaki segmentlere böler. Böylece, alıcı cihaz bu segmentleri sırayla ve eksiksiz alabilir. TCP’nin segmentleme işlemi, verinin ağ üzerinden daha verimli taşınmasını sağlar ve alıcıya ulaştığında tekrar birleştirilmesine olanak tanır.

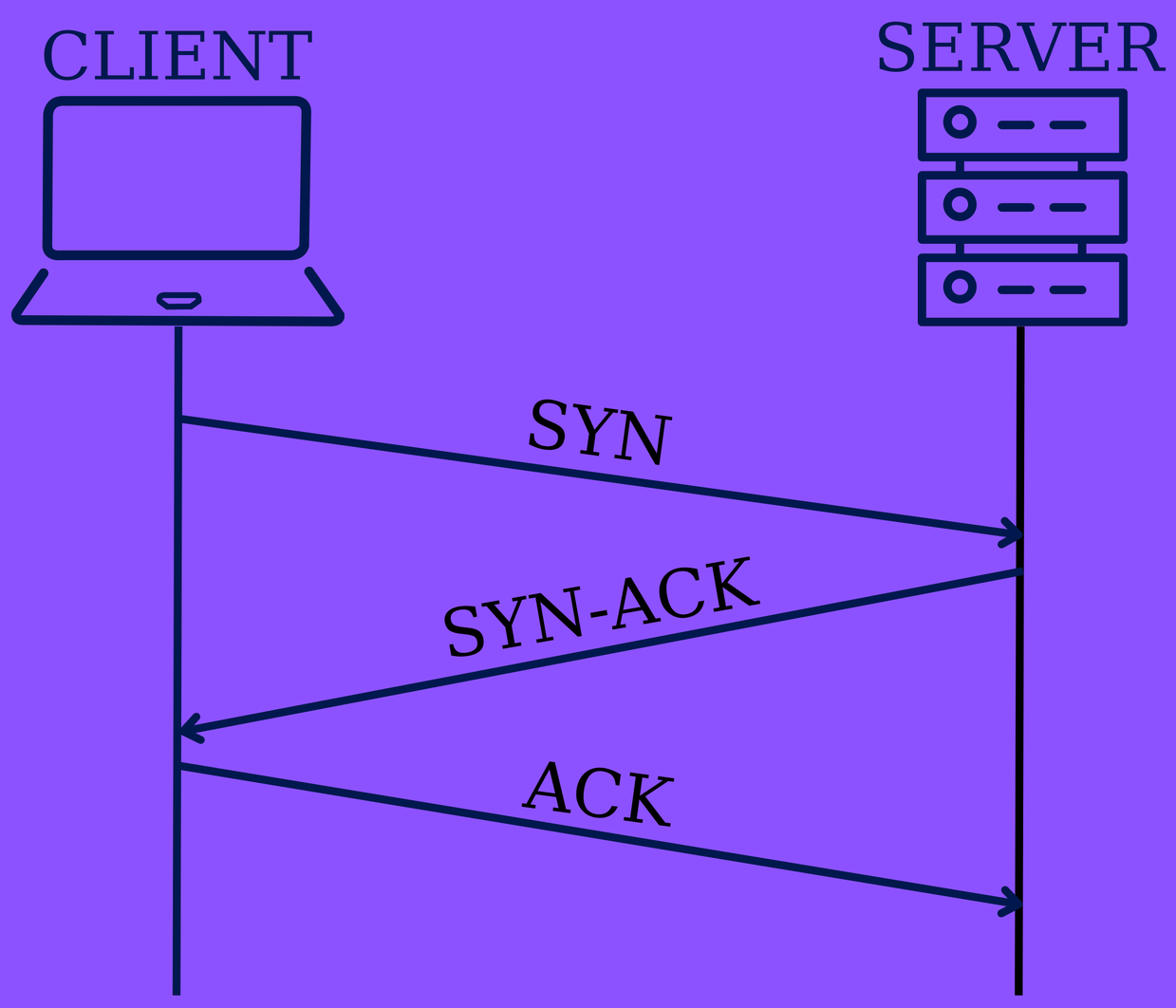
Congestion Control

TCP, ağ tıkanıklığını önlemek için Congestion Control (Tıkanıklık Kontrolü) mekanizmalarını kullanır. Bu mekanizmalar, hem ağın aşırı yüklenmesini engeller hem de veri akışını düzenler. İki temel faktöre dikkat eder:

1. Ağ Durumu: Eğer ağda yoğunluk varsa, TCP veri akış hızını otomatik olarak düşürür.
2. Alıcının Kapasitesi: Alıcının veri işleme kapasitesini aşmamak için "Pencere Boyutu" (Window Size) mekanizması kullanılır.

3-Way Handshake

TCP, bağlantı başlatırken güvenilir bir iletişim kurmak için "3-Way Handshake" mekanizmasını kullanır. Bu süreç şu adımlardan oluşur:
1.SYN (Synchronization): İstemci, sunucuya bağlantı isteği gönderir.
2.SYN-ACK (Synchronization-Acknowledgment): Sunucu, isteği kabul ettiğini ve kendisinin de bağlanmaya hazır olduğunu belirten bir yanıt yollar.
3.CK (Acknowledgment): İstemci, sunucunun yanıtını doğrular ve bağlantı kurulur.
Bu süreç, bağlantının her iki taraf için de hazır olmasını sağlar ve TCP'nin güvenilir bir iletişim mekanizması kurmasına yardımcı olur.



4) Network Layer

Verinin kaynak cihazdan hedef cihaza yönlendirilmesini ve IP adresleme işlemlerini yönetir. Bu katmanda, router'lar (yönlendiriciler) ve yönlendirme protokolleri kullanılarak paketlerin en verimli yoldan iletilmesi sağlanır. IP (Internet Protocol), her cihaza benzersiz bir adres atayarak veri paketlerinin doğru hedefe ulaşmasını garanti eder.

Router

Router (Yönlendirici), farklı ağları birbirine bağlayan ve veri paketlerini en uygun yol üzerinden yönlendiren bir ağ cihazıdır. IP adreslerine bakarak paketleri hedefe ulaştırır ve ağ trafiğini düzenler. Router’lar, statik veya dinamik yönlendirme yöntemleriyle çalışabilir.

Router’lar iki temel bileşenden oluşur

- Control Plane (Kontrol Düzlemi): Yönlendirme tablolarının oluşturulmasını ve ağın nasıl çalışacağını belirleyen mekanizmadır.
- Data Plane (Veri Düzlemi): Paketin fiziksel olarak yönlendirilmesini ve doğru hedefe ulaşmasını sağlayan mekanizmadır.

IP

IP (Internet Protocol), ağ cihazlarına benzersiz adresler atayan ve verilerin bu adresler üzerinden yönlendirilmesini sağlayan protokoldür. IPv4 ve IPv6 olmak üzere iki ana sürümü vardır.
Her IP adresi, bir ağ (network) ve bir cihaz (host) kısmından oluşur.

192.168.2.30

network adresi (subnet) cihaz adresi (host)

IPv4

32 bit adresleme kullanır.Adresler noktalı olarak biçimlendirilmiştir (192.168.1.1) . Ancak internet kullanıcılarının artmasıyla yetersiz hale gelmiştir.

IPv6

Yetersiz olma sorununu çözmek için geliştirilmiş olup 128 bit adresleme kullanır ve trilyonlarca benzersiz IP adresi sağlar. IPv6 adresleri sekiz gruptan oluşan hex formatında (2001:db8::ff00:42:8329) yazılır. IPv6, daha iyi güvenlik, otomatik adres atama ve daha verimli yönlendirme sunar.