

OSI MODEL

[Hazırlayan](#) - [Kaynak](#)

İÇERİK

1. OSI Modeli Nedir? (The OSI Model)
2. OSI Katmanları

OSI Modeli Nedir? (The OSI Model)

OSI Modeli (Open Systems Interconnection - Açık Sistemler Arabağlantısı), ağ dünyasının anayasası gibidir. Farklı üreticiler tarafından geliştirilen cihazların (örneğin bir iPhone ile bir Windows PC veya bir Cisco Switch) birbirleriyle sorunsuz konuşabilmesini sağlayan, 7 katmandan oluşan standart bir çerçeve sunar.

Bu modelin en büyük avantajı **tekdüzelik (uniformity)** sağlamasıdır. OSI standartlarına uyan bir cihazdan çıkan veri, dünyanın öbür ucundaki farklı bir cihaz tarafından doğru şekilde yorumlanabilir.

OSI Modelinin Yapısı ve 7 Katman

OSI modeli, en üstte kullanıcıya en yakın olan katmandan (Layer 7), en alta fiziksel kablolama ve sinyallere (Layer 1) kadar uzanan **7 katmana** ayrılmıştır. Veri bu katmanlar arasında seyahat ederken her aşamada farklı işlemlerden geçer.

Katman No	Katman Adı (Türkçe / İngilizce)	Temel Görevi
Layer 7	Uygulama (Application)	Kullanıcının etkileşime girdiği katman (HTTP, FTP, SSH).
Layer 6	Sunum (Presentation)	Verinin formatlanması, şifrelenmesi ve sıkıştırılması.
Layer 5	Oturum (Session)	Cihazlar arası bağlantının kurulması ve yönetilmesi.
Layer 4	Taşıma (Transport)	Verinin parçalanması ve hata kontrolü (TCP, UDP).
Layer 3	Ağ (Network)	Yönlendirme ve IP adresleme (Routerlar buradadır).
Layer 2	Veri Bağlantısı (Data Link)	Fiziksel adresleme ve hata tespiti (MAC, Switchler).
Layer 1	Fiziksel (Physical)	Kablolar, elektrik sinyalleri, bitler (0 ve 1'ler).

Kapsülleme (Encapsulation) Nedir?

OSI modelinde verinin her bir katmandan geçerken bir üst katmandan gelen bilginin üzerine kendi protokol bilgilerini (başlık/header) eklemesi işlemine **Encapsulation (Kapsülleme)** denir.

- **Mantık:** Bir mektup yazdığınıza düşünün (Uygulama). Mektubu bir zarfa koyarsınız (Taşıma), zarfin üzerine adres yazarsınız (Ağ), mektubu posta arabasına yüklersiniz (Fiziksel). Her aşamada mektuba yeni bir "katman" veya "bilgi" eklenir.
- **Ters İşlem (De-encapsulation):** Veri alıcıya ulaştığında, Layer 1'den başlayarak her katman kendi eklediği bilgiyi "soyarak" bir üst katmana iletir. En sonunda sadece saf veri kullanıcıya ulaşır.

Neden OSI Modelini Öğreniyoruz?

1. **Troubleshooting (Arıza Tespiti):** Bir ağ sorunu olduğunda "Kablo takılı mı?" (Layer 1) sorusundan başlayarak "IP alabiliyor mu?" (Layer 3) sorusuna kadar sistematik bir kontrol yapmamızı sağlar.
2. **Güvenlik:** Siber saldırıların hangi katmanda gerçekleştiğini anlamak için kritiktir. Örneğin; bir **DDoS** saldırısı Layer 3'te (IP seviyesi) mi yoksa Layer 7'de (Uygulama/HTTP seviyesi) mi oluyor?
3. **Standartlaşma:** Farklı donanım ve yazılımların bir arada çalışabilmesini (Interoperability) garantiler.

7. Application

6. Presentation

5. Session

4. Transport

3. Network

2. Data link

1. Physical

OSI Katmanları

Katman 1: Fiziksel Katman (Physical Layer)

Anlaması en kolay katmandır çünkü tamamen fiziksel donanımlar ve elektriksel sinyallerle ilgilidir. OSI modelinin en alt basamağıdır.

- **Veri Tipi:** Bu katmanda veri, **Binary** (ikilik) sistemdeki **1 ve 0'lar** olarak temsil edilir.
- **İletişim:** Cihazlar arasındaki veri transferi elektriksel sinyaller, ışık sinyalleri (fiber) veya radyo dalgaları (Wi-Fi) aracılığıyla gerçekleşir.
- **Bileşenler:** **Ethernet kabloları**, konnektörler, hublar ve tekrarlayıcılar (repeater) bu katmanda yer alır. Kısacası, elinizle tutabildiğiniz ağ ekipmanları Katman 1'in konusudur.

Katman 2: Veri Bağlantısı Katmanı (Data Link Layer)

Bu katman, verinin fiziksel olarak nasıl iletileceğine ve cihazların birbirini ağ üzerinde nasıl tanıyalacağına odaklanır.

- **MAC Adresi (Physical Addressing):** Her ağ kartının (**NIC - Network Interface Card**) üretim aşamasında içine "kazınmış" (hardcoded), dünyada eşi benzeri olmayan bir **MAC Adresi** vardır.
 - **Önemli:** IP adresleri değişimdir ancak MAC adresleri kalıcıdır (ancak yazılımsal olarak **Spoofing** yani taklit edilebilirler).
- **Kapsülleme İşlemi:** Bu katman, bir üst katmandan (Network Layer) gelen IP paketini alır ve üzerine hem gönderenin hem de alıcının **MAC adresini** ekleyerek bir **Frame** (Çerçeve) haline getirir.
- **Görevleri:**
 - Veriyi fiziksel iletime uygun formata sokar.
 - Hata tespiti yapar.
 - Yerel ağdaki (LAN) cihazların birbirini fiziksel olarak bulmasını sağlar.

Katman 3: Ağ Katmanı (Network Layer)

"Yönlendirme büyüsünün" gerçekleştiği, verinin parçalara ayrıldığı ve bu parçaların (chunk) tekrar birleştirildiği katmandır.

- **IP Adresleme:** Bu katmanda her şey **192.168.1.100** gibi mantıksal IP adresleri üzerinden yürürl.
- **Yönlendirme (Routing):** Verinin hedef bilgisayara gitmesi için en "optimal" yolu belirler.
- **Yönlendirme Karar Kriterleri:** Verinin hangi yoldan gideceğine şu faktörlere bakılarak karar verilir:
 1. **En Kısa Yol:** Paket en az kaç cihaz (hop) üzerinden geçecek?
 2. **Güvenilirlik:** Daha önce bu yolda paket kaybı yaşandı mı?
 3. **Hız:** Yol üzerindeki fiziksel bağlantı nedir? (Bakır kablo mu, fiber mi?)

- Protokoller:** Bu kararları vermek için **OSPF** (Open Shortest Path First) ve **RIP** (Routing Information Protocol) gibi protokoller kullanılır.
- Cihazlar:** IP adreslerini okuyabilen ve paketleri yönlendirebilen **Router** (Yönlendirici) cihazları **Layer 3** cihazı olarak adlandırılır.

Katman 4 - Taşıma Katmanı (Transport Layer)

Katman 4, verinin ağ üzerinden nasıl iletileceğinin "kurallarını" koyan, iletişim kalitesini ve yöntemini belirleyen hayatı bir katmandır. Bu katmanda veriler **Segment** (Segmentlere ayırma) olarak adlandırılır. Bir cihazdan diğerine veri gönderilirken, ihtiyaca göre iki ana protokolden biri seçilir: **TCP** veya **UDP**.

1. TCP (Transmission Control Protocol - İletim Kontrol Protokolü)

TCP, "garantici" protokoldür. Verinin eksiksiz, hatasız ve doğru sırada karşı tarafa ulaşmasını her şeyin üzerinde tutar.

- Bağlantı Temelli (Connection-Oriented):** Veri gönderilmeden önce iki cihaz arasında sürekli bir bağlantı kurulur ve veri aktarımı bitene kadar bu hat açık tutulur.
- Hata Kontrolü (Error Checking):** Katman 5'ten gelen veri parçalarının (chunks) karşı tarafa ulaşıp ulaşmadığını kontrol eder. Eğer bir parça kaybolursa, TCP o parçayı tekrar gönderir.
- Sıralama:** Veri paketlerinin gönderildiği sırayla karşı tarafta birleştirilmesini sağlar. (Örneğin; 1, 2, 3 numaralı paketler karışık gelse bile TCP bunları 1-2-3 şeklinde dizer).

TCP'nin Avantaj ve Dezavantajları

Avantajlar	Dezavantajlar
Veri Doğruluğu: Verinin hatasız iletileceğini garanti eder.	Bağlantı Bağımlılığı: Cihazlar arasında güvenilir bir hat gerektirir. Bir parça eksikse tüm veri kullanılamaz hale gelir.
Senkronizasyon: İki cihazın birbirini veri yağmuruna tutmasını (flooding) engeller.	Yavaşlık: Veri akışı sırasında alıcı cihazda kaynak ayırdığı (reserve) için yavaş bağlantılarında darboğaz oluşturabilir.
Güvenilirlik: Hata kontrolü için çok daha fazla işlem yapar.	Hantal Yapı: UDP'ye göre çok daha fazla kontrol süreci olduğu için daha yavaştır.

- Kullanım Alanları:** Dosya paylaşımı (FTP), web tarayıcıları (HTTP/HTTPS) ve e-posta (SMTP). Çünkü bir dosyanın veya e-postanın yarısının eksik olması kabul edilemez.

2. UDP (User Datagram Protocol - Kullanıcı Veri Bloğu Protokolü)

UDP, TCP'nin "hızlı ve umursamaz" kardeşidir. TCP'nin sunduğu hata kontrolü, sıralama veya bağlantı garantisini gibi özelliklerin hiçbirine sahip değildir.

- Bağlantısız (Connectionless):** Veriyi gönderir ve karşıya ulaşıp ulaşmadığını kontrol etmez. "Gönder ve unut" mantığıyla çalışır.
- Garanti Yok:** Veri yolda kaybolabilir, sırası karışabilir; UDP bunu düzeltmeye çalışmaz. Sadece elinden geldiğince hızlı gönderir.

UDP'nin Avantaj ve Dezavantajları

Avantajlar	Dezavantajlar
Çok Hızlıdır: TCP'deki onay mekanizmaları (handshake) olmadığı için gecikme minimumdur.	Güvenilmez: Verinin ulaşıp ulaşmadığı umurunda değildir.
Esneklik: Paketlerin ne kadar hızlı gönderileceği kararını uygulama katmanına bırakır.	Kötü Deneyim: Kararsız bağlantınlarda veri kaybı çok olduğu için kullanıcı deneyimi bozulur (görüntüde donma vb.).
Kaynak Tüketimi: TCP gibi sürekli bir bağlantı rezerve etmez, sistem kaynaklarını yormaz.	Sıralama Garantisi Yok: Paketler karışık giderse uygulama bunu düzeltmek zorundadır.

- Kullanım Alanları:** Video akışı (Netflix, YouTube Live), online oyunlar, VoIP (sesli aramalar) ve bazı keşif protokolleri (**ARP, DHCP**).
- Mantık:** Bir videoda birkaç saniyelik piksellenme (kayıp veri) olması, videonun tamamen durup o pikselleri beklemesinden daha iyidir.

TCP vs UDP: Özeti Karşılaştırma

TCP Örneği: Bir kedi resmini TCP ile gönderdiğinizde, resim 100 parçağa bölünür. Bilgisayar bu parçaları 1'den 100'e kadar dizer. Eğer 45. parça eksikse, TCP onu tekrar ister ve resim kusursuz bir şekilde birleştirilir.

UDP Örneği: Aynı kedi resmini UDP ile gönderirseniz, bilgisayar 1, 3, 7 numaralı parçaları alabilir, 2 numara yolda kaybolabilir. Sonuçta kedi resminin yarısı pikseli veya eksik görünür ama resim çok daha hızlı "gelir".

Katman 5: Oturum Katmanı (Session Layer)

Veri, Katman 6'da (Sunum) formatlandıktan sonra Katman 5'e gelir. Bu katmanın temel görevi, iki bilgisayar arasındaki iletişimini başlatmak, yönetmek ve sonlandırmaktır.

- Oturum Yönetimi:** Bir bağlantı kurulduğunda bir "oturum" (session) oluşturulur. Bu bağlantı aktif olduğu sürece oturum da açık kalır.
- Bağlantı Denetimi:** Eğer bir bağlantı uzun süre kullanılmazsa veya beklenmedik şekilde koparsa, bu durumu fark edip bağlantıyı güvenli bir şekilde kapatmak Katman 5'in görevidir.
- Checkpoint (Kontrol Noktaları):** Veri iletimi sırasında "kontrol noktaları" oluşturur.

- **Örnek:** Büyük bir dosya indirirken bağlantı koparsa, tüm dosyayı en baştan indirmek yerine kalınan son kontrol noktasından devam edilmesini sağlar. Bu, ciddi bir bant genişliği tasarrufu sağlar.
- **Benzersizlik:** Her oturum kendine hastır. Veriler farklı oturumlar arasında çapraz geçiş yapamaz; veri sadece ait olduğu oturum kanalında akar.

Katman 6: Sunum Katmanı (Presentation Layer)

Bu katman ağın "çevirmeni" ve "standardizasyon merkezi"dir. Yazılım geliştiriciler uygulamalarını farklı şekillerde kodlayabilirler, ancak verinin her cihazda aynı şekilde görünmesi gereklidir.

- **Veri Çevirisi:** Uygulama katmanından (Layer 7) gelen verileri ağ üzerinden gönderilebilecek ortak bir dile veya formata çevirir. Alıcı tarafta ise ağdan gelen veriyi uygulamanın anlayacağı formata dönüştürür.
 - **Örnek:** Sen Outlook kullanırken arkadaşın Gmail kullanıyor olabilir. Yazılımlar farklı olsa da, bu katman sayesinde gönderdiğiniz e-postanın içeriği arkadaşının ekranında tipki senin yazdığınız gibi görünür.
- **Güvenlik ve Şifreleme:** Verinin güvenliği burada başlar. Günlük hayatı sıkça kullandığımız **HTTPS** (güvenli web sitesi ziyareti) gibi şifreleme işlemleri bu katmanda gerçekleşir. Veri, sunum katmanında şifrelenir (Encryption) ve karşı tarafta yine bu katmanda çözülür (Decryption).
- **Sıkıştırma:** Verinin daha hızlı iletilmesi için Katman 6'da sıkıştırma işlemleri yapılabilir.

Katman 7 - Uygulama Katmanı (Application Layer)

OSI modelinin en tepesine, yani piramidin zirvesine ulaştık. **Katman 7**, son kullanıcının doğrudan etkileşime girdiği, ağ üzerindeki veriyi anlamlı bir hizmete dönüştüren katmandır.

Uygulama Katmanı Nedir?

Bu katman, kullanıcının en aşina olduğu bölümdür. Bilgisayarınızda veya telefonunuzda açığınız uygulamaların ağ ile nasıl iletişim kuracağınızı belirleyen protokoller ve kurallar burada çalışır.

- **Kullanıcı Etkileşimi:** Verinin gönderilmesi veya alınması sırasında kullanıcının bu veriyle nasıl etkileşime gireceğini belirler.
- **GUI (Grafiksel Kullanıcı Arayüzü):** Uygulama katmanı, ham veriyi kullanıcı için anlamlı hale getiren dost canlısı arayüzler sağlar. Örneğin, sadece kodlarla uğraşmak yerine **FileZilla** gibi bir yazılımla dosyalarınızı sürükle-bırak yöntemiyle sunucuya taşırsınız.

Temel Protokoller ve Araçlar

Bu katmanda çalışan protokoller, günlük internet kullanımımızın temelini oluşturur:

- **DNS (Domain Name System):** Internetin telefon rehberidir. Biz tarayıcıya `google.com` yazdığımızda, uygulama katmanındaki DNS protokolü devreye girerek bu ismi yönlendiricilerin anlayabileceği bir **IP adresine** çevirir.
- **HTTP / HTTPS:** Web tarayıcılarınızın (Chrome, Firefox) web sitelerini görüntülemesini sağlar.
- **SMTP / IMAP / POP3:** E-posta istemcilerinin (Outlook, Thunderbird) e-posta gönderip olmasını sağlar.
- **FTP / SFTP:** Dosya transfer işlemlerini (FileZilla gibi araçlarla) yönetir.

Önemli Not: Siber Güvenlik Bakış Açısı

Siber güvenlikte "**Layer 7 Attacks**" (Uygulama Katmanı Saldırıları) terimini çok sık duydunuz. Saldırganlar ağıın alt katmanlarıyla (kablolar veya yönlendirme protokoller) uğraşmak yerine, doğrudan kullanıcının etkileşimde olduğu bu katmana saldırırlar.

- **Örnekler:** SQL Injection, Cross-Site Scripting (XSS) veya HTTP Flood (DDoS) saldırıları doğrudan bu katmandaki zayıflıkları veya protokollerini hedef alır.
- **Savunma:** Bu katmandaki saldırıları durdurmak için standart firewall cihazları yerine **WAF (Web Application Firewall)** gibi daha zeki, uygulama trafiğini analiz edebilen sistemler kullanılır.

OSI Modeli Genel Özeti (L1 - L7)

Katman	Adı	Veri Birimi	Temel Görev	Siber Güvenlik Odağı
L7	Application	Data	Kullanıcı Arayüzü & Protokoller	Web Açıkları (XSS, SQLi)
L6	Presentation	Data	Şifreleme & Formatlama	SSL/TLS Güvenliği
L5	Session	Data	Oturum Yönetimi	Session Hijacking
L4	Transport	Segment	TCP/UDP (Hata Kontrolü)	Port Tarama, Syn Flood
L3	Network	Packet	IP Adresleme & Yönlendirme	IP Spoofing, Routing Attacks
L2	Data Link	Frame	MAC Adresleme & Switch	ARP Spoofing, MAC Flooding
L1	Physical	Bit	Kablolar & Elektrik	Fiziksel Sızma, Kablo Kesme