Ağ Topolojileri (Network Topologies)

Bir ağın topolojisi, ağdaki cihazların birbirine nasıl bağlandığını (fiziksel) ve verinin bu cihazlar arasında nasıl iletildiğini (mantıksal) tanımlar. Ağ tasarımında topolojiyi anlamak, sorun giderme (troubleshooting) ve ağ performansı açısından kritik bir öneme sahiptir.

Topolojiler temel olarak ikiye ayrılır: **Fiziksel Topoloji** ve **Mantıksal Topoloji**.

1. Fiziksel Topoloji (Physical Topology)

Cihazların, kabloların ve diğer ağ bileşenlerinin fiziksel olarak nasıl yerleştirildiğini ve birbirine nasıl bağlandığını gösteren haritadır. Bir sunucu odasına girdiğinizde kabloların nereye gittiğini gösteren şema fiziksel topolojidir.

CCNA kapsamında bilinmesi gereken temel fiziksel topolojiler şunlardır:

Bus (Ortak Yol) Topolojisi

- **Yapısı:** Tüm cihazlar tek bir merkezî omurga kablosuna (backbone) zincirleme bağlanır.
- **Özellikleri:** Kurulumu kolay ve maliyeti düşüktür. Ekstra bir merkezî cihaza (Switch/Hub) ihtiyaç duyulmaz.
- **Dezavantajları:** Omurga kablosunda meydana gelen bir kopukluk, **tüm ağın çökmesine** neden olur. Günümüzde yerel ağlarda (LAN) artık kullanılmamaktadır. Çakışma (collision) ihtimali çok yüksektir (Half-Duplex çalışır).

Ring (Halka) Topolojisi

- **Yapısı:** Her cihaz, sağındaki ve solundaki komşusuna bağlanarak kapalı bir halka oluşturur.
- **Özellikleri:** Veri halka etrafında tek bir yönde akar. Çakışmaları önlemek için genellikle "Token (Jeton)" mantığıyla çalışır (Sadece jetona sahip olan cihaz veri gönderebilir).
- **Dezavantajları:** Tıpkı Bus topolojisi gibi, kablodaki tek bir kopukluk veya bir cihazın arızalanması tüm ağı etkileyebilir (FDDI gibi çift halkalı yedekli sistemler hariç).

Star (Yıldız) Topolojisi

- **Yapısı:** Tüm uç cihazların (PC, yazıcı vb.) merkezî bir cihaza (genellikle bir Switch) bağlandığı topolojidir. **Günümüzdeki LAN (Yerel Ağ) yapılarında en çok kullanılan topolojidir.**
- **Avantajları:** Kurulumu ve yönetimi kolaydır. Bir bilgisayarın kablosu kopsa bile sadece o bilgisayar ağdan düşer, **ağın geri kalanı etkilenmez**.
- **Dezavantajları:** Merkezdeki Switch arızalanırsa (Single Point of Failure), o Switch'e bağlı tüm cihazların ağ iletişimi kesilir.

Mesh (Örgü) Topolojisi

- **Yapısı:** Cihazların (genellikle Router veya Switch'lerin) birden fazla yolla birbirine bağlandığı topolojidir. Kendi içinde ikiye ayrılır:

    - **Full-Mesh (Tam Örgü):** Her cihazın ağdaki *diğer tüm cihazlara* doğrudan bağlı olduğu yapıdır. Yüksek yedeklilik sağlar ancak maliyeti çok yüksektir. **Partial-Mesh (Kısmi Örgü):** Sadece kritik cihazların birbirine birden fazla bağlantıyla bağlandığı, daha uygun maliyetli bir çözümdür.
- **Özellikleri:** Bir bağlantı kopsa bile veri alternatif bir yoldan hedefine ulaşır. Yüksek erişilebilirlik (High Availability) istenen WAN bağlantılarında tercih edilir.

Spine-Leaf (Modern Veri Merkezi Topolojisi)

- **Yapısı:** Geleneksel 3 katmanlı (Core, Distribution, Access) ağ yapısının yerini alan, modern veri merkezlerinde (örneğin Cisco ACI donanımlarında) kullanılan 2 katmanlı bir topolojidir.
- **Özellikleri:** * **Spine (Omurga) Switch'ler:** Ağın merkezindedir. Tüm Leaf switch'ler her bir Spine switch'e doğrudan bağlanır. Spine switch'ler asla birbirine bağlanmaz.
    - **Leaf (Yaprak) Switch'ler:** Uç cihazların (Sunucular vb.) bağlandığı switch'lerdir. Leaf switch'ler de asla birbirine bağlanmaz.
- **Avantajı:** Herhangi iki sunucu arasındaki veri iletimi her zaman tam olarak aynı sayıda sekme (hop) üzerinden gerçekleşir. Bu da gecikmeyi (latency) tahmin edilebilir ve çok düşük kılar.

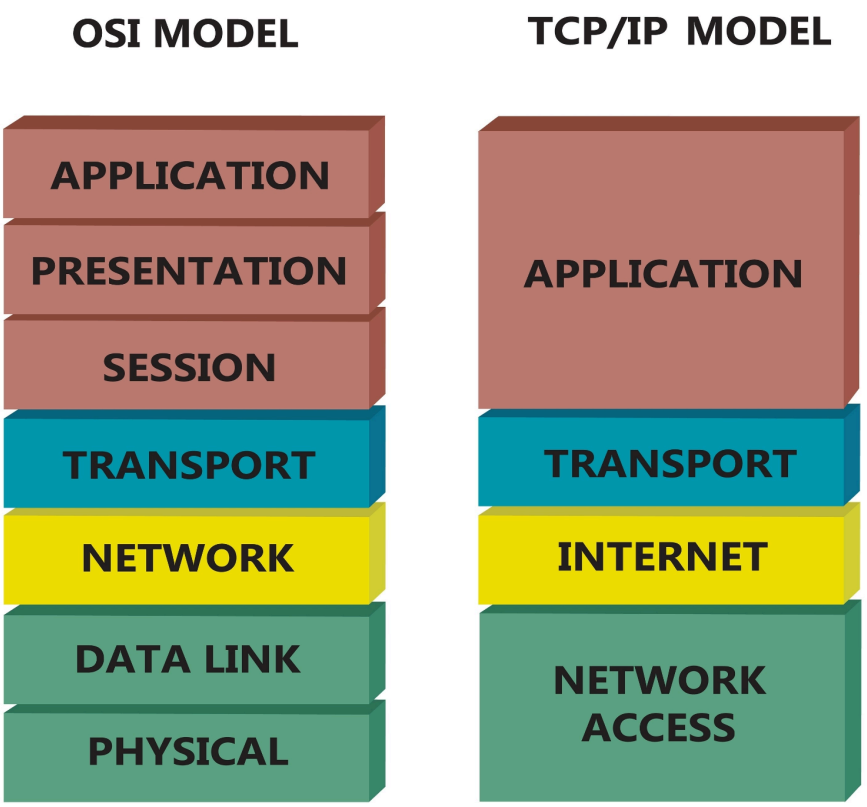
2. Mantıksal Topoloji (Logical Topology)

Fiziksel bağlantıların nasıl göründüğünden bağımsız olarak, **verinin ağ üzerinde hedef cihaza ulaşırken izlediği yolu** ve IP adresleme şemasını ifade eder. Ağın akış kurallarını gösterir.

- Bir ağ fiziksel olarak Yıldız (Star) topolojisinde kurulmuş olabilir (herkes merkezdeki bir Hub'a bağlıdır), ancak Hub gelen veriyi tüm portlara kopyalayarak gönderdiği için (Broadcast) **mantıksal olarak Bus topolojisi** gibi davranır.
- Modern ağlarda, merkezde Switch kullanıldığı için (MAC adresine göre hedefe doğrudan iletim), ağ hem fiziksel hem de mantıksal olarak Yıldız topolojisindedir.
- Mantıksal topoloji şemalarında genellikle cihazların fiziksel odaları veya kablo türleri değil; subnetler (alt ağlar), IP adresleri ve yönlendirme (routing) protokollerinin sınırları gösterilir.

OSI Referans Modeli ve TCP/IP Modeli

Ağ standartları, farklı üreticilerin (Cisco, Juniper, Microsoft vb.) ürettiği cihazların ve yazılımların birbirleriyle uyumsuzluk yaşamadan ortak bir dilde haberleşebilmesi için ortaya çıkmıştır. Bu katmanlı mimarinin en büyük avantajı, bir katmandaki gelişmenin diğer katmanları etkilememesidir (Örneğin; fiziksel olarak fiber kablo kullanmaya başladığınızda, bilgisayarınızdaki web tarayıcısını değiştirmek zorunda kalmazsınız).



1. OSI Referans Modeli (Open Systems Interconnection)

ISO tarafından geliştirilen 7 katmanlı, teorik bir referans modelidir. Ağ trafiği akarken birebir bu 7 adım sayılmaz ancak ağ mühendisleri için harika bir sorun giderme (troubleshooting) haritasıdır.

- **Katman 7 - Application (Uygulama Katmanı):** Kullanıcının ve ağ uygulamalarının ağ servislerine eriştiği noktadır. HTTP, HTTPS, SMTP, DNS, DHCP, FTP gibi protokoller burada çalışır. (Örneğin; ASP.NET Core ile geliştirdiğin "Jinx" gibi bir N-tier backend projesinin dış dünyaya veri sunduğu API uç noktaları bu katmanda iletişim kurar.)
- **Katman 6 - Presentation (Sunum Katmanı):** Verinin ağ üzerinden gönderilmeden önce karşı tarafın anlayacağı ortak bir formata çevrildiği, şifrelendiği (Encryption - örn. SSL/TLS) ve sıkıştırıldığı katmandır.
- **Katman 5 - Session (Oturum Katmanı):** İki cihaz arasındaki iletişimi (oturumu) başlatır, yönetir, senkronize eder ve sonlandırır.

- **Katman 4 - Transport (Taşıma Katmanı):** Verinin uçtan uca nasıl iletileceğinden sorumludur. Üst katmandan gelen veriyi **Segmentlere** böler. Hangi uygulamanın hangi veriyi alacağını belirleyen Port Numaraları (Source/Destination Port) burada eklenir.
- **Katman 3 - Network (Ağ Katmanı):** Verinin kaynaktan hedefe ulaşması için en iyi yolun (Best Path) seçilmesinden (Routing) ve mantıksal adreslemeden (**IP Adresleri**) sorumludur. IPv4, IPv6 ve ICMP protokolleri burada çalışır. Router (Yönlendirici) cihazları 3. katman cihazlarıdır.
- **Katman 2 - Data Link (Veri Bağlantı Katmanı):** Ağ katmanından gelen paketleri fiziksel ortama aktarılmak üzere çerçeveler (Frame). Yerel ağdaki iletişimi sağlayan fiziksel adresleme (**MAC Adresi**) burada yapılır. Veri bütünlüğünü kontrol etmek için çerçeveye bir hata kontrol mekanizması (FCS) ekler. Switch'ler bu katmanda çalışır.
- **Katman 1 - Physical (Fiziksel Katman):** Verinin kablo (Bakır, Fiber) veya hava (Wireless) üzerinden elektrik sinyalleri, ışık veya radyo dalgaları halinde **Bit**'lere (0 ve 1) dönüştürülerek iletildiği en alt katmandır. Hub'lar ve kablolar bu katmandadır.

2. TCP/IP Modeli

OSI modelinin teorik yapısına karşın, günümüz internetinin temelini oluşturan, daha pratik ve gerçek dünyada yaygın olarak kullanılan protokoldür. 4 temel katmandan oluşur.

TCP/IP Katmanı	Eşleştiği OSI Katmanları	Görevi ve Özellikleri
4. Application (Uygulama)	Application, Presentation, Session (7, 6, 5)	Uygulamalara ağ erişimi sağlar, veriyi formatlar ve oturumları yönetir.
3. Transport (Taşıma)	Transport (4)	TCP (Güvenilir, bağlantı odaklı) ve UDP (Hızlı, bağlantısız, CS2 gibi rekabetçi oyunlarda veya canlı yayınlarda tercih edilen) protokolleri ile veriyi taşır.

2. Internet (İnternet)	Network (3)	Mantıksal IP adreslemesini ve paketlerin ağlar arası yönlendirilmesini (Routing) yapar.
1. Network Access (Ağ Erişimi)	Data Link, Physical (2, 1)	MAC adreslemesini gerçekleştirir ve veriyi fiziksel ortama (kablo/sinyal) aktarır.

3. Veri Kapsüllemesi (Data Encapsulation) ve PDU'lar

Verinin kaynaktan çıkıp kabloya ulaşana kadar her katmanda üzerine bir başlık (Header) eklenerek paketlenmesi işlemine **Kapsülleme (Encapsulation)** denir. Hedef cihaza ulaştığında ise bu başlıklar alttan üste doğru sırayla okunup sökülür, buna da **Açma (Decapsulation)** denir.

Her katmanda oluşan bu yeni veri paketinin kendine has bir adı vardır. Buna **PDU (Protocol Data Unit - Protokol Veri Birimi)** denir.

Kapsülleme süreci yukarıdan aşağıya şu şekilde gerçekleşir:

1. **Application, Presentation, Session (Katman 7, 6, 5):** Bu üç katmanda üretilen ham bilginin genel PDU adı **Data (Veri)**'dır.
2. **Transport (Katman 4):** Data'ya kaynak ve hedef Port numaralarını içeren bir Taşıma Başlığı eklenir. PDU'nun yeni adı **Segment**'tir.
3. **Network (Katman 3):** Segment'e kaynak ve hedef IP adreslerini içeren bir IP Başlığı eklenir. PDU'nun yeni adı **Packet (Paket)**'tir.
4. **Data Link (Katman 2):** Paket'e kaynak ve hedef MAC adreslerini içeren bir Çerçeve Başlığı (Header) ve verinin yolda bozulup bozulmadığını kontrol etmek için bir Artbilgi (FCS - Frame Check Sequence) eklenir. PDU'nun yeni adı **Frame (Çerçeve)**'dir.
5. **Physical (Katman 1):** Frame yapısı fiziksel ortama aktarılmak üzere elektrik, ışık veya radyo sinyallerine, yani **Bit**'lere (0 ve 1) dönüştürülür ve kabloya bırakılır.

Ağ Cihazları, İletişim Türleri ve Fiziksel Medya

Bir ağı tasarlarken kullanılacak cihazların kapasiteleri ve bu cihazları birbirine bağlayacak kablolama altyapısı ağın performansını doğrudan belirler.

1. Temel Ağ Türleri (Network Types)

Ağlar, kapsadıkları coğrafi alanın büyüklüğüne ve kullanım amaçlarına göre farklı isimler alırlar:

- **PAN (Personal Area Network):** Kişisel cihazların (telefon, tablet, akıllı saat, kablosuz kulaklık) birbirine bağlandığı en küçük ağ türüdür. Genellikle Bluetooth veya NFC teknolojileri kullanılır. Kapsama alanı birkaç metredir.
- **LAN (Local Area Network - Yerel Alan Ağları):** Ev, okul, laboratuvar veya tek bir ofis binası gibi sınırlı bir coğrafi alandaki cihazları birbirine bağlar. Yüksek veri transfer hızı sunar ve yönetimi genellikle tek bir kurumun elindedir.
- **WLAN (Wireless Local Area Network):** LAN'ın kablosuz versiyonudur. Cihazlar bir Access Point (Erişim Noktası) üzerinden Wi-Fi teknolojisiyle ağa bağlanır.
- **CAN (Campus Area Network):** Bir üniversite kampüsü veya büyük bir askeri üs gibi, birbirine yakın birden fazla LAN'ın birleşmesiyle oluşur. LAN'dan büyük, MAN'dan küçüktür.
- **MAN (Metropolitan Area Network):** Bir şehri veya büyük bir yerleşim merkezini kapsayan ağ türüdür. Şehirdeki üniversiteleri, devlet dairelerini veya banka şubelerini birbirine bağlamak için kullanılır (Örneğin; Metro Ethernet yapıları).
- **WAN (Wide Area Network - Geniş Alan Ağları):** Birbirinden çok uzakta olan (şehirler arası, ülkeler arası veya kıtalar arası) LAN'ları birbirine bağlar. İnternet dünyadaki en büyük WAN örneğidir. Genellikle servis sağlayıcıların (ISP) altyapısı kullanılır.
- **SAN (Storage Area Network - Depolama Alanı Ağları):** Sunucuların, büyük depolama ünitelerine (Storage) çok yüksek hızda erişmesini sağlayan özel, yüksek performanslı bir ağ türüdür. Genellikle veri merkezlerinde (Data Center) bulunur.
- **SOHO (Small Office / Home Office):** Küçük ofislerde veya evlerde kullanılan, genellikle hepsi bir arada (all-in-one) bir modem/router üzerinden dış dünyaya bağlanan basit ağ yapılarıdır.

2. Ağ Üzerindeki İletişim Çeşitleri

- **Unicast (Bire Bir):** Bir kaynaktan çıkan mesajın ağdaki *sadece belirli tek bir cihaza* gitmesidir (Örn: Bir web sitesine bağlanmak).
- **Broadcast (Bire Tüm):** Bir kaynaktan çıkan mesajın ağdaki *her cihaza* gönderilmesidir (Örn: ARP istekleri veya DHCP keşif paketleri).
- **Multicast (Bire Çok):** Bir kaynaktan çıkan mesajın ağdaki *belirli bir grup cihaza* iletilmesidir (Örn: OSPF yönlendirme protokolü güncellemeleri veya IPTV yayınları).

3. Hub ve Switch Karşılaştırması

Özellik	Hub (Dağıtıcı)	Switch (Anahtar)
Çalıştığı Katman	Katman 1 (Fiziksel)	Katman 2 (Veri Bağlantı)
Veri İletimi	Gelen veriyi (sinyali) aldığı port hariç tüm portlara kopyalar (Broadcast mantığı).	Çerçeveyi (Frame) okur ve sadece hedef MAC adresine sahip porttan dışarı yollar.
İletişim Modu	**Half-Duplex:** Aynı anda ya veri gönderir ya veri alır. İkisi aynı anda olursa çakışma (Collision) olur.	**Full-Duplex:** Aynı anda hem veri gönderip hem alabilir. Çakışma olmaz.
Bölünme (Domain)	Tüm portlar tek bir Collision Domain (Çakışma Alanı) içindedir.	**Her bir port ayrı bir Collision Domain'dir.**

Switch MAC Adreslerini Nasıl Öğrenir?

Switch, ağdaki cihazların hangi portta olduğunu **MAC Adres Tablosu (CAM Table)** aracılığıyla bilir. Öğrenme süreci şu şekildedir:

1. Switch bir porttan veri (Frame) aldığında, çerçevenin içindeki **Kaynak MAC (Source MAC)** adresine bakar.
2. Bu MAC adresini ve verinin geldiği port numarasını MAC tablosuna kaydeder.
3. Hedef MAC adresini bulmak için tabloya bakar. Eğer hedef MAC tabloda yoksa (Bilinmeyen Unicast), veriyi geldiği port hariç tüm portlara yollar (Flooding).
4. Hedef cihaz cevap verdiğinde, onun da Kaynak MAC adresini öğrenir ve tabloyu günceller. *(Not: Bu tabloyu görüntülemek için* `show mac address-table` *komutu kullanılır.)*

PoE (Power over Ethernet)

IP kameralar, VoIP telefonlar veya Access Point'ler gibi ağ cihazlarının, çalışmak için ihtiyaç duydukları elektrik gücünü harici bir adaptöre gerek kalmadan doğrudan Ethernet kablosu üzerinden (Switch'in portundan) alabilmesi teknolojisidir.

4. Ethernet LAN Bağlantı Medyaları (Kablolama)

Bakır Kablolar

Veriyi elektrik sinyalleri halinde taşırlar. 100 metrelik mesafe sınırları vardır.

- **Koaksiyel Kablo (Coaxial):** Günümüzde ağlardan ziyade kablo TV ve eski internet hizmetlerinde (DOCSIS) kullanılır.
- **Bükümlü Çift (Twisted Pair):** İçinde 8 adet ince kablo (4 çift) bulunur. Çiftlerin birbirine bükülü olması, elektromanyetik parazitleri (EMI/RFI) engeller. Hız kapasitelerine göre Cat5e, Cat6, Cat6a gibi sınıflara ayrılır.
    - **UTP (Unshielded Twisted Pair):** Korumasızdır, en yaygın ve ucuz olandır.
    - **STP (Shielded Twisted Pair):** Kablo çiftlerinin etrafında metalik bir koruma kalkanı vardır, endüstriyel ve parazitin bol olduğu ortamlarda kullanılır.

Kablo Sonlandırma ve Çapraz/Düz Mantığı: Kabloların uçlarına RJ-45 konnektörleri çakılırken T568A veya T568B standartları kullanılır.

- **Düz Kablo (Straight-through):** Kablonun iki ucu da aynı standartta (Örn: İki ucu da T568B) çakılır. *Farklı* türdeki cihazları bağlamak için kullanılır (Örn: PC - Switch, Switch - Router).
- **Çapraz Kablo (Crossover):** Bir ucu T568A, diğer ucu T568B çakılır. *Aynı* türdeki cihazları birbirine bağlamak için kullanılır (Örn: Switch - Switch, PC - PC, PC - Router).
- *Güncel CCNA Notu:* Modern Cisco Switch ve Router'larda bulunan **Auto-MDIX** özelliği sayesinde cihazlar takılan kablonun türünü otomatik algılar ve pinleri ona göre elektronik olarak değiştirir. Bu sayede günümüzde neredeyse her yerde sadece Düz kablo kullanmak yeterlidir.

Fiber Optik Kablolar

Veriyi elektrik sinyali yerine ışık (lazer veya LED) ile iletirler. Elektromanyetik parazitlerden kesinlikle etkilenmezler ve kilometrelerce uzağa veri taşıyabilirler.

- **Single-Mode Fiber (SMF - Tek Modlu):** Işık kaynağı olarak lazer kullanır. Çekirdek çapı çok incedir (9 mikron). Işık tek bir yol izler. Uzun mesafe WAN bağlantılarında kullanılır.
- **Multi-Mode Fiber (MMF - Çok Modlu):** Işık kaynağı olarak LED kullanır. Çekirdek çapı daha kalındır (50-62.5 mikron). Işık çekirdek içinde yansıyarak birden fazla yol izler. Genellikle bir kampüs içi veya bina içi (1-2 km) bağlantılarda kullanılır.
- **Yaygın Fiber Konnektörleri:** ST (Tak-çevir), SC (Kare yapılı tak-çıkar), LC (Küçük boyutlu, günümüzde en çok tercih edilen çiftli konnektör).

5. MAC Adresi (Media Access Control)

Fiziksel adrestir. Katman 2'de (Data Link) çalışır ve cihazın ağ kartına (NIC) üretim aşamasında kalıcı olarak yazılır.

- 48 bit (6 Byte) uzunluğundadır ve Hexadecimal (On altılık) sayı sistemiyle ifade edilir.
- İlk 24 biti (OUI - Organizationally Unique Identifier) üretici firmayı temsil eder (Cisco, Apple, Intel vb.). Kalan 24 biti cihaza özel benzersiz numaradır.

IP Adresleme, Subnetting ve IPv6 Temelleri

İnternet Protokolü (IP), cihazların ağ üzerinde birbirlerini bulmasını ve veri paketlerinin kaynaktan hedefe doğru yönlendirilmesini sağlayan 3. Katman (Network Layer) protokolüdür.

- **Bağlantısızdır (Connectionless):** Hedef cihazla önceden bir oturum kurmaz.
- **Best Effort (En İyi Çaba):** Paketlerin hedefe ulaşacağını veya sırayla ulaşacağını garanti etmez (Bu görevi 4. katmandaki TCP üstlenir).

1. IPv4 Temelleri ve Sınıfları

IPv4 adresleri **32 bit** uzunluğundadır ve 8 bitlik 4 oktete (bölüme) ayrılır. İki ana kısımdan oluşur: **Network (Ağ)** bölümü ve **Host (Cihaz)** bölümü. Bu ayrımı belirleyen şey **Alt Ağ Maskesi'dir (Subnet Mask)**.

Sınıf	İlk Oktet Bitleri	Adres Aralığı	Varsayılan Maske (CIDR)	Kullanım Alanı
A	0.....	1.0.0.0 - 126.255.255.255	255.0.0.0 (/8)	Çok büyük ağlar (Milyonlarca host)
B	10.....	128.0.0.0 - 191.255.255.255	255.255.0.0 (/16)	Orta ve büyük ölçekli kurumlar

C	110.....	192.0.0.0 - 223.255.255.255	255.255.255.0 (/24)	Küçük ağlar (LAN, SOHO)
D	1110....	224.0.0.0 - 239.255.255.255	Yok	**Multicast** (Çoklu yayın, OSPF vb.)
E	1111....	240.0.0.0 - 255.255.255.255	Yok	Araştırma ve askeri amaçlı (Rezerve)

Özel Durumlar:

- `127.0.0.0/8` ağı **Loopback (Geri Döngü)** adresidir. Cihazın kendi TCP/IP yığınını test etmesi için kullanılır (Örn: `ping 127.0.0.1`).
- `169.254.X.X` ağı **APIPA** adresidir. Bir cihaz DHCP'den IP alamazsa kendi kendine bu aralıktan geçici bir IP atar.

2. Genel (Public) ve Özel (Private) IP Adresleri

IPv4 adreslerinin tükenmesini önlemek için belirli IP blokları yerel ağlarda kullanılmak üzere ayrılmıştır. Bu **Özel IP'ler internete doğrudan çıkamaz**, yönlendirici (Router) üzerinde **NAT (Network Address Translation)** işlemi ile Public IP'ye çevrilmeleri gerekir.

- **A Sınıfı Özel:** 10.0.0.0 - 10.255.255.255
- **B Sınıfı Özel:** 172.16.0.0 - 172.31.255.255
- **C Sınıfı Özel:** 192.168.0.0 - 192.168.255.255

3. Alt Ağlara Bölme (Subnetting)

Tek bir büyük ağı, daha küçük ve yönetilebilir alt ağlara bölme işlemidir.

Neden Subnetting Yaparız?

1. **Broadcast Trafiğini Azaltmak:** Büyük ağlarda broadcast (bire-tüm) mesajları performansı düşürür. Ağları bölerek çakışma ve gürültüyü sınırlarız.
2. **Güvenlik:** Departmanları (Muhasebe, IT, Misafir) farklı IP bloklarına alarak aralarına yönlendirici (Router) ve kural (ACL) koyabiliriz.
3. **IP İsrafını Önlemek:** 2 bilgisayarlık bir WAN bağlantısı için /24 (254 host) yerine /30 (2 host) kullanarak adresleri verimli kullanırız.

Subnetting Formülleri ve Hesaplama

Network bitlerinden (Subnet maskesindeki 1'ler) ödünç alınarak host bitleri (0'lar) daraltılır.

- **Oluşacak Alt Ağ (Subnet) Sayısı:** 2^n (*n = Ödünç alınan network bit sayısı*)
- **Bir Alt Ağdaki Kullanılabilir Host Sayısı:** 2^h - 2 (*h = Kalan sıfırların sayısı*). *Not: -2'nin sebebi, ilk IP'nin "Network Adresi", son IP'nin ise "Broadcast Adresi" olması ve cihazlara atanamamasıdır.*
- **Blok Boyutu (Atlama Değeri):** 256 - İlgili oktetteki alt ağ maskesi değeri

Örnek: 192.168.1.0/24 ağını 4 farklı departmana bölmek istiyoruz.

- /24'ten 2 bit ödünç alırsak /26 olur. Subnet maskesi: 255.255.255.192
- Ağ Sayısı: 2^2 = 4 adet yeni ağ oluşur.
- Host Sayısı: Kalan 6 bit için 2^6 - 2 = 62 adet cihaz bağlanabilir.
- Blok Boyutu: 256 - 192 = 64 (Ağlar 64'er 64'er artacak).

Oluşan Ağlar:

1. Ağ: 192.168.1.0 (Ağ adresi) - 192.168.1.63 (Broadcast) | Kullanılabilir: 1-62
2. Ağ: 192.168.1.64 (Ağ adresi) - 192.168.1.127 (Broadcast) | Kullanılabilir: 65-126
3. Ağ: 192.168.1.128 (Ağ adresi) - 192.168.1.191 (Broadcast) | Kullanılabilir: 129-190
4. Ağ: 192.168.1.192 (Ağ adresi) - 192.168.1.255 (Broadcast) | Kullanılabilir: 193-254

4. IPv6 Temelleri

IPv4 adreslerinin dünya çapında tükenmesi üzerine geliştirilen yeni nesil adresleme yapısıdır.

- **128 bit** uzunluğundadır (IPv4 32 bitti).
- Milyarlarca cihaza benzersiz IP verilebilir. **NAT kullanılmasına gerek kalmaz.**
- Güvenlik (IPsec) protokolün içine gömülüdür.
- Rakamlar ve harflerden oluşan **Hexadecimal (On altılık)** sistemle yazılır (Örn: 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

IPv6 Kısaltma Kuralları

1. Her bloktaki (hextet) **öndeki sıfırlar** atılabilir (0db8 -> db8 / 0000 -> 0).
2. Sadece bir defaya mahsus olmak üzere, art arda gelen tamamen sıfır blokları **Çift İki Nokta (::)** ile kısaltılabilir.
   (Yukarıdaki adresin kısaltılmış hali: 2001:db8:85a3::8a2e:370:7334)

IPv6 İletişim Türleri

IPv6'da Broadcast (Bire-Tüm) **yoktur**. Bunun yerine gelişmiş Multicast kullanılır.

- **Global Unicast Adres (GUA):** İnternete çıkabilen, benzersiz public adreslerdir. Genellikle 2000::/3 ile başlar.
- **Link-Local Adres:** Sadece o yerel ağda (kablo üzerinde) geçerli olan adreslerdir. İnternete çıkmaz. Yönlendiriciler (Router) OSPFv3 veya komşuluk kurarken bu IP'leri kullanır. Her IPv6 aktif cihazda otomatik oluşur. FE80::/10 ile başlar.

- **Unique Local Adres:** IPv4'teki Private (Özel) IP'lerin karşılığıdır. Dışarı çıkamaz. FC00::/7 veya FD00::/8 ile başlar.
- **Multicast Adres:** Belirli bir gruba yayın yapmak için kullanılır. FF00::/8 ile başlar.

5. Subnetting Pratik Çözümleri ve Örnek Sorular

Sınavlarda ve gerçek hayatta subnetting genellikle üç farklı senaryo üzerinden karşımıza çıkar: Bir IP'nin hangi ağa ait olduğunu bulma, belirli bir host sayısına göre ağı bölme veya belirli bir şube/alt ağ sayısına göre ağı bölme.

Soru 1: Ağ (Network) ve Yayın (Broadcast) Adresini Bulma

Senaryo: Ağdaki bir bilgisayarın IP adresi 192.168.5.100/27 olarak yapılandırılmıştır. Bu bilgisayarın bulunduğu alt ağın ağ adresini, broadcast adresini ve bu ağdaki kullanılabilir IP aralığını bulunuz.

Çözüm Adımları:

1. **Subnet Maskesini Bulma:** /27 demek, 27 tane 1 biti demektir. Bu da 255.255.255.224 yapar.
2. **Blok Boyutunu (Atlama Değerini) Hesaplama:** Sihirli sayımız 256'dır. Son oktetteki değeri 256'dan çıkarırız: 256 - 224 = 32. Alt ağlar 32'şer 32'şer artacaktır.
3. **Ağları Listeleme:** 192.168.5.0, 192.168.5.32, 192.168.5.64, 192.168.5.96, 192.168.5.128...
4. **Sonuç:** Bize verilen .100 IP'si, .96 ile .127 arasındadır.
    - **Ağ Adresi:** 192.168.5.96
    - **Broadcast Adresi (Bir sonraki ağdan bir eksik):** 192.168.5.127
    - **Kullanılabilir IP Aralığı:** 192.168.5.97 - 192.168.5.126

Soru 2: İhtiyaç Duyulan Host (Cihaz) Sayısına Göre Bölme

Senaryo: Şirketinizin yeni açılan bir departmanında 120 adet bilgisayar, yazıcı ve IP telefon bulunacaktır. Elinizde 192.168.10.0/24 ana IP bloğu var. Bu departmana IP israfı yapmadan atanabilecek en uygun Prefix (/) değeri ve Subnet Maskesi nedir?

Çözüm Adımları:

1. **Host Formülünü Kullanma:** İhtiyacımız 120 host. Formülümüz: 2^h - 2 >= İhtiyaç
2. **"h" (Sıfır) Değerini Bulma:** 2^7 = 128. (128 - 2 = 126 kullanılabilir IP). Demek ki host kısmı için 7 adet 0 bitine ihtiyacımız var.
3. **Prefix'i Bulma:** Toplam 32 bitimiz var. 32 - 7 = 25. Yeni Prefix değerimiz **/25** olmalıdır.
4. **Sonuç:** /25'in Subnet Mask karşılığı 255.255.255.128'dir. Ağı tam ortadan ikiye bölmüş olduk (0-127 ve 128-255).

Soru 3: İhtiyaç Duyulan Alt Ağ (Şube) Sayısına Göre Bölme

Senaryo: Elinizde B sınıfı 172.16.0.0/16 ağ bloğu bulunmaktadır. Şirketiniz hızla büyüyor ve bu ağı, her biri eşit kapasitede olacak şekilde **en az 50** farklı şubeye bölmeniz isteniyor. Yeni Prefix (/) değeri ne olmalıdır ve her şubeye kaç adet IP düşer?

Çözüm Adımları:

1. **Subnet Formülünü Kullanma:** İhtiyacımız 50 alt ağ. Formülümüz: 2^n >=İhtiyaç (n = ağ kısmına eklenecek, yani 1 yapılacak bit sayısı).
2. **"n" Değerini Bulma:** 2^5 = 32 (yetmez). 2^6 = 64 (50'yi karşılar). Ana maskemize 6 bit daha eklemeliyiz.
3. **Yeni Prefix'i Bulma:** Mevcut /16 idi. Üzerine 6 bit daha eklersek yeni Prefix **/22** olur.
4. **Host Sayısını Bulma:** 32 bitten 22 ağ bitini çıkarırsak geriye 10 host biti kalır. 2^10 - 2 = 1022.
5. **Sonuç:** Yeni yapılandırma /22 (Subnet maskesi: 255.255.252.0) olacaktır. Bu şekilde 64 adet şube ağı oluşturulabilir ve her şubede kullanılabilir 1022 adet IP adresi bulunur.

Anahtarlama Temelleri (Switching Basics)

Katman 2'de (Veri Bağlantı Katmanı) çalışan switchler (anahtarlar), yerel ağdaki (LAN) cihazların birbirleriyle haberleşmesini sağlayan en temel ağ cihazlarıdır. Gelen veri çerçevelerini (frames) içindeki MAC adreslerine bakarak sadece ilgili hedefe yönlendirirler.

1. Çakışma Alanı (Collision Domain) ve Yayın Alanı (Broadcast Domain)

Ağ tasarımında ve sorun gidermede bu iki kavramı bilmek hayati önem taşır.

- **Çakışma Alanı (Collision Domain):** Ağ üzerindeki iki cihazın aynı anda veri gönderdiğinde sinyallerinin çarpışma (çakışma) ihtimalinin olduğu fiziksel alandır.
    - Hub (Dağıtıcı) kullanılan bir ağda tüm portlar tek bir çakışma alanı içindedir.
    - **Switchlerin her bir portu ayrı bir çakışma alanıdır.** Switchler, doğaları gereği çakışmaları böler ve mikro bölümler (micro-segmentation) oluşturur.
- **Yayın Alanı (Broadcast Domain):** Bir cihazın ağa gönderdiği bir "Broadcast" (bire-tüm) mesajının (örneğin bir ARP isteği veya DHCP keşif paketi) ulaşabildiği sınırların tamamıdır.
    - Switchler broadcast mesajlarını bölemez; gelen bir broadcast mesajını aldığı port hariç diğer tüm portlara iletir (Flood).
    - **Broadcast alanını yalnızca Router (Yönlendirici) veya VLAN'lar (Sanal LAN) bölebilir.** Routerların her bir bacağı ayrı bir yayın alanıdır.

2. Switch MAC Adreslerini Nasıl Öğrenir? (MAC Learning)

Switchler ağdaki cihazların nerede olduğunu **MAC Adres Tablosu (CAM Table - Content Addressable Memory)** oluşturarak öğrenir. Tablo oluşturma işlemi daima paketi gönderen cihazın adresine bakılarak yapılır.

Öğrenme ve İletme Adımları:

1. **Öğrenme (Learning):** Switch bir portundan çerçeve aldığında, çerçevenin içindeki **Kaynak MAC (Source MAC)** adresini ve o çerçevenin geldiği port numarasını MAC tablosuna kaydeder (Bu kayıtlar genellikle 5 dakika boyunca tutulur).
2. **İletme veya Taşma (Forwarding / Flooding):** Daha sonra switch, çerçevenin içindeki **Hedef MAC (Destination MAC)** adresine bakar.
    - Eğer hedef MAC adresi tabloda **varsa**, çerçeveyi sadece o hedefin bulunduğu porta yönlendirir (Forwarding / Unicast iletişim).
    - Eğer hedef MAC adresi tabloda **yoksa** (Bilinmeyen Unicast) veya hedef MAC bir Broadcast adresi ise (`FF:FF:FF:FF:FF:FF`), çerçeveyi geldiği port hariç ağdaki tüm portlara gönderir (Flooding). Hedef cihaz cevap verdiğinde onun da kaynak MAC adresini öğrenir ve tabloyu günceller.

> **Komut Notu:** Switch üzerindeki MAC tablosunu görmek için ayrıcalıklı modda (Privileged EXEC) `show mac address-table` komutu kullanılır.

3. Duplex (Çift Yönlü İletişim) Modları

İki cihaz arasındaki veri iletiminin yönünü ve eşzamanlılığını belirler. Bağlanan cihazın portu hangi modda çalışıyorsa, switch otomatik olarak o moda geçer (Auto-negotiation).

- **Half-Duplex (Yarı Çift Yönlü):** Veri iletimi ve alımı aynı anda yapılamaz. Telsiz mantığıyla çalışır; biri konuşurken diğeri dinlemelidir. Çakışma (Collision) riski vardır (Hub'lar bu modda çalışır).
- **Full-Duplex (Tam Çift Yönlü):** Aynı anda hem veri gönderilip hem veri alınabilir. Telefon görüşmesi gibidir. Çakışma olmaz. Modern Switchler ve bilgisayarlar varsayılan olarak bu modda çalışır.

4. Çerçeve İletim Yöntemleri (Frame Forwarding Methods)

Bir switch, gelen veriyi diğer porta aktarırken arka planda iki ana yöntemden birini kullanır:

- **Store-and-Forward (Depola ve İlet):** Switch çerçevenin *tamamını* alır ve sonundaki Artbilgi (FCS) kısmına bakarak hata kontrolü yapar. Hata yoksa hedefe iletir. Güvenilirdir ancak çerçevenin boyutu büyüdükçe mikro saniyelik gecikmeler (latency) artar. Cisco switchlerin LAN ortamlarındaki varsayılan yöntemidir.

- **Cut-Through (Kestirme):** Switch sadece çerçevenin başındaki hedef MAC adresini okur okumaz (ilk 14 byte) veriyi hedefe iletmeye başlar. Hata kontrolü yapmaz. Çok hızlıdır ancak bozuk paketleri de ağa yayma riski barındırır.