# AĞ OLUŞTURMA NEDİR?

Hazırlayan - Kaynak

# İÇERİK



## Ağ (Network) Nedir?

En temel tanımıyla **Network**, birbirine bağlı nesneler bütünüdür. Bu bağlamda karmaşık teknik terimlere girmeden önce mantığı kavramak gerekir.

- **Sosyal Örnek:** Arkadaş çevresi bir ağdır. İnsanlar ortak ilgi alanları, hobiler veya yetenekler nedeniyle birbirine bağlıdır.

Bu bağlantı mantığı hayatın her alanında karşımıza çıkar:

- **Toplu Taşıma Sistemi:** Şehirdeki noktaların birbirine bağlanması.
- **Altyapı (Infrastructure):** Ulusal elektrik şebekesinin evlere dağılması.
- **Posta Sistemi:** Mektup ve paketlerin gönderici ile alıcı arasında taşınması (Bu aslında veri paketlerinin iletim mantığına çok benzer).
- **Sosyal Etkileşim:** Komşularla selamlaşmak bile bir ağ iletişimidir.

### 2. Bilişim Dünyasında Ağ (Computing Networking)

Fiziksel dünyadaki "bağlantı" fikrinin, teknolojik cihazlara uygulanmış halidir.

- **Amaç:** Erişim sağlamak. Örneğin, bir akıllı telefonu kullanma sebebimiz, onun üzerinden farklı servislere veya verilere erişebilmektir.
- **İletişim Kuralları:** Cihazların birbirleriyle nasıl konuştuğu ve hangi kuralları (Protokoller) izlediği ağ yönetiminin ana konusudur.

#### Ağın Ölçeği ve Kapsamı

Bilişimde bir ağın boyutu çok değişkendir:

- **Minimum:** 2 cihazın birbirine bağlanmasıyla oluşabilir.
- **Maksimum:** Milyarlarca cihazı kapsayabilir (İnternet).

**Cihaz Çeşitliliği (Önemli):** Ağ sadece laptop veya telefonlardan ibaret değildir. Modern dünyada ağa bağlı cihazlar şunları içerir:

- Güvenlik kameraları (CCTV).
- Trafik ışıkları.
- Tarım teknolojileri (Farming equipment).
- Ev aletleri (IoT - Internet of Things - Nesnelerin İnterneti).

> **Not:** Bir siber güvenlikçi için bu çeşitlilik, "saldırı yüzeyinin" (Attack Surface) ne kadar geniş olduğunu gösterir. Bir trafik ışığı bile ağa bağlıysa, potansiyel bir hedef veya giriş noktası olabilir.

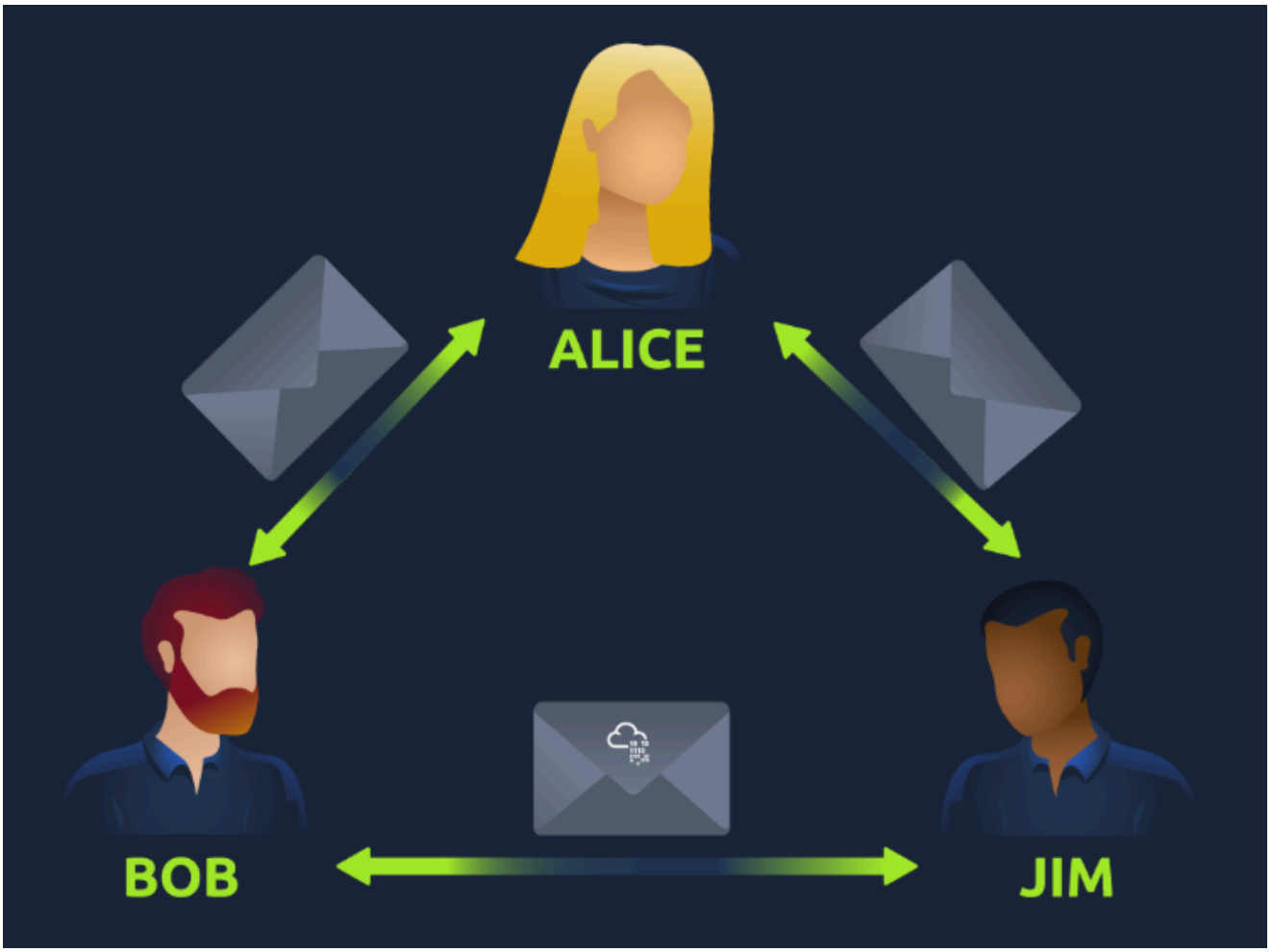
## 3. Siber Güvenlikte Ağ Bilgisinin Önemi

Ağlar modern yaşamın içine tamamen entegre olmuş durumdadır. Hava durumu verisinin toplanmasından, evlere elektriğin dağıtılmasına veya trafikte geçiş üstünlüğünün belirlenmesine kadar her şey ağlar üzerinden yönetilir.

- **Neden Önemli?** Ağlar hayatın bu kadar merkezindeyken, **Networking** (Ağ İletişimi) kavramını anlamak, siber güvenliğin en temel yetkinliğidir.
- Sistemin nasıl çalıştığını (verinin nasıl aktığını) bilmeden, onu koruyamaz veya zafiyetlerini (vulnerabilities) tespit edemeyiz.

## 4. Örnek Topoloji: Alice, Bob ve Jim

*(Diyagram referansı)* Senaryoda Alice, Bob ve Jim kendi aralarında bir ağ oluşturmuşlardır. Bu basit yapı, cihazların birbirini tanıması ve iletişim kurması (Identification ve Communication) prensibini temsil eder. Modülün ilerleyen kısımlarında bu cihazların birbirini nasıl bulduğu ve veri alışverişi yaptığı detaylandırılacaktır.



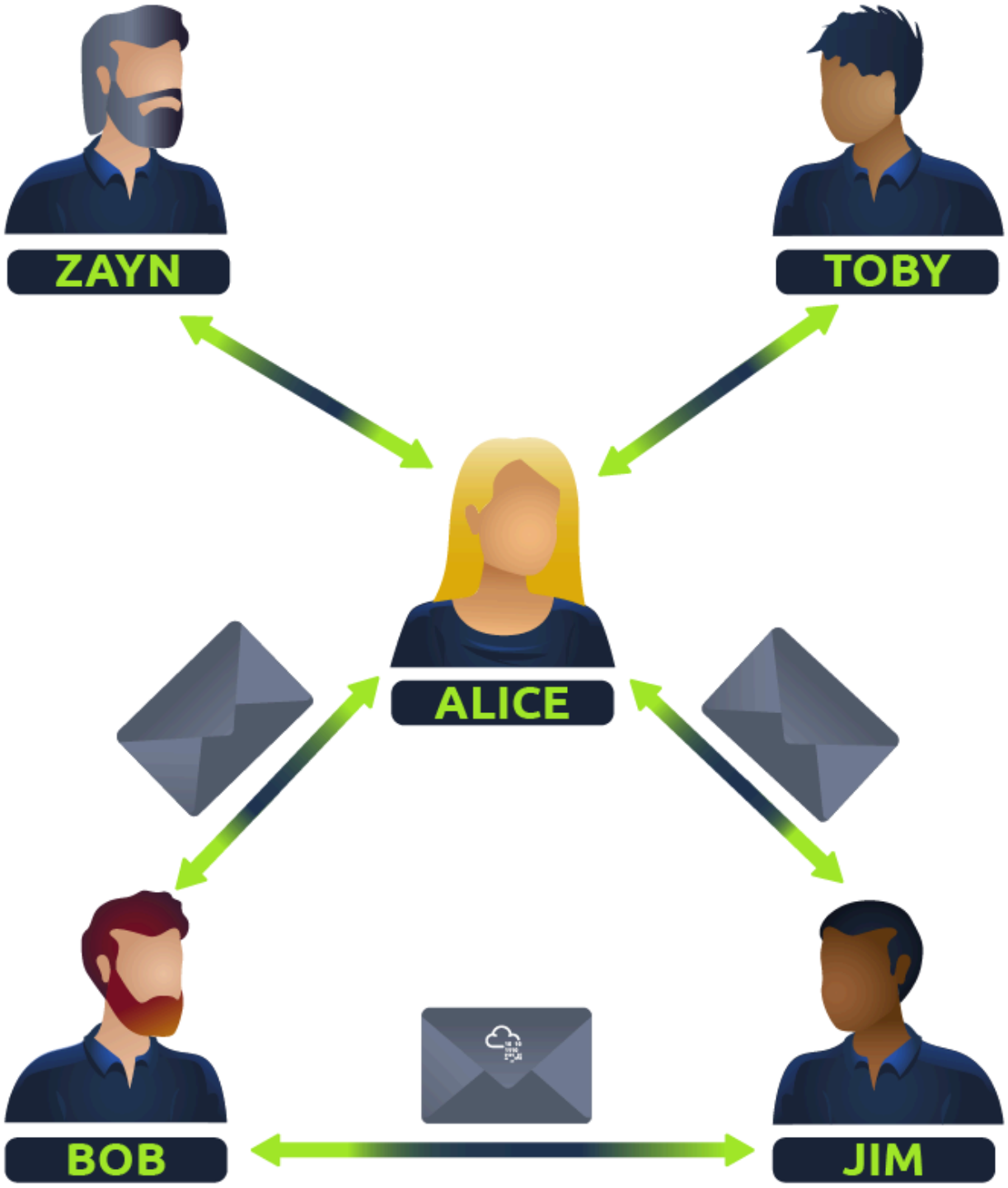

# İnternet Nedir?

İnternet, teknik olarak tek bir devasa ağ değil, **kendi içinde sayısız küçük ağı barındıran dev bir ağlar bütünüdür (Network of Networks)**.

## Alice Analojisi (Yönlendirme/Routing Mantığı)

Metindeki örnek üzerinden ağların nasıl birleştiğini anlamak kritik:

- **Durum:** Alice'in Bob ve Jim ile bir ağı var.
- **Yeni Gelişme:** Alice, Zayn ve Toby adında yeni arkadaşlar ediniyor.
- **Sorun:** Zayn ve Toby'nin dilini sadece Alice biliyor; Bob ve Jim bilmiyor.
- **Çözüm:** Alice, bu iki grup arasında **mesaj taşıyıcı (messenger)** görevi görüyor.




> **Teknik Yorum:** Bu senaryoda Alice, teknik dünyadaki **Router (Yönlendirici)** veya **Gateway (Ağ Geçidi)** rolünü üstlenmektedir. İki farklı ağ (Bob/Jim ağı ile Zayn/Toby ağı) birbiriyle doğrudan konuşamazken, her iki tarafı da tanıyan bir "aracı" (Alice) sayesinde iletişim kurabilirler. Bu birleşim yeni ve daha büyük bir ağı oluşturur.

## 2. İnternetin Kısa Tarihi

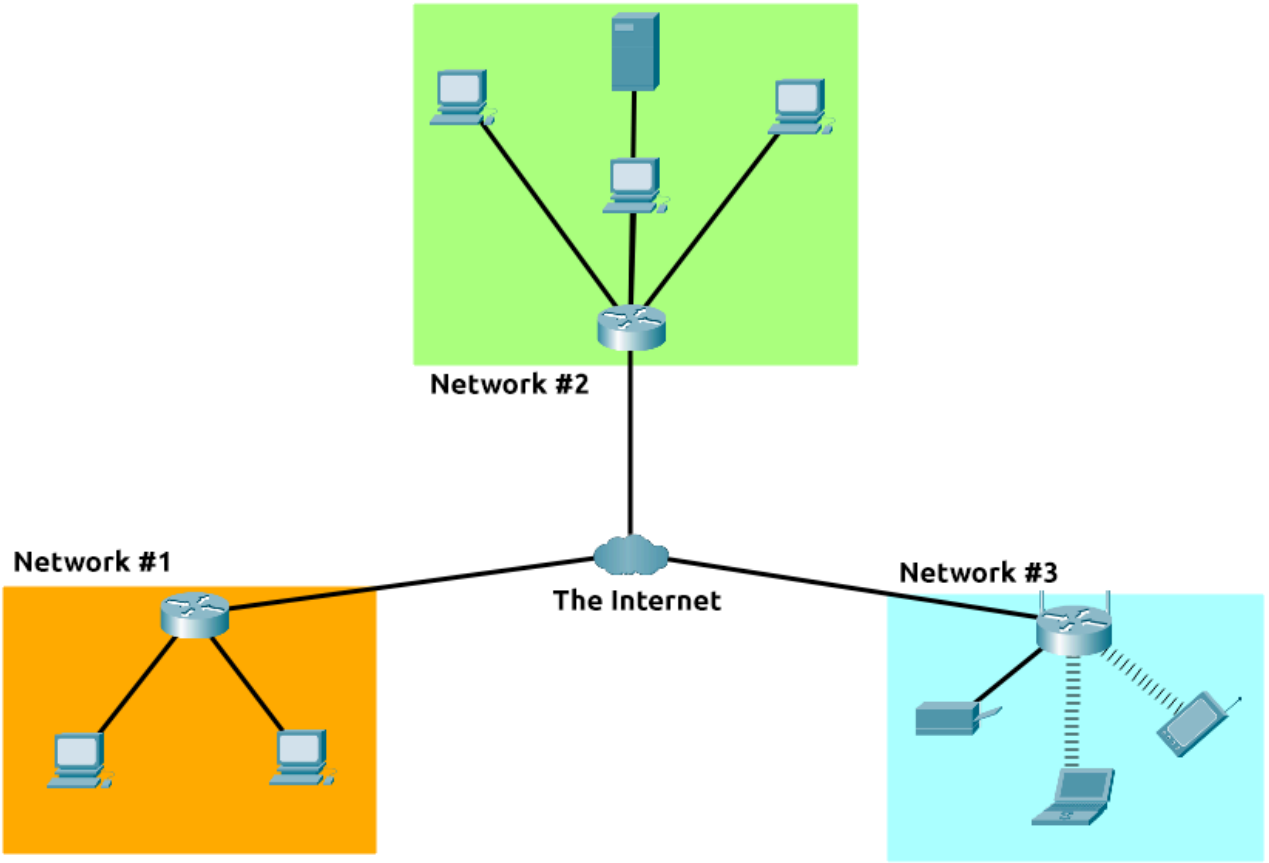
İnternetin evrimi iki ana aşamada incelenir:

1. **ARPANET (1960'ların sonu):**
   - Amerika Birleşik Devletleri Savunma Bakanlığı (US Defence Department) tarafından finanse edilmiştir.
   - Çalışır haldeki **ilk belgelenmiş ağdır**.

- İnternetin altyapısal atasıdır.

2. **World Wide Web - WWW (1989):**
   - **Tim Berners-Lee** tarafından icat edilmiştir.
   - İnternetin günümüzdeki haliyle "bilgi saklama ve paylaşma deposu" (repository) olarak kullanılmaya başlandığı noktadır.
   - *Dikkat:* İnternet (altyapı) ve WWW (üzerinde çalışan servis) aynı şey değildir; WWW, interneti halka açan ve kullanışlı kılan katmandır.

## 3. Ağ Türleri: Private vs Public




İnternet yapısına baktığımızda, diyagramlar bize birbirine bağlı birçok küçük küme gösterir. Bu yapı bizi iki temel ağ türüne götürür:

- **Private Network (Özel Ağ):**
  - Küçük, kendi içinde kapalı ağlardır (Örn: Evdeki WiFi ağın, bir ofis içi ağ).
  - Alice'in arkadaş grubu örneğindeki izole kümelerdir.
- **Public Network (Genel Ağ):**
  - Bu küçük özel ağları birbirine bağlayan ağdır.
  - **İnternet** teknik olarak bir Public Network'tür.
  - Erişimin herkese açık olduğu, verilerin dolaştığı ana otobandır.

> **Özet:** Cihazlar önce bir **Private Network**'e dahil olur, bu ağlar da **Public Network** (İnternet) üzerinden diğerlerine bağlanır.

# Identifying Devices on a Network (Ağdaki Cihazları Tanımlamak)

## 1. Kimliklendirme Mantığı (İnsan Analojisi)

Ağdaki cihazlar, tıpkı insanlar gibi iki farklı tanımlama yöntemine sahiptir. Bu analoji konuyu anlamak için çok kritiktir:

1. **İsim (Adımız) = IP Adresi:**
   - İsmimizi mahkeme kararıyla değiştirebiliriz.
   - Geçicidir, ortama göre değişebilir.
2. **Parmak İzi (Fingerprints) = MAC Adresi:**
   - Doğuştan gelir, biyolojiktir.
   - İsmi değiştirsek bile parmak izimiz arkadaki "gerçek kimliği" tutar.
   - *(Not: Teknik olarak MAC adresi de değiştirilebilir -Spoofing- ama tasarım amacı fiziksel ve kalıcı olmasıdır.)*

## 2. IP Adresi (Internet Protocol Address)

Cihazın ağ üzerindeki **mantıksal** adresidir. Belirli bir süre için bir cihaza atanır, sonra değişip başka bir cihaza verilebilir.

### Yapısı (IPv4)

Bir IPv4 adresi, noktalarla ayrılmış 4 bölümden (**Octet**) oluşur.

Örnek: `192.168.1.77`

- Her bir bölüm (octet) bir sayıyı temsil eder.
- Bu yapı, **IP Addressing & Subnetting** (ileride görülecek) kuralları ile hesaplanır.
- **Kural:** Aynı ağ içinde iki cihaz *asla* aynı anda aynı IP adresine sahip olamaz (IP Çakışması).

### Private (Özel) vs. Public (Genel) IP

Cihazlar hem yerel ağda (ev/ofis) hem de internette var olurlar. Bu yüzden iki farklı IP türüne sahiptirler:

1. **Private Address (Özel IP):**
   - Cihazın, yerel ağdaki diğer cihazlar (yazıcı, diğer PC'ler) arasında tanınmasını sağlar.
   - İnternete doğrudan çıkamaz.
2. **Public Address (Genel IP):**
   - Cihazın **İnternet** üzerinde tanınmasını sağlar.
   - **ISP (Internet Service Provider)** tarafından atanır ve genellikle aylık ücrete tabidir.

**Önemli Tablo Analizi (NAT Mantığı):**

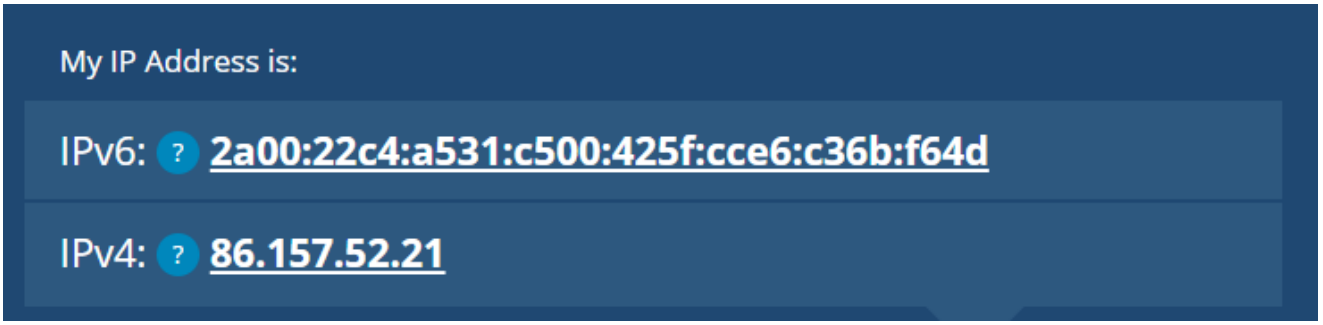
Aşağıdaki tablo, aynı ağdaki iki farklı cihazın durumunu gösteriyor:

| Cihaz Adı | IP Adresi (Private) | IP Adresi (Public) | Durum |
|---|---|---|---|
| **DESKTOP-KJE57FD** | `192.168.1.77` | `86.157.52.21` | Private IP farklı |
| **CMNatic-PC** | `192.168.1.74` | `86.157.52.21` | **Public IP AYNI!** |

> **Kritik Not:** Fark ettiysen iki cihazın **Public IP'si aynı**. Çünkü bu cihazlar internete çıkarken, evdeki Router (Modem) üzerinden çıkarlar. İnternet dünyası, evinizin içindeki `192.168...` adreslerini görmez; sadece modemin dış bacağındaki `86.157.52.21` adresini görür. Veri modeme gelir, modem kime aitse ona dağıtır.

### IPv4 Sorunu ve IPv6 Çözümü

- **IPv4:** $2^{32}$ adresleme kapasitesi var (~4.29 Milyar adres).
  - Cisco'nun tahminine göre 2021 sonunda 50 milyar cihaz olacaktı. Adresler bitti!
- **IPv6:** Yeni nesil adresleme.
  - Kapasite: $2^{128}$ adres (~340 Trilyon+).
  - Daha verimli ve güvenli metodolojiler içerir.




## 3. MAC Adresi (Media Access Control)

Cihazın ağ kartına (Network Interface Card - NIC) fabrikada üretim sırasında "kazınmış" **fiziksel** ve **eşsiz** seri numarasıdır.

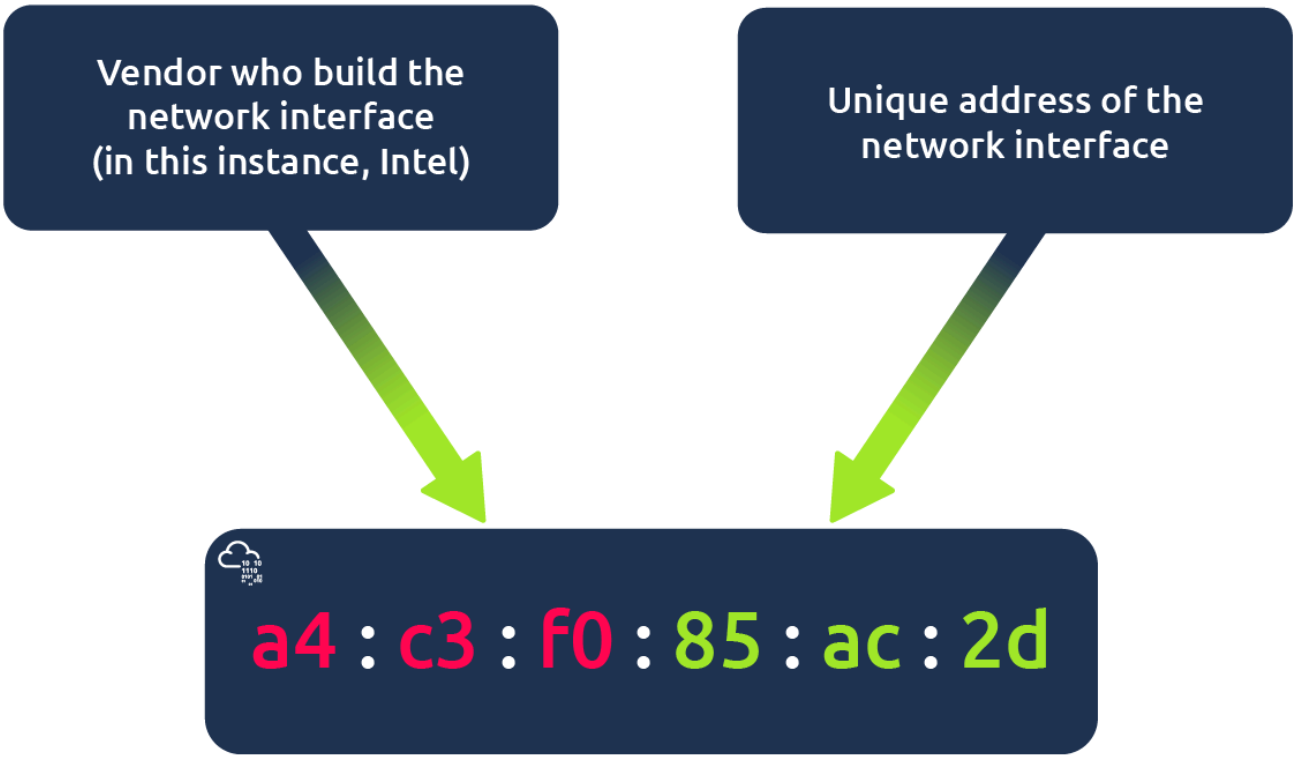
### Yapısı

12 karakterli **Hexadecimal** (16'lık sayı sistemi) bir dizidir. İkili gruplar halinde `:` ile ayrılır.

Örnek: `a4:c3:f0:85:ac:2d`

Bu adresi okumak bize cihaz hakkında istihbarat verir:

- **İlk 6 Karakter (OUI):** Üretici firmayı temsil eder (Örn: Intel, Apple, Dell).
- **Son 6 Karakter:** O kartın benzersiz seri numarasıdır.




### MAC Spoofing (MAC Sahteciliği)

MAC adresi donanımsal olsa da, yazılımsal olarak "taklit edilebilir". Buna **Spoofing** denir.

- **Neden Tehlikeli?** Bazı güvenlik sistemleri (Firewall, Wi-Fi filtreleri) sadece MAC adresine güvenecek şekilde kötü yapılandırılmış olabilir.
- **Senaryo:** Bir sistem yöneticisinin (Admin) MAC adresine tüm yetkiler verilmişse; saldırgan kendi MAC adresini Admin'inkiyle değiştirip ( `a4:c3...` ) sisteme "Ben Adminim" diyebilir. Firewall, paketin içini değil etiketini (MAC) kontrol ettiği için bunu yutar.

## 4. Practical Lab: Otel Wi-Fi Senaryosu

Bu bölümde interaktif bir laboratuvar var. Senaryo şu:

- **Ortam:** Ücretli bir Otel Wi-Fi ağı.
- **Alice (Yeşil Paketler):** Parasını ödemiş, internete çıkabiliyor.
- **Bob (Mavi Paketler):** Para ödememiş, Router paketlerini çöpe (bin) atıyor.
- **Görev:** Bob'un internete çıkmasını sağlamak.

**Çözüm Adımları (Walkthrough):**

Router, kimin para ödediğini **MAC Adresine** bakarak anlıyor. IP adresi sürekli değişebileceği için otel sistemleri genellikle cihazı MAC adresiyle hatırlar.

1. Alice'in trafiği geçiyor. Demek ki Router, Alice'in MAC adresini "İzinli Listesi"nde (Whitelist) tutuyor.
2. Bob'un internete çıkması için sistemin onu Alice sanması lazım.

3. **Aksiyon:** Bob'un MAC adresini değiştirip, Alice'in MAC adresinin aynısını yazıyoruz (Spoofing).
4. **Sonuç:** Router, gelen paketin göndericisine baktığında Alice'in kimliğini görüyor ve paketi geçiriyor.

> **Ders:** Asla sadece MAC adresine dayalı güvenlik (MAC Filtering) kullanma. Saldırganlar ağdaki izinli bir cihazı dinleyip (sniffing), onun MAC adresini kopyalayarak saniyeler içinde bu önlemi aşabilirler.

# Ping (ICMP)

Bir ağ yöneticisi veya siber güvenlikçi için `ping`, bir doktorun stetoskopu gibidir; "hasta yaşıyor mu?" sorusunun ilk cevabıdır.

## 1. Ping Nedir ve Nasıl Çalışır?

Ping, iki cihaz arasındaki bağlantının durumunu test etmek için kullanılan bir komut satırı aracıdır.

- **Protokol: ICMP** (Internet Control Message Protocol) kullanır.
  - Ping, taşıma katmanı protokollerini (TCP/UDP) **kullanmaz**. Doğrudan ağ katmanında çalışır.
- **Mekanizma:**
  1. Kaynak cihaz, hedefe bir **ICMP Echo Request** (Yankı İsteği) paketi gönderir.
  2. Hedef cihaz ulaşılabiliyorsa ve ayarları açıksa, kaynağa bir **ICMP Echo Reply** (Yankı Cevabı) paketi döner.
- **Amaç:**
  - **Bağlantı Var mı? (Connectivity):** Hedef cihaz açık mı ve ağ üzerinde erişilebilir mi?
  - **Performans (Reliability/Latency):** Paketlerin gidip gelmesi ne kadar sürüyor? Bağlantı stabil mi?

## 2. Kullanım (Syntax)

Ping, hem Windows hem de Linux işletim sistemlerinde varsayılan olarak yüklü gelir.

**Temel Komut:**

Bash

```
ping <IP Adresi veya URL>
```

*Örnek:* `ping 8.8.8.8` veya `ping google.com`

> **Not:** URL (örn. https://www.google.com/url?sa=E&source=gmail&q=google.com) pinglediğinde, bilgisayarın önce DNS sunucusuna gidip o URL'in IP karşılığını öğrenir, sonra o IP'ye ping atar. Yani ping aynı zamanda DNS'in çalışıp çalışmadığını da dolaylı yoldan test eder.

## 3. Çıktı Analizi (Output Breakdown)

Metindeki örnekte, `192.168.1.254` (Private IP) adresine atılan ping çıktısı incelenmiştir. Bir ping çıktısını okumak, ağdaki sorunu teşhis etmek için kritiktir.

Örnek Senaryo Çıktısı:

```
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=4.16 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=4.15 ms
...
--- 192.168.1.254 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
```

**Satır Satır Anlamları:**

- `icmp_seq` **:** Paketin sıra numarası. Paketlerin sırayla gidip gitmediğini veya arada kaybolan (dropped) olup olmadığını gösterir.
- `ttl` **(Time To Live):** Paketin yaşam süresi. Bu değer, paketin sonsuz döngüye girmesini engeller. Ayrıca, işletim sistemi tahmini (OS Fingerprinting) yaparken ipucu verir (Örn: Linux genelde 64, Windows 128 ile başlar).
- `time=4.16 ms` **:** Gecikme süresi (Latency/RTT). Paketin bizden çıkıp, karşı tarafa ulaşıp, cevabın bize dönmesi için geçen toplam süre.
  - Süre çok yüksekse veya dalgalıysa (Jitter) ağda yavaşlık var demektir.
- `0% packet loss` **:** Gönderilen 6 paketin hepsi geri dönmüş. Ağ sağlıklı. Eğer bu oran %10-20 olsaydı, bağlantı "kararsız" (unreliable) demekti.