

# AĞINIZI GENİŞLETME

[Kaynak](#)

## İÇERİK

1. Port Yönlendirme (Port Forwarding) Giriş
2. Güvenlik Duvarları 101 (Firewalls 101)
3. VPN Temelleri (Virtual Private Networks)
4. Yerel Ağ (LAN) Cihazları: Router ve Switch

## Port Yönlendirme (Port Forwarding) Giriş

**Port Forwarding** (Port Yönlendirme), yerel bir ağda (LAN) çalışan uygulamaların veya servislerin internete açılmasını sağlayan hayati bir köprüdür. Bu işlem olmadan, bir web sunucusu veya veritabanı sadece o ağa doğrudan bağlı cihazlar tarafından erişilebilir kalır.

## Port Yönlendirme Neden Gerekli? (İç Ağ vs. Dış Ağ)

Bir yerel ağ içindeki cihazlar, birbirlerine özel (private) IP adresleri üzerinden erişebilirler. Ancak bu adresler internet üzerinde yönlendirilemez (non-routable).

- **Senaryo (İç Ağ - Intranet):** Diyelim ki ağınızdaki bir sunucunun IP adresi **192.168.1.10** ve bu sunucu **80** portunda bir web sitesi barındırıyor.
  - Aynı ağdaki diğer iki bilgisayar, tarayıcılarına bu IP'yi yazarak siteye girebilir.
  - Fakat dış dünyadaki (internetteki) bir kullanıcı bu IP'ye erişemez çünkü bu IP "dahili" bir adrestir.
- **Çözüm (Port Forwarding):** Eğer bu sitenin halka açık olmasını istiyorsanız, yönlendiricinizde (router) bir "kapı yönlendirme" kuralı oluşturmanız gerekir.

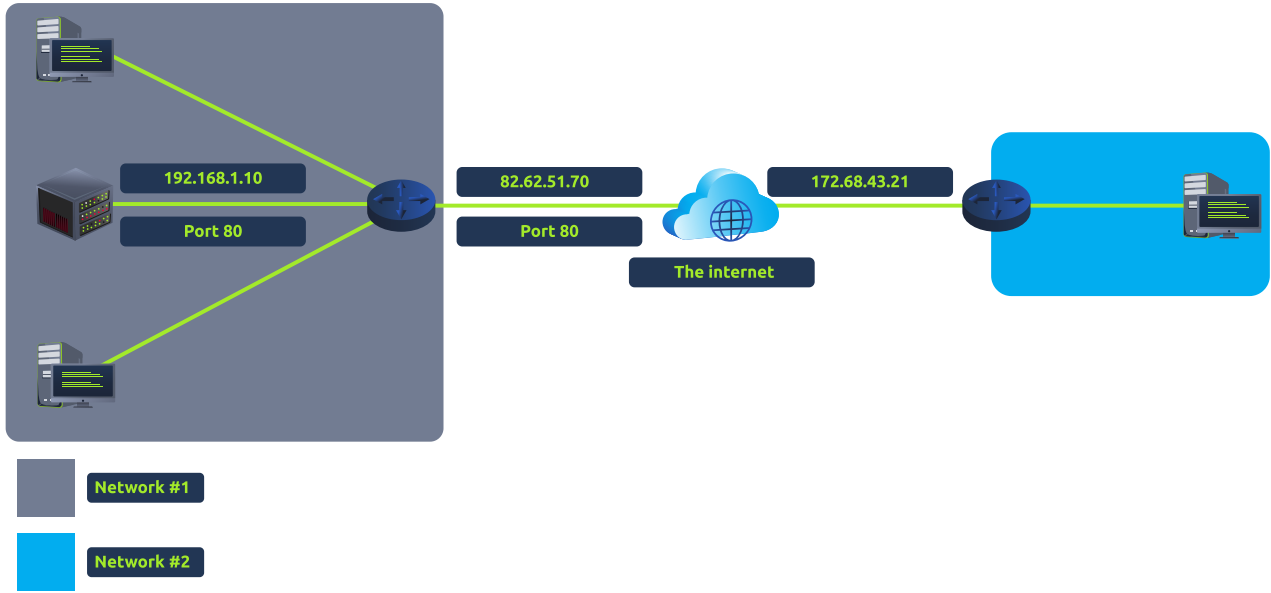
## Port Yönlendirme Nasıl Çalışır?

Port yönlendirme, ağın giriş kapısı olan **Router** üzerinde yapılandırılır. Router, dış dünyadan gelen istekleri alır ve bunları iç ağdaki doğru cihaza iletir.

## Örnek Akış:

1. **Ağ #1 (Sunucu Tarafı):** Kamu (Public) IP adresi **82.62.51.70** olsun. İçerideki sunucusu ise **192.168.1.10** adresinde ve **80** portunda çalışıyor.
2. **Kural Tanımlama:** Yönetici, Router'a şu talimatı verir: *"Eğer dışarıdan biri benim 82.62.51.70 adresime 80 portu üzerinden gelirse, onu içerideki 192.168.1.10:80 adresine gönder."*

3. **Ağ #2 (Dış Kullanıcı):** İnternet üzerindeki herhangi bir kullanıcı, sunucunun yerel IP'sini bilmesine gerek kalmadan, sadece kamu IP adresini (**82.62.51.70**) kullanarak web sitesine erişebilir.



## Kritik Ayrım: Port Forwarding vs. Firewall

Bu iki kavram sıkça birbirine karıştırılır ancak görevleri tamamen farklıdır:

- **Port Forwarding (Port Yönlendirme):** Belirli portları "açmaya" ve bu portlara gelen trafiği iç ağdaki belirli bir hedefe (cihaz+port) yönlendirmeye yarar. Paketlerin nereye gideceğini belirleyen bir **yol haritasıdır**.
- **Firewall (Güvenlik Duvarı):** Port yönlendirme ile bir port açılmış olsa bile, o porttan geçen trafiğin **güvenli olup olmadığına** karar verir. Trafiği inceler ve kural dışı bir durum varsa (örneğin zararlı bir payload) geçişi engeller.

**Özet:** Port Forwarding kapıyı açar ve yolu tarif eder; Firewall ise o kapıdan geçmek isteyenlerin kimliğini ve eşyalarını kontrol eden korumadır.

## Siber Güvenlik Bakış Açısı

Sızma testlerinde (Pentesting) veya saldırı senaryolarında, bir sistemin dışarıya hangi portları yönlendirdiğini bilmek çok kritiktir.

- **Risk:** Yanlış yapılandırılmış bir port yönlendirmesi, normalde sadece iç ağda kalması gereken hassas bir servisi (örneğin bir veritabanı veya SMB paylaşımı) tüm dünyaya açarak büyük bir güvenlik açığı oluşturabilir.
- **Yöntem:** Dış ağdan yapılan taramalarda (Nmap), router'ın kamu IP'sine bakarak hangi iç servislerin dışarıya "forward" edildiğini analiz edebiliriz.

## Güvenlik Duvarları 101 (Firewalls 101)

Bir ağın sınır güvenliğıinden sorumlu olan en temel bileşen **Firewall** (Güvenlik Duvarı) sistemidir. Güvenlik duvarını, bir ağın "gümrük kapısı" veya "sınır güvenliğıi" olarak düşünebiliriz. Bu cihaz veya yazılım, ağıya giren ve ağıdan çıkan trafiğı belirli kurallar çerçevesinde denetler, izin verir (**permit**) veya engeller (**deny**).

## Güvenlik Duvarı Karar Mekanizması

Bir ağı yöneticisi, güvenlik duvarını yapılandırırken trafiğın geçip geçemeyeceğıine karar vermek için şu kritik soruları baz alan kurallar tanımlar:

- **Trafik nereden geliyor? (Source):** Belirli bir IP adresinden veya güvenilmeyen bir ağıdan gelen trafik yasaklanmış mı?
- **Trafik nereye gidiyor? (Destination):** İç ağıdaki hassas bir bölgeye (örneğin veritabanı sunucusu) erişim kısıtlanmış mı?
- **Hangi port hedefleniyor?:** Sadece web trafiğıne mi (Port 80/443) izin var, yoksa SSH (Port 22) gibi yönetim portları dışarıya kapalı mı?
- **Hangi protokol kullanılıyor?:** Trafik TCP mi, UDP mi yoksa ICMP mi?

Güvenlik duvarları bu soruların cevaplarını bulabilmek için **Packet Inspection** (Paket İnceleme) denilen yöntemi kullanır; yani geçen her paketin başlık bilgilerini okur.

## Güvenlik Duvarı Türleri ve Kategorileri

Güvenlik duvarları, kurumsal ağlardaki devasa donanım cihazlarından, evimizdeki basit modemlere veya **Snort** gibi yazılımsal çözümlere kadar çok farklı formlarda karşımıza çıkar. Ancak çalışma mantığı açısından en temel iki kategoriye ayrılırlar:

### 1. Stateful Firewall (Durumlu Güvenlik Duvarı)

Bu tür, paketleri tek tek değil, **bağlantının tamamını (oturumunu)** izleyerek karar verir.

- **Çalışma Mantığı:** Bir cihazın tüm bağlantı geçmişini ve davranışını analiz eder. Dinamik bir karar verme sürecine sahiptir.
- **Örnek:** Bir TCP el sıkışmasının (handshake) ilk adımlarına izin verip, ilerleyen aşamalarda şüpheli bir durum sezerse tüm bağlantıyı koparabilir. Eğer bir host'tan gelen bağlantı "kötü" olarak işaretlenirse, o cihazın tüm trafiğı bloklanır.
- **Kaynak Tüketimi:** Karar süreci dinamik ve hafıza gerektiren bir takip (state table) içerdiği için, stateless sistemlere göre **çok daha fazla sistem kaynağı** (CPU, RAM) tüketir.

### 2. Stateless Firewall (Durumsuz Güvenlik Duvarı)

Bu tür, bağlantının geçmişine bakmaz; her paketi birbirinden bağımsız birer birim olarak, elindeki **statik kurallara** göre değerlendirir.

- **Çalışma Mantığı:** Elindeki kurallar listesine bakıp; "Gelen paket Port 80'e mi gidiyor? Evet. O zaman geçsin" der. Paketin bir önceki adımda ne yaptığıyla ilgilenmez.
- **Örnek:** Bir cihaz kötü niyetli bir paket gönderirse sadece o paket engellenir, ancak cihazın kendisi otomatik olarak tamamen bloklanmaz (kuralda aksi belirtilmedikçe).
- **Avantajı:** Çok hızlıdır ve az kaynak tüketir. Özellikle büyük miktarda trafik akışı olan durumlarda veya **DDoS (Distributed Denial-of-Service)** saldırılarını göğüslerken yüksek performans gösterir.
- **Zayıflığı:** "Daha aptal" bir sistemdir. Kural setinde tam bir eşleşme yoksa etkisiz kalır. Bağlantı durumunu takip edemediği için karmaşık saldırıları tespit etmekte zorlanır.

## Karşılaştırma Özeti

Özellik	Stateful Firewall	Stateless Firewall
Bakış Açısı	Bağlantının tamamı (Oturum bazlı)	Tekil paketler (Paket bazlı)
Kaynak Tüketimi	Yüksek (Bellek kullanımı yoğun)	Düşük (Hızlı ve hafif)
Esneklik	Dinamik ve akıllı	Statik ve kural bağımlı
Kullanım Alanı	Hassas iç ağ koruması	Yüksek trafikli ağ girişleri, DDoS koruması

**Önemli Not:** Modern ağlarda genellikle bu iki yapının hibrit versiyonları kullanılır. Bir saldırgan olarak güvenlik duvarını atlatmaya çalışırken (Firewall Evasion), sistemin paketleri mi yoksa oturumu mu takip ettiğini anlamak, göndereceğimiz payload'un yapısını belirler.

## VPN Temelleri (Virtual Private Networks)

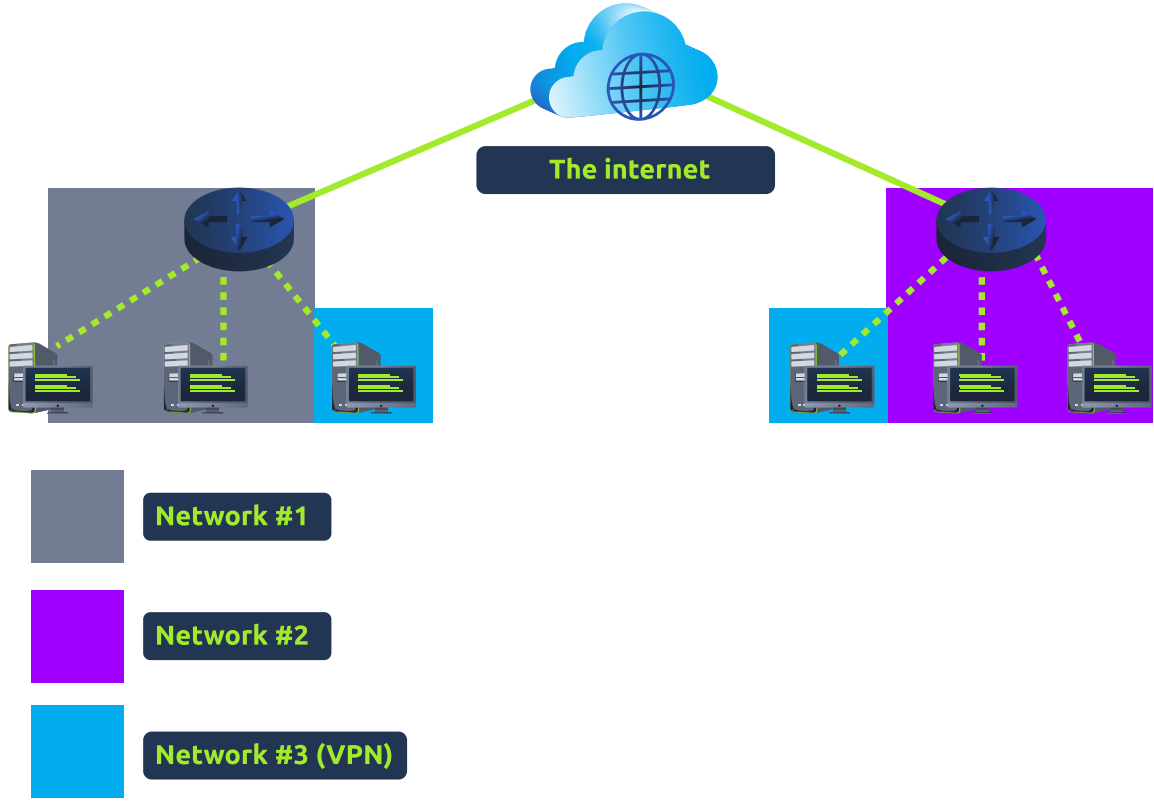
**VPN (Sanal Özel Ağ)**, internet gibi halka açık ve güvensiz bir ağ üzerinde, iki cihaz veya ağ arasında sanki doğrudan bir kablo çekilmişçesine güvenli bir yol (buna **Tunnel/Tünel** diyoruz) oluşturulmasını sağlayan teknolojidir. Bu tünel içindeki cihazlar, coğrafi olarak nerede olurlarsa olsunlar kendi özel ağlarını kurarlar.

## VPN Nasıl Çalışır? (Tünelleme Mantığı)

Normalde farklı şehirlerdeki veya binalardaki iki ofis birbiriyle doğrudan konuşamaz. VPN, bu iki noktayı internet üzerinden birbirine bağlayarak sanki aynı odadaymış gibi iletişim kurmalarını sağlar.

- **Örnek Senaryo:**
  - **Ofis A (Ağ #1)** ve **Ofis B (Ağ #2)** birbirinden bağımsızdır.
  - İki ofisten belirli cihazlar VPN ile birbirine bağlandığında **Ağ #3 (VPN Ağı)** oluşur.

- Bu cihazlar hala kendi yerel ağlarının bir parçasıdır ancak artık sadece VPN üyelerinin görebildiği **özel bir kanal** üzerinden de veri alışverişi yapabilirler.



## VPN Kullanmanın Temel Faydaları

VPN sadece "yasaklı sitelere girmek" için değildir; siber güvenlik ve kurumsal yapılar için kritik avantajlar sunar:

Fayda	Teknik Açıklama
<b>Coğrafi Bağlantı</b>	Farklı konumlardaki ofislerin tek bir merkezdeki sunuculara veya altyapıya erişmesini sağlar.
<b>Gizlilik (Privacy)</b>	VPN trafiği <b>şifreler (Encryption)</b> . Bu sayede veriler, gönderici ve alıcı dışında kimse tarafından okunamaz. Özellikle şifresiz halka açık Wi-Fi noktalarında (kafe, havaalanı vb.) "sniffing" (paket koklama) saldırılarına karşı tam koruma sağlar.
<b>Anonimlik</b>	Normalde trafiğiniz İSS (İnternet Servis Sağlayıcısı) ve aracı kurumlar tarafından izlenebilir. VPN, trafiği bir tünel içine aldığı için anonimlik sağlar. <b>Kritik Not:</b> VPN sağlayıcınız log (kayıt) tutuyorsa, anonimlik sadece bir illüzyondur.
<b>Güvenli Laboratuvar</b>	<b>TryHackMe</b> gibi platformlar, zafiyetli makineleri doğrudan internete açmak yerine VPN kullanır. Böylece hem siz makinelerle güvenli konuşursunuz hem de İSS'niz bir saldırı yaptığınızı sanıp hattınızı kapatmaz.

# VPN Teknolojileri ve Protokolleri

VPN teknolojisi yıllar içinde gelişmiş ve farklı protokoller ortaya çıkmıştır. Her birinin güvenlik ve kurulum zorluğu seviyesi farklıdır:

## 1. PPP (Point-to-Point Protocol)

PPTP (aşağıda açıklanan) tarafından kimlik doğrulama ve şifreleme sağlamak için kullanılan temel teknolojidir.

- **Çalışma Mantığı:** SSH'a benzer şekilde bir **Özel Anahtar (Private Key)** ve **Kamu Sertifikası (Public Certificate)** kullanır. Bağlantı için anahtar ve sertifikanın eşleşmesi şarttır.
- **Kısıtlama:** Kendi başına bir ağın dışına çıkamaz (**non-routable**), yani yönlendirilemez.

## 2. PPTP (Point-to-Point Tunneling Protocol)

PPP protokolünden gelen verinin ağ dışına çıkmasını ve internet üzerinde taşınmasını sağlayan teknolojidir.

- **Avantaj:** Kurulumu çok kolaydır ve neredeyse her cihaz tarafından desteklenir.
- **Dezavantaj:** Diğer alternatiflere göre şifreleme seviyesi oldukça zayıftır; modern saldırılara karşı direnci düşüktür.

## 3. IPSec (Internet Protocol Security)

Veriyi mevcut IP çerçevesini kullanarak şifreleyen daha gelişmiş bir protokoldür.

- **Avantaj:** Çok güçlü şifreleme standartlarına sahiptir ve geniş cihaz desteği sunar.
- **Dezavantaj:** PPTP'ye kıyasla yapılandırması ve yönetimi oldukça zordur, teknik bilgi gerektirir.

# Yerel Ağ (LAN) Cihazları: Router ve Switch

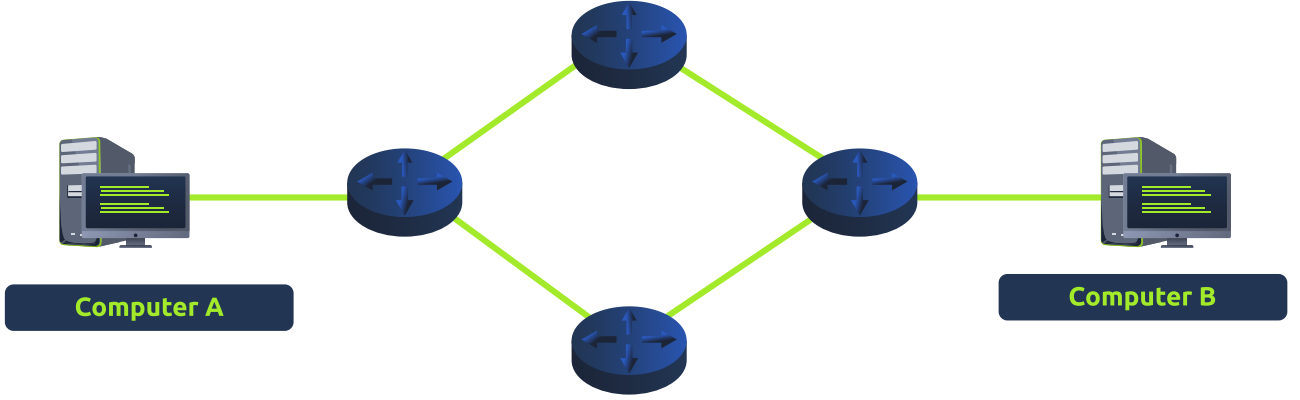
Ağ cihazlarını anlamak, verinin fiziksel kablolardan mantıksal hedeflere nasıl ulaştığını kavramaktır. Bir siber güvenlik uzmanı için bu cihazların hangi katmanda çalıştığını bilmek, saldırı yüzeyini analiz etmek için hayati önem taşır.

## 1. Router (Yönlendirici) Nedir?

Bir **Router**'ın temel görevi, farklı ağları birbirine bağlamak ve bu ağlar arasında veri iletimini sağlamaktır. Bu işleme **Routing (Yönlendirme)** adı verilir.

- **Katman:** OSI modelinin **3. Katmanı (Network Layer)** üzerinde çalışır.
- **İşleyiş:** Bir veri paketi hedefine giderken önünde birden fazla yol olabilir. Router, paket için en uygun yolu (en kısa, en güvenilir veya en hızlı) belirler.
- **Yönlendirme Karar Kriterleri:**

- Hangi yol daha kısa? (Mesafe/Hop sayısı)
- Hangi yol daha güvenilir? (Hata oranı düşük)
- Hangi yol daha hızlı? (Örn: Bakır kablo yerine fiber optik hattın tercih edilmesi)

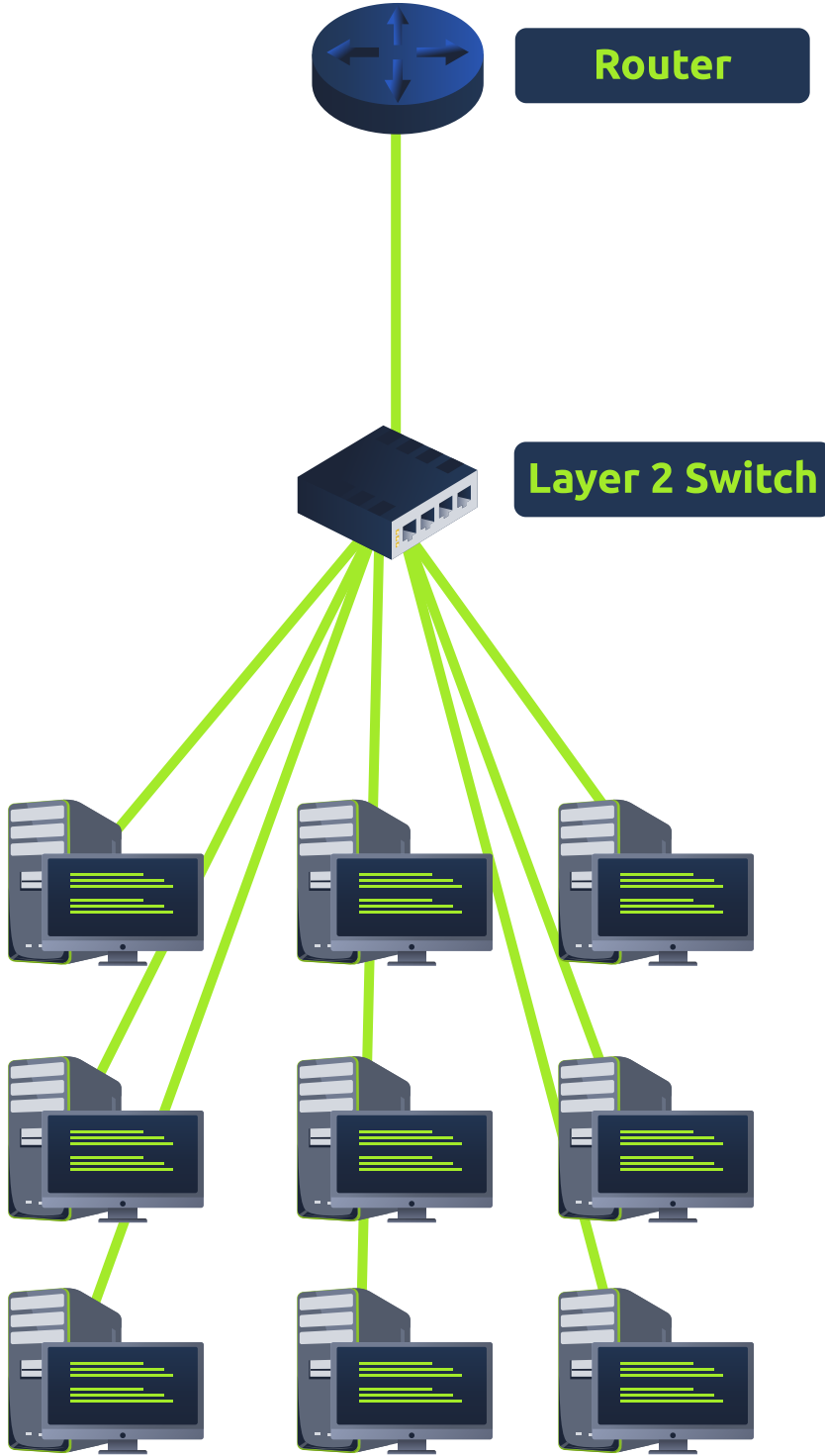


**Yönetim:** Router'lar genellikle bir web arayüzü veya konsol (CLI) üzerinden yönetilir. Burada **Port Forwarding** (Port Yönlendirme) ve **Firewall** (Güvenlik Duvarı) kuralları gibi kritik konfigürasyonlar yapılır.

## 2. Switch (Anahtar) Nedir?

**Switch**, bir yerel ağ (LAN) içindeki birden fazla cihazı birbirine bağlayan özel bir cihazdır. Ethernet kabloları aracılığıyla 3'ten 63'e kadar (veya daha fazla) cihazı bir araya getirebilir.

Switch'ler operasyonel yeteneklerine göre ikiye ayrılır:



## A) Layer 2 Switch (Katman 2 Anahtarı)

Sadece OSI modelinin **2. Katmanı (Data Link Layer)** üzerinde çalışır.

- **Veri Birimi:** Bu cihazlar **Frame (Çerçeve)** seviyesinde işlem yapar. (Hatırla: IP paketleri çerçevelerin içinde kapsüllenmiştir).
- **Adresleme:** Veriyi doğru cihaza iletmek için **MAC adreslerini** kullanır.
- **Sınır:** Sadece yerel ağ içindeki cihazların birbiriyle konuşmasını sağlar; farklı ağlara paket yönlendiremez.

## B) Layer 3 Switch (Katman 3 Anahtarı)

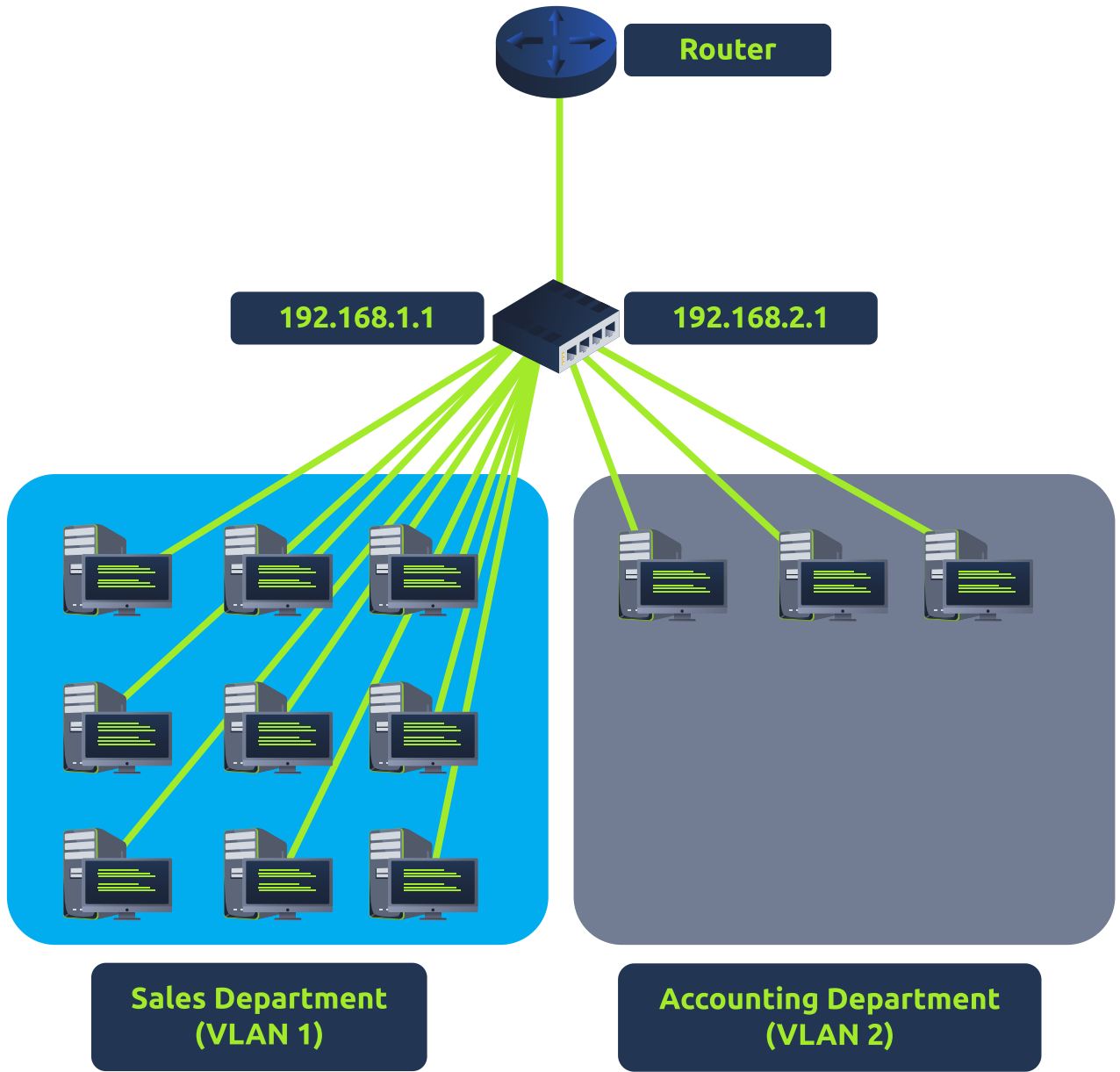
Daha sofistike cihazlardır. Hem Layer 2 hem de Layer 3 görevlerini yerine getirebilirler.

- **Yetenek:** Hem MAC adreslerini kullanarak çerçeve iletebilir (Switch görevi), hem de IP protokolünü kullanarak paketleri yönlendirebilir (Router benzeri görev).
- **Routing Kapasitesi:** Router kadar karmaşık dış ağ yönlendirmeleri yapamasa da iç ağdaki (Intranet) trafiği yönetmekte çok hızlıdır.

## 3. VLAN (Sanal Yerel Ağ) Teknolojisi

Layer 3 Switch'ler ile kullanılan en önemli teknolojilerden biri **VLAN**'dir. VLAN, aynı fiziksel switch'e bağlı cihazları mantıksal olarak birbirinden ayırmaya yarar.

- **Neden Kullanılır?** Bir şirketteki "Satış Departmanı" ve "Muhasebe Departmanı" aynı switch'e takılı olabilir. Ancak güvenlik gereği muhasebe verilerinin satış departmanı tarafından görülmemesi gerekir.
- **Güvenlik ve İzolasyon (Segregation):** VLAN sayesinde bu iki departman sanal olarak farklı ağlardaymış gibi davranır.
  - Her iki departman da aynı internet bağlantısını kullanabilir.
  - Ancak aradaki kurallar izin vermediği sürece birbirlerinin cihazlarına erişemezler.
- **Örnek Senaryo:**
  - Ağ 1: 192.168.1.1 (Sales)
  - Ağ 2: 192.168.2.1 (Accounting)
  - Bu iki ağ aynı switch üzerindedir ancak birbirlerinden izoledir.



#### Üniversite Notu / Kritik Bilgi:

- **Router:** IP adresine bakar, farklı ağları bağlar. (Layer 3)
- **Layer 2 Switch:** MAC adresine bakar, aynı ağdaki cihazları bağlar. (Layer 2)
- **Layer 3 Switch:** Hem MAC hem IP'ye bakabilir, VLAN'lar arası geçişi (inter-VLAN routing) yönetebilir. (Layer 2 + 3)