LOCAL AREA NETWORK'e GİRİŞ

Hazırlayan- Kaynak

İÇERİK

LAN Topolojilerine Giriş (Introducing LAN Topologies)

Bir ağın tasarımı, güvenliği ve sürekliliği üzerinde doğrudan etkilidir. Siber güvenlikte **Enumeration** (Numaralandırma/Keşif) aşamasında, sızmaya çalıştığımız ağın fiziksel veya mantıksal yapısını (topolojisini) anlamak, saldırı vektörlerini belirlemek için kritiktir. Bir ağın tasarımı veya "görünümü" olan **Topology**, verinin nasıl aktığını ve nerede kesintiye uğrayabileceğini belirler.

1. Yıldız Topolojisi (Star Topology)

Günümüz modern ağlarında, özellikle kurumsal ortamlarda en sık karşılaşılan tasarım budur. Bu yapıda tüm cihazlar merkezi bir ağ cihazına (**Switch** veya **Hub**) tekil olarak bağlanır.

- **Veri Akışı:** Herhangi bir cihaz veri gönderdiğinde, bu veri önce merkezdeki cihaza gider, ardından merkezdeki cihaz veriyi hedefe iletir.
- **Ölçeklenebilirlik (Scalability):** Ağın genişlemesi oldukça kolaydır; yeni bir cihaz eklemek için sadece merkeze bir kablo çekmek yeterlidir.
- **Maliyet:** Diğer topolojilere göre daha pahalıdır. Çünkü hem her cihaz için ayrı kablolama hem de merkezde konumlandırılacak özel donanımlar (Switch vb.) gerektirir.
- **Bakım ve Arıza:** Ağ büyüdükçe bakım ihtiyacı artar. Arıza tespiti (Troubleshooting) bazen karmaşıklaşabilir.
- **Kritik Nokta (Single Point of Failure):** Eğer merkezdeki donanım arızalanırsa, ona bağlı olan **tüm cihazlar** arasındaki iletişim kopar. Ancak bu merkezi cihazlar (Switchler) genellikle oldukça dayanıklı (robust) üretilirler.

2. Bus (Veriyolu) Topolojisi

Bu topoloji, **Backbone Cable** (Omurga Kablosu) adı verilen tek bir ana hat üzerine kuruludur. Cihazlar bu ana hattan dallanarak ağa dahil olurlar. Bir ağacı ve dallarını düşünebilirsiniz.

- **Veri Darboğazı (Bottleneck):** Tüm veri trafiği aynı hat üzerinden geçtiği için, birden fazla cihaz aynı anda veri talep ederse ağ hızla yavaşlar.
- **Arıza Tespiti:** Oldukça zordur. Veri tek bir rotada aktığı için hangi cihazın sorun çıkardığını belirlemek zordur.
- **Maliyet ve Kurulum:** En ucuz ve kurulumu en kolay topolojilerden biridir. Çok az kablo ve ek donanım gerektirir.
- **Yedeklilik (Redundancy) Eksikliği:** En büyük zayıflığı budur. Omurga kablosunda (Backbone) oluşacak tek bir fiziksel hasar, **tüm ağın** çökmesine neden olur. Veri iletimi tamamen durur.

3. Ring (Halka) Topolojisi

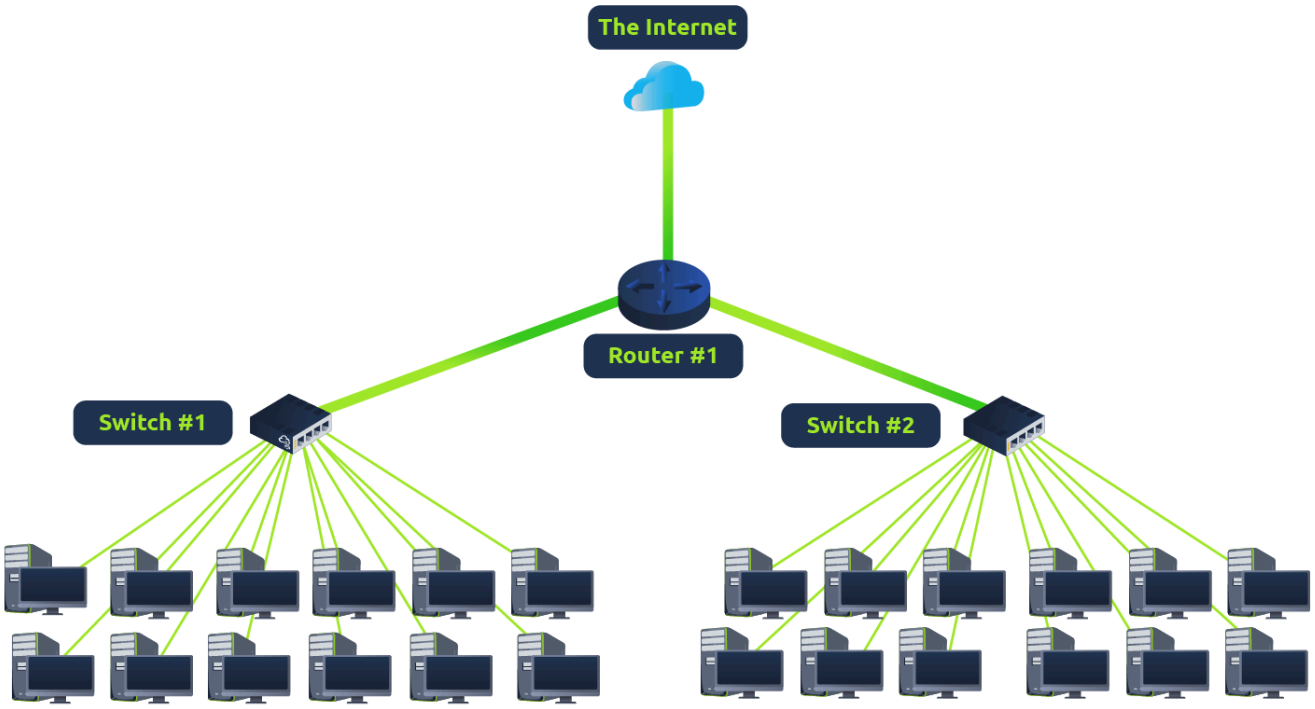
Cihazlar birbirine doğrudan bağlanarak kapalı bir döngü (loop) oluşturur. Bu yapıya bazen **Token Topology** de denir.

- **Veri İletim Mekanizması:** Veri halka boyunca döner. Bir cihaz, gelen veriyi eğer kendisi bir şey göndermeyecekse bir sonraki cihaza iletir. Eğer kendi göndereceği veri varsa, önce kendi verisini halkaya salar, sonra diğerlerini iletir.
- **Yön ve Hız:** Veri tek yönde hareket eder. Bu durum arıza tespitini kolaylaştırır ancak verimliliği düşürür. Veri, hedefe ulaşana kadar birçok ara cihazı ziyaret etmek zorunda kalabilir.
- **Trafik Durumu:** Bus topolojisinin aksine darboğazlara karşı daha dirençlidir çünkü aynı anda devasa miktarda veri ağda dolaşmaz.
- **Kırılganlık:** Tasarımı gereği, halkadaki tek bir cihazın bozulması veya bir kablonun kesilmesi **tüm döngüyü bozar** ve ağ iletişimi kesilir.

4. Switch (Anahtar) Nedir?

Switch, bir yerel ağ (LAN) içindeki bilgisayarları, yazıcıları ve diğer ethernet uyumlu cihazları birbirine bağlayan özel bir cihazdır.

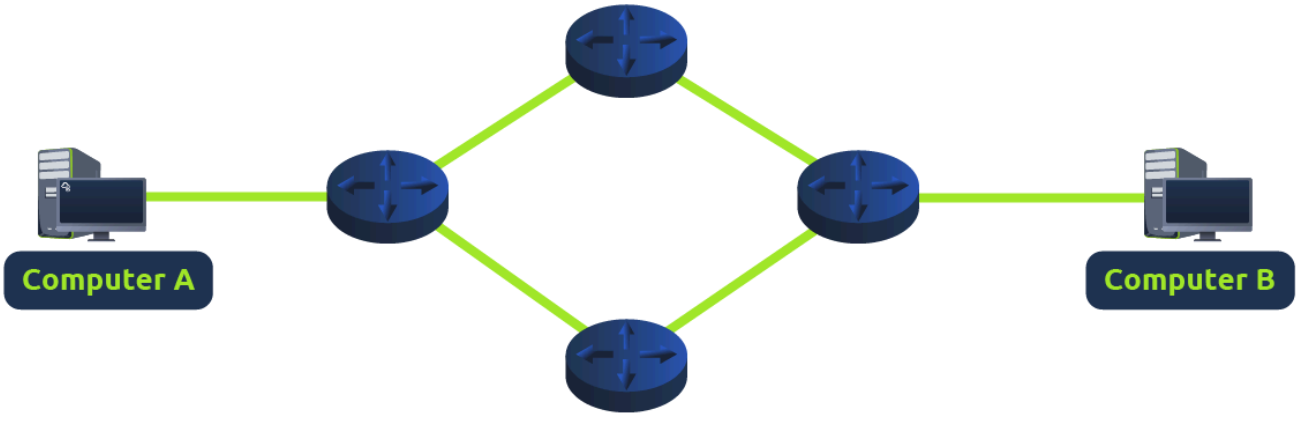
- **Portlar:** İhtiyaca göre 4, 8, 16, 24, 32 veya 64 portlu olabilirler.
- **Hub vs Switch:** Switch'ler, Hub'lara (veya Repeater'lara) göre çok daha akıllıdır.
  - **Hub:** Gelen paketi ayırt etmeksizin tüm portlara gönderir (**Broadcasting**). Bu da gereksiz trafik ve güvenlik açığı demektir.
  - **Switch:** Hangi portta hangi cihazın (MAC adresi üzerinden) bağlı olduğunun kaydını tutar. Veri geldiğinde onu sadece hedefin olduğu porta yönlendirir. Bu işlem ağ trafiğini ciddi oranda azaltır.
- **Yedeklilik (Redundancy):** Birden fazla Switch birbirine bağlanarak verinin gitmesi için alternatif yollar oluşturulabilir. Eğer bir Switch veya kablo arızalanırsa veri diğer yol üzerinden akmaya devam eder. Bu durum performansı (gecikme nedeniyle) bir miktar düşürse de sistemin tamamen kapanmasını (downtime) engeller.



5. Router (Yönlendirici) Nedir?

Router'ın temel görevi, **farklı ağları** birbirine bağlamak ve aralarında veri transferi yapmaktır.

- **Routing (Yönlendirme):** Verinin ağlar arasında seyahat etmesi işlemine verilen isimdir. Router, verinin hedefe ulaşması için en uygun yolu (path) oluşturur veya seçer.
- **Kullanım Senaryosu:** Eğer cihazlar arasında birden fazla yol varsa, Router bu yolları yöneterek verinin başarıyla teslim edilmesini sağlar.



Teknik Özet Tablosu

Topoloji	Maliyet	Arıza Direnci	Ölçeklenebilirlik	Temel Zayıflık
Star	Yüksek	Yüksek (Donanım hariç)	Çok Kolay	Merkezi cihazın (Switch) bozulması.
Bus	Düşük	Çok Düşük	Zor	Ana kablonun (Backbone) kopması.

Topoloji	Maliyet	Arıza Direnci	Ölçeklenebilirlik	Temel Zayıflık
Ring	Orta	Düşük	Orta	Tek bir kablo/cihaz hatasında tüm ağın çökmesi.

Alt Ağlara Bölme Esasları (A Primer on Subnetting)

Ağlar dünyasında her zaman "tek ve devasa" bir yapı işimize yaramaz. **Subnetting** (Alt ağlara bölme), büyük bir ağı kendi içinde daha küçük, yönetilebilir parçalara ayırma işlemidir. Bunu bir pastayı dilimlemek gibi düşünebilirsin; elimizde bir bütün pasta var ama herkesin payını (departmanların veya cihaz gruplarının sınırlarını) önceden belirlememiz gerekiyor.

Subnetting Neden Yapılır?

Büyük bir şirketi hayal edelim. Şirkette **Muhasebe**, **Finans** ve **İnsan Kaynakları** gibi farklı departmanlar bulunur. Fiziksel dünyada bir evrakın hangi departmana gideceğini biliriz; ancak ağ dünyasında yönlendirme yapabilmek için mantıksal sınırlar çizilmelidir. Sistem yöneticileri, ağın belirli kısımlarını bu departmanlara atamak için alt ağlara bölme yöntemini kullanır.

Temel Avantajlar:

- **Verimlilik (Efficiency):** Gereksiz ağ trafiğini (broadcast) sınırlar.
- **Güvenlik (Security):** Farklı departmanların veya kullanıcı gruplarının birbirinin verisine doğrudan erişmesini engeller.
- **Tam Kontrol (Full Control):** Ağın hangi bölgesinde ne kadar cihaz olacağını ve kimin nereye gidebileceğini yönetmenizi sağlar.

> **Güvenlik Örneği:** Bir kafeyi düşün. Kafede iki ayrı ağ vardır: Biri çalışanlar ve yazar kasalar için, diğeri ise müşterilerin kullanımı için (Hotspot). Subnetting sayesinde bu iki grup aynı internet hattını kullansa bile birbirlerinden tamamen yalıtılırlar. Bu sayede bir müşteri, yazar kasaların olduğu ağa sızamaz.

Alt Ağ Bileşenleri ve Adresleme

Alt ağ oluşturma işlemi, bir ağda barınabilecek **Host** (cihaz/istemci) sayısının belirlenmesiyle yapılır. Bu sınırı belirleyen sayıya **Subnet Mask** (Alt Ağ Maskesi) denir.

Tıpkı IP adresleri gibi, Subnet Mask de 4 oktetten (8'er bitlik 4 bölüm, toplam 32 bit) oluşur ve her bir oktet **0-255** arası bir değer alır. Bir alt ağda IP adresleri üç temel amaçla kullanılır:

1. Ağ Adresi (Network Address)

Ağın başlangıcını ve varlığını tanımlayan adrestir. Bu adres bir cihaza (PC, Yazıcı vb.) atanamaz.

- **Örnek:** `192.168.1.100` IP'sine sahip bir cihaz, `192.168.1.0` ağ kimliğine sahip bir alt ağda bulunur.

2. Cihaz/Host Adresi (Host Address)

Alt ağ içerisindeki her bir cihazı (bilgisayar, telefon, sunucu) tekil olarak tanımlayan adrestir.

- **Örnek:** `192.168.1.1` ile başlar, ağın büyüklüğüne göre devam eder.

3. Varsayılan Ağ Geçidi (Default Gateway)

Verinin kendi yerel ağından çıkıp başka bir ağa (örneğin internete veya başka bir departmana) gitmesini sağlayan "çıkış kapısı" adresidir.

- **Mantık:** Eğer hedef IP adresi yerel ağda (aynı subnet'te) değilse, veri otomatik olarak bu adrese (genellikle bir Router) gönderilir.
- **Genel Kullanım:** Genellikle ağın kullanılabilir ilk adresi (`.1`) veya son adresi (`.254`) bu iş için ayrılır.

Teknik Özet Tablosu

Kavram	Amacı	Örnek
Network Address	Ağın başlangıcını ve kimliğini belirtir.	`192.168.1.0`
Host Address	Ağdaki spesifik bir cihazı tanımlar.	`192.168.1.100`
Default Gateway	Dış dünyaya açılan kapıdır (Router IP'si).	`192.168.1.254`

Önemli Notlar

- **Ev Ağları:** Genellikle tek bir subnet kullanırız çünkü evde 254'ten fazla cihazın aynı anda bağlı olması pek rastlanan bir durum değildir.
- **Kurumsal Ağlar:** Ofislerde yüzlerce PC, yazıcı, kamera ve sensör olduğu için subnetting bir zorunluluktur.
- **IP Yapısı:** Bir IP adresinin hangi kısmının ağa (Network), hangi kısmının cihaza (Host) ait olduğunu **Subnet Mask** belirler.

ARP (Address Resolution Protocol)

Bir önceki konulardan hatırlayacağımız üzere, ağdaki cihazların iki temel kimliği vardır: **MAC Adresi** (fiziksel kimlik) ve **IP Adresi** (mantıksal kimlik). Ancak bir veri paketinin doğru cihazın donanımına ulaşabilmesi için bu iki kimliğin birbiriyle eşleşmesi gerekir. İşte bu "kimlik eşleştirme" görevini üstlenen teknolojiye **ARP (Address Resolution Protocol - Adres Çözümleme Protokolü)** denir.

ARP'nin Temel Amacı

En basit tabiriyle ARP; bir cihazın, ağ üzerindeki IP adresini bildiği bir başka cihazın MAC adresini öğrenmesini sağlar.

Cihazlar birbirleriyle haberleşmek istediklerinde, verinin donanım seviyesinde nereye gideceğini bilmek zorundadırlar. Bu yüzden her cihaz, ağdaki diğer cihazların IP-MAC eşleşmelerini tuttuğu küçük bir günlük tutar.

ARP Nasıl Çalışır? (Mekanizma ve Mesaj Tipleri)

Ağdaki her cihazın, bu bilgileri geçici olarak sakladığı bir belleği bulunur; buna **ARP Cache** (ARP Önbelleği) denir. Eğer bir cihaz, hedef IP'nin MAC adresini önbelleğinde bulamazsa şu iki mesaj tipini kullanarak süreci başlatır:

1. ARP Request (ARP İsteği)

İletişimi başlatmak isteyen cihaz, tüm ağa bir **Broadcast** (Yayın) mesajı gönderir. Bu mesaj temel olarak şunu sorar:

> "Şu IP adresine (örneğin 192.168.1.5) sahip olan cihaz kimse, lütfen bana MAC adresini söylesin?"

- **Önemli:** Bu bir "Broadcast" mesajıdır; yani ağdaki **tüm** cihazlara gider.

2. ARP Reply (ARP Yanıtı)

Ağdaki tüm cihazlar bu isteği alır, ancak sadece söz konusu IP adresine sahip olan cihaz bu mesajı ciddiye alır. Diğerleri mesajı görmezden gelir. Hedef cihaz, isteği gönderen tarafa doğrudan (**Unicast**) bir yanıt döner:

> "Aradığın IP adresi bende ve benim fiziksel MAC adresim şudur: `AA:BB:CC:DD:EE:FF`."

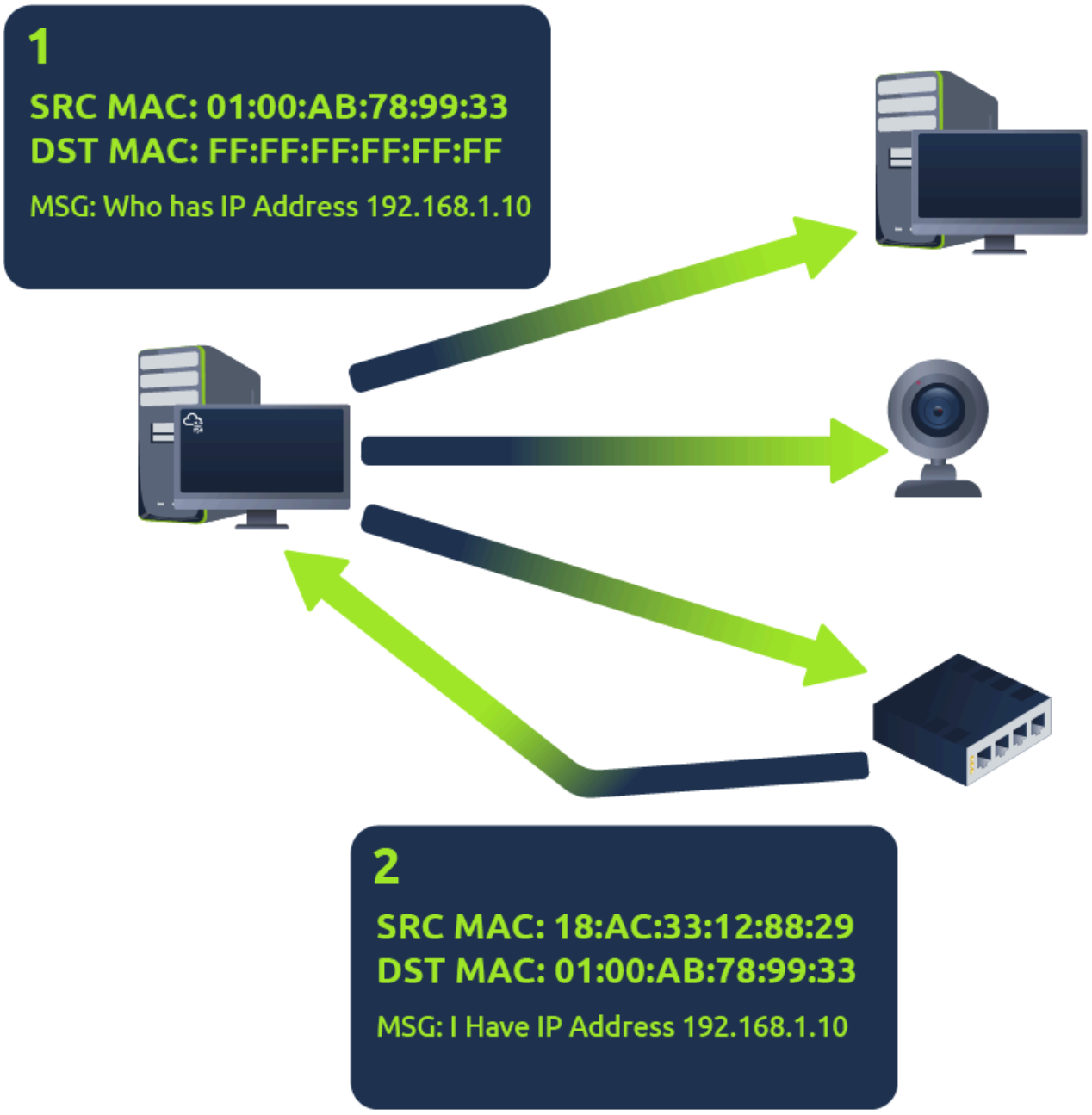
ARP Cache (Önbellek) ve Süreç

Yanıtı alan cihaz, bu bilgiyi hemen kullanır ve gelecekte tekrar sormamak için **ARP Cache** tablosuna kaydeder.

Adım Adım Mantık Zinciri:

1. **Sorgu:** Cihaz A, Cihaz B'ye paket göndermek ister. B'nin IP'sini bilir ama MAC'ini bilmez.
2. **Önbellek Kontrolü:** A, önce kendi **ARP Cache** tablosuna bakar. Bilgi yoksa işleme devam eder.
3. **Yayın (Broadcast):** A, tüm ağa "Bu IP kimin?" diye bağırır (**ARP Request**).
4. **Cevap (Reply):** Sadece B cihazı "Benim!" der ve MAC adresini gönderir (**ARP Reply**).
5. **Kayıt:** Cihaz A, bu bilgiyi önbelleğine yazar ve veri paketini artık donanım seviyesinde doğru adrese gönderir.

> **Güvenlik Notu:** ARP protokolü doğası gereği "güven esaslı" çalışır. Yani bir cihaz "Bu IP benim" dediğinde sorgulayan cihaz buna inanır. Bu durum siber güvenlikte **ARP Spoofing** (ARP Zehirlemesi) dediğimiz, saldırganın kendisini "Gateway" veya "Hedef Cihaz" gibi tanıtmasına olanak sağlayan bir zafiyete yol açar.



DHCP (Dynamic Host Configuration Protocol)

Ağdaki cihazların birbirleriyle iletişim kurabilmesi için bir IP adresine ihtiyaçları vardır. Bu adresler iki şekilde atanabilir: **Statik** (el ile manuel giriş) veya **Dinamik** (otomatik atama). Günümüzde evlerden devasa şirket ağlarına kadar en yaygın kullanılan yöntem, IP adresleme sürecini otomatize eden **DHCP** protokolüdür.

DHCP Nedir?

DHCP, bir ağa dahil olan cihazlara IP adresi, alt ağ maskesi (subnet mask), varsayılan ağ geçidi (default gateway) ve DNS sunucusu gibi kritik yapılandırma bilgilerini otomatik olarak dağıtan bir servistir. Bu sayede her yeni cihaz için manuel ayar yapma zahmetinden ve "IP çakışması" (iki cihazın aynı IP'yi alması) riskinden kurtulmuş oluruz.

DHCP DORA Süreci (Dört Adımda Bağlantı)

Bir cihaz ağa bağlandığında, DHCP sunucusu ile arasında gerçekleşen bu "pazarlık" süreci teknik olarak 4 ana adımdan oluşur. Akılda kalması için buna baş harflerinden dolayı **DORA** süreci denir:

1. DHCP Discover (Keşif)

Cihaz ağa ilk girdiğinde henüz bir IP'si yoktur. Bu yüzden ağdaki tüm cihazlara bir **Broadcast** (yayın) paketi göndererek "Burada bana IP verebilecek bir DHCP sunucusu var mı?" diye bağırır.

- **İşlem:** İstemci -> Sunucu (Yayın)

2. DHCP Offer (Teklif)

Ağdaki DHCP sunucusu bu çağrıyı alır ve elindeki havuzdan (pool) boşta olan bir IP adresini seçer. Bu adresi ve diğer ağ bilgilerini içeren bir teklif paketini istemciye gönderir.

- **İşlem:** Sunucu -> İstemci (Teklif)

3. DHCP Request (İstek)

İstemci, gelen teklifi (veya birden fazla sunucu varsa gelen tekliflerden birini) kabul ettiğini belirtmek için sunucuya bir onay mesajı gönderir: "Tamam, bana sunduğun bu IP adresini kullanmak istiyorum, lütfen benim için rezerve et."

- **İşlem:** İstemci -> Sunucu (İstek)

4. DHCP ACK (Onay / Acknowledgment)

Son aşamada sunucu, IP adresinin o cihaz için kaydedildiğini onaylar. "Anlaşıldı, bu IP artık senindir, süresi bitene kadar kullanabilirsin" der. Bu mesajdan sonra cihaz artık ağda aktif olarak iletişim kurmaya başlar.

- **İşlem:** Sunucu -> İstemci (Kesin Onay)

Teknik Özet Tablosu

Adım	Mesaj Tipi	Kimden Kime	Amacı
Discover	Broadcast	İstemci -> Tümü	Sunucu arama.
Offer	Unicast/Broadcast	Sunucu -> İstemci	IP adresi önerme.

Adım	Mesaj Tipi	Kimden Kime	Amacı
Request	Broadcast	İstemci -> Sunucu	Teklifi kabul etme.
ACK	Unicast/Broadcast	Sunucu -> İstemci	İşlemi tamamlama ve onay.

Neden Önemli?

Siber güvenlik perspektifinden bakarsak; **DHCP Starvation** (DHCP Aç bırakma) saldırılarıyla saldırganlar sunucudaki tüm IP'leri tüketebilir veya **Rogue DHCP** (Sahte DHCP) sunucusu kurarak ağdaki kurbanlara kendi kontrolündeki (yanlış gateway veya DNS içeren) IP bilgilerini dağıtabilirler. Bu yüzden bu 4 adımın nasıl çalıştığını bilmek, ağ güvenliğini anlamak için temeldir.