T.C.

AKSARAY ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ

SİBER GÜVENLİK

Öğretim Üyesi:

Doç.Dr. Bilal ŞENOL

Hazırlayan:

Sultan KARAPINAR - 220211204

İÇİNDEKİLER

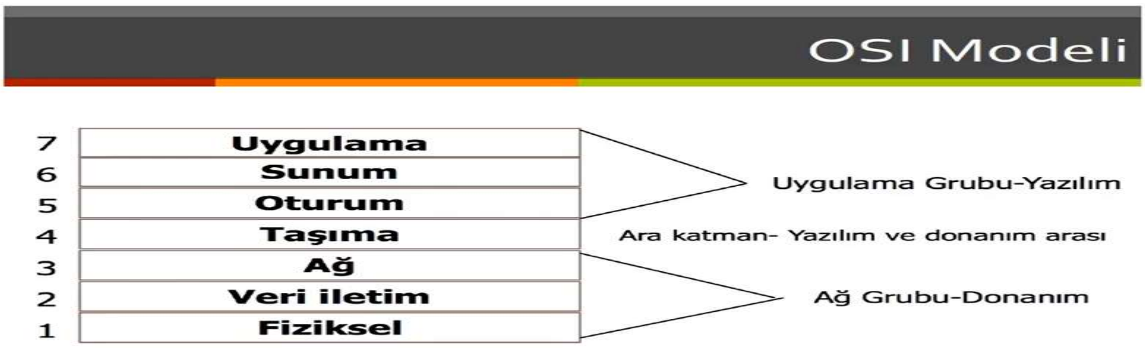
OSI Modeli

Ağların temel amacı cihazların birbiri ile veri paylaşabilmesini sağlayabilmek. Bunun için ağ üzerindeki tüm yapıların ortak bir "protokol" ile iletişim kurabiliyor olması gerek.

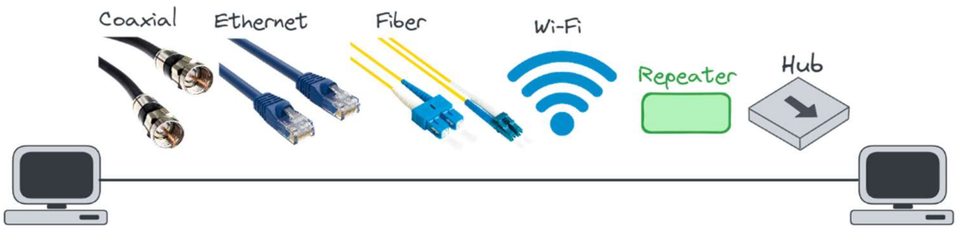
Burada bahsi geçen "**protokol**" kelimesi aslında "**ortak iletişim yöntemi**"ni temsil eden bir kavram. Gerçek dünyadan bir örnek verecek olursak, iki insanın birbiri ile iletişim kurabilmesi için her ikisinin de aynı dili biliyor olması gerek. Örneğin ben Türkçe konuştuğumda karşı tarafın beni anlaması için onun da Türkçe bilmesi gerek. Çünkü Türkçe'nin kendi içinde pek çok kuralı var. Bu kuralları bilmeyen kişiler bu dili anlayıp iletişime dahil olamazlar. Bu örnekteki protokol, karşılıklı olarak iletişim kurmamızı sağlayan Türkçe dilidir. Bu dili bilen herkes birbiri ile haberleşebilir.

Söz konusu "ağ" olduğunda da, benzer şekilde cihazların birbiri ile iletişim kurabilmesi için takip etmesi gereken kurallar yani çeşitli protokoller vardır. Bunlar da "**OSI Model**" olarak tek bir çatı altında toplanıp standart kabul edilmiş kurallardır. Bu kuralları kabul eden ve uygulayan tüm cihazları birbiri ile haberleştirmek mümkün. Yani örneğin Windows sistemi ile Linux sistemi birbiri ile haberleşebilir ya da X marka bir ağ kartı Y marka bir ağ kartıyla veri alışverişinde bulunabilir. Çünkü OSI modeline uyan tüm cihazlar iletişim için gereken kuralları bilir ve protokole uygun hareket ederler.

OSI modelinde 7 katman bulunuyor. Bu katmanların her biri veri iletişimi sürecindeki belirli görevleri ve kuralları tanımlıyor.



Layer 1 – Physical(Fiziksel Katman)

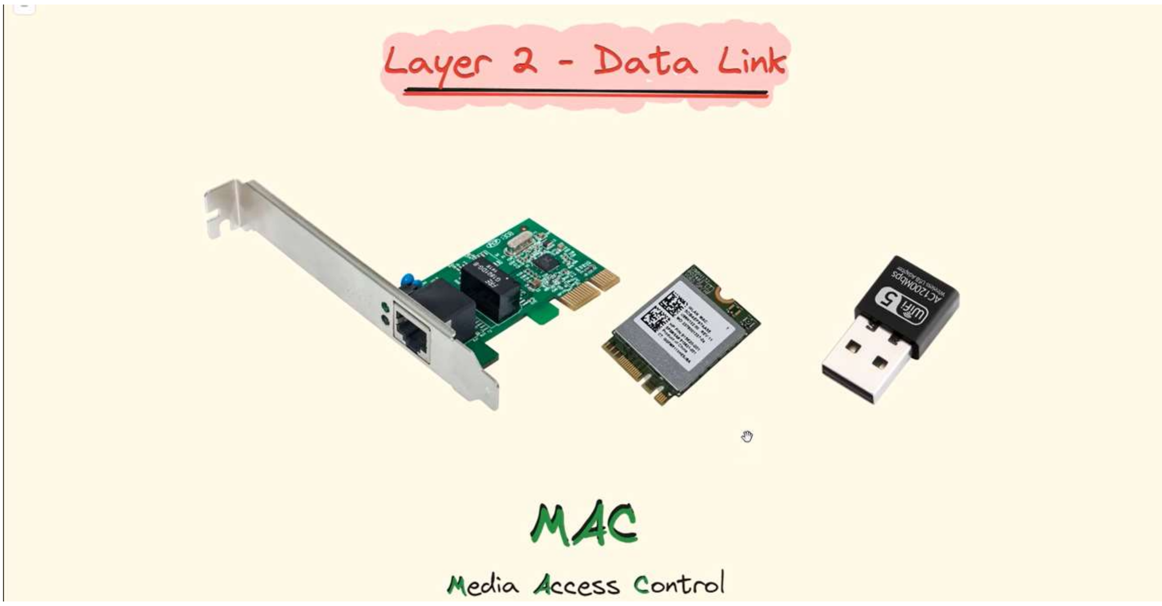


İlk katman fiziksel katmandır ve verilerin bitler halinde yani 0 ve 1'ler ile fiziksel hat üzerinden taşınmasını sağlar. Ethernet, coaxial, fiber, wi-fi gibi kanallar aracılığı ile veriler kablolu veya kablosuz şekilde taşınabiliyor. Bu katmandaki amaç verilerin hat boyunca taşınmasını sağlamak.

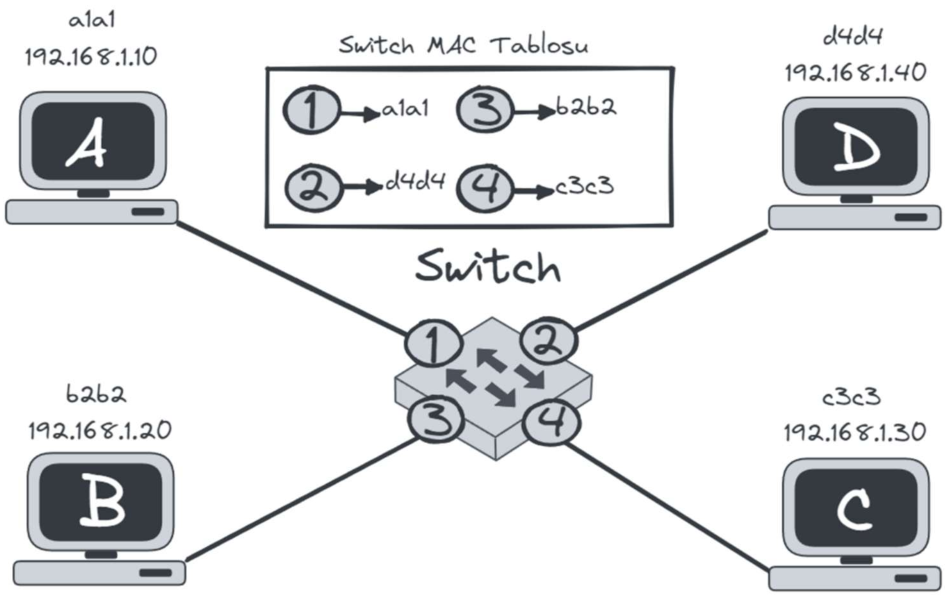
Ayrıca bunlar dışında örneğin sinyalleri tekrarlayarak hat üzerinde daha uzak noktalara iletilmesini sağlayan "repeater" cihazları da bu katmanda sayılabilir. Çünkü repeater cihazının tek yaptığı, aldığı veri sinyallerini tekrarlamaktır.

Hatta Hub olarak geçen cihazlar da aslında fiziksel(layer 1) katmandadır çünkü bağlı bulunan hostlar arasında ayrım yapmadan verileri tüm hostlara aynı şekilde iletiyor. Bu bağlamda sıradan bir ethernet kablodan farkı yoktur çünkü herhangi bir ayrım yapmadan bağlı bulunan tüm uç noktalara veriyi iletir.

Layer 2 - Data Link (Veri İletimi)



Data link katmanı, ilk katman olan fiziksel katman ile iletişime geçilmesini sağlar. Bu katmanda kablolu bağlantı için kullanılan NIC(network interfaces card) ya da kablosuz bağlantı için kullanılan “wi-fi access card” aygıtları bulunuyor. Bu aygıtlar fiziksel katmandan taşınmış olan bitleri alıyorlar ve benzer şekilde bir cihazın ürettiği bitleri de fiziksel katmana iletiyorlar.



Bu katmandaki her bir cihazın yani ağ kartlarının her birinin, benzersiz kimlikleri olan **MAC** adresleri vardır. Mac adresi, “**M**edia **A**ccess **C**ontrol” ifadesinin kısaltmasından geliyor. Ağa bağlanmak isteyen tüm cihazların ağ kartı olması gerektiği için. Ağ kartlarındaki bu MAC adresi yani bu kimlik sayesinde ağa bağlı olan tüm cihazları birbirinden ayırabiliyoruz. Tıpkı IP adresleri gibi fakat bu MAC adresleri, cihaz üreticileri tarafından aygıtlara tek seferliğine tanımlanan benzersiz bir kimliktir.

Örnek adres göstermemiz gerekirse, **MAC** adresi “**00-B0-D0-63-C2-26**” şekilde gözüküyor.

Fiziksel katmandan gelen verilerin doğru hedeflere iletilebilmesi için de MAC adresi bulunması zorunludur. Çünkü fiziksel katmandaki veriler bu MAC adres bilgisine göre doğru ağ kartına yönlendiriliyor.

Örneğin switch aygıtları her bir portuna bağlı olan hostun MAC adresinin bilgisini tutar ve bu bilgiye göre yönlendirme yapar. Bu sebeple Switch aygıtları da aslında fiziksel katmandan gelen verileri, MAC bilgisi sayesinde doğru adrese yönlendiren 2. katmandaki yani “data link” katmanındaki bir cihazdır.

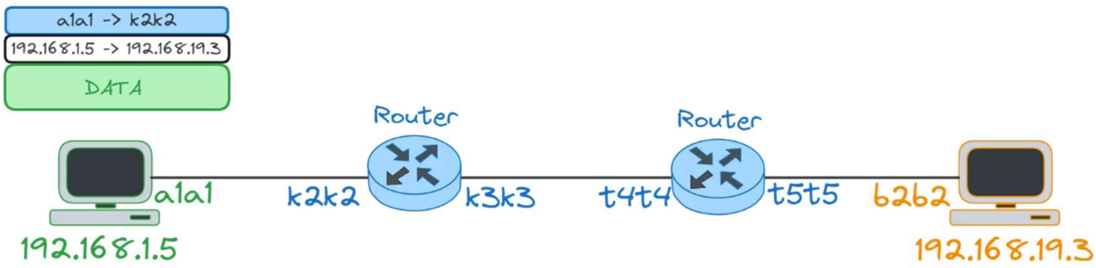
Genellikle lokal ağımız dışında diğer ağlardaki cihazlar ile iletişime geçmek istediğimizde, karşılıklı iletişimi birden fazla router aygıtı üzerinden geçerek gerçekleştiriyoruz. Genellikle bu aradaki cihazlar da router aygıtları oluyor. Zaten Router ayıtlarının birden fazla ağı birbirine bağlar. Router aygıtları da ağlara bağlanırken NIC yani ağ kartları kullandığı ve her bir ağ kartının da benzersiz bir MAC adresi olduğu için aslında veriler fiziksel kanaldan MAC adresleri yardımıyla bir ağ kartından bir diğerine adım adım aktarılıyor.

MAC yardımıyla 2. katman olan "Data Link" katmanında, aslında bir ağ kartından bir diğerine fiziksel katman aracılığı ile veri iletilmesi mümkün oluyor.

İlgili paketin uzaktaki hedefine ulaşabilmesi için, yani uçtan uça veri alışverişininsürdürülebilmesi için de **3. katman** olan "**Network**" katmanına ihtiyacımız var.

Layer 3 – Network(Ağ)

"Network" yani "Ağ" katmanının ana işlevi, veri paketlerini kaynak cihazdan hedef cihaza ulaştırmak ve farklı ağlardan geçerken yönlendirme yapmaktır. Hedef belirtme ve yönlendirme işlemleri de, her bir cihazın sahip olduğu IP adresi sayesinde mümkün oluyor.



Daha iyi anlamak için birbirinden farklı iki ağdaki cihazların veri alışverişinde bulunmak istediğini düşünelim. Yönlendirme işinden routerlar sorumlu olduğu için biz hedef IP adresini belirtip, bizim ağımıza bağlı bulunan routera bu paketi iletiyoruz. Router da bağlı olduğu ağlardan uygun olanlara bu paketi iletip, ilgili IP adresine sahip hosta bu paketin ulaşmasını sağlıyor. Nasıl olduğunu adım adım ele alalım:

- Öncelikle, kaynak ve hedef IP adresleri pakete eklendi. Ayrıca bu paketi uygun yere yönlendirebilmesi için router cihazının MAC adresi de hedef adres olarak eklendi.

- Bu paket routera geldiğinde router alıp inceliyor ve hedef IP adresinin kendisine bağlı olan bir ağda olup olmadığını kontrol ediyor.

- Kendisine bağlı bir ağda bu IP adresine sahip cihaz olmadığı için bunu, bağlı olduğu diğer router cihazına, MAC adresi yardımıyla yönlendiriyor.

- Bu paket ikinci router cihazına geldiğinde router hedef IP adresini kontrol ediyor

- Hedef IP adresinin, bağlı olduğu ağdaki bir hosta ait olduğunu öğrendiğinde bu hosta bu paketi iletmek için hedef MAC adresi olarak bu hostun MAC adresini ekleyip gönderiyor.

- Bu paketi alan host, paketin göndericisini ve hedefini kontrol ediyor. Bu sayede paketin kendisi için olup olmadığını ve yanıt vermek istediğinde yanıtını hangi IP adresine göndermesi gerektiğini öğrenmiş oluyor.

- IP adresi kendisine ait olduğu için bu paketi kabul edip, içeriğini yani DATA kısmını okuyor.

Böylelikle farklı ağlardaki iki hostun iletişim kurması mümkün oluyor.

Adım adım ele aldığımız gibi; bağlı bulunan ağlarda IP eşleşmesi olmadığı sürece routerlar MAC adresleri sayesinde ilgili paketin, kendilerine bağlı bulunan bir sonraki noktaya yönlendirilmesini sağlıyor. En son router da hedef IP adresindeki hostun kendi ağında olduğunu bildiği için bu hosta, MAC adresi sayesinde bu paketi ulaştırıyor.

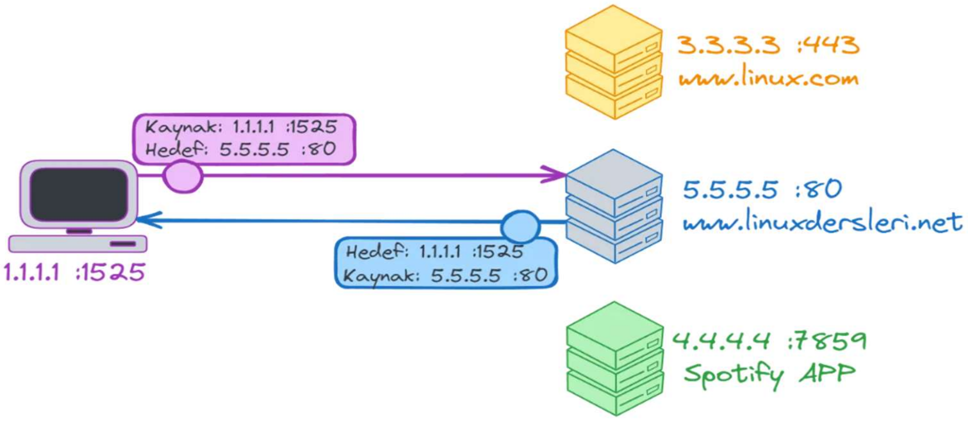
Özetle MAC adresleri birbirine bağlı bulunan ağ kartları arasındaki iletişim ve aktarım için kullanılıyorken, IP adresi ağların ve ağlardaki hostların tanınması için yani uçtan uça aktarım için kullanılıyor.

Burada router cihazlarının IP ile MAC adresini eşleştirebilmesini sağlayan "**ARP**" isimli bir protokol bulunuyor. Bu protokol sayesinde IP ve MAC bilgisi elde edilip, routerların kendi tablosuna bu bilgiler ekleniyor. Bu sayede routerlar, hangi IP adreslerinin hangi MAC ile eşleştiğini bilip buna göre yönlendirme yapabiliyor.

Layer 4 – Transport(Aktarma)

Şimdiye kadar ele aldığımız anlatımlarda, verilerin tek bir hat üzerinden iletildiğini gördük. Peki ama tüm veriler tek bir hat üzerinden iletiliyorken, doğru programın doğru paketi aldığından nasıl emin olabiliyoruz ?

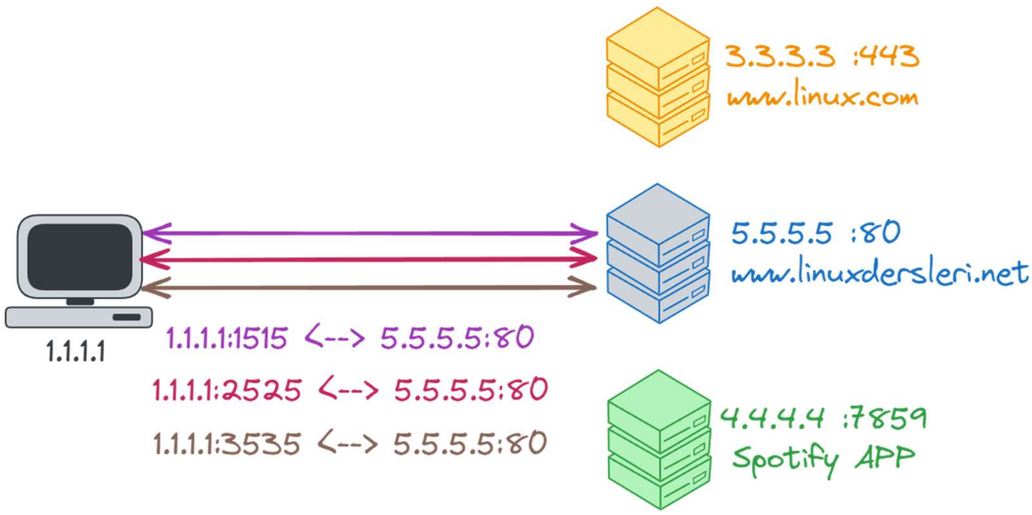
Örneğin ben web tarayıcısı, discord ve spotify gibi internet bağlantısını gerektiren uygulamaları aynı anda kullanabiliyorum. Bu uygulamaların sorunsuzca veri alışverişinde bulunması için doğru paketlerin doğru araca iletilmesi gerek. Bu da "adresleme şeması" ya da doğrudan "**port**" olarak ifade edilen bir yaklaşım sayesinde mümkün oluyor.



Her bir aracın kendisine ait bir port numarası bulunuyor. Bu sayede veriler bu portlar aracılığı ile yalnızca ilgili olan araçlara iletilebiliyor. Yani tek bir hat üzerinden geliyor olsa da veriler birbirinden izole şekilde, yalnızca doğru portlara iletiliyor.

Servislerle iletişim kurulurken gönderici, rastgele bir port üzerinden veri gönderip yine aynı port üzerinden veri alabiliyor. Örneğin bir websitesini ziyaret etmek istediğinizde aşağıdaki gibi IP ve port numaraları üzerinden iletişim kuruyorsunuz.

Örneğin web tarayıcısını kullandığınızda açtığınız her yeni sekme aslında rastgele farklı bir port üzerinden ilgili servislere haberleşecek. Bu sayede farklı sekmelerdeki veriler birbirinden izole şekilde doğru sekmeye iletilebiliyor. Ben farklı sekmelerde aynı websitesini ziyaret edecek olursam aşağıdaki gibi bir iletişim söz konusu olacak.



Rastgele tanımlanan port numaraları haricinde çeşitli servisler için kullanılan bazı standart portlar vardır. Örneğin birkaç tanesi aşağıdaki gibidir:

- HTTP: 80
- HTTPS: 443

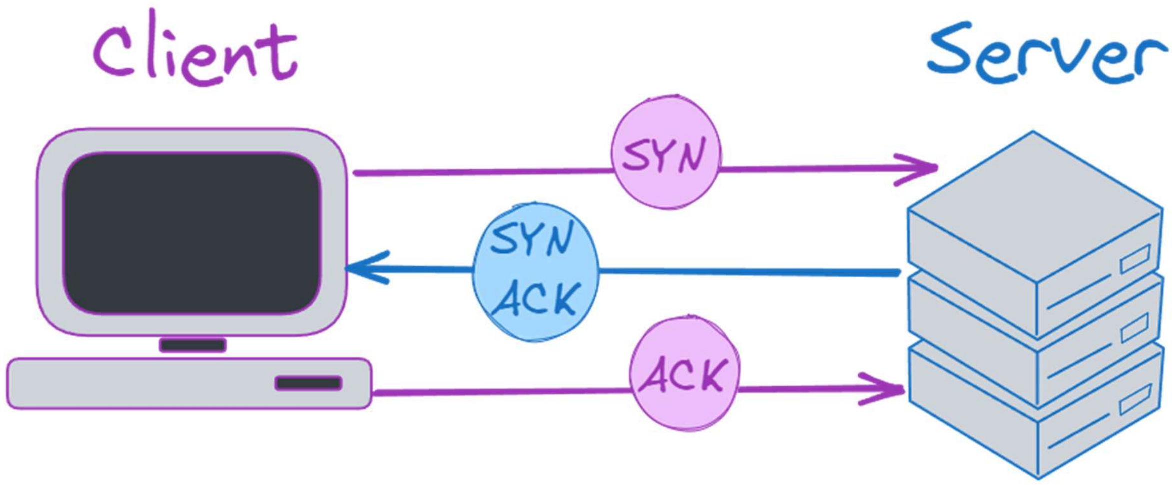
- FTP (File Transfer Protocol): 21
- SSH (Secure Shell): 22
- Telnet: 23
- SMTP (Simple Mail Transfer Protocol): 25

Bunlar sadece birkaç örnek. Birçok farklı servis, protokol ve uygulama kendi standart port numaralarını kullanabiliyor. Bu sayede standart konfigürasyonlar için başvurulacak standart bir adres oluyor. Örneğin web içeriklerini almak istediğimizde http protokolü için ilgili IP adresinin 80 numaralı portuna istekte bulunuyoruz. Eğer web içeriklerinin şifreli şekilde iletilmesini istiyorsak da bu kez https protokolü için 443 portundan ilgili IP adresiyle iletişime geçiyoruz. Özetle port numaraları taşıma katmanında doğru paketin doğru adrese iletilmesi için çok önemlidir.

Üstelik transport yani taşıma katmanında yalnızca port numarası değil, verinin ne şekilde taşınacağı da önemli. Veri taşıma için TCP ve UDP olmak üzere iki temel alternatif yöntem bulunuyor.

TCP

TCP, "**T**ransmission **C**ontrol **P**rotocol" ifadesinin kısaltmasından geliyor ve isminde de olduğu şekilde veri iletimini kontrollü bir şekilde gerçekleştiriyor. TCP, bağlantı temelli(connection oriented) bir protokoldür. Yani veri paketlerini göndermeden önce, alıcının bu paketleri almaya hazır olduğunu kontrol etmek için öncelikle alıcı ile bağlantı gerçekleştirir. Bu yaklaşım, verilerin iletim sırasında kaybolmamasını, sırasının bozulmamasını ve doğru bir şekilde ulaşmasını sağlar.



Alıcı ile bağlantı kurulmasına da üçlü el sıkışma(Three-Way Handshake) deniyor.

Örneğin bir veri paketi TCP ile taşınacaksa öncelikle hedef sunucuya senkronizasyon için **SYN**(**Syn**chronize**)** isimli bir kontrol paketi gönderilir.

Hedef sunucu bu **SYN** paketini alırsa, yanıt olarak istemciye onay yani **SYN-ACK(Acknowledgment)** paketi ile bağlantı kurmaya hazır olduğunu bildirir.

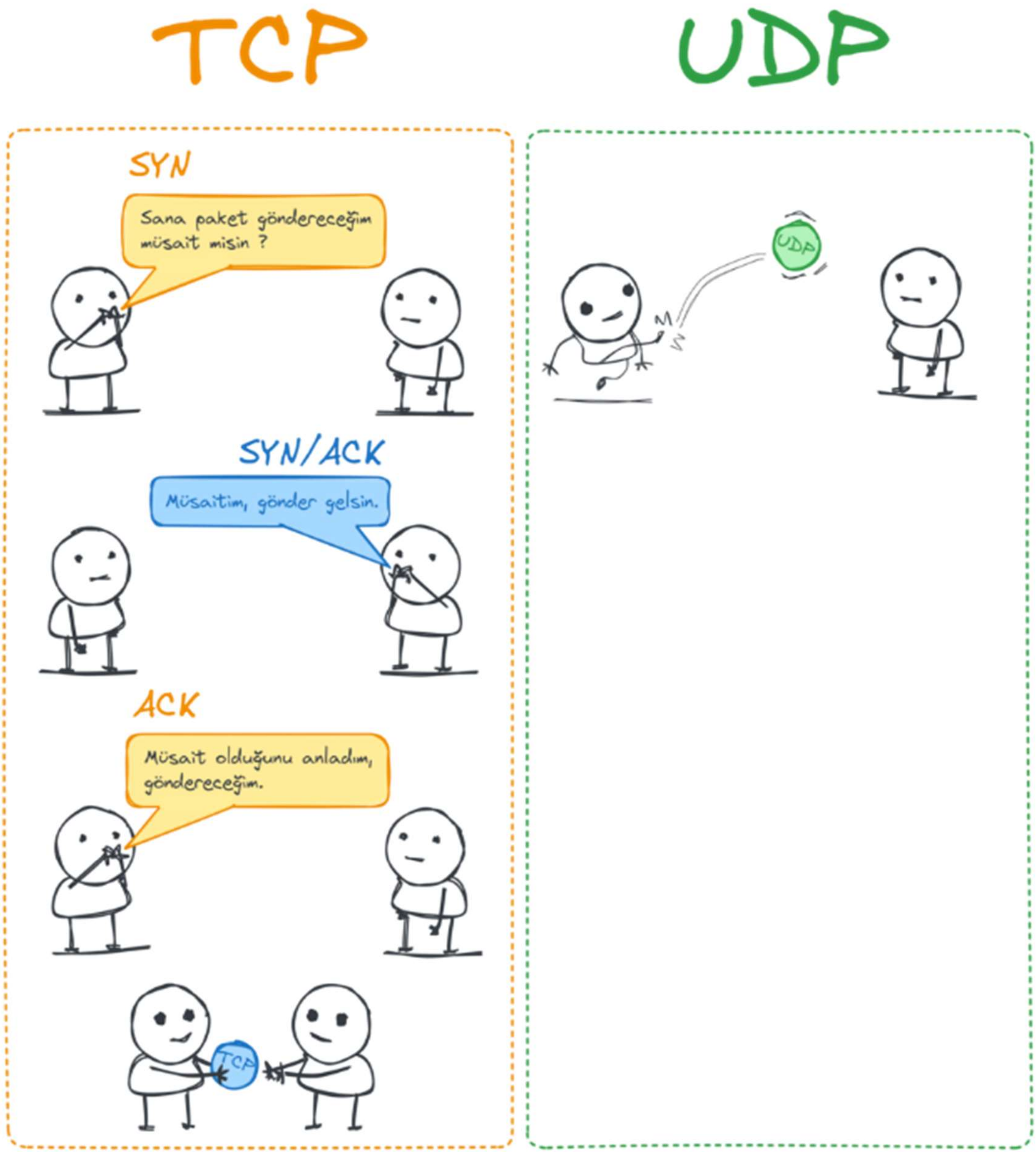
İstemci, hedef sunucunun SYN-ACK paketini aldığında bu bağlantıyı **ACK** onaylar ve her ikisi de gerçek veri aktarımını başlatacakları güvenilir bir bağlantı kurar.

Daha sonra veri paketleri hedefe gönderilir. Ayrıca veri iletimi sırasında, gönderilen veri paketleri kaybolabilir, gecikebilir veya bozulabilir. Ancak TCP, bu tür sorunlarla başa çıkmak için hata kontrolü ve eksik veya bozulmuş verinin yeniden iletilmesi gibi mekanizmalara sahiptir. Bu sayede, güvenilir ve düzenli veri iletimi sağlanır. Bu yaklaşımı sebebiyle TCP, veri bütünlüğünün önemli olduğu durumlarda eksiksiz iletim için kullanılıyor. Örneğin e-posta, websitesi içeriğinin alınması, veya dosya indirme gibi tüm verilerin eksiksiz iletiminin şart olduğu durumlarda TCP kullanılıyor.

UDP

UDP, "**U**ser **D**atagram **P**rotocol" ifadesinin kısaltmasından geliyor. Bu iletim protokolü TCP gibi bağlantı tabanlı değildir. Yani verileri göndermeden önce alıcı ile bağlantı kurup alıcıyı kontrol etmez. Veri paketlerini doğrudan gönderir. Bu sayede çok daha hızlı veri transferi mümkündür fakat, tüm verilerin hedefe ulaşıp ulaşmayacağı garanti edilmez. Çünkü verilerin ulaşıp ulaşmadığına dair bir kontrol mekanizması yoktur. Bu sebeple, hız gerektiren ama veri bütünlüğü veya doğruluğunun önemsiz olduğu durumlarda tercih edilir. Örneğin sesli ve görüntülü iletişim, video oyunları ve yayın hizmetleri gibi alanlarda sıkça kullanılır. Zaten özellikle görüntülü ve sesli iletişim uygulamalarını kullanırken, ara sıra kesintiler olduğuna bizzat şahit olmuşsunuzdur. UDP tüm paketlerin hedefe ulaşmasını garanti etmediği için arada paket kayıpları yaşanması olağandır. Fakat getirdiği hız dolayısıyla bu tür uygulamalarda verilerin taşınması için kullanılması da kaçınılmazdır.

Kısacası, TCP güvenilir veri iletimini sağlarken, UDP hızlı ancak veri bütünlüğü konusunda daha az güvenilir bir iletim sağlıyor.



Layer5-Session (Oturum Katmanı)

Oturum katmanında iki bilgisayardaki uygulama arasındaki bağlantının yapılması, kullanılması ve bitilmesi işlemleri yapılır. Bir bilgisayar birden fazla bilgisayarlarla aynı anda iletişim içinde olduğunda, gerektiğinde doğru bilgisayarla konuşabilmesini sağlar. Bu, sunum katmanına yollanacak veriler farklı oturumlarla birbirinden ayrılarak yapılır. NetBIOS, RPC, Named Pipes ve Sockets gibi protokoller bu katmanda çalışır.

NetBIOS (Ağ Temel Giriş/Çıkış Sistemi)

NetBIOS, 1980'lerde geliştirilmiş bir API'dir (Uygulama Programlama Arayüzü) ve ağ üzerinde bilgisayarların iletişim kurmasını sağlar.

Amaç : Bilgisayarların reklamlarını çözmek, mesajı saklamak ve oturum yönetimini sağlamak.

Reklam Hizmetleri : Bilgisayarların reklamlarını IP adreslerine çevirir.

Oturum Hizmetleri : İki bilgisayar arasında oturum açılır ve yönetilir.

Datagram Hizmetleri : Bağlantısız veri iletişimini sağlar.

Kullanım Alanı : Yerel ağlarda (LAN) dosya ve yazıcı paylaşımı gibi işlemler.

Dezavantajları : Modern protokollere kıyasla sınırlı bir kapsama alanı vardır ve güvenlik riskleri taşır.

RPC (Uzaktan Prosedür Çağrısı)

RPC, bir programın ağ üzerinde başka bir bilgisayarda çalıştırılan bir prosedürü çağırmasına olanak tanır. Bu, prosedürün yerel bir çağrı gibi görünmesini sağlar.

Amaç : Farklı sistemler arasında fonksiyon çağrıları yaparak dağıtılmış bir yapı sağlamaktır.

İstemci, uzak sistemdeki bir fonksiyonu çağırır.RPC çıktısı bu isteği sunucuya iletir.Sunucu işleminin ve sonucunun değiştirilmesine döner.

Kullanım Alanı : Mikroservis mimarilerinde, Windows ve Unix tabanlı sistemlerde hizmet çağrıları için kullanılır.

Named Pipes

Named Pipes, iki işlem arasında veri alışverişini sağlayan bir mekanizmadır. Aynı sistem ya da dağ üzerinden farklı sistemler arasında çalışabilir.

Bir işlem "Pipe" oluşturur ve diğer işlem bu "Pipe" ile veri alışverişi yapar.

Adlandırılmış olması, farklı oranların arasında kullanılabilmesini sağlar.

Kullanım Alanı : Windows ve Unix sistemlerinde, özellikle yazıcı-sunucu uygulamaları.

Örnek : SQL Server, çıktı-sunucu arasındaki iletişimde Named Pipes kullanabilir.

Soketler

Soketler, iki cihaz arasında ağ üzerinden veri alışverişi sağlayan bir API'dir. Modern internet protokollerinin yapılandırılmasını sağlar.

Amaç : İstemci ve sunucu arasında veri elde etmek.

Çalışma Prensibi :

Bir cihaz, bir "soket" oluşturur ve bir porta kemeridir.

Diğer cihaz bu porta bağlanarak iletişim kurulur.

Veri alışverişi, TCP veya UDP gibi protokollerle yapılır.

Kullanım Alanı : Web uygulamaları, anlık mesajlaşma sistemleri, oyun sunucuları.

Layer 6- Presentation (Sunum)

Sunum katmanının en önemli görevi yollanan verinin karşı bilgisayar tarafından anlaşılacak şekilde çevrilmesidir. Bu sayede farklı programların birbirlerinin verisini kullanabilmesi mümkün olur. Sunum katmanı uygulama katmanına verileri yollar daha sonra bu katmanda verinin yapısı, biçimi ile ilgili düzenlemeler yapılır, verinin formatı belirlenir. Ayrıca verinin şifrelenmesi, açılması, sıkıştırılması da bu katmanda yapılır. GIF, JPEG, TIFF, EBCDIC, ASCII vb. bu katmanda çalışır.

- **GIF** : Az renk kullanan basit animasyonlar ve şeffaf görüntüler için kullanılan bir resim formatıdır.
- **JPEG** : Fotoğrafları kaybolan sıkıştırmayla depolayan yaygın resim formatıdır.
- **TIFF** : Yüksek kaliteli, kayıpsız görüntülerin saklanması için kullanılan profesyonel bir resim formatıdır.
- **EBCDIC** : IBM sistemlerinde kullanılan, karakterleri 8-bit kodlarla temsil eden bir sertifikalı standarttır.
- **ASCII** : Metin ve sembolleri temsil etmek için kullanılan, bilgisayarların anlayabileceği 7-bit bir karakter yazma sistemidir.

Layer 7 - Application (Uygulama)

Uygulama katmanı bilgisayar uygulaması ile ağ arasında bir arabirim sağlar. OSI katmanları arasında sadece bu katman diğer katmanlara servis sağlamaz.

Uygulamaların ağ üzerinde çalışması sağlanır.
Uygulama katmanı ağ servisini kullanacak olan programdır. Bu katman kullanıcıların gereksinimini karşılar. SSH, telnet, FTP, TFTP, SMTP, SNMP, HTTP, DNS protokolleri ve tarayıcılar bu katmanda çalışır.
E-posta ve veritabanı gibi uygulamalar bu katman aracılığıyla yapılır.

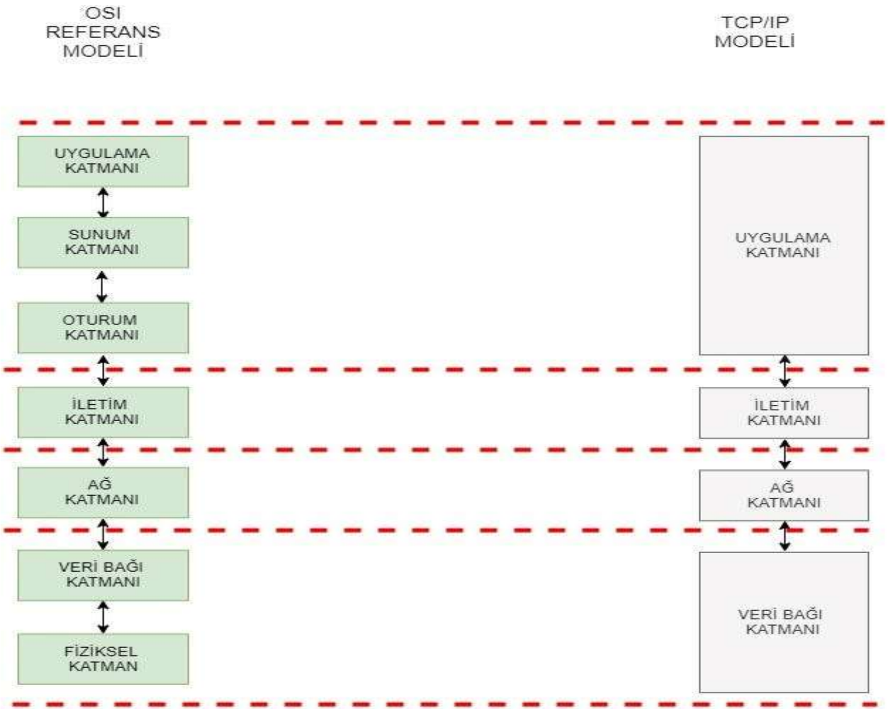
- **SSH** : Güvenli bir şekilde bir cihaza bağlanmak ve komut çalıştırmak için kullanılan şifreli bir protokoldür.
- **Telnet** : Şifreleme olmadan bir cihaza bağlanmak için kullanılan eski bir protokoldür.
- **FTP** : Dosya aktarımı yapmak için kullanılan, orijinalliği düzenli bir protokoldür.
- **TFTP** : Basit ve güvenliksiz bir şekilde dosya aktarımı sağlayan hafif bir protokoldür.
- **SMTP** : E-posta gönderimi için kullanılan standart protokoldür.
- **SNMP** : Ağ cihazlarını izlemek ve yönetmek için kullanılan bir protokoldür.
- **HTTP** : Web sayfalarının tarayıcıda görüntülenmesi için kullanılan protokoldür.
- **DNS** : Alan adlarını IP adreslerine çeviren bir isim çözümleme protokolüdür.

Şimdiye kadar ele aldığımız OSI modelinde, ağ ile ilgili uygulamaların iletişimi üç farklı katmanda ele alınıyor.

Fakat günümüzde daha yaygın kullanımda olan **TCP/IP** isimli ağ modelinde ise tüm bu katmanlar **Application** katmanı altında tek bir katmanda ele alınıyor.

Her iki model de aynı temel standartları ifade ediyor olmasına karşın TCP/IP isimli ağ modeli biraz daha sadeleştirilmiş bir temsile sahip. Yoksa OSI ve TCP/IP modellerinin her ikisi de aynı şekilde sorunsuz ağ iletişimi için gereken temel protokollerin tanımlandığı modellerdir.

Ağdaki veri akışını anlamak için önemli olan OSI modelinde **1-4** veya **TCP/IP** modelinde **1-3** katmanlardaki yapılar aslında. Bunun dışındaki katmanlar uygulamaların veri iletimi için kullandığı özel protokollerden ibaret.

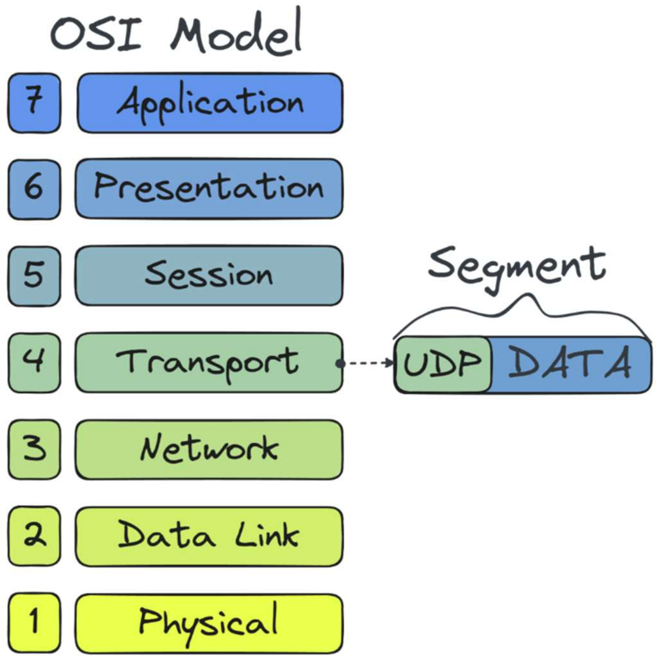


Encapsulation Decapsulation | Kapsülleme Kapsül Açma İşlemleri

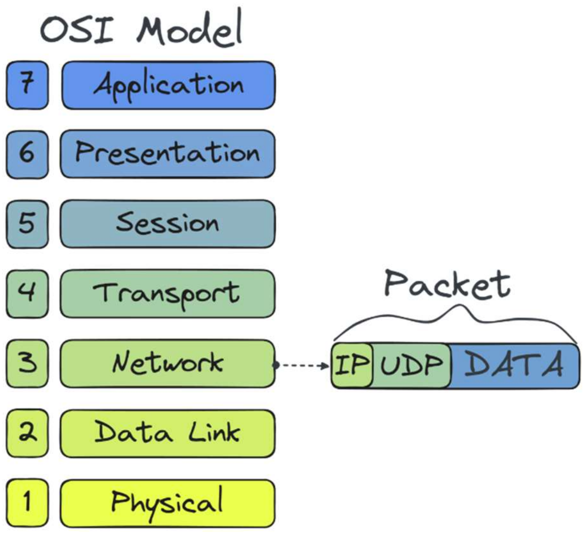
Encapsulation

Uygulama katmanından gönderilen veriler “encapsulation” yani “kapsülleme” denilen bir metotla alt katmanlara iletiliyor.

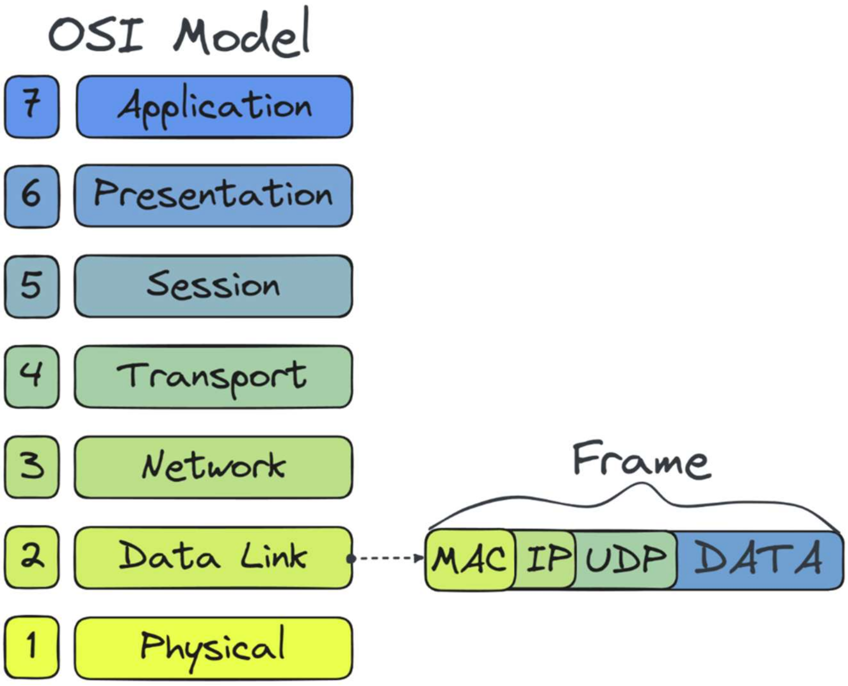
Uygulama katmanından gelen veriye öncelikle hangi taşıma yöntemi ile taşınacağının bilgisi eklenerek bu veri kapsülleniyor. Verinin bu haline de “**Segment**” deniyor.



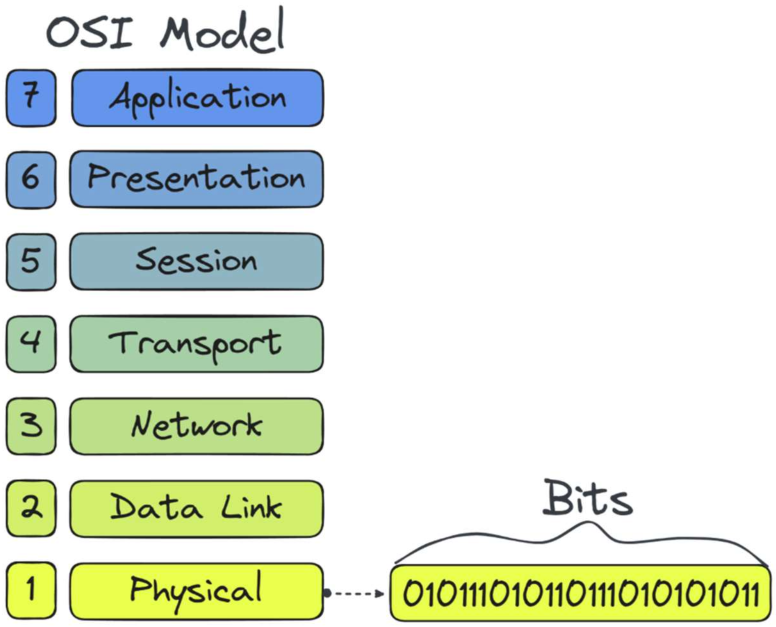
Ağ katmanında gönderici ve alıcı IP adresi ekleniyor. Buna da “**packet**” deniyor.



Data link katmanında da gönderici ve alıcı MAC adresi eklenip hedef cihazın belirtilmesi sağlanıyor. Buna da "**frame**" yani "**çerçeve**" deniyor.



En nihayetinde fiziksel katmanda frame, hat üzerinden iletilmek üzere 0 ve 1'lere dönüştürülüp hat üzerinde hedefe gönderiliyor.



Özetle "encapsulation" yani "kapsülleme" işlemi bu şekilde.

Decapsulation

Alıcı ise aynı işlemleri tersten gerçekleştirerek, kapsülü katman katman açıyor. Buna "**decapsulation**" yani "**kapsülü açma**" deniyor.

Yani 0 ve 1'leri frame haline çevirip data link katmanına gönderiyor.

Buradaki MAC bilgisine bakılarak hangi ağ kartının MAC adresinin hedeflendiği öğreniliyor.

Daha sonra IP adresine bakılarak bu adresin doğruluğu kontrol ediliyor. IP adresi, verinin nereye yönlendirilmesi gerektiğini gösterir. Eğer IP adresi doğruysa, veri taşıma katmanına iletilir.

Taşıma katmanında TCP veya UDP sayesinde verilerin taşınma yöntemi ve hangi porta veri gönderildiği öğrenilip bu porta veri yönlendiriliyor.

Son olarak uygulama katmanı da, kendisine gönderilen veri paketini alıp uygun şekilde işliyor.

İşte kapsülleme ve kapsülü açma işlemi yani ağ üzerinden veri akışı bu şekilde.

Hostlar Nasıl Haberleşir ?

Aynı Ağdaki Cihazlar Nasıl Haberleşir ?

Bir host aynı ağda olduğu bir başka hosta veri göndereceği zaman, hedef hostun IP adresini bilmesinin yanında MAC adresini de bilmek zorunda. Çünkü daha önce ele aldığımız OSI ve TCP/IP modellerinde de bizzat gördüğümüz gibi cihazların IP adresinden önce MAC adresi tanınıyor.

Doğru MAC eşleşmesi olmadan IP adresinin kontrolü de gerçekleşmediği için öncelikle MAC adresi belirtilmeli.

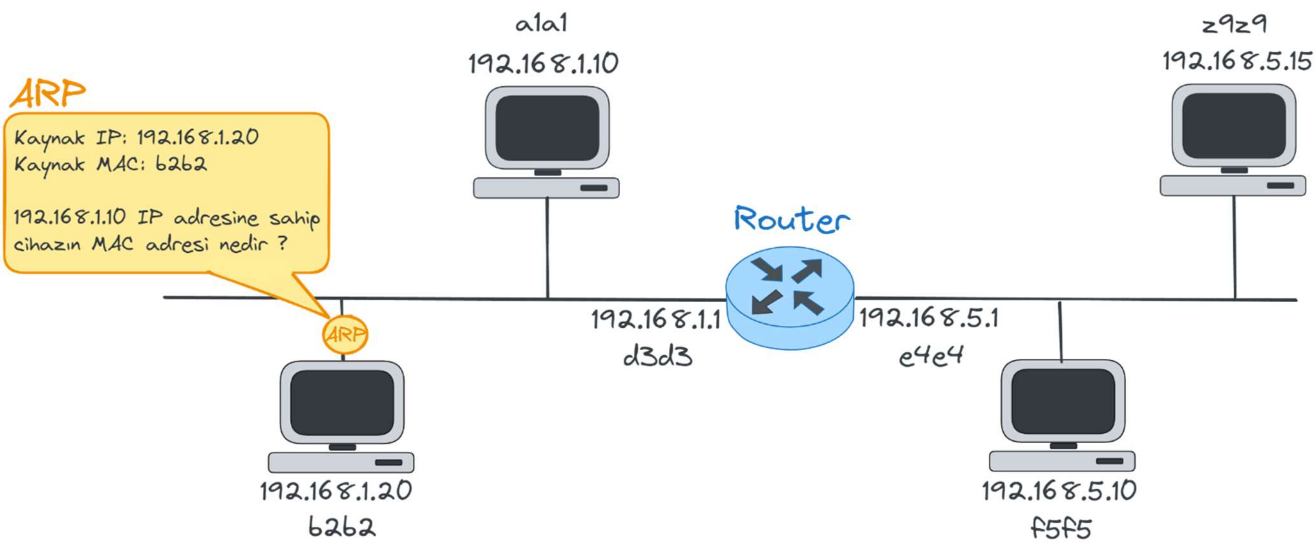
Örneğin ethernet ile birbirine bağlı olan cihazlarda veri iletişimi için öncelikle hedef cihazı temsil eden MAC adresine ihtiyacımız var. Neticede ağ bağlantısı aslında ağ kartı ile gerçekleştiriliyor ve bu ağ kartlarının kimlikleri de benzersiz MAC adresleridir. Dolayısıyla MAC adresini bilmeden verileri doğru makineye iletemeyiz.

Ağ yapısı gereği MAC adresleri donanımlara kalıcı olarak tanımlanmışken, IP adresleri mantıksal olarak tanımlanmış adreslerdir. Dolayısıyla duruma göre zaman içinde aynı cihaza farklı IP adresleri tanımlanabiliyor. Bu sebeple IP adresi ile MAC adreslerini arasında organik bir bağ yoktur. Bizim IP adresini bildiğimiz cihaza veri gönderebilmek için bu cihazın MAC adresini öğrenmemizi sağlayan ARP protokolünü kullanmamız gerek.

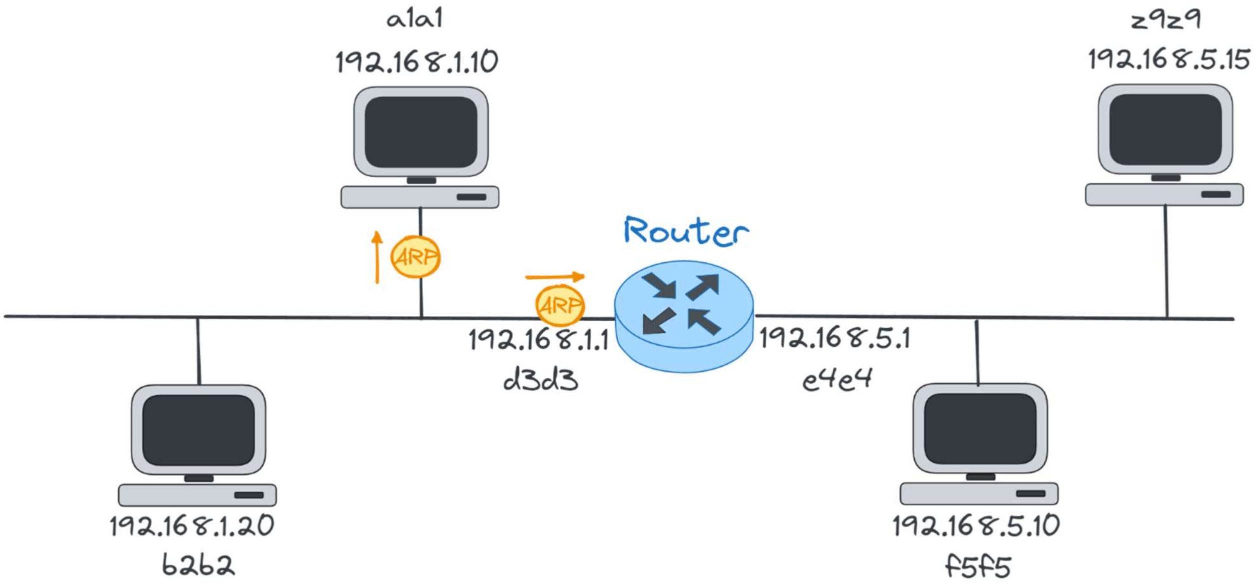
ARP ifadesi "**A**ddress **R**esolution **P**rotocol" yani "adres çözümleme protokolü" ifadesinin kısaltmasından geliyor. Nasıl çalıştığını hemen örnek üzerinden ele alalım.

Aşağıdaki gibi iki LAN ağının birbirine router ile bağlı olduğunu varsayalım.

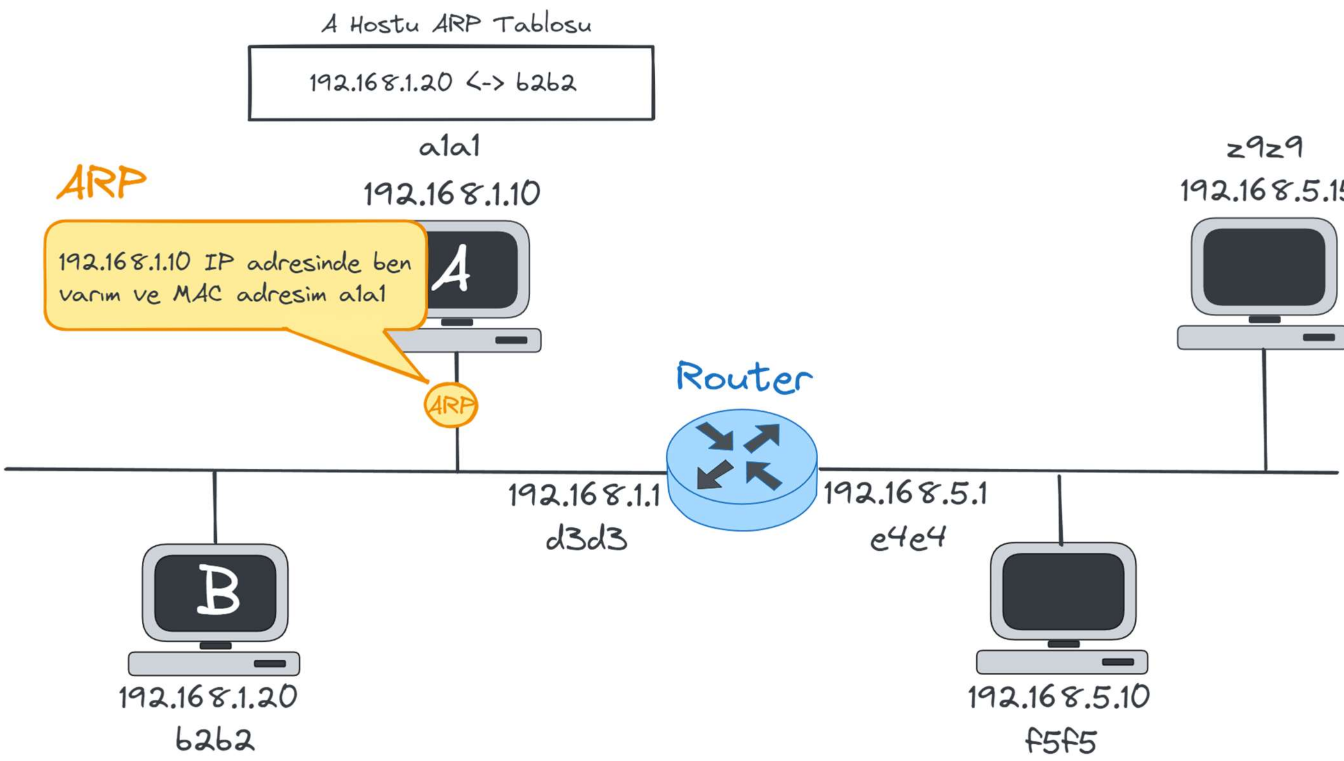
192.168.1.20 IP numaralı host, 192.168.1.10 IP adresli hosta veri göndermek isterse öncelikle bu hostun MAC adresini öğrenmesi gerek. Bunun için ARP broadcast yayını ile herkese bu IP adresinin MAC adresini sorabilir. Bu ARP paketinde da kendi IP ve MAC adresi ve hedef IP adresi yer alır.



Bu ARP sorgusu lokal ağdaki tüm cihazlara gönderilir. Router özellikle konfigüre edilmediği sürece broadcast yayınını diğer ağlara taşımaz. Bu sebeple ARP mesajı yalnızca lokal ağdaki cihazlara ulaştırılır.



ARP mesajını da yalnızca hedefteki IP adresine sahip olan host yanıtlar. Yanıtlama işlemi sırasında da kaynağın IP ve MAC bilgisini öğrendiği için bunları, daha sonra kullanmak üzere kendi ARP tablosuna ekler. Kaynak adresini öğrendiği için de yanıtı doğrudan kaynağa unicast olarak iletir.



ARP yanıtı sayesinde B hostu da, A hostunun IP ve MAC bilgisini kendi ARP tablosuna ekler. Bu sayede artık B hostuna yani 192.168.1.10 IP adresini veri iletmek istediğinde MAC adresini buradan kontrol edip doğrudan o hosta veri iletebiliyor olacak. En yalın haliyle lokal ağdaki bir cihazın MAC adresinin öğrenilmesi bu şekilde gerçekleşiyor.

Tam da bu noktada, “*MAC adresi bilinmeden cihazlara veri gönderilemiyorken nasıl ARP sorgusu gönderilebiliyor?*” diye düşünmüş olabilirsiniz.

ARP gönderilirken broadcast yani tüm cihazları hedefleyerek gönderildiği için hedef MAC adresi olarak da tüm cihazları temsil eden özel bir MAC(FFFF.FFFF.FFFF) adresi kullanılıyor. Bu sayede daha öncesinde MAC adresini bilmeye gerek kalmadan ağdaki tüm cihazlara broadcast yayını ile mesajı göndermek mümkün oluyor.

Farklı Ağdaki Cihazlar Nasıl Haberleşir ?

Bir host harici bir ağdaki host ile iletişime geçmek istediğinde, hedef IP adresine bakarak bu hostun kendi ağına dahil olmadığını biliyor. Çünkü kendi IP adresini ve alt ağ maskesini yani subnet mask değerini biliyor. Bu sayede kendi ağındaki IP aralığını kontrol edip, bu ağın kendi ağındaki bir host olmadığını öğrenebiliyor.

Elbette bu bilgi yeterli değil çünkü hedef cihazın MAC adresinin de bilinmesi gerekiyor. Bu noktada devreye router aygıtının yardımı giriyor. Router bağlı olduğu ağlardaki cihazların IP ve MAC kayıtlarını kendi tablosunda tuttuğu için paketlerin hangi cihazlara gönderilmesi gerektiğini belirleyebiliyor.

Routerlar ağlar arasındaki “gateway”lardır. Bu sebeple her host bağlı olduğu gateway adresini yani routerın bu ağdaki IP adresini biliyor. Bu sebeple eğer iletişime geçeceği IP adresi kendi ağında değilse bu paketi gateway olarak bilinen routera teslim ediyor. Fakat teslim etme işlemi için de elbette ilk olarak bu routerın MAC adresini bilmesi gerek. Çünkü sizin de bildiğiniz gibi yalnızca IP adresi ile veri iletilemez.

Host, Router aygıtının MAC adresini öğrenmek üzere ARP ile bu IP adresinin MAC adresini broadcast şeklinde kendi ağındaki herkese soruyor.

Bu ARP sorgusuna yalnızca hedef IP adresine sahip olan router cevap veriyor. Bu sayede hem router hem de sorgu yapan host birbirilerinin IP ve MAC bilgilerini kendi tablolarına kaydediyorlar.

Artık böylelikle lokal ağ dışındaki bir hosta veri göndermek için bu verileri routera teslim etmemiz gerekiyor. Yani hedef IP olarak harici ağdaki hostun IP adresini belirtiyorken, MAC adresi olarak default gateway olan router aygıtının MAC adresini belirtiyoruz.

Bu sayede bu frame halindeki veri paketi routera ulaştığında router bu frame’i açarak hangi IP adresine gönderildiğini öğreniyor. Bu IP adresi kendisine bağlı olan ağdaysa bunu ilgili adrese iletiyor.

Paketi alan host, gönderici IP adresi olarak diğer ağdaki hostun olduğunu öğrendiği için yanıt verirken benzer yolu izleyerek yanıtı ilgili hosta ulaştırabiliyor.

Router bağlı olduğu ağlardaki cihazların IP ve MAC bilgilerini de ARP ile öğrenip kendi tablosunu tuttuğu için ağlar arasında yönlendirme işlemi gerçekleştirebiliyor. Bu sayede lokal ağımızın dışında bulunan bir ağdaki host ile veri alışverişinde bulunabiliyoruz.

Örneğin geniş ağ olan internet üzerinde başka bir IP adresine paket iletmek istediğinizde, yine kendi ağınızdaki default gateway olarak kullanılan routera bu paketi teslim ediyorsunuz. Default gateway da internet servis sağlayıcınıza bağlı olduğu için ilgili paketin hedefe ulaştırılması bu noktadan sonra onların yönlendirmesine bağlı oluyor. Zaten servis sağlayıcınız da internet ağına bağlı olduğu için ilgili paket internet ağı üzerinden hedefe ulaştırılmış oluyor.

DNS - Domain Name System

“Server” yani “sunucu” olarak isimlendirdiğimiz cihazların aslında içerisinde gerekli hizmeti sunabilecek yazılımlar kurulu sıradan bilgisayarlar olduğunu biliyorsunuz. Örneğin HTTP isteklerine yanıt vermek için gereken yazılımları bir bilgisayara kurup bu bilgisayarı websitemizi sunması için internete açtığımızda, websitemizi ziyaret etmek isteyen istemciler bu bilgisayara HTTP isteği gönderiyor olacaklar. Bu durumda websitesinin dosyalarını isteyen taraf client iken, bu dosyaları HTTP vasıtası ile istemcilere ileten ise server yani sunucu olacaktır.

Dolayısıyla aslında sunucular da IP adresine sahip olan birer host cihazlarıdır. Host cihazlarının birbiri ile iletişim kurmak için IP adreslerini kullandığını da biliyoruz. Bu sebeple **sunucular ile iletişim kurmak istediğimizde bu sunucuların IP adresini bilmek zorundayız**.

Fakat IP adreslerini akılda tutması kolay değil. Örneğin **sultankrp.net** websitesine erişmek için **175.199.108.173** IP adresini akılda tutmak ve her defasında eksiksiz olarak yazmak oldukça zahmetli. Kaldı ki tüm internet yalnızca tek bir websitesinden ibaret olmadığı için tüm websitelerinin IP adreslerini hatırlamamız ve eksiksiz olarak yazmamız pek olası değil.

Zaten bizler de bu sebeple domain olarak geçen alan isimlerini kullanıyoruz. Örneğin sultankrp.net websitesini ziyaret etmek için yalnızca bu ismi tarayıcımıza yazıp onaylamamız yeterli oluyor. Bu domain ismi arka planda, IP adresine dönüştürülerek bizim doğru sunucu ile iletişim kurmamız da mümkün oluyor.

Hostlar arasında iletişim kurmak için IP adreslerinin bilinmesi gerektiğinden, bir sunucu ile iletişim kurmak istediğimizde bu sunucun IP adresini bilmek zorundayız. İşte burada dönüşümü gerçekleştiren yapı da **DNS** olarak geçen protokoldür.

IP ve domain bilgileri DNS server üzerinde tutuluyor. Biz de domain adresi üzerinden gerekli olan IP bilgisini almak için bu DNS sunucusuna başvuruyoruz.

Eğer harici olarak bir konfigürasyon gerçekleştirmediyseniz bu DNS sunucusu sizin internet servis sağlayıcınızdır. Örneğin Google'ın DNS sunucusu olan 8.8.8.8 sunucusunu kullandığınızı varsayacak olursak sorgulama işlemi aşağıdaki gibi gerçekleşir.

Yani DNS aslında internet dünyası için son derece önemli bir protokoldür. Örneğin internet servis sağlayıcınız sizin bazı sitelere erişmenize engel olmak isterse, kendi DNS sunucuları üzerinde bu domain adreslerinin karşılığı olan IP adreslerini geçersiz olarak tanımlayabilirler. Genellikle hostun kendi lokal IP adresi olan 127.0.0.1 adresi tanımlanır. Bu sayede gitmek istediğiniz domain'in IP adresi bulunamadığı için ilgili web sunucusu ile iletişim kuramazsınız. Bu sebeple sıklıkla Google Cloudflare gibi DNS hizmeti sağlayan harici DNS sunucuları kullanılır.

Ayrıca, harici DNS sunucuları dışında kullanmakta olduğunuz cihazın işletim sistemi içerisinde de dahili DNS hizmeti bulunur. Bu sayede cihazdaki programların hangi sunuculara erişip hangilerine erişmeyeceğini cihaz bazında kısıtlamamız da mümkün oluyor.

DNS nasıl çalışır?

DNS'yi nasıl kullanabileceğinizden bahsetmeden önce, sistemin nasıl çalıştığını anlamamız gerekiyor. IP adreslerini alan adlarıyla eşleştirdiğini zaten biliyoruz, bu bilgiler de ad sunucularında saklanıyor.

Ad sunucuları, etki alanının IP adresi ile eşleştiğini söyleyen asıl dosya olan DNS kayıtlarını depolar. Ad sunucuları, her alanı saklamak yerine TLD'nin (üst düzey alan adları) konumlarını depolarlar. TLD'ler, *.com* gibi bir alan adını sonlandıran iki veya üç karakterden oluşur. Her TLD'nin, DNS kayıtlarını depolamak için kimin yetkili olduğunu belirten bilgileri depolayan, kendi ad sunucuları vardır. Bir alan adını sorguladığınızda, ilk adımınız aslında kök ad sunucularında olmayacaktır. Bunun yerine, tarayıcınız yerel çözümleyici ad sunucunuza o etki alanı için DNS kayıtlarının önbelleğe alınmış olup olmadığını soracaktır. Çözümleyen ad sunucusu tipik olarak ISS'nizdir (İnternet Servis Sağlayıcısı) ve youtube.com gibi popüler bir web sitesiyse, kayıt büyük olasılıkla önbelleğinde olacaktır. Bu durumda, DNS arama işleminin geri kalanını atlarsınız, ancak bu kayıtlar yalnızca kısa bir süre için saklanır. Bir kayıt oluşturduğunuzda, bir TTL (Yaşam Süresi) ayarlama seçeneğiniz vardır. TTL, ad sunucularına kayıt bilgilerini ne kadar süre saklayabileceklerini söyler. TTL'ler 30 saniye ile bir hafta arasında değişebilir.

İnternetteki her cihaza bir IP adresi verilir ve bu adres, belirli bir evi bulmak için kullanılan bir sokak adresinin kullanılması gibi, uygun internet cihazını bulmak için gereklidir. Bir kullanıcı bir web sayfasına ulaşmak istediğinde, bu kullanıcının web tarayıcısına (örnek.com) yazdığı şey ile örnek.com web sayfasını bulmak için gerekli adres arasında bir çeviri yapılmalıdır. Web tarayıcısı için, DNS araması "sahne arkasında" gerçekleşir ve kullanıcının bilgisayarından ilk istek dışında herhangi bir etkileşim gerektirmez.

En İyi DNS Sunucusu Nedir?

DNS saldırıları ve sorunları, DNS konusu İSS'niz için bir öncelik olmadığında ortaya çıkar. Bu sorunlardan uzaklaşmak, DNS güvenliğini ve gizliliğini öncelik haline getiren bir hizmete geçmek kadar basit olabilir.

Google DNS, hatırlanması çok kolay olan 8.8.8.8 ve 8.8.4.4 IP adresleriyle yaklaşık 10 yıldır kullanılmaktadır. Google, hız avantajlarının yanı sıra saldırılara karşı güçlendirilmiş güvenli bir DNS bağlantısı da sunuyor.

2005'te kurulan **OpenDNS**, güvenli DNS'yi Google'dan daha da uzun süredir sunuyor. Google'ınki gibi akılda kalıcı IP adreslerine sahip değil ancak o da gayet işlevsel bir kullanım sunmaktadır. Gizlilik ve güvenliğe odaklanan DNS sunucularına ek olarak, uygunsuz içeriği filtreleyen FamilyShield sunucuları olarak adlandırdığı bir uygulaması var. Şirket ayrıca ebeveynlere filtreleme üzerinde daha ayrıntılı denetim sağlayan birinci sınıf ebeveyn denetimi sistemi de sunuyor.

Cloudflare, hiç duymadığınız en büyük internet şirketlerinden biri olabilir. Dünya çapında genişleyen sunucu koleksiyonuyla, diğer hizmetlerin yanı sıra web sitelerine internet güvenliği ve DDoS "Dağıtılmış Hizmet Reddi" saldırılarına karşı koruma sağlıyor. Geçen yıl Cloudflare, 1.1.1.1 ve 1.0.0.1 gibi akılda kalan IP adreslerinde güvenli DNS'yi kullanıma sundu. Daha yakın zamanda şirket, 1.1.1.1 mobil uygulamasının VPN korumasının yerini alması için bir plan başlattı.

BIND nedir?

Berkeley İnternet Adı Etki Alanı (BIND), günümüzde kullanılan en popüler DNS sunucusularından biridir. 1980'lerde Berkeley Üniversitesi'nde geliştirilmiştir ve şu anda sürüm 9'da bulunmaktadır. BIND, Mozilla Kamu Lisansı altında sunulan, indirmesi ve kullanması ücretsiz bir açık kaynak sistemidir.

BIND, bir DNS sunucusunu önbelleğe alma veya yetkili bir ad sunucusunu çalıştırmak için kullanılabilir ve yük dengeleme, bildirim, dinamik güncelleme, bölünmüş DNS, DNSSEC, IPv6 gibi özellikler sağlar.

DNS Bölge (DNS Zone) Dosyaları Nedir?

DNS veri tabanındaki etki alanları hakkındaki bilgiler, bölge dosyalarında saklanır. Bir bölge dosyası, yönergelerden ve kaynak kayıtlarından oluşur. Yönergeler, ad sunucusuna görevleri gerçekleştirmesini veya bölgeye özel ayarlar uygulamasını söyler. Kaynak kayıtları bölgenin parametrelerini tanımlar ve ana bilgisayar bilgilerini depolar. Yönergeler isteğe bağlıdır, ancak kaynak kayıtları gereklidir. Bir kaynak kaydında aşağıdaki alanlar bulunur (Türe bağlı olarak bazı alanlar isteğe bağlıdır):

DNS Değiştirme, DNS Neden Değiştirilir?
Coğrafi konumunuzdan kısıtlanan içeriğe erişmek için IP adresinizi bir VPN ile değiştirebilirsiniz. Benzer şekilde, DNS maskelerinizi değiştirmek konumunuzu da değiştirir. Aradaki fark, VPN aslında bağlantınızı farklı bir bölge üzerinden yeniden yönlendirirken, DNS sunucuya farklı bir konumda olduğunuzu söyler. VPN ayrıca şifreleme yoluyla daha fazla gizlilik sunar ve bu da bağlantınızı yavaşlatabilir. DNS'nizi değiştirmek istemenizin bazı nedenleri şunlar olabilir:

- Fiziksel konumunuzla sınırlı olan web üzerindeki içeriğe erişmek (Netflix gibi)
- İnternet bağlantınızı hızlandırmak (bazen üçüncü taraf DNS sunucuları varsayılandan daha hızlıdır)
- Çocuklarınızı korumak için güvenli web taramasını deneyimlemek
- Ek güvenlik özellikleriyle üçüncü taraf DNS sunucuları aracılığıyla cihazlarınızı ve verilerinizi korumak (esas olarak kimlik avını önleme odaklı)
- İnternet bağlantınız çalışmıyorsa ve bunun DNS ile ilgili bir sorun olduğundan şüpheleniyorsanız

DNS’nizi değiştirmek isteyebilirsiniz.

Dizüstü Bilgisayarımın DNS Sunucusunu Nasıl Değiştiririm?
Windows 10'da:

- Windows düğmesini tıklayın,
- Ayarları seçin,
- Ağ ve İnternet'i tıklayın,
- Bağdaştırıcı Seçeneklerini Değiştir'i tıklayın,
- Wi-Fi bağlantısına sağ tıklayın ve Özellikleri seçin,
- İnternet Protokolü Sürüm 4'ü seçin ve Özellikler düğmesini tıklayın,
- Aşağıdaki DNS sunucu adreslerini kullan etiketli öğeyi tıklayın,
- İki adresi girin,
- Tamam'a tıklayın ve gerekirse
- İnternet Protokolü Sürüm 6 için işlemi tekrarlayın.

VPN Nedir?

VPN, doğrudan çevirecek olursak İngilizce sanal özel ağ **(virtual private network)** anlamına geliyor ve olmadığınız bir yerdeki fiziksel bir ağa sizi uzaktan bağlıyor. Kimisi bu teknolojiyi şirketlerinin yerel ağına sanki oradaymış gibi bağlanmak için kullansa da bazı zorunluluklardan dolayı bu kavramı tıpkı DNS gibi öğrenmek zorunda kalan yoldaki vatandaş için VPN girilemeyen sitelere girilebilmesini sağlayan **mucizevi bir çözüm.**

Nasıl çalışır?

VPN, birçok farklı protokol ve teknolojiyi kullansa da temel olarak bilgisayarınızın fiziksel olarak bulunduğu yerden karşıdaki ağa şifreli (kripto anlamında) bir tünel açar. Bu tünel içinden iletilen bilgi dışarıdan bakıldığında şifreli olduğu için **dışarıdan görüntülenemez.** Konuya hakim güvenlik uzmanları şifreli veri aktığını görür ama içeriğinin ne olduğunu (çok zayıf bir güvenlik kullanmıyorsa) anlayamaz. VPN çözümleri bilgisayarınıza veya mobil cihazınıza özelleşmiş bir ağ sürücüsü kurar (veya mobil cihazlarda bu gömülü olarak gelir) ve bu noktada sanal bir ağ bağdaştırıcısı gibi davranarak size karşıdaki ağdan bir IP numarası da verir. Bu sayede izin verilen uygulamalara veya yerel adreslere erişebilirsiniz.

VPN Kullanımı

Günümüzde üç farklı popüler VPN kullanımı var. Bunlardan bir tanesi nasıl çalışır kısmında temel mekanizmayı anlattığımız, örneğin evinizdeki bilgisayardan ofisteki sistemlere, hizmetlere veya bilgisayarınıza bağlanmanızı sağlayan VPN sistemleri. Bu sistemler sayesinde uzaktaki bir ağa sanki oradaymışçasına girebilir ve orada işlem yapabilirsiniz. Bunu da gayet **güvenli şekilde** yapabilirsiniz.

İkinci kullanım alanı, ülkemizde iş kullanımı dışında oldukça yaygın olan, tüm trafiği toplu şekilde alıp farklı bir konumdan (genellikle başka bir ülkeden) internet ortamına çıkış sağlayan sistemler. Bu VPN teknolojisinin bir avantajı da özellikle **kamuya açık ağlarda** işe yaraması. Örneğin şifreli veya şifresiz olarak bağlandığınız bir kablosuz ağ var. Şifre varsa ağa bağlı diğer bilgisayarlar, şifre yoksa da çevredeki herkes burada akan veriyi görebilir ve sosyal mühendislik tekniklerini kullanarak sizle veya çalıştığınız firmayla ilgili saldırı vektörleri oluşturabilir. Bu noktada devreye giren VPN sistemi, bilgisayar veya mobil cihazınızdan akan veriyi "koklanabilir" (sniffing, veri paketlerini toplayıp analiz etme işi) ağdan uzaklaştırıp internete çıkarttığı için neredeyse tam güvenlik sağlar. Bu noktadan sonra, interentte gezebilir, bulut hizmetlerindeki dosyalarınızı hangi hizmeti kullandığınızı göstermeden senkronize edebilir, güvenli olmayan FTP hizmetleri üzerinden daha güvenli şekilde dosya gönderebilirsiniz.

Son VPN türü ise özellikle oyuncuların hayatlarını kurtaran ve yanlış yönlendirme (routing) sorunları nedeniyle yükselen sunucu cevap sürelerini (ping) düşüren özelleşmiş sistemlerdir. Bu sistemler internet servis sağlayıcınızın oyun verisini ayırt etmeden noktadan noktaya sektirmesi sorununu çözüp size daha kısa bir rota çizer ve özellikle MMO diye tabir ettiğimiz çok oyunculu online oyunlarda gözle görülür ve sinir katsayılarını düşürür nitelikte etki etmektedir. Bir önceki VPN çözümlerine göre **daha ucuz** veya pahalı olabilirler ama genellikle oyundan oyuna göre sürekli güncellenen ayarlara sahip olmaları sayesinde hayat kurtarır niteliktelerdir.

VPN İle İzimi Kaybettirebilir Miyim?

Bulunduğunuz ağ üzerinde kendinizi görünmez olmasa da anlaşılmaz hale getirebileceğiniz genel VPN hizmetlerinde, hizmet sağlayıcı tarafında çeşitli kayıt sistemleri kullanılıyor. Bu kayıt sistemleri elbette birçok ülkeye (yani hizmeti sağlayan şirketin ülkesine) göre değişiyor. Bunu satın aldığınız hizmetin sağlayıcısından öğrenebilirsiniz. Sizi farklı ülkeye taşıdıktan sonra internete taşıyan sistemlerde çıkış yaptığınız andan o ülkenin internet regülasyonları sizi olumlu veya olumsuz şekilde etkileyebilir. Şirketinize doğru veya şirketinizdeki ağ üzerinden yapacağınız erişimlerde ise, eğer iyi bir sistem yönetim kadronuz varsa, VPN erişimiyle nerelere bağlandığınızın kaydı tutulacaktır. Dolayısıyla VPN teknolojisi **sizi görünmez yapmaz**; yapacağınız işi daha güvenli şekilde yapmanızı sağlar.

Vpn Engellenebilir Mi?

Aslında bu soruya tam olarak “evet veya hayır” diye cevap vermek biraz güç. Çünkü VPN servislerine erişim engellenebilir ama bu engellemenin sürekli olması teknik olarak zor görünüyor.

VPN servislerini ve engellenebilme olanaklarını biraz daha iyi anlamak için kullandıkları protokolleri de incelemek gerekir. **VPN yazılımlarının kullandığı protokolleri**; Noktadan Noktaya Tünel Protokolü (PPTP), Katman 2 Tünel Protokolü (L2TP) veya Güvenli Yuva Tünel Protokolü (SSTP) olarak özetleyebiliriz. Kişisel kullanım amaçlı VPN servislerinin büyük bir çoğunluğu **PPTP ve L2TP protokollerini** kullanıyor ve son dönemde engellendiği öne sürülen VPN servisleri de bu protokolleri kullanan servisler.

VPN servisleri son dönemde oldukça popüler ve bu pazarda çok fazla rekabet var (**Opera VPN** ve **VPN Chrome** eklentisi gibi). Olası bir engellemede bu servisler de **VPN engeli kaldırma** konusunda ellerindeki tüm manevraları kullanarak, engellemelerin etrafından dolaşmaya çalışıyorlar. Yani engellenen bir protokolden **başka bir protokole geçmeleri** veya engellenen **IP adreslerini değiştirmeleri** başvurdukları yöntemler.

Wi-Fi Güvenlik Türlerinin Önemi

Kablosuz internet ağınızın güvenliğini sağlamak için sadece şifre koymak yeterli olmayabiliyor. Kötü niyetli kişilerin Wi-Fi ağınıza erişememesi için de birtakım güvenlik önlemleri almanız gerekebilir. Sadece bu amaçla da güvenlik yöntemleri kullanılmaz. Ayrıca kablosuz ağ güvenlik türleri, bir cihazdan başka bir cihaza veri gönderirken bunların şifrelenmesini sağlar. Böylece verilerinizi de korumuş olursunuz. WEP, WPA ve WPA2 bu güvenlik türleridir. Bu şifreleme türleri, verilerinizi şifreleyerek sizin güvenliğinizi sağlarlar. Bu sebeple de kendinize uygun olan şifreleme türünü seçmeniz oldukça önem taşır. Kablosuz internet ağınız açık olduğu takdirde kötü niyetli saldırıların da hedefi olabilir. Sizin IP adresiniz kullanılarak yasa dışı işler yapılabilir, önemli dosyalarınız ele geçirilebilir ve hatta kişisel verileriniz internet korsanlarının eline geçebilir. Bu sebeple, IP adresi ve kablosuz internet ağınızı korumanız hayati derecede önemlidir. Aksi takdirde verileriniz başka insanlar tarafından ele geçirebileceği gibi yasa dışı faaliyetler için de kullanılabilirler. WEP, WPA ve WPA2 internette güvenliği sağlamak için ortaya çıkmış şifreleme türleridir. Bu şifreleme türleri sayesinde verileriniz korunur ve ağınıza sizden başka biri farklı amaçlarla yazılımlar yükleyemez

WEP nedir?

Kablosuz ağlar verileri radyo dalgaları aracılığıyla ilettiğinden, güvenlik önlemleri olmadığında veriler kolayca ele geçirilebilir. 1997 yılında sunulan Kablolu Eşit Gizlilik (WEP), kablosuz ağ koruması sağlamaya yönelik ilk girişimdi. Amaç, verileri şifreleyerek kablosuz ağlara güvenlik eklemekti. Kablosuz veriler ele geçirilmeleri halinde, şifrelenmiş olduklarından alıcılar tarafından tanımlanmaları mümkün olmayacaktı. Ancak ağda yetkili olan sistemler, verileri tanımlayarak deşifre edebiliyordu. Bunun nedeni, ağdaki cihazların aynı şifreleme algoritmasını kullanmasıydı.

WEP, trafik verilerini on altılı karakterler olarak 64 veya 128-bit anahtar kullanarak şifreler. Bu statik bir anahtardır, yani bütün trafik, cihazdan bağımsız olarak tek anahtar kullanılarak şifrelenir. WEP anahtarı, bir ağdaki bilgisayarların birbirine şifreli mesajlar göndermesine imkan tanır ve bu sırada mesajların içeriklerini saldırganlardan gizler. Kablosuz güvenliğin etkin olduğu bir ağa bağlanmak için bu anahtar kullanılır.

WEP'in temel hedeflerinden biri, Ortadaki Adam saldırılarını önlemekti ve bunu bir süreliğine başardı. Ancak protokolde yapılan revizyonlar ve anahtar boyutunun artırılmasına rağmen, zaman içinde WEP standardında çeşitli güvenlik kusurları keşfedildi. Bilgi işlem gücü arttıkça suçluların bu kusurlardan yararlanması kolaylaştı. Wi-Fi İttifakı, WEP'i açıklarından dolayı 2004 yılında emekliye ayırdı. WEP güvenliği günümüzde eski olarak kabul edilse de bazen hala kullanılır. Bunun nedeni, ya ağ yöneticilerinin kablosuz yönlendiricilerindeki varsayılan güvenliği değiştirmemiş olmasıdır ya da cihazların WPA gibi daha yeni şifreleme yöntemlerini destekleyemeyecek kadar eski olmasıdır.

WPA nedir?

WEP'ten sonra WPA ya da Wi-Fi Korumalı Erişim ortaya çıktı. Bu protokol, 2003 yılında Wi-Fi İttifakı tarafından WEP yerine sunuldu. WEP ile benzer özellikleri vardı ancak güvenlik anahtarlarının yönetilmesi ve kullanıcıların yetkilendirilmesi şeklinde iyileştirmeler sunuyordu. WEP her yetkili sisteme aynı anahtarı sunarken, WPA, sistemlerin kullandığı anahtarı dinamik olarak değiştiren Temporal Key Integrity Protocol (TKIP) kullanır. Bu, saldırganların güvenlik ağı tarafından kullanılan anahtarla eşleşen kendi şifreleme anahtarlarını oluşturmasını engeller. TKIP şifreleme standardı daha sonra Gelişmiş Şifreleme Standardı (AES) ile yenilendi.

WPA ayrıca bir saldırganın veri paketleri yakalayıp yakalamadığını ya da bunları değiştirip değiştirmediğini belirlemek için mesaj bütünlük denetimleri de içeriyordu. WPA'nın kullandığı 256-bit anahtarlar, WEP sisteminde kullanılan 64 bit ve 128-bit anahtarlara göre önemli bir artış sunuyordu. Ancak bu iyileştirmelere rağmen WPA'nın bazı unsurlarındaki açıklardan yararlanmak mümkün oldu ve bunun sonucunda WPA2 sunuldu.

Bazen WPA'yla ilgili olarak "WPA anahtarı" ifadesi kullanılır. WPA anahtarı, kablosuz bir ağa bağlanmak için kullandığınız bir paroladır. WPA parolasını ağ yöneticisinden alabilirsiniz. Bazı durumlarda, kablosuz yönlendiricilerin üzerinde basılı olan varsayılan bir WPA parolası bulunabilir. Yönlendiricinizin parolasını belirleyememeniz halinde yönlendiriciyi sıfırlamanız mümkün olabilir.

WPA2 nedir?

2004 yılında sunulan WPA2, WPA'nın yükseltilmiş bir versiyonuydu. WPA2 Robust Security Network (RSN) mekanizmasına dayanır ve iki modda çalışır:

- Erişim için paylaşılan bir parolaya dayanan ve genellikle ev ortamlarında kullanılan **Kişisel mod veya Önceden Paylaşılan Anahtar (WPA2-PSK)**.
- **Kurumsal mod (WPA2-EAP)**: Adından da anlaşıldığı gibi bu daha çok kurumsal ya da işletme kullanımına yöneliktir.

Her iki mod da, açılımı Counter Mode Cipher Block Chaining Message Authentication Code Protocol olan CCMP'yi kullanır. CCMP protokolü, mesaj kimlik doğrulaması ve bütünlük doğrulama sağlayan Gelişmiş Şifreleme Standardı (AES) algoritmasına dayanır. WPA'nın orijinal Temporal Key Integrity Protocol'undan (TKIP) daha güçlü ve güvenilir olan CCMP, saldırganların örüntüleri tespit etmesini zorlaştırır.

Ancak WPA2'nın dezavantajları da vardır. Örneğin, yeniden anahtar yükleme saldırılarına (KRACK) açıktır. KRACK, WPA2'daki açıklardan yararlanır ve bu da saldırganların kopya bir ağ gibi davranarak kurbanı başka kötü amaçlı bir ağa bağlanmaya zorlar. Bu, korsanın az miktarda veriyi deşifre ederek biriktirmesine ve şifreleme anahtarını kırmasına imkan tanıyabilir. Ancak cihazlara yama uygulanabilir ve WPA2, hala WEP veya WPA'dan daha güvenli kabul edilmektedir

WPA3 nedir?

WPA3, Wi-Fi Korumalı Erişim protokolünün üçüncü yinelemesidir. Wi-Fi İttifakı, WPA3'ü 2018 yılında sunmuştur. WPA3 hem kişisel hem de kuruluş kullanımına yönelik aşağıdaki gibi yeni özellikler sunmuştur:

Kişiselleştirilmiş veri şifrelemesi: Herkese açık bir ağa giriş yapılırken, WPA3 yeni bir cihazı paylaşılan bir paroladan farklı bir işlemle kaydeder. WPA3, ağda cihazlara izin vermek için kullanıcıların Yakın Alan İletişimi(NFC) etiketleri veya QR kodları kullanmasına imkan tanıyan bir Wi-Fi Device Provisioning Protocol (DPP) sistemi kullanır. WPA3 güvenliği ek olarak, daha önce kullanılan 128-bit şifreleme yerine GCMP-256 şifreleme kullanır.

Eşzamanlı Eşit Kimlik Doğrulama protokolü: Bu, bir ağ cihazının kablosuz bir erişim noktasına bağlandığı ve her iki cihazın da kimlik doğrulamasını ve bağlantıyı onaylamak için iletişim kurduğu güvenli bir el sıkışması oluşturmak için kullanılır. Kullanıcı parolası zayıf olsa bile WPA3, Wi-Fi DPP kullanarak daha güvenli bir el sıkışması sağlar.

Daha güçlü kaba kuvvet saldırısı koruması: WPA3, çevrimdışı parola tahminlerine karşı koruma sağlamak için kullanıcının yalnızca bir tahmin yapmasına izin verir ve kullanıcıyı Wi-Fi cihazıyla doğrudan etkileşime girmesi için zorlar. Bu, parolayı her tahmin etmek istediklerinde fiziksel olarak cihazın başında olmaları gerektiği anlamına gelir. WPA2 herkese açık ağlarda dahili şifrelemeye sahip değildir ve bu da kaba kuvvet saldırılarını ciddi bir tehdit haline getirir.

WPA3 cihazları 2019 yılında oldukça yaygın hale gelmiştir ve WPA2 protokolü kullanan cihazlarla geriye doğru uyumludur.

Wi-Fi'ımın güvenlik türü ne?

Wi-Fi şifreleme türünüzü bilmek ağın güvenliği için önemlidir. Eski protokoller yenilere göre saldırılara daha açıktır ve bu yüzden bir korsan saldırısına maruz kalma ihtimalleri daha fazladır. Bunun nedeni eski protokollerin, korsanların yönlendiricilere nasıl saldırdığı tam olarak anlaşılmadan önce tasarlanmış olmasıdır. Daha yeni protokoller bu açıkları düzeltmiştir ve bu yüzden en iyi Wi-Fi güvenliğini sundukları düşünülmektedir.

Wi-Fi güvenlik türünüzü nasıl belirlersiniz?:

Windows 10'da:

- Görev çubuğunda Wi-Fi bağlantısı simgesini bulun ve üzerine tıklayın
- Ardından geçerli Wi-Fi bağlantınızın altındaki **Özellikler** öğesine tıklayın
- Aşağı kaydırın ve **Özellikler** öğesi altında Wi-Fi ayrıntılarını arayın
- Bunun altında, Wi-Fi protokolünü gösteren **Güvenlik Türü** öğesini arayın

macOS'ta:

- **Seçenek** tuşunu basılı tutun
- Görev çubuğunda **Wi-Fi simgesine** tıklayın
- Bu, Wi-Fi güvenlik türünü de içeren ağ ayrıntılarını gösterir

Android'de:

- Android telefonunuzda **Ayarlar** öğesine gidin
- **Wi-Fi** kategorisini açın
- Bağlandığınız yönlendiriciyi seçin ve ayrıntılarını inceleyin
- Bu, bağlantınızın Wi-Fi güvenlik türünü gösterir
- Bu ekrana giden yol, cihazınıza göre değişiklik gösterebilir