-BÜYKLÜKLERİNE GÖRE AĞLAR –

Bilgisayarlar arasında iletişim kurmayı ve paylaşım ortamı oluşturmayı sağlayan yapıya **Bilgisayar Ağı** denir. Bilgisayar ağları büyüklüklerine göre üçe ayrılır. Bunlar;

1. **LAN (Local Area Network - Yerel Alan Ağları)**
2. **WAN (Wide Area Network - Geniş Alan Ağları)**
3. **MAN (Metropolitan Area Network - Şehir Alan Ağları)**
4. **PAN (Personal Area Network – Kişisel Alan Ağı )**
5. **VPN (Virtual Private Network –Özel Sanal Ağ )**
6. **CAN (Controller Area Network – Kontrolör Alan Ağı )**
7. **SAN (Storage Area Network – Depolama Alan Ağı )**
8. **BAN - Vücut alan ağı (Body Area Network)**

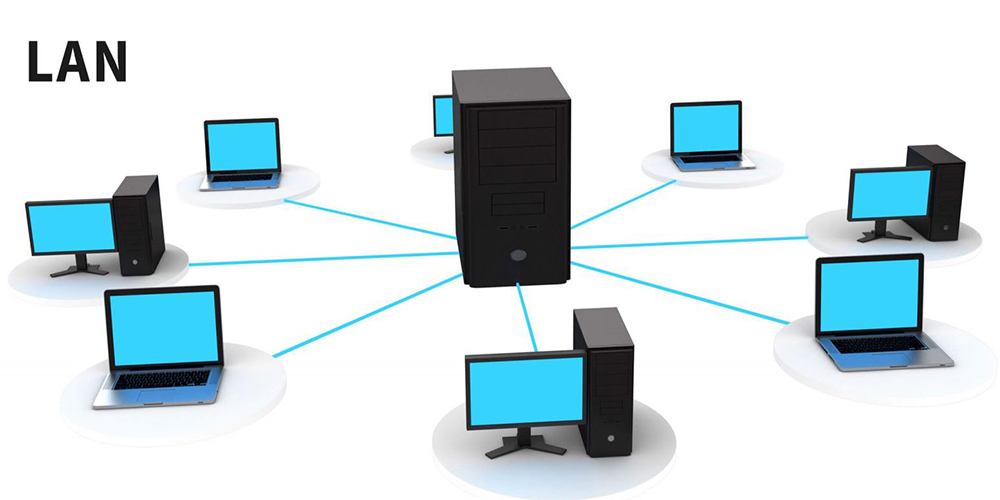
**1) LAN (Local Area Network - Yerel Alan Ağları)**

Birbirine yakın yerlerde konumlandırılmış ve kablolar ile fiziksel olarak birbirlerine bağlanmış yapıdaki ağlara **LAN**denir. Bir binada bulunan bütün bilgisayarların birbirlerine bağlanmasıyla oluşan yapıyı örnek verebiliriz.

LAN uygulamasında kablolama alt yapısı oldukça önemlidir; kablo türü, seçilecek teknoloji, ağın yayılabileceği fiziksel genişliği ve port arasındaki iletişim hızını belirlemede baskındır. LAN'larda temel özellik, sistemlerin aynı ortamda veya birbirlerine yakın mesafede olmasıdır. LAN uygulamalarında kullanılan teknolojiler;

1. Ethernet
2. Jetonlu Halka (Token Ring)
3. Jetonlu Yol (Token Bus)
4. 100VGAnyLAN
5. ATM (Asynchronous Transfer Mode)
6. FDDI (Fiber Distributed Data Interface)

LAN uygulamalarında ucuzluğu,kurulum kolaylığı ve değişik hızlarda çeşitliliği olması ve bu teknolojiyi içeren ürünlerin çokluğu açısından yoğun olarak Ethernet teknolojisi kullanılır. Ethernet teknolojisinin yetersiz kaldığı durumlarda ise ATM veya FDDI teknolojisi kullanılır.



1 LAN ( Local Area Network - Yerel Alan Ağı )

**2) WAN (Wide Area Network - Geniş Alan Ağları)**

İki ya da daha fazla LAN'ın birbirlerine bağlanmasıyla oluşan yapıda **WAN**denir. Bu yapıda bilgisayarlar fiziksel olarak birbirlerine çok uzak olabilirler. Uzak kullanıcılardan ve bunların birbirleriyle haberleşmeleri veya merkez noktaya erişebilmeleri için WAN bağlantıları içerir. WAN uygulamalarında kullanılan teknolojiler;

# Çevirmeli (Dial-up) modem

# Kiralık hat

# X.25

# FR

# ISDN

# xDSL

# ATM

# B-ISDN

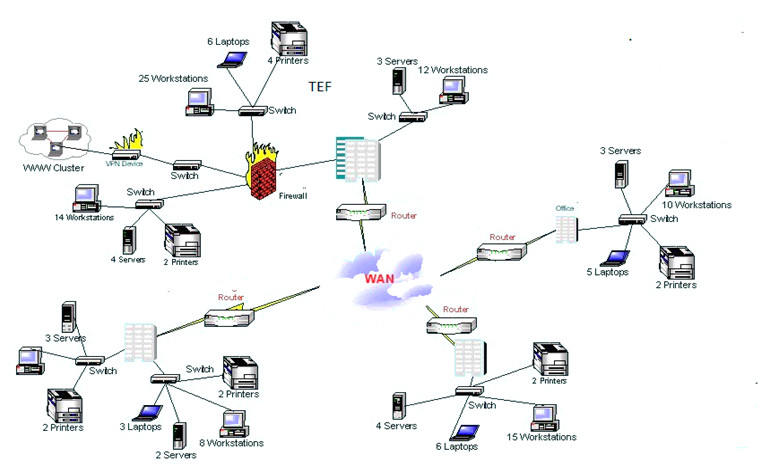
# SMDS

**WAN teknolojileri genellikle aşağıdaki gibi sınıflandırılır;**

# Bağlantı durumuna göre

# Anahtarlama yönetime göre

# Topolojik yapısına göre



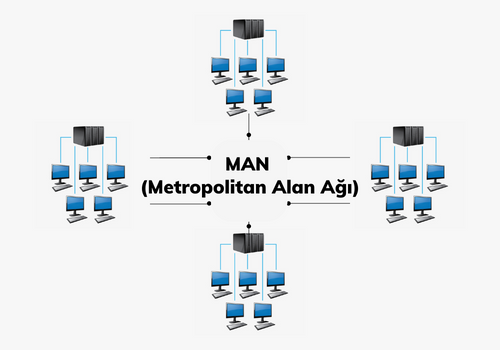
2

WAN ( Wide Area Network - Geniş Alan Ağı )

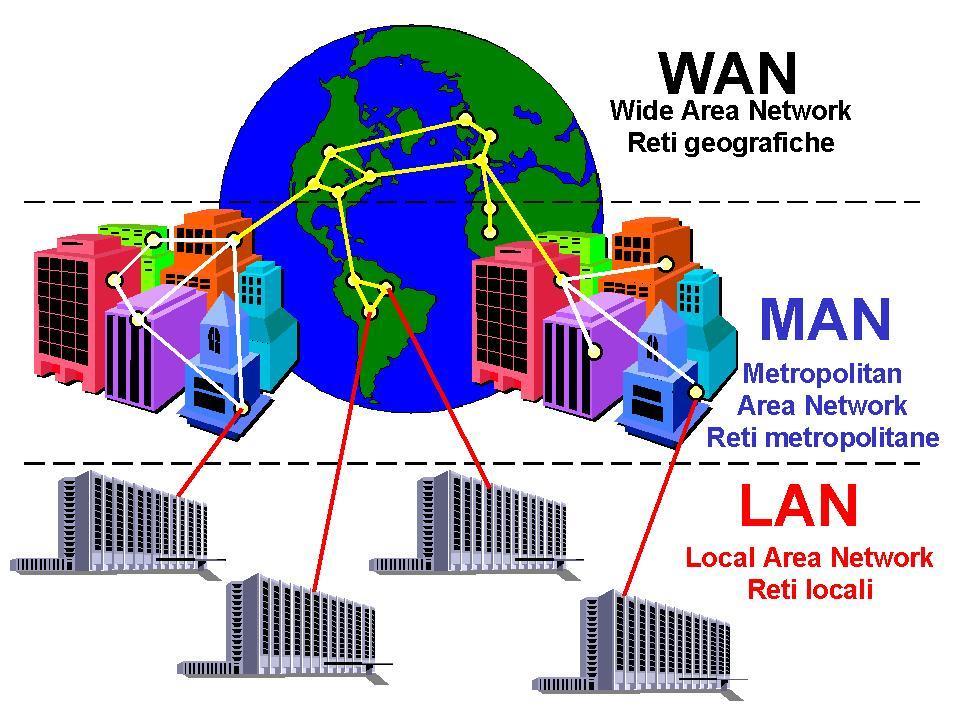
**3) MAN (Metropolitan Area Network - Şehir Alan Ağları)**

MAN'lar, LAN'ların şehir çapındaki büyük türleridir ve LAN'lara benzer teknolojileri kullanır. Bir MAN, veri ve ses haberleşmesi sağlayabileceği gibi yerel kablolu TV ağına da bağlantı kurabilir.

* Metropolitan adıyla anılmasının sebebi, bu tür ağların genelde bir şehrin tümünü veya büyük bir kısmını kapsıyor olmasıdır.
* Yerel alan ağlarından daha geniş bir bilgisayar ağ grubunu kapsar.
* Orta ölçekli ağ sistemidir. Bir kampüs içerisinde veya şehir içerisinde yönlendirme , güçlendirme ve doğrulama işlemleri için yardımcı ağ aygıtlarına gereksinim duyar; bünyesinde birden çok LAN sistemi barındıran ve birbirine bağlayan ağ sistemidir. Bunlara en güzel örnek, Intranet sistemidir. Büyük iş yerlerinde oluşturulan ağlar da bu kategoriye girer.
* Bu ağlar için LAN’ın kapsadığı alanda daha geniş , fakat WAN’ın kapsadığından daha dar mesafeler arası iletişimi sağlar demek doğru olur. Genellikle de şehir içi bilgisayar sistemlerinin birbiriyle bağlanmasıyla oluşturulur.
* En iyi bilinen örneklerinden birisi kablo TV hatları üzerinden , kullanılmayan bantları kullanarak iki yönlü iletişimin kurulduğu internet bağlantısıdır.



3 MAN (Metropolitan Area Network - Şehirsel Alan Ağı)



4 AĞ TÜRLERİ

**4) PAN ( PERSONAL AREA NETWORK – KİŞİSEL ALAN AĞI ) ;**

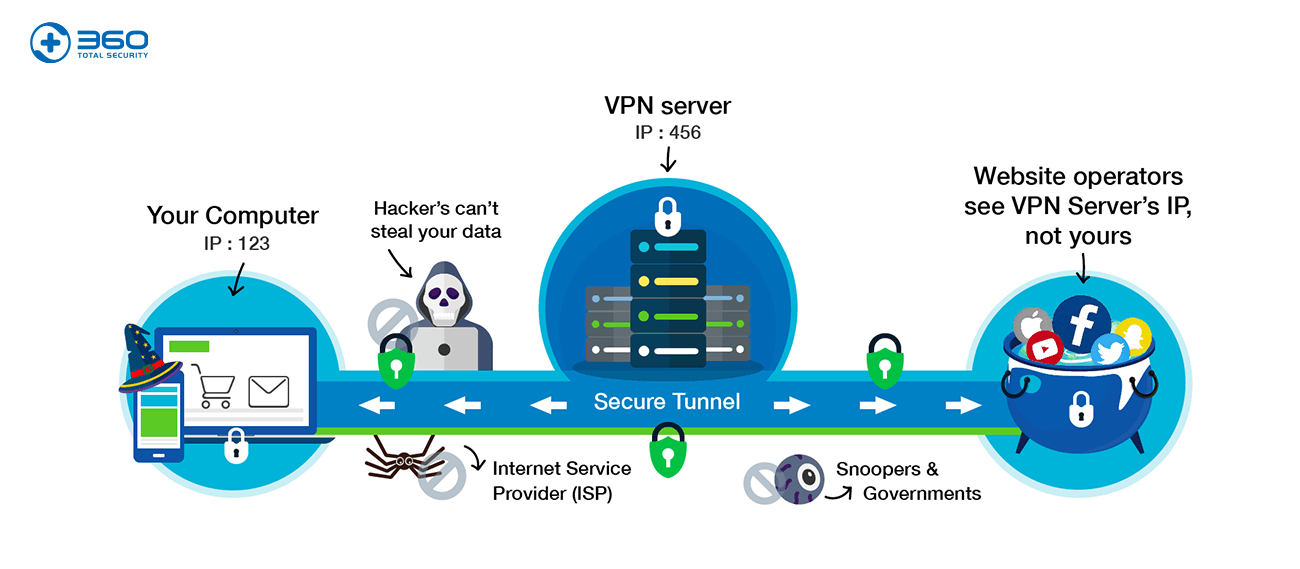
* Kişisel alan ağı (Personal Area Network ) bil bilgisayar ağı sistemidir. Günümüzde bir endüstri standardıdır. Bir kişisel alan ağı kişisel dijital asistanların ve telefonların da dahil olduğu bilgisayar aygıtları arasında iletişim için kullanılan bilgisayar ağıdır.
* “ Persona Area Network “ , yaklaşık 10 metrelik bir alanı kapsayan, kişisel alan kavramıyla kastedilen cihazların birbirlerine bağlanmasıyla oluşturulan ağı tanımlamaktadır. Örneğin ; üzerinde saat, çağrı cihazı , cep telefonu, pda, mp3 player ve dizüstü bilgisayar gibi cihazlar taşıyan bir kişi, 5 adet ekran, 3 adet klavye ve 4 adet iletişim cihazı taşıyor demektir. Bu cihazlar arasında uygun bir veri paylaşım ağı oluşturulduğunda basit anlamda bir PAN kurulmuş olur.
* Pan’lar, internet veya daha yüksek seviyeli ağa bağlanmak için veya kişinin kendi kişisel aygıtları arasında iletişim için kullanılır. Kişisel alan ağlarında Firewire ve USB gibi bilgisayar kablosu kullanılır. Bir kablosuz kişisel alan ağı IrDA, bluetooth, kablosuz USB, Z-Wave ve ZigBee gibi kablosuz ağ teknolojileri ile yapılır.
* PAN cihazları ayrıca, gündelik giyilen nesnelerin şeklini de alabilirler: kemer, saat, kredi kartı, cüzdan, mikrofon, tişört vb.çeşitli sensörlerle birleştirilmiş PAN cihazları insan vücudundaki biyolojik değişimlerin gözlemlenmesi amacıyla da kullanılabilmektedir. Kişinin kan basıncı, kalp ritmi ve solunumu gibi sağlık göstergelerinin uygun ölçme teknikleriyle donatılmış algılayıcılarla işlenip, veri çıkışının da kol saatinin ekranına yönlendirilmesi PAN teknolojisinin uygulama alanı örneklerindendir.



5 PAN (Personal Area Network - Kişisel Alan Ağı )

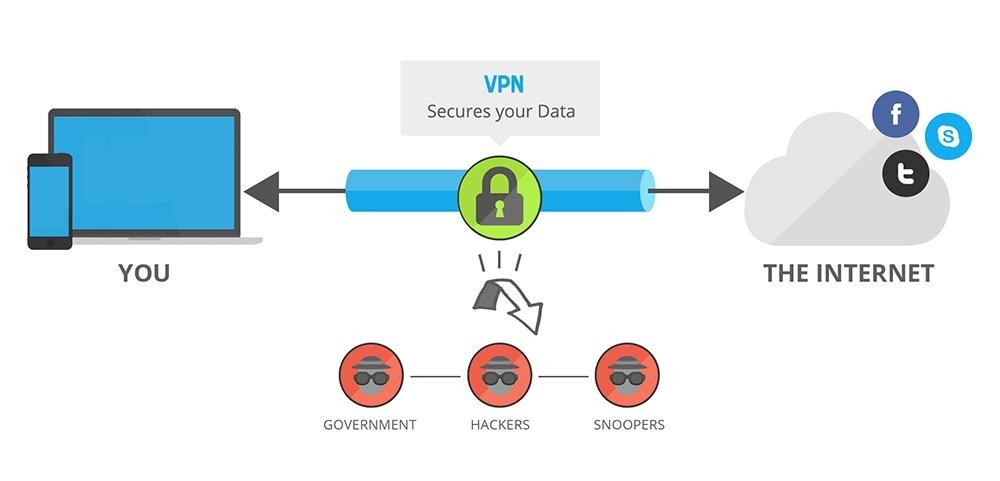
**5) VPN ( Virtual Private Network – Özel Sanal Ağ );**

* Sanal özel ağ ; uzaktan erişim yoluyla farklı ağlara bağlanmayı sağlayan bir internet teknolojisidir.
* VPN sanal bir ağ uzantısı oluşturduğu için, VPN kullanarak ağa bağlanan bir cihaz, fiziksel olarak bağlıymış gibi o ağ üzerinden veri alışverişinde bulunabilir. Kısacası Virtual Private Network (VPN), internet ya da başka bir açık ağ üzerinden özel bir ağa bağlanmayı sağlayan bir bağlantı çeşitidir.
* VPN üzerinden bir ağa bağlanan kişi, o ağın fonksiyonel, güvenlik ve yönetim özelliklerini kullanmaya da devam eder.



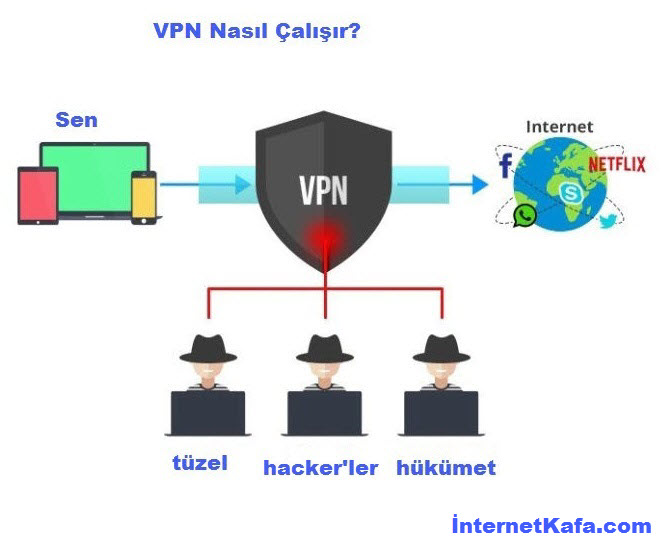
6 VPN (Virtual Private Network - özel sanal ağ )

* VPN istemcisi, internet üzerinden bağlantı kurmak istediği kaynakla sanal bir noktadan-noktaya (point-to-point ) bağlantı kurar, kaynak yada uzaktan erişime geçmek istediği sunucu kimlik bilgilerini kontrol eder ve doğrulama sonrasında VPN istemcisiyle uzaktan erişime geçtiği sunucu arasında veri akışı gerçekleşir. Veriler, akış sırasında noktadan-noktaya bağlantı gibi üst bilgi kullanılarak kapsüllenir. Üst bilgi, verilerin bitiş noktasına erişimleri için paylaşılan veya ortak ağ üzerinden yönlendirme bilgileri sağlar. Özel ağ bağlantısını taklit etmek için, gönderilen veriler gizlilik amacıyla şifrelenir. Paylaşılan veya ortak ağda ele geçirilen paketlerin şifreleri, şifreleme anahtarları olmadan çözülemez. Özel ağ verilerinin kapsüllendiği ve şifrelendiği bağlantı VPN bağlantısı olarak bilinir.
* Özel sanal ağlar ile internet gibi halka açık ağlar üzerinden güvenli bir şekilde kullanıcıların kendi kurum kaynaklarına erişmeleri sağlanmaktadır.
* Özel sanal ağ, ağlara güvenli bir şekilde uzaktan erişimde kullanılan bir teknolojidir.
* Özel sanal ağlar, yerel internet servis sağlayıcı ve kurumsal yerel ağlar arasında güvenli bir tünel üzerinden veri iletimi gerçekleştirerek çalışır.
* Uzaktan erişim VPN ve Siteden siteye VPN olmak üzere iki çeşit VPN bağlantısı bulunmaktadır. Tüm VPN çözümlerinde internet erişimi üzerinden kurulan güvenli tüneller söz konusudur.
* VPN teknolojisi, firmaların şubeleri ve iş ortakları ile aralarında veri iletişimini güvenilir. Kolay ve ekonomik biçimde sağlanmasına olanak veren bir tünelleme teknolojisidir. Kurumların yerel ağlarını internet ortamı üzerine taşınmasını sağlar.
* VPN teknolojisinde, noktalar arası ekonomik ve güvenilir bağlantılar kurulurken iletişim maliyetini minimum seviyede tutabilmek için internet ortamını “ iletişim omurgası “ olarak kullanılır.
* VPN’lerde kullanılan ağ kamuya açık bir ağdır, ancak ileti bir noktadan diğer noktaya kadar özel bir tünel aracılığı ile şifrelenerek ulaşır. Personel ve yöneticiler dünyanın neresinde olurlarsa olsunlar, yerel ağlarına sanki ofislerindeymiş gibi erişebilme imkanına sahip olurlar.



7 VPN (Virtual Private Network - Özel Sanal Ağ )

* Günümüzde sadece büyük kuruluşlar değil küçük ve orta ölçekli firmalar da ofislerini, bayilerini, iş ortaklarını kolayca ve ekonomik yoldan birbirine bağlayarak veri, hatta ses veya video iletişimi sağlama ihtiyacı duymaktadır. Bu network yapısını firmaların kendi başına kurmaları son derece yüksek maliyetli ve zahmetli olduğundan firmalar, bağlantı ihtiyaçlarını VPN’ler sayesinde daha düşük maliyetler karşılığında, ülke geneline dağılmış erişim noktalarına ve yüksek performanslı bir ulusal omurgaya sahip İSS’ler aracılığı ile karşılamayı tercih etmektedir.

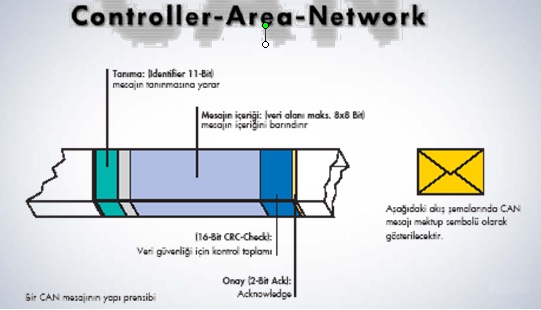


8 VPN nasıl çalışır?

**6) CAN ( Controller Area Network – Kontrol Alan Ağı );**

* CAN ingilizce açılımı ile Controller Area Network türkçesi ile ise Kontrol Alan Ağı Veri Yolu olan endüstriyel alanlarda çözüm sunarak haberleşmeyi sağlayan protokoldür.Performansı ve güvenilirliği oldukça yüksektir ki bu sebeple  gerçek zamanlı uygulamalarda tercih edilmektedir.
* 1983 yılında CAN-Bus olarak BOSH tarafından geliştirilmiş, 1986 yılında resmi olarak SAE tarafından piyasaya sürülmüş ve ilk CAN Chip 1987 yılında intel tarafından üretilmiştir.
* **CAN(Controller Area Network)** seri bir ağ teknolojisidir ve  oluşabilecek elektriksel gürültülerden etkilenmeyecek bir yapı ile geliştirilmiştir. Bunun için CAN-Hi ve CAN-Lo olmak üzere 2 ayrı kablo kullanılır. Bir başka önemli özelliği ise CAN kullanan bir sistemdeki farklı modüllere öncelik atamasının yapılabilmesidir. Örneğin  otomobilde hava yastığı, fren, abs gibi modüllerin ihtiyaç anında bir kullanım sırası ve duruma göre önceliği vardır. Ciddi oranda yüksek olan işlem hızı ile TCP/IP den ayrılırken gerçek zamanlı sistemler içinde önemli ve avantajlıdır. Bir başka önemli özelliği ise hızlı hata tespit ve düzeltmesidir.
* Baseband iletişim yaparken topoloji olarakta bus, star ve ring topolojiyi kullanır. Erişim metodu olarak CSMA/CR kullanılır.
* Katman yapısı olarak ise OSI ve TCP/IP den tamamiyle ile farklıdır.  3 katmandan oluşmaktadır.

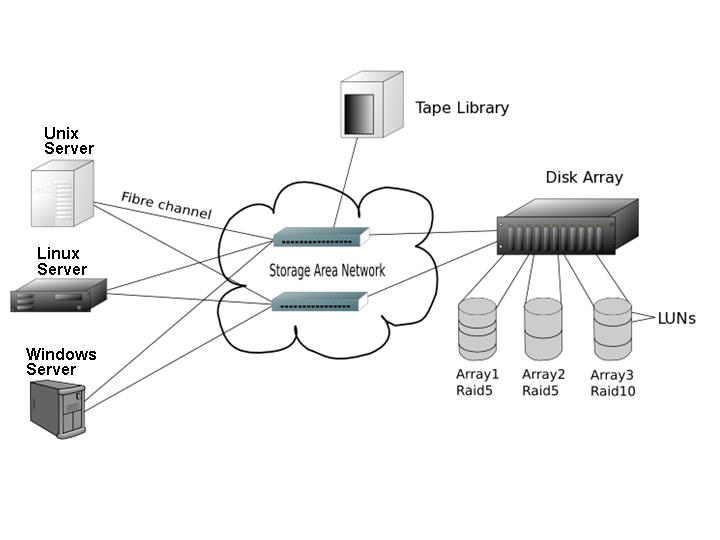
1. Nesne Katmanı
2. Transfer Katmanı
3. Fiziksel Katman



9CAN (Controller Area Network - Kontrol Alan Ağı )

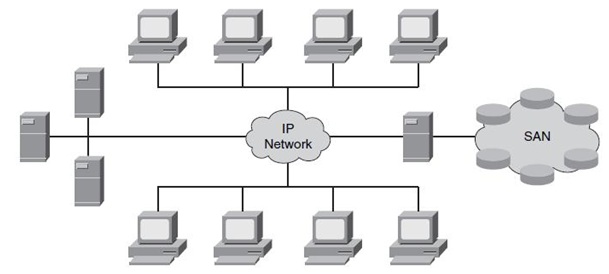
**7) SAN (Storage Area Network – Depolama Alan Ağı );**

* Depolama alan ağı ; büyük ağ kullanıcılarına hizmet vermek üzere veritabanı sunucuları ile birlikte farklı tipteki veri depolama cihazlarını birbirine bağlayan ve bu cihazlar arasında veri alışverişine olanak veren özel amaçlı, yüksek hızlı bir ağdır. Bir depolama alan ağı, yönetim katmanına fiziksel bağlantılar sağlayan ve aynı zamanda bilgisayar sistemlerini, depo birimlerini ve bu birimlerin aralarındaki bağlantıları düzenleyen bir iletişim altyapısından oluşmaktadır.
* Bir depolama alan ağı aynı zamanda depolama birimleri, depolama aygıtları, bilgisayar sistemleri ve/veya uygulama aracı gibi birimlerden oluşan ve ağ üzerinden iletişim sağlayan bir depolama sistemi olarak da düşünülebilir. Depolama alan ağı, LAN ve WAN’da olduğu gibi benzer bileşenleri kullanarak depolama aygıtlarını ve sunucularını birbirine bağlar.
* Artan depolama alanı gereksinimleri büyük kuruluşların geleneksel dosya sunucularından daha gelişmilş olan SAN çözümlerine yönelmesine sebep olmuştur.
* SAN uygulamasında bir depolama ünitesi herhangi tek bir sunucunun özel malı olmak yerine, depolama birimleri ağdaki sunucu ve diğer depolama ünitelerinin ortak malıdır.
* Yedekleme ve geri yükleme sürecinde verileri taşımak için yerel ağ kullanılmayarak, yerel ağ üzerindeki hizmetler ve kullanıcılar için performans artışı sağlanmaktadır. Bu tür depolama uygulaması, yerel ağdan bağımsız yedekleme çözümü olarak anılmaktadır. Kısa zamanda fazla veri depolanmasını sağlamakta ve merkezi bir yönetime olanak vermektedir.
* Sunucular, saklama ortamı olarak üzerlerine düşen görevi yapmasına karşılık, kapasiteleri sınırlıdır ve aynı bilgiye birçok kişi erişmeye çalıştığında darboğaz oluşabilir. Bu yüzden birçok kuruluşta teyp üniteleri, RAID diskler ve optik saklama sistemleri gibi çevre birimi saklama aygıtları kullanılmaktadır. Bu tür aygıtlar verinin çevrimiçi yedeklenmesinde ve büyük miktarlarda bilginin saklanmasında etkin rol oynarlar.
* Sunucu boyutları ve yoğun uygulamalar arttıkça geleneksel saklama ortamı stratejileri iflas etmektedir. Çünkü bu çevre birimi aygıtlarına erişim yavaştır ve her kullanıcının bu saklama aygıtlarına saydam bir şekilde erişimi mümkün olamayabilir. SAN’lar verilere daha hızlı erişim ve daha fazla seçenek sunmaktadır. Kısacası SAN ; sunucuları depolama birimlerine, depolama birimlerini birbirlerine ve sunucuları birbirine bağlamaktadır.



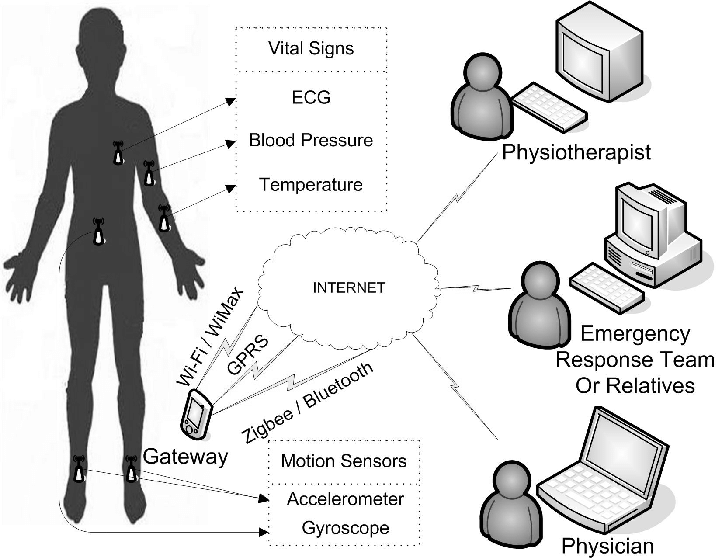
10 SAN (Storage Area Network - Depolama Alan Ağı )

* Şekilde temel bir SAN topolojisi görünmektedir.



### **8) Vücut Alan Ağı – Body Area Network (BAN) ;**

Vücut Alan Ağı bir kişinin vücuduna takılan veya yerleştirilen bilgi işlem cihazlarının birbirlerine bağlanmasıyla elde edilen bir kablosuz ağ çeşididir. Bu ağı giyilebilir bir kablosuz ağ olarak da ifade etmek mümkündür.



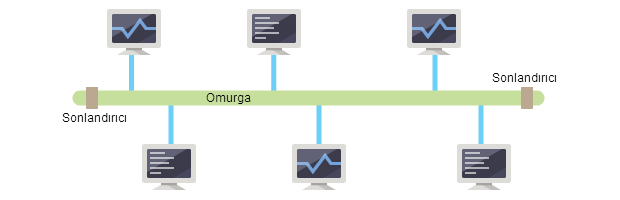
11 Vücut Alan Ağı – Body Area Network (BAN)

-**AĞ TOPOLOJİLERİ –**

* “ bir ağı oluşturan cihazların fiziksel ve mantıksal yerleşimidir”. Ağ topolojileri fiziksel topoloji ve mantıksal topoloji olmak üzere 2 sınıfa ayrılır.
* **FİZİKSEL TOPOLOJİ;** Ağ cihazlarınınbağlantı şekilleri, kullanılan kablolar ve kabloların yerleşim düzeni, cihazların ağ üzerideki yerleşimleri fiziksel topoloji olarak tanımlanır. Fiziksel topoloji türleri ortak yol, halka, yıldız, genişletilmiş yıldız, örgü ve ağaç topolojisidir.
* **ORTAK YOL (BUS) TOPOLOJİSİ;** **Ortak yol topolojisinde** iletişim omurga (backbone) denilen tek bir hat üzerinden gerçekleştirilir. Ağda gönderilen veri hedefe ulaşıncaya kadar veya sonlandırıcıya gelinceye kadar hat üzerinde bulunan tüm cihazlara uğrar. Bu sebeple ağ performansı oldukça düşük bir topolojidir.

Bus topolojisinde genellikle koaksiyel kablo kullanılır. İnce koaksiyel kablo kullanıldığında hattın uzunluğu 185 metre, kalın koaksiyel kablo kullanıldığında en fazla 500 metredir. Ağa maksimum 30 cihaz bağlanabilir.

Ağ üzerindeki bir cihaz veri göndermeden önce hattın başka bir cihaz tarafından kullanılıp kullanılmadığını kontrol eder. Ağ kullanımdaysa hattın boşalmasını bekler.



1 ORTAK YOL (BUS) TOPOLOJİSİ

**Ortak yol topolojisinin avantajları;**

* Ağın kurumu kolaydır.
* Ağa yeni cihaz eklenmesi kolaydır.
* Ekonomiktir.
* Daha az kablo kullanılır.
* Switch/hub gerektirmez.

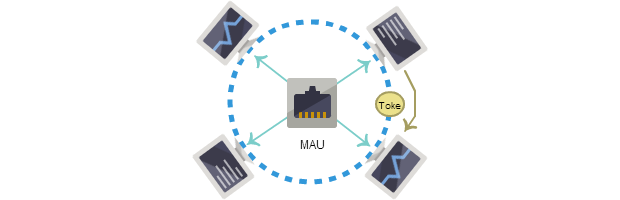
**Ortak yol topolojisinin dezavantajları;**

* Ağa bağlanabilecek cihaz sayısı sınırlıdır.
* Ağın hat uzunluğu sınırlıdır.
* Omurga üzerindeki bir sorun tüm ağı etkiler.
* Yaşanabilecek sorunların tespiti ve giderilmesi zordur.
* Ağın bant genişliği düşüktür.

## **Halka Topolojisi (Ring);**

**Halka topolojisinde**, halka biçimindeki ağ üzerinden gönderilen veri alıcı cihaza ulaşıncaya kadar ağ üzerindeki tüm cihazlara teker teker uğrar. Ağ üzerindeki veri 3 byte’ lık jeton (token) denilen bir kılavuz ile gönderilir. Jeton ağ üzerinde sürekli dolaşır ve göndericiden aldığı veriyi alıcıya ulaştırır. Halka topolojisinde ağa bağlı cihazlardan birinin arızalanması ağın çökmesine sebep olur.

Halka topolojisinin yapısı merkezde bulunan bir Multistation Access Unit (MAU) ve ağa bağlı cihazlardan oluşur. Ağ bağlantısı çift burgulu kablolar ile gerçekleştirilir. **Halka topolojisi**, ağ topolojileri içerisinde en az kullanıma sahip topolojidir.



2 Halka Topolojisi (Ring);

**Halka topolojisinin avantajları;**

* Bağlı tüm cihazlar aynı yetkiye sahiptir.
* Sunucuya ihtiyaç yoktur.
* Ağın büyütülmesi performansı az etkiler.

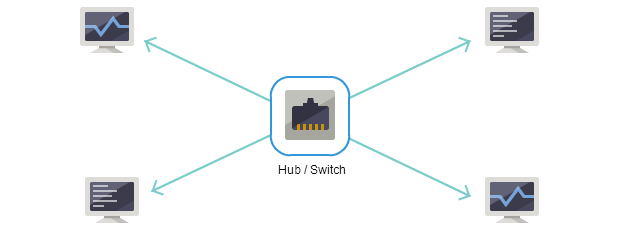
**Halka topolojisinin dezavantajları;**

* Bağlı cihazlardan birindeki arıza ağın çökmesine neden olur.
* Ağ arayüz kartları ve MAU, ethernet ve switch’ e göre pahalıdır.

## **Yıldız Topolojisi (Star);**

**Yıldız topolojisi** en yaygın kullanıma sahip topolojidir. Merkezdeki bir hub ya da swith’ e bağlı cihazların iletişimi merkezde bulunan cihaz üzerinden gerçekleştirilir. Ağa bağlı bir göndericiden çıkan veri önce merkezdeki hub ya da switch’ e gelir, oradan da alıcı cihaza gönderilir. Hub ya da switch’ teki bir sorun tüm ağı etkiler.

Yıldız topolojisinde çift burgulu kablolar kullanılır. Cihazların hub ya da switch uzaklığı en fazla 100 metredir. 100 metreden sonra performans büyük oranda düşer.



3 Yıldız topolojisi (Star)

**Yıldız topolojisinin avantajları;**

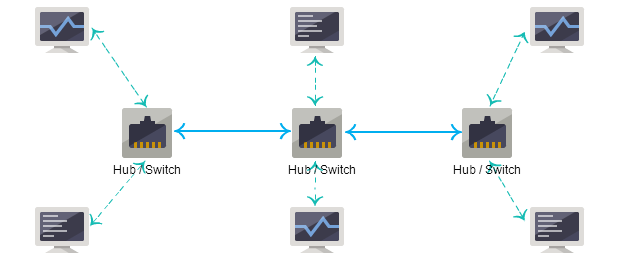
* Ağın yönetimi ve sorun tespiti kolaydır.
* Ağa yeni cihaz eklemek kolaydır.
* Bağlı cihazda oluşacak sorun ağı etkilemez.

**Yıldız topolojisinin dezavantajları;**

* Merkezdeki cihazda oluşacak sorun tüm ağı etkiler.
* Çok fazla kablo bağlantısı gerektirir.

**Genişletilmiş Yıldız Topolojisi (Extended Star);**

Yıldız topolojisinin genişletilmiş halidir. Merkezde bulunan hub ya da switch’ e yeni hub/switch eklenmesi ile oluşturulur. Ağa bağlanacak cihaz sayısının çok olması ve hub/switch’ in port sayısının yetersiz kaldığı durumlarda ağa yeni hub/switch’ lerin bağlanması **genişletilmiş yıldız** topolojisinin kullanımına örnektir.

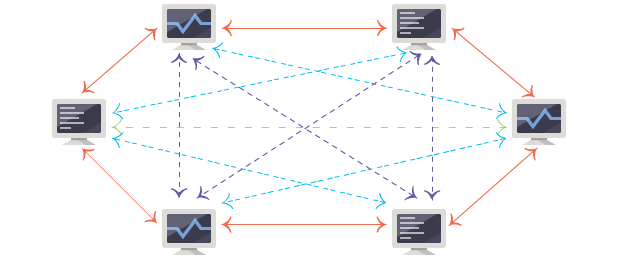


4 Genişletilmiş Yıldız Topolojisi (Extended Star)

Genişletilmiş yıldız topolojisinin avantaj ve dezavantajları yıldız topolojisi ile aynıdır.

* **Örgü Topolojisi (Mesh);**

**Örgü topolojisinde**, ağa bağlı bir cihaz ağdaki diğer cihazlara doğrudan bağlantılıdır. Çoğunlukla geniş alan ağları (WAN) arasında kullanılır. Ağa bağlı cihaz sayısı ‘**N**‘ ise, ağ üzerindeki bağlantı sayısı ‘**N\*(N-1)/2**‘ adettir.



5 Örgü Topolojisi (Mesh)

**Örgü topolojisinin avantajları;**

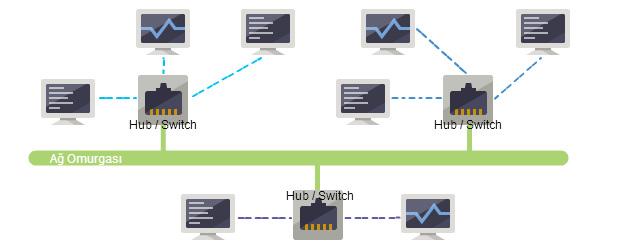
* Bir cihaza bağlı hatta sorun oluşması cihazın iletişimini kesmez.
* Veri iletim hızı oldukça yüksektir.
* Ağın genişletilmesi diğer bağlantıları etkilemeden yapılabilir.

**Örgü topolojisinin dezavantajları;**

* Bağlantı sayısı çoktur.
* Karmaşık bir yapısı vardır.
* Çok fazla kablo kullanılır.
* Maliyeti yüksektir.
* **Ağaç Topolojisi (Tree);**

**Ağaç topolojisi** yıldız topolojisi ile ortak yol topolojisinin birlikte kullanıldığı topolojidir. Merkezdeki bir ortak yol (omurga) üzerine yerleştirilmiş hub ya da switch’ lere bağlı cihazlarla oluşturulur.

Bu topolojiye **ağaç topolojisi** denmesinin nedeni omurganın ağaç gövdesini, hub ya da switch üzerinden bağlanan bilgisayarların da ağacın dallarını modellemesidir. *Ağaç topolojisi* büyük ağların omurgalarını oluşturmak için kullanılır.



6 Ağaç Topolojisi (Tree)

**Ağaç topolojisinin avantajları;**

* Farklı üreticilerin donanımları ile uyumlu çalışır.
* Ağın genişletilmesi kolaydır.
* Sorunların tespiti ve giderilmesi kolaydır.
* Ağın yönetimi ve bakımı kolaydır.
* Dallardan birinde oluşacak sorun diğerlerini etkilemez.

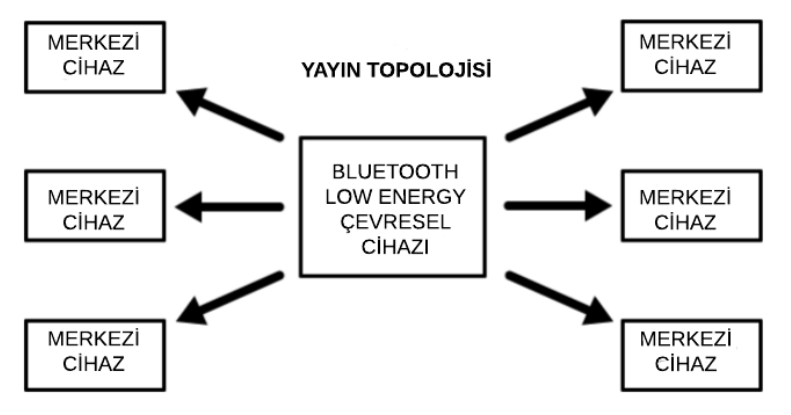
**Ağaç topolojisinin dezavantajları;**

* Kablolama işlemi zordur.
* Dallanma arttıkça ağın bakımı ve yönetimi zorlaşır.
* Omurgada yaşanacak bir sorun tüm ağı etkiler
* **MANTIKSAL TOPOLOJİ;**

Ağ üzerindeki cihazların haberleşme şekilleri ve kullandıkları iletişim protokolleri **mantıksal topoloji** ile açıklanır. Mantıksal ağ topolojileri yayın topolojisi ve jetonlu geçiş topolojisi olmak üzere 2 sınıfa ayrılır.

**Broadcast – Yayın Topolojisi;**

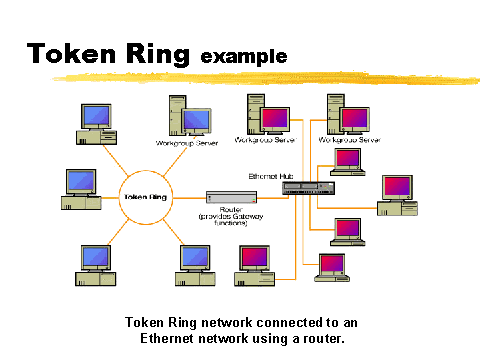
Bu topolojide gönderici cihaz veriyi ağa bırakır, veri alıcıya ulaşıncaya kadar tüm ağı dolaşır. Ağa bağlı cihazların öncelik hakkı yoktur ve ağdaki tüm cihazlara veri iletimi gerçekleştirilir.



7 Broadcast – Yayın Topolojisi

**Token Passing – Jetonlu Geçiş Topolojisi;**

Halka topolojisinde olduğu gibi tüm ağı dolaşan bir jeton (token) veri iletimini gerçekleştirir. Jeton ağ üzerinde dolaşırken sıraylatüm cihazlarla iletişime geçer ve gönderilecek ya da alınacak veri olup olmadığını kontrol eder.



8 Token Passing – Jetonlu Geçiş Topolojisi

**-** **BAĞLANTI ORTAMLARINA GÖRE AĞLAR –**

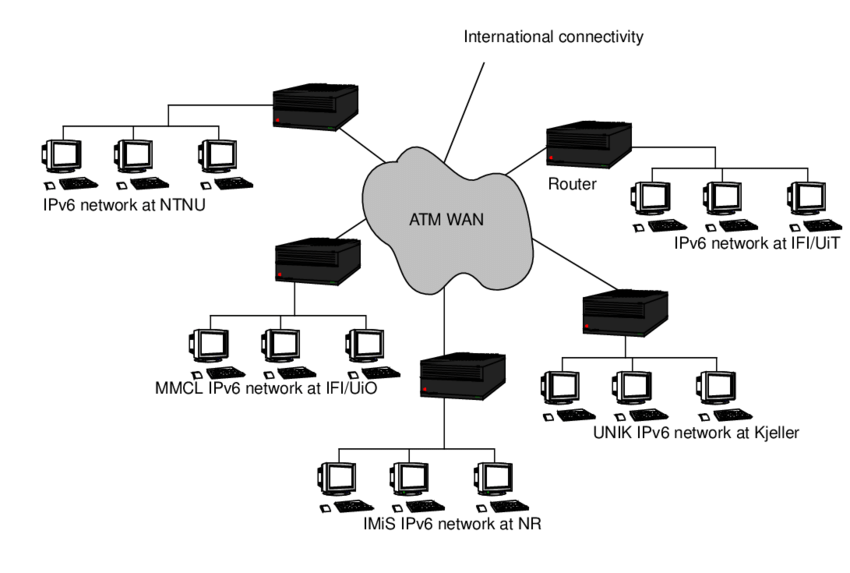
1. **ATM (Asynchronous Transfer Mode – Eşzamansız Aktarım Modu)**
2. **FDDI (Fiber Distributed Data Interface – Fiber Dağıtılmış Veri Arayüzü)**
3. **Token Ring (Andıçlı Halka )**
4. **Ethernet**

Bir ağ tasarımı yaparken ağın hızı, maliyeti ve kablolama şekline göre bir seçim yapılmalıdır. Bu seçimler şunlar olabilir;

|  |  |  |  |
| --- | --- | --- | --- |
| **PROTOKOL** | **KABLO** | **HIZ** | **TOPOLOJİ** |
| Ethernet | UTP, Koaksiyel | 10-100 Mbps | Ortak yol, yıldız,ağaç |
| Token ring | UTP | 4-16 Mbps | Yıldız-mantıksal halka |
| FDDI | Fiber optik | 100 Mbps | İkili halka |
| ATM | UTP, Fiber optik | 155-2488 Mbps | Ortak yol, yıldız,halka |

**ATM (Asynchronous Transfer Mode – Eşzamansız Aktarım Modu ;**

* Asynchronus Transfer Mode (ATM- Asenkron Aktarım Modu ) Paket anahtarlama temeline göre çalışan bir protokolüdür. 155 Mbps ve üzerinde veri iletişim imkanı sağlar. ATM, sabit büyüklükte küçük paketler halinde veri iletişimi yaparak çalışır. Diğer protokoller veri iletişimini değişken paket uzunluklarında yapar.
* ATM omurgaya bir bilgisayar bağlanması için ATM ağ kartı kullanılır. ATM ağa bağlı uç sistemler, gelen LAN emülator yazılım aracılığıyla birden fazla LAN tek bir kart ile üye olabilir.
* ATM ile birbirine uzak ağların iletişimi sağlanır ya da bir ağ omurgası (backbone) oluşturulabilir. Genellikle iki veya daha fazla yerel alan ağını bi1234rbirlerine bağlamakta kullanılır. En önemli özelliği her bağlantı için ayrı bir yol sunmasıdır böylece kaynağa aynı anda birden fazla kullanıcı bağlanabilir. ATM, her fiber optik kablolama hem de çift bükümlü kablo üzerinden yıldız topolojide çalışır.
* Çeşitli uygulamalar için özel band ayırabilir. Böylece gecikmeye duyarlı ses ve görüntü iletimi de kolaylıkla gerçekleştirilebilir. Ancak Ethernet bağlantısının çok yoğun olması sebebiyle yaygınlaşamamıştır.
* Çok yüksek hıza ihtiyaç duyan ve yoğun çalışan bilgisayarlarda bağlantıların aynı anda gerçekleşmesi amacıyla kullanılmaktadır. ATM sunduğu üstün özellikler sayesinde büyük ağlara sahip kurumların ana omurgasını oluşturmada kullanılmaktadır.ses ve görüntü iletişimini aynı ağ üzerinden iletilmesini sağladığından yerel ve geniş alan ağlarında kullanımı yaygınlaşmaktadır.
* ATM teknolojisi pek çok ağ cihazı ile uyumlu çalışabilir. Bunlar ;
* PC, iş istasyonu ve sunucu ağ arabirim kartları
* Anahtarlamalı Ethernet ve token ring çalışma grubu hub’ları
* Çalışma grubu ve kampüs anahtarları
* ATM enterprise ağ anahtarları
* ATM çoğullayıcıları
* ATM uç anahtarları
* ATM omurga anahtarları



9 ATM ( Asenkron Aktarım Modu )

**HUB;**

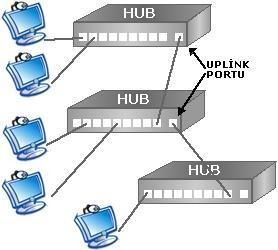
Ağ elemanlarını birbirine bağlayan çok portlu bir bağdaştırıcıdır. En basit ağ elemanıdır. Hub kendisine gelen bilgiyi gitmesi gerektiği yere değil portlarına bağlı bütün bilgisayarlara yollar. Bilgisayar gelen bilgiyi analiz ederek kendisine gelmişse kabul eder.



10 HUB

Hublar 4, 8, 12, 16, 24 portlu olarak üretilir. Hub’a UTP kablo ile bağlanılır. Ve her bir bağlantı 100 metreden daha uzun olamaz. Hub çalışırken herhangi bir portundan kablo çıkartmanız veya takmanız herhangi bir sorun çıkartmaz.

Ağ kurulduktan sonra ortaya çıkan problemlerden biri ağın genişlemesidir. Ağ genişledikçe mevcut hub’ın port sayısı yeterli olmayabilir. Böyle durumlarda ya daha çok porta sahip bir hub alınır ya da başka bir hub ile mevcut hub birbirine bağlanır. Hub’lar birbirine bağlanarak ağın daha da genişlemesi sağlanabilir. Hub’ların birbirine bağlanması için hub’ların çoğunluğunda bulunan uplink portu kullanılır.



11 Hub'ların birbirine bağlanması

**FDDI (Fiber Distributed Data Interface – Fiber Dağıtılmış Veri Arayüzü);**

* Fiber Distributed Data Interface (FDDI- Fiber Dağıtılmış Veri Arayüzü ), genellikle uzak mesafelerdeki bir veya daha fazla yerel alan ağını birbirine bağlamak için geliştirilmiş ağ protokolüdür.
* Yüksek hıza ihtiyaç duyulan ağlarda kullanılır. 100 Mbps hızında token-passing ( jeton atlatma ) erişim tekniğine sahiptir. Fiber optik kablo teknolojisi ile bağlantı sağlanır. Ancak günümüzde bakır telden yapılmış kabloyla da iletim sağlanabilmektedir.

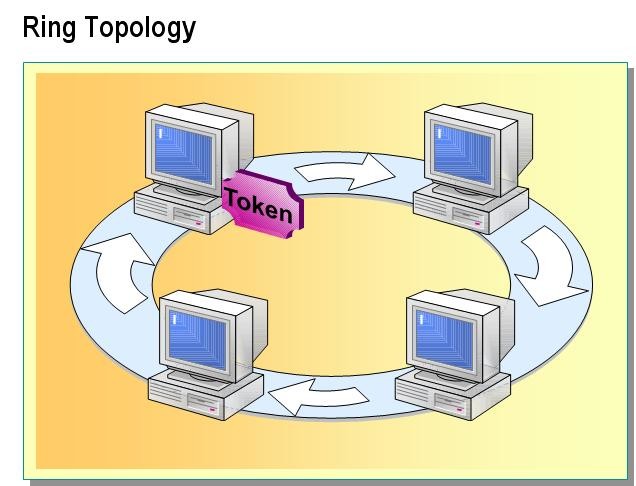


12 FDDI Ağ Kartı

* Token ring ağlarda bir bilgisayar token’a veri yüklendikten sonra token tekrar boşalıncaya kadar ağ üzerinde tekrar başka bir iletim olmaz yani ağ tam kapasiteyle kullanılamaz. Ancak FDDI ağlarda jeton’un boşalması beklenmeden yeni veriler ardı ardına gönderilebilir. Bir ağa koymuş olduğu veri tekrar kendisine ulaşıncaya kadar halkada dolaşır.
* Bu protokolün en büyük üstünlüğü, çalışmaların sayısını azaltmasıdır. Bu yüzden bu protokol 100 Mbps hızında daha verimli olarak çalışabilmektedir. FDDI Fiber-optik tabanlı olduğundan çok daha büyük kablo uzunluklarına imkan sağlar. Böylece tek bir fiber-optik kablo ile 200 km’ye kadar iletişim sağlanabilir.

**TOKEN RİNG (Andıçlı Halka );**

* Token ring network IBM tarafından geliştirilmiş. Daha sonra ANSI/IEEE standardı (IEEE 802.5) olmuştur. Token passing ( jeton aktarım ) erişim yöntemini kullanır.
* Token ring ağında bilgisayarlar yıldız bağlantı şekline göre kurulur ve bir merkezi birime bağlanır. Mantıksal bir halka bağlantısı varmış gibi çalışırlar. Sinyal bu mantıksal halka içinde dolanır. Bu ağa jeton ( token ) adı verilen bir veri vardır. Bu jeton ağda dolanır. Bir bilgisayar veri iletmek istiyorsa veriyi jetona ekler ve veri halkadaki dolaşımına devam eder. Jeton her bilgisayara uğrar. Bilgisayar kendisine gelmiş bir bilgi varsa bu bilgiyi alır ve jetonu tekrar halkaya bırakır.



13 Token ring ağında jetonun dolaşımı

* Bu sistemde verilerin çalışması mümkün değildir. Bu sebeple ağın genişlemesi ile ortaya çıkan performans düşüklüğü bu yöntemde daha azdır. Ancak token ring için gereken ağ donanımının Ethernet’e göre 4-5 kat daha pahalı olması bu sistemin en büyük sakıncasıdır.

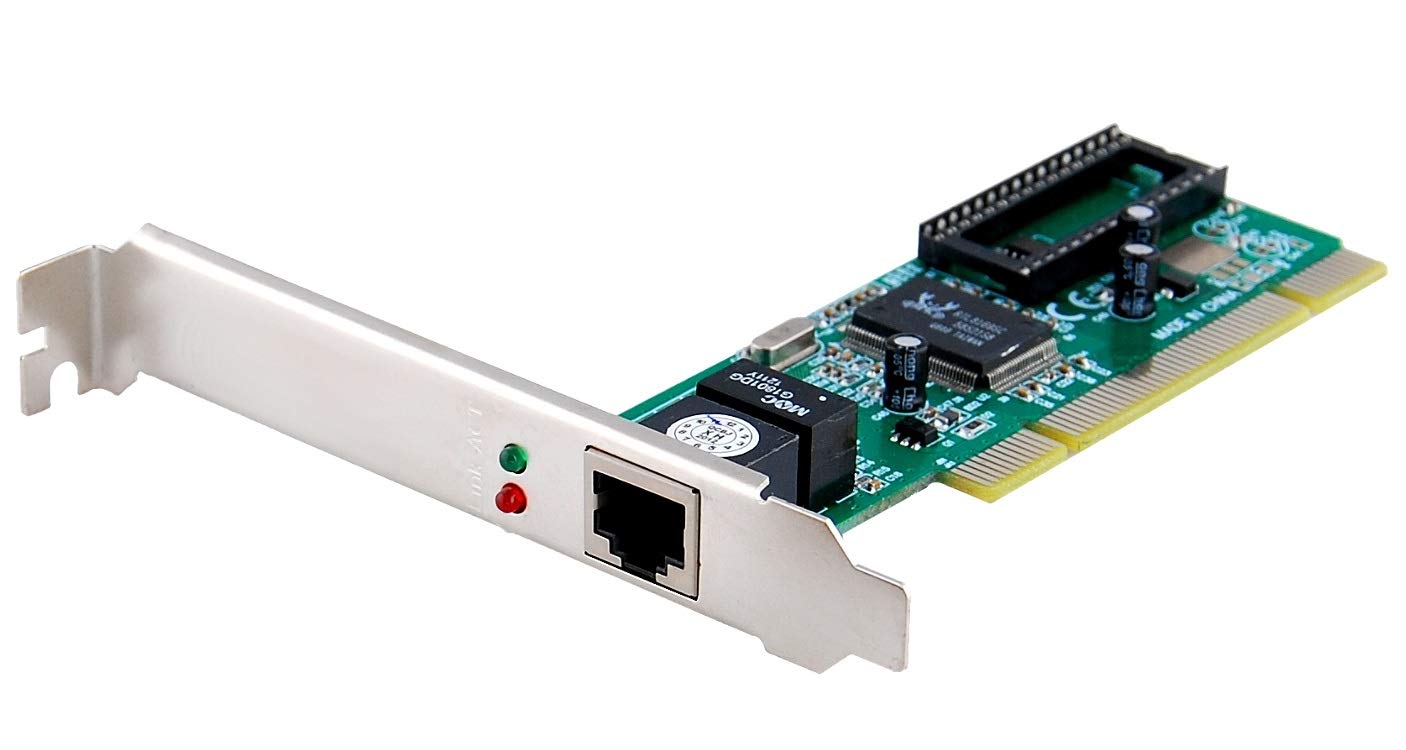


14 Token ring Ağ kartı

* Token ring fiber optik kablo veya twisted pair kablo kullanılır. Yıldız – kablolamalı halka ( star – wired ring ) topolojisi ile ağ üzerine yerleştirilir. 4 Mbps veya 16 Mbps veri iletişim hızlarında çalışır.
* Pek yaygın değildir. Yaygın olmamasının ana sebebi, bu yapıyı geliştiren tek bir firma vardır. Ortak geliştirilmediği için genel anlamda pek kabul görmemiştir.
* Token ring ağlarında MAU ( Media Access Unit – ortam erişim birimi ) adı verilen, Ethernet’teki hub’a benzeyen merkezi birim bulunur. Ağdaki bilgisayarlar yıldız şeklinde MAU’ya bağlanır. MAU içinde mantıksal yapı tutulur. Ancak token ring kartlar ve MAU’nu fiyatı oldukça yüksektir.

**ETHERNET;**

* Ethernet en bilinen ve en çok kullanılan ağ teknolojisidir. Kullanımı çok yaygınlaşmıştır. Ağ kartı ile Ethernet kartı aynı anlamda kullanılmaktadır. Ethernet ortaya çıktığından beri kullanım kolaylığı ve üretim haklarının herkese açık olması sebebiyle en çok kullanılan LAN teknolojisi olarak ağ dünyasında büyük bir yer edinmiştir.



15 Ethernet kartı

* Belirli standartlar kullanarak 100 Mbps ( mega bit per second/ saniyede transfer edilen veri miktarı) hıza kadar veri transferi gerçekleştirilebilir. Gelişmiş kablolama sistemleri ( fiber optik ) ile daha yüksek hızlara ulaşmak mümkündür.
* İnternet’in DSL ve kablo modem gibi yüksek hızlı geniş bant cihazlar ile her eve girmesi, ethernet’e olan ihtiyacı arttırmaktadır.
* IEEE 1985 yılında “ IEEE 802.3 Carrier Sense Multiple Access With Collision Detection ( CSMA/CD) Access Method and Physical Layer Specifications “ ismiyle yeni Ethernet standardını yayınladı. Bu tarihten sonra standart belirleme işi ISO tarafından yapılmaktadır. Bu tarikten itibaren üretilen tüm ürünler IEEE 802.3 CSMA/CD standardına uygun olarak üretilmiştir. Piyasada IEEE 802.3 CSMA/ CD standardına göre üretilen ürünler Ethernet teknoloji olarak adlandırılır.
* IEEE kurumu tarafından belirlenen Ethernet tipleri şunlardır. Burada 10 ifadesiz hız yani 10 MBPS anlamına gelmektedir. Base ifadesi baseband, broad ifadesi broadband anlamına gelmektedir.
* Ethernet kablo teknolojileri ;
* **10Base2:** İnce koaksiyon kablo ile 10 Mbit hızında Ethernet ağı. Ucuzlğu sebebiyle ( cheapernet ) veya ince kablo kullanıldığı için ince Ethernet (thinnet ) olarak da adlandırılır. 2 rakamı maksimum kablo uzunluğunu ifade etmektedir. Ki ince koaksiyonel kablo maksimum 185 m olmalıdır.
* **10Base5:** Kalın koaksiyonel kablo ile 10 Mbit hızında Ethernet ağı. Kalın Ethernet (thicknet ) olarak da adlandırılır. 5 rakamı maksimum 500 m olmalıdır.
* **10BaseF:** Fiber optik kablo ile 100 Mbit hızında Ethernet ağı. F ifadesi fiber optik kablo kullanıldığını belirtir.
* **10BaseT:** Korunmasız çift bükümlü ( unshielded twisted pair) kablo üzerinde 10 Mbit hızında Ethernet. T ifadesi kablo tipini (twisted pair) belirlemektedir. Fast Ethernet ( hızlı Ethernet ) olarak da anılır. 10BaseT, ortak yol – yıldız topolojileri kullanan Ethernet kablolama sistemini tanımlar. Kullanılan kablo haricinde Ethernet paket yapısı ve çalışma mantığı 10Base2 ve 10Base5 ile aynıdır.
* **100BaseT:** Korumasız çift bükümlü (unshielded twisted pair) kablo üzerinde 100Mbit hıznda Ethernet T ifadesi bükümlü kablo (twisted pair) kullanıldığını belirtir.
* **10Base36:** Broadband yayın yapan kablo ile 10Mbit hızında Ethernet ağı kablo uzunluğu maksimum 3600 metre olabilir.
* Ethernet çalışma esası ;
* Ethernet kartı veriyi hatta (kabloya) bırakmadan önce hattı denetler. Hat başkası tarafından kullanılmıyorsa gönderen ve alıcının MAC adreslerini içeren veriyi hatta bırakır.
* Ethernet veriyi çerçeveler haline getirerek diğer bilgisayarlarla gönderir. Veri hatta bırakılmadan önce protokollerden faydalanılarak verinin baş ve son tarafına çeşitli bilgiler eklenir.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ÖNTAKI** | **BAŞLA AYIRACI** | **ALICI ADRESİ** | **GÖNDERİCİ ADRESİ** | **PAKET UZUNLUĞU (TÜR)** | **VERİ** | **CRC** |
| 7 byte | 1 byte | 6 byte | 6 byte | 2 byte | 46-1500 byte | 4 byte |

Ethernet çerçeve formatı

**ÖNTAKI:** Alıcı ile verici saatinin senkronize olmasını sağlar.

**ALICI ADRESİ:** Çerçeveyi alacak bilgisayarın MAC adresini içerir.

**GÖNDERİCİ ADRESİ:** Çerçeveyi gönderen bilgisayarın MAC adresini içerir.

**PAKET UZUNLUĞU ( TÜR ):** Alınan çerçevelerin hangi üst katman protokolüne veya fonksiyonuna gönderileceğini belirler.

**VERİ:** Aktarılacak veridir. 10Mbps’lık ağlarda 46 ile 1500 byte arasında olmalıdır.

**ÇERÇEVE HATA SINAMA (CRC):** Bir tür hata sınama algoritmasıdır. Öntakı dışında çerçevenin tüm bitleri için yapılır. Verinin karşıya doğru ulaşıp ulaşmadığını denetler.

**TCP/IP MODELİ;**

## TCP/IP Modeli, en az iki bilgisayarın ağ üzerinde haberleşme kurallarını belirleyen, iletişimi sağlayan bir yapıdır ve 5 katmandan oluşur.

Bu katmanlar ;

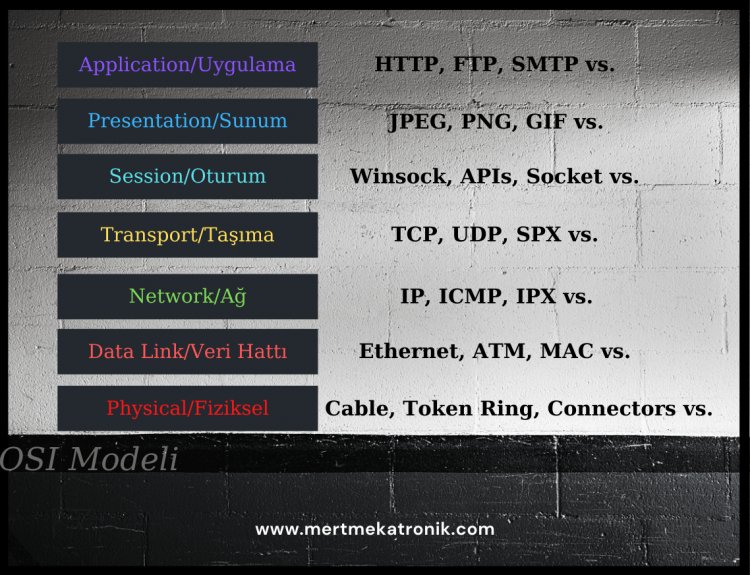
* **UYGULAMA KATMANI**
* **TAŞIMA KATMANI**
* **AĞ KATMANI**
* **VERİ HATTI KATMANI**
* **FİZİKSEL KATMAN**

İnternet ortamında iletişim kurabilmek için bazı gereçlere ihtiyaç vardır. Bunu kendi dünyamızda iletişim kurmak için kullandığımız konuşma diline benzetebiliriz. İnternetin de kullanılabilmesi için iletişimini sağlayan dile protokol deriz.

**Protokol:** En az iki bilgisayarın ağda iletişim kurabilmesini sağlayan kurallar dizisidir. Farklı iletişim türleri için farklı protokoller mevcuttur. (TCP, IP, UDP, HTTP, FTP, SMTP, DNS, DHCP, TFTP, SNMP vs.). Bu protokoller OSI, TCP/IP gibi modellerin farklı katmanlarında çalışırlar.

## **OSI Modeli;**

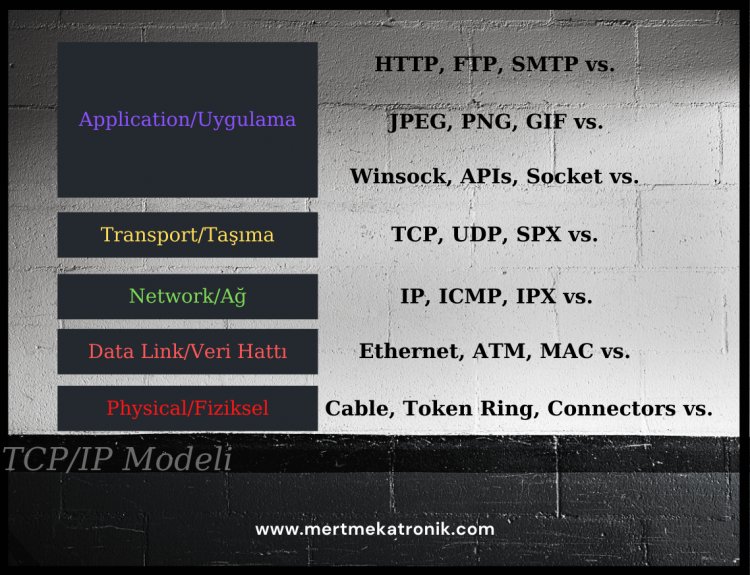
**Açılımı:** Open Systems Interconnection. Bilgisayarların hayatımıza girdiği ilk zamanlarda farklı üreticiler farklı protokoller ile iletişimi sağlıyordu. Bu sebeple farklı firmalarda üretilen cihazların entegrasyonu zorlaşıyordu (Cihazlar farklı dil konuştuğu için anlaşamıyordu diyebiliriz.). Bunu ortadan kaldırmak için OSI modeli üretildi ve kısa sürede tüm üreticiler tarafından kabul gördü. OSI modeli 7 katmandan oluşan bir yapıdır.



16 OSI Modeli

## **TCP/IP;**

Zaman ilerledikçe OSI modeli yerine daha az katman ile iletişimi sağlayabilen TCP/IP modeli geliştirildi. Bu model sayesinde internet ortamında iletişimi sağlamak için 7 olan katman sayısı 5’e düştü. OSI modelinin İlk 3 katmanın yaptığı işi TCP/IP, Uygulama katmanında yapılabilir hale getirdi. Ancak yine de ağ oluşturma sürecini detaylı bir şekilde anlattığı için OSI Modeli, anlatımlarda tercih edilir.



17 TCP/IP Modeli

### **TCP/IP Nasıl Çalışır?**

TCP/IP internet ortamında bilgisayarlar arası iletişimi sağlar. Gönderilmek istenen bir paket, bir bilgisayardan diğerine hareket ederken TCP/IP’nin her katmanında belirli işlemlerden geçer. Kullanıcılar, bu katmanların içinde sadece uygulama(application) katmanı ile birebir etkileşime girer.

**Örneğin;** bir kullanıcı (istemci) bir web sitesini ziyaret etmek istiyor olsun. Bunun için tarayıcıda adrese tıkladığı an uygulama (application) katmanında HTTP protokolünü çalıştırmış olur. HTTP protokolü bu isteği taşıma (transport) katmanına iletir ve hangi portlar üzerinden hangi formatlar ile bağlanıldığı bilgisi eklenir. Daha sonra ağ (network) katmanında IP adresi çözümlenir ve hem istemcinin hem de sunucunun adresleri eklenir. Veri hattı (data link) katmanında ise MAC adresi bilgileri elde edilir. Fiziksel (physical) katmanda tüm bu bilgiler, bitlere ve sinyallere dönüştürülerek kablolar üzerinden veya kablosuz olarak, adreslenen sunucuya gönderilir. Bit olarak gönderilen veriler karşı tarafın TCP/IP modelinin fiziksel katmanına iletilir ve aşağıdan yukarıya olacak şekilde tüm bilgiler okunur ve istenen paketler istemciye gönderilir. Daha sonra sayfa yüklenir ve istemci tarafında görüntülenir.

### **TCP/IP Katmanları ve Çalışan Protokoller**

**UYGULAMA KATMANI;**

Bu katman, uygulamaların canlıya çıktığı bölümdür. Bu katmandaki protokoller uzak bir bilgisayar ile iletişim sağlayabilmek için taşıma katmanını kullanırlar. Uygulamalar, taşıma katmanının verdiği port numaraları üzerinden iletişime geçerler.

Uygulama katmanı protokolleri;

**HTTP (Hyper Text Transfer Protocol, Üstün Metin Transfer Protokolü):** Web sayfalarını görüntüleyen protokoldür. Kullanıcılar web üzerinde bir sayfayı görüntülemek istediklerinde bu protokol çalışır. Varsayılan port numarası 80’dir.

**SMTP (Simple Mail Transfer Protocol, Basit Posta Aktarım Protokolü):** E-Posta gönderip almayı sağlayan protokoldür. Bu protokolün birkaç özelliği yeterli görünmediğinden POP3 veya IMAP protokolleri ile birlikte kullanılır. Yaygın olarak 587 numaralı port üzerinden ve TLS güvenlik katmanı ile erişim sağlanır.

**FTP (File Transfer Protocol, Dosya Aktarım Protokolü):** En az iki bilgisayar arasında ağ üzerinden dosya gönderip almayı sağlayan protokoldür. Varsayılan port numarası 21’dir

**SSH (Secure Shell, Güvenlik Kabuğu):** Yerel makinelerden sunuculara ağ üzerinden uzaktan bağlantıyı güvenli bir şekilde sağlayan protokoldür. Varsayılan port numarası 22’dir.

**Telnet:** SSH gibi istemci-sunucu arasında güvenli bağlantıyı sağlar. Ancak SSH’ın kullandığı şifreleme tekniklerini kullanmaz. Varsayılan port numarası 23’tür.

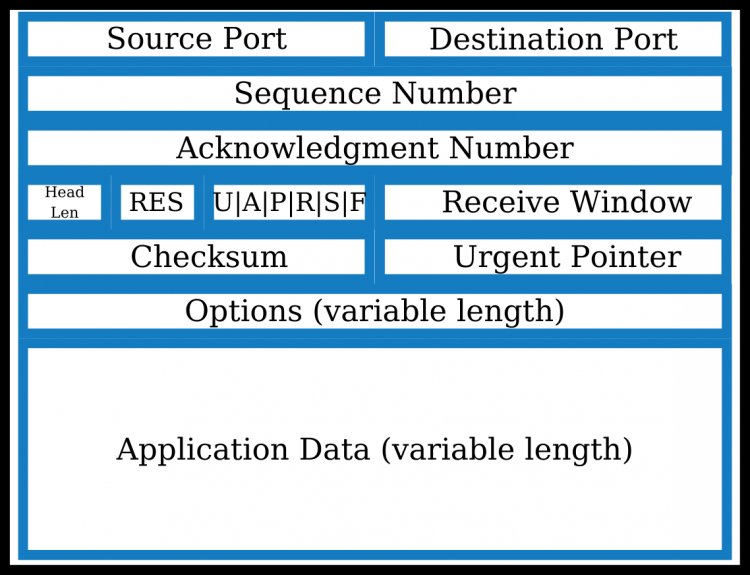
**DNS (Domain Name Service, Alan Adı Hizmeti):** Alan adlarının hangi IP’lere ait olduğunu kontrol eden protokoldür. Taşıma katmanında hem TCP hem de UDP protokolü üzerinde çalışabilir. Varsayılan port numarası 53’tür.

**NOT;** UDP Protokolü üzerinde uygulama katmanında çalışan bazı protokoller şu şekildedir; DNS, SNTP, TFTP, SNMP,DHCP, NBNS vs. yukarıda bahsedilen protokoller TCP üzerinde çalışan protokollerdir.

#### **Taşıma Katmanı**

TCP/IP modelinin taşıma katmanında genel olarak 2 protokol çalışır. Bunlar TCP ve UDP’dir. TCP; güvenliği yüksek tutan, veri kaybını engelleyen, ve kontrollü ilerlenmesini sağlayan bir protokoldür. UDP ise hızı ön plana almış, TCP’ye göre güvenliği düşük fakat yüksek performanslı bir protokoldür. Genel olarak videolar, canlı yayınlar gibi veri transferinin hızlı olması gerektiği yerlerde kullanılır.

**TCP:** TCP protokolü, verilerin güvenli bir şekilde cihazlar arasında taşınmasında görev alır. Bunun için veriyi parçalar ve paketler halinde gönderir.



18 TCP’nin yapısı ve veriyi ne şekilde sakladığı gösterilmiştir.

**Source Port (16 bit):** İstemciye ait olan port bilgisidir. Başka bir deyişle verinin bilgisayardan dışarıya (internete) çıkış kapısıdır.

**Destination Port (16 bit):** Verinin gideceği hedef port bilgisidir. Hedef sunucuya giriş kapısıdır.

**Sequence Number (32 bit):**Gönderilen verinin ilk baytının numarasıdır. Başta söylediğimiz gibi veriler parçalara ayrılır. Örneğin; 100 MB’lık bir veri gönderiyorsanız karşı tarafın alabileceği bayt kadar segmentlere ayrılır. Veri 16 bit olarak ayrılıyorsa ilk seq=0, ikincisi ise seq=17 olarak gönderilir. Verinin ayrılma şekli; 0-16,17-33,34-50… olarak 100’e kadar devam eder.

**Acknowledgment Number (32 bit):** Gönderilmesi beklenen verinin baytının numarasıdır.

**Header Length (4 bit):** TCP’nin veriye eklediği başlığın uzunluğunu gösterir. Minimum 5 kelime (20 bayt), maximum 15 kelimedir (60 bayt)

**Reserved (3 bit):** Gelecekte kullanım için ayarlanan bölümdür ancak kullanımı tercih edilmez. 0’a ayarlanmalıdır.

**Flags (Bayraklar):** U (1 bit), A (1 bit), P (1 bit), R (1 bit), S (1 bit), F (1 bit) baş harflerinden oluşan bölümdür. Kullanımı yaygın olanlar açıklanacaktır. Sırasıyla;

* **Urgent:** Verinin acil olduğunun belirtilmesi gerekiyorsa bu alana “1” yazılır. Genel olarak bu belirtilmez ve değeri “0” olarak verilir.
* **ACK:** Onay alanının önemli olduğunu gösterir. İstemci tarafından gönderilen ilk SYN paketinden sonraki tüm paketler bu bayrak setine sahip olmalıdır.
* **PSH:** Arabelleğe alınan verilerin alıcı uygulamaya gönderilmesini ister. Gönderilemeyen verileri itme görevi görür.
* **RST:** Bağlantıyı sıfırlar.
* **SYN:** Sıra numaralarını senkronize eder. Yalnızca her uçtan (istemciden ve sunucudan) gönderilen ilk pakette bu bayrak ayarlanmalıdır.
* **FIN:** Göndericiden gelen son paketi temsil eder.

**Receive Window (16 bit):** Veri akışını kontrol eden bölümdür. Verileri göndermek istediğimiz sunucunun bir seferde ne kadarlık veri alabileceğini gösterir. Her bilgisayarın bağlantı hızı, alabileceği veri miktarı gibi özellikleri farklıdır. Karşı tarafın alabileceğinden çok veri göndermek, veri trafiğini tıkar ve bağlantı sorunlarına neden olur.

**Checksum (16 bit):** Hata kontrolü için kullanılan alandır. Kaynak IP adresini, hedef IP adresini, TCP protokolü için protokol numarasını (6) ve TCP başlıklarını ve yükün uzunluğunu (bayt cinsinden) kontrol eder. Bu bilgiler TCP’nin eklediği başlık altındadır.

**Urgent Pointer (16 bit):** URG bayrağı ayarlanmışsa bu alan, son acil veri baytını gösteren sıra numarasından bir ofsettir.

**Options (uzunluğu 0–320 bit arasında değişir. “32 bitlik birimlerde”):** Bu alanın uzunluğu “Header Length” kısmında belirlenir. Options, en fazla 3 alana sahiptir; tür, uzunluk ve veri(değişken).

**Application Data:** Uygulama verisidir.

##### **Handshaking (3'lü El Sıkışma)**

TCP protokolü üzerinden istemci ve sunucu arasında veri alışverişinin başlatılmasına ve aynı işlemle bitirilmesine verilen isimdir.

İstemci bir sunucuya bağlanmaya çalışmadan önce, sunucunun bağlantılara açılması için önce bir bağlantı noktasına bağlanması ve onu dinlemesi gerekir: buna **pasif açık** denir. Pasif açık bir kez kurulduğunda, bir istemci üç yollu el sıkışmayı kullanarak **aktif bir açık başlatarak** bir bağlantı kurabilir:

**SYN:** Aktif açma, istemci tarafından sunucuya bir SYN göndererek gerçekleştirilir. İstemci, segmentin sıra numarasını rastgele bir ***“A”*** değerine ayarlar.

**SYN-ACK:** Yanıt olarak, sunucu bir SYN-ACK ile yanıt verir. Onay numarası, alınan sıra numarasından bir fazlaya, yani***“A+1'e”*** ayarlanır ve sunucunun paket için seçtiği sıra numarası, başka bir rasgele sayı ***“B”*** olarak belirlenir.

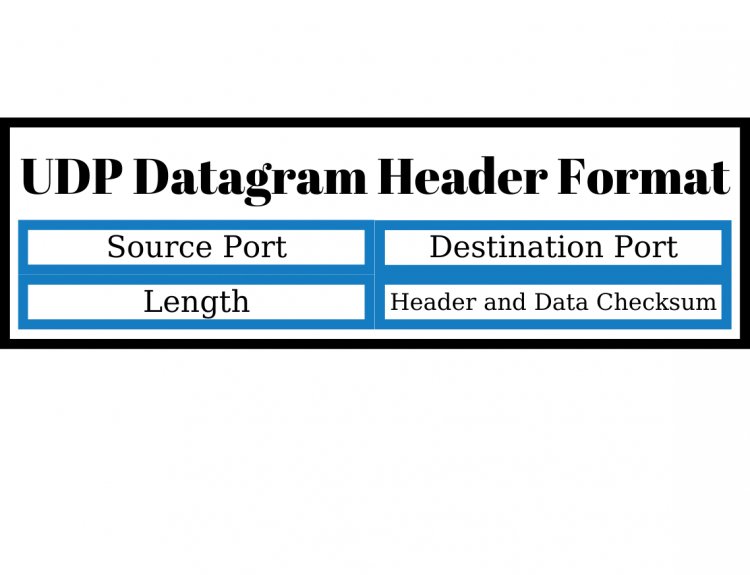
**ACK:** Son olarak, istemci sunucuya bir ACK gönderir. Sıra numarası, alınan alındı ​​değerine, yani ***“A+1'e”*** ayarlanır ve alındı ​​numarası, alınan sıra numarasından bir fazlaya, yani ***“B+1'e”*** ayarlanır.

SYN ve SYN-ACK, bir yön için sıra numarasını belirler ve onaylar. SYN-ACK ve ACK ise diğer yön için sıra numarasını belirler ve onaylar. Bu adımların tamamlanmasının ardından hem istemci hem de sunucu, veri alışverişine hazır hale gelir.

**NOT;** Veri alışverişi tamamlandıktan sonra aynı işlem FIN ve ACK ile tekrarlanır ve bağlantı sonlandırılır. bu bağlantı için ayrılmış kaynaklar serbest bırakılır.

**UDP**

UDP protokolünde TCP’nin yapmış olduğu doğrulama işlemleri yapılmamaktadır. Bu sayede veri iletimi çok daha hızlıdır.



#### **Ağ Katmanı**

* İnternet katmanı da denir. Taşıma katmanından gelen pakete IP başlığını ekler. Kaynak IP ve Hedef IP bilgilerini kaydederek Veri Hattı katmanına iletir.
* Veri Hattı katmanından gelen paketi ise kontrol etme görevine sahiptir. Paket içerisinde gönderici bilgisayarın IP adresi varsa veriyi Taşıma katmanına iletir.
* Bu katmanda IP protokolü çalışır. IPv4, IPv6 gibi versiyonları mevcuttur. Local makineyi dış dünyaya açan katmandır. Switch ve Router gibi fiziksel cihazlar bu katmanda çalışır.

#### **Veri Hattı Katmanı**

* IP katmanından gelen veriye MAC adresi bilgisini ekleyen katmandır. Bu katmana gelene kadar yukarıdaki katmanlarda, bilgisayarın fiziksel adresi bilinmemektedir.
* Aynı şekilde Fiziksel katmandan gelen paketin içerisinde kaynak ve hedef MAC adresinin olup olmadığını kontrol eder. Bir problem ile karşılaşmadığında veriyi Veri Hattı katmanına iletir.
* Ağdaki her ana bilgisayarın en az bir MAC adresi bulunur. Evdeki modemlerde; yerel ağ ve internet için ve dizüstü bilgisayarlarda kablolu ve kablosuz LAN bağlantısı için tipik olarak 2 adet MAC adresi bulunur. Ethernet kartı, ATM gibi teknolojiler bu katmanda kullanılır.

#### **Fiziksel Katman**

Veri Hattı katmanında MAC adresinin eklenmesi ile de çerçevelenen paket bu katmanda bitlere ve sinyallere dönüştürülür. Bu sayede veri, kablolar üzerinde veya kablosuz olarak taşınabilir hale gelir. Bu katmanda kablolar, ağ topolojileri ve birleştiriciler(connectors) kullanılır.

MELİKE HANLI

OKUL NO:222703016