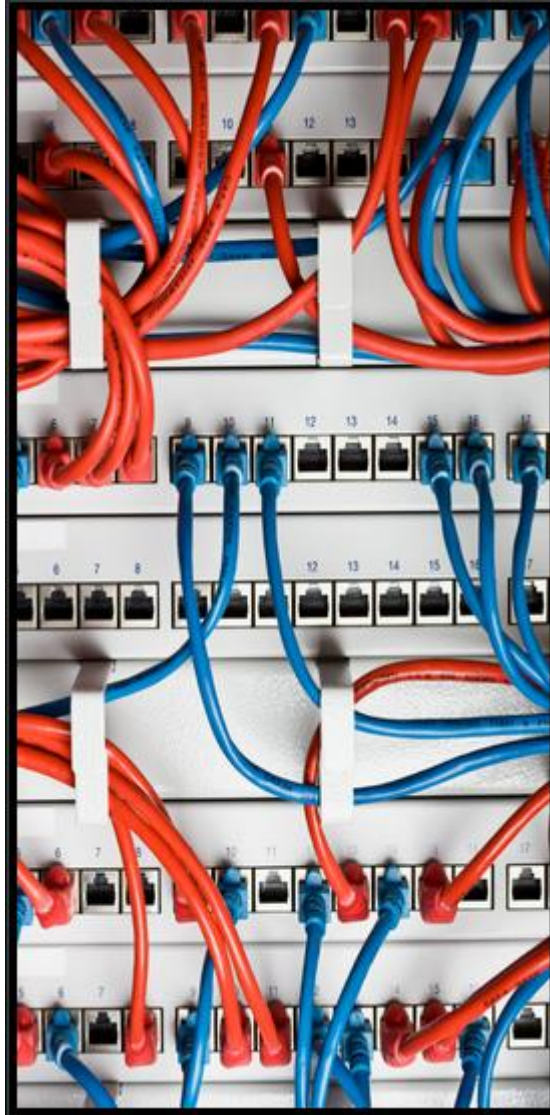


Bilgisayar Ağları

Ders Notları



Cemal TANER

Fatih ÖCAL

2014

Manisa

İçindekiler

İçindekiler	2
Bilgisayar Ağlarının Temelleri	6
Ağ Sistemlerinin Yararları	6
Ağ Bileşenleri	6
Ağ İşletim Sistemleri	7
Kablolama Sistemi	7
Ağ Cihazları	7
İletişim Protokolleri	7
Network Interface Card NIC(Ağ Kartı)	7
Ağ Mimarisi.....	8
Ağ Topolojileri	8
Kablo Erişim Metodu	8
Büyükliklerine Göre Ağlar.....	8
Open Systems Interconnection (OSI)	9
OSI Nedir?.....	9
Application Katmanı	10
Presentation Katmanı.....	10
Session Katmanı.....	10
Transport Katmanı.....	10
Network Katmanı.....	11
Data Link Katmanı.....	11
Physical Katman.....	11
Data Encapsulation.....	11
OSI Katmanları ve Cihazlar	11
TCP/IP Protokol Takımı.....	12
TCP/IP Nedir?	12
Kullanım Alanları.....	12
TCP/IP Protokolünün Temel Yapısı ve OSI ile İlişkisi.....	13
OSI ve TCP/IP	13
TCP/IP Katmanları.....	13
Application.....	13
Transport.....	14
TCP.....	14

Three-Way Handshake	14
UDP.....	15
Port Numaraları.....	16
Internet.....	17
ARP	17
ICMP	18
Network Interface	19
TCP/IP Protokülünde İletişim Nasıl Kurulur?.....	19
Paketlerin Ağa Yönlendirilmesi.....	19
IP Adreslerinin Ağda Tanımlanması.....	19
Subnet Mask.....	19
IP Adresi Sınıfları.....	20
IP Adresi Kuralları	20
Haberleşme Biçimleri	21
Ağ Cihazları	22
Repeater	22
Hub	22
Bridge	23
Switch	24
Router.....	25
Firewall	26
Ağ Tipleri.....	26
Local Area Network (LAN)	27
Bazı LAN standartları:	27
CSMA/CD	28
Half Duplex / Full Duplex.....	28
Ethernet Protokolleri.....	29
Wide Area Network (WAN)	29
WAN Bağlantı Tipleri	30
WAN Cihazları.....	30
Router	30
WAN Switch.....	30
Modem	31
Channel Service Unit / Data Service Unit (CSU/DSU)	31

Data Terminal Equipment / Data Circuit-Terminating Equipment (DTE/DCE)	31
WAN Terminolojisi.....	32
Metropolitan Area Network (MAN)	32
Virtual Private Network (VPN).....	33
Ağ Topolojileri	33
Bus Topoloji	33
Star Topoloji	33
Ring Topoloji.....	34
Mesh Topoloji.....	34
Hybrid Topoloji	34
Extended Star	35
Ağ Kabloları.....	35
Twisted Pair Kablolar	35
Unshielded Twisted Pair.....	35
Shielded Twisted Pair	36
Screened Twisted Pair	36
Kategoriler	36
Bağlantı Tipleri.....	37
Düz (Straight) Kablo.....	38
Çapraz (Crossover) Kablo.....	38
Fiber Optik Kablolar	39
Single Mode Fiber.....	39
Multi Mode Fiber.....	40
Ethernet Kablo Standartları.....	40
Ağ Teknolojileri.....	41
LAN Teknolojileri	41
Ethernet.....	41
Logical Link Control (LLC) Altkatmanı	42
Media Access Control (MAC) Altkatmanı	42
Switching	42
Virtual LAN (VLAN)	43
Token Ring	44
Token Passing.....	44
Fiber Distributed Data Interface (FDDI).....	45

Token Passing	45
Wireless LAN (WLAN)	45
WLAN Bileşenleri	45
WLAN Topolojileri.....	46
WLAN Teknolojileri.....	47
Diğer WLAN Standartları	48
WLAN Güvenliği.....	48
WAN Teknolojileri.....	49
Frame-Relay.....	49
Frame-Relay Terminolojisi.....	50
Digital Subscriber Line (xDSL)	51
DSL Tipleri.....	51
ADSL.....	51
ADSL Yapısı	52
ATM	53

Bilgisayar Ağları

Bilgisayar Ağlarının Temelleri

Bilgisayarlar ilk geliştirilmeye başlandıkları zamanlarda tek başlarına çalışan birimlerdi. Ancak şirketlerde kullanılan bilgisayar sayısının artması sonucu bu durumun işletmeler için etkin ve ucuz olmadığı anlaşıldı. Maliyeti düşürmek için ve işlerin daha hızlı ve kolay yapılabilmesi için bilgisayarların haberleşmesi gerektiği fikri ortaya çıktı. Sonunda günümüzde vazgeçilmez olan ağ yapıları geliştirildi.

Ağ; birbirleri ile belirli kurallar çerçevesinde iletişim kurabilen cihazların oluşturduğu yapıdır. Bilgisayarların birbirleri ile haberleşmeleri için ağlar kurulmalıdır.

Ağlar, yazılım ve donanım olarak sınıflandırılan bileşenlerden oluşur.

Ağ donanımı olarak kablo, switch, router gibi cihazlar kullanılır.

Yazılım olarak da ağ işletim sistemleri, iletişim protokolleri ve ağ programları mevcuttur.

Ağ Sistemlerinin Yararları

Bir ağ kurmanın amacı, bilgiye daha hızlı ulaşabilmektir. Ağ, sağladığı olanaklarla bunu gerçekleştirir. Bir kullanıcı kendisinden kilometrelerce uzaktaki bilgiye bir kaç saniye gibi kısa sürelerde erişebilir. Ağın faydaları:

Program Paylaşımı: Bir ağ ortamında, tüm kullanıcılar merkezi bir bilgisayara kurulmuş olan programı kullanabilir. Program tek tek bütün bilgisayarlara kurulmak zorunda değildir.

Dosya Paylaşımı: Kullanıcılar, işlerini yaparken kullandıkları dosya kaynaklarına, ağdaki herhangi bir bilgisayardan ulaşabilirler. Her kullanıcı bu dosya kaynaklarından sadece kendisine gerekli olanı okumaya yetkilidir.

Yazıcı Paylaşımı: Bir ağda, çok sayıda kullanıcı aynı anda aynı yazıcıları kullanabilir. Her bilgisayara bir yazıcı bağlamak gerekmez. Bu durum maliyeti önemli ölçüde düşürür.

Güvenlik: Bir ağa bağlanıp, kaynakları kullanmak isteyen her kullanıcı kimliğini doğrulamak zorundadır. Sadece önceden oluşturulmuş hesapları olan kullanıcılar kaynaklara erişebilir. Her kullanıcı hesabının yetkileri farklı olabilir.

Merkezi Yönetim: Bir ağdaki bilgisayarlar ve cihazlar, yöneticiler tarafından uzaktan yönetilebilirler. Tüm bilgisayarlara aynı anda bir program kurulabilir ve ortak güvenlik politikaları topluca uygulanabilir.

Ağ Bileşenleri

Ağlar, yazılım ve donanımlardan oluşur. Donanım; kablo, switch, router gibi cihazlardan oluşur. Yazılım ise ağ işletim sistemleri, iletişim protokolleri ve ağ programlarından oluşur.

Ağ İşletim Sistemleri

Ağ ortamında çalışabilme özelliği olan her işletim sistemi, Ağ İşletim Sistemidir. Örnek olarak; MSDOS 5.0 ve daha üstü, tüm MS Windows sürümleri, Linux, Netware gibi. Bu işletim sistemlerinin hepsi ağ ortamında çalışabilir fakat bazıları ağda çalışabilmeleri için optimize edilmiştir. Bu işletim sistemlerinin ağ kullanabilme özellikleri diğerlerine göre daha gelişmiştir.

Örnek olarak; Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2012 ve Windows Server 2014 verilebilir.

Ağ ortamında işletim sistemleri iki farklı rol üstlenebilirler. Bu roller:

Server (Sunucu): Adında "Server" kelimesi olan her işletim sistemi sunucu özelliğine sahiptir. Sunucu bilgisayarlar, ağ kaynaklarını tutan ve bu kaynakları diğer bilgisayarların ve kullanıcıların kullanımına sunan bilgisayarlardır. Örneğin, yazıcı ve dosya kaynaklarını kullanıma sunan bilgisayarlar gibi.

Client (İstemci): Kullanıcıların sunulan kaynaklara erişirken kullandıkları sistemlerdir.

Kablolama Sistemi

Kablolar verilerin iletimini sağlayan ortamlardır. Kablolar hızlarına ve malzemelerine göre çok çeşitlidirler. Ancak kullanılan kablo, ağın hızını ve performansını etkileyeceği için kablo seçimi çok önemlidir. Günümüzde en yaygın kullanılan kablo türü "Twisted" (UTP) kablodur.

Ağ Cihazları

Ağı genişletmek ve başka ağlar ile birleşmesini sağlamak amacı ile birçok ağ cihazı kullanılabilir.

En çok kullanılan ağ cihazları şunlardır:

Hub: Star topoloji yapısında kullanılan merkezi bağlantı noktasıdır. (Günümüzde kullanılmamaktadır)

Switch: Star topoloji yapılarında kullanılan fakat hub'tan daha etkin olan ve günümüzde onun yerini alan bir cihazdır.

Router: Birbirinden uzak noktalardaki ağ sistemlerini haberleştirmek için kullanılır.

İletişim Protokolleri

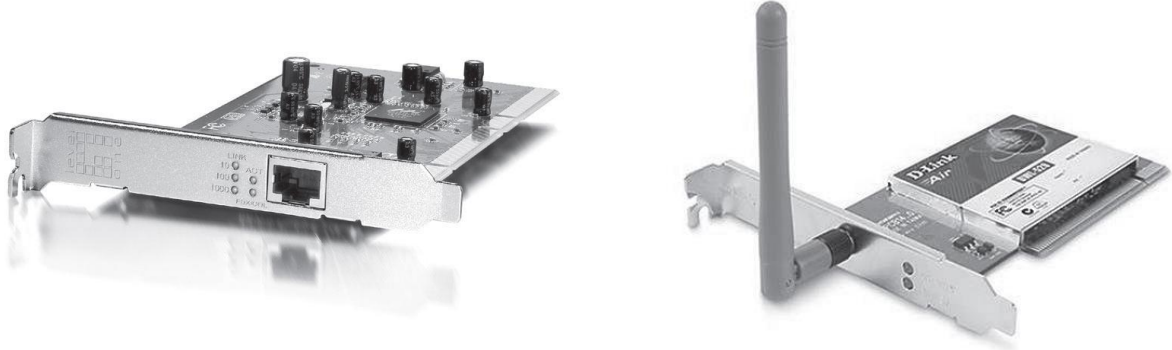
Ağda çalışan cihazların iletişim kurabilmeleri için gerekli kurallar bütünüdür. Ağ protokollerini dillere benzetebiliriz. İnsanların anlaşabilmek için aynı dili konuşmaları gerektiği gibi iki bilgisayarın da iletişim kurabilmeleri için aynı protokolü kullanmaları gerekir.

Günümüzde en yaygın kullanılan protokol, TCP/IP'dir.

TCP/IP : (*Transmission Control Protocol / Internet Protocol*). TCP/IP, her türlü ağda rahatlıkla kullanılabilen esnek ve gelişmiş bir protokoldür. Kullanılmak istenilen protokolü işletim sistemleri sağlar.

Network Interface Card NIC(Ağ Kartı)

Ağa bağlanan her bilgisayarda olması zorunlu olan ve ağa fiziksel bağlantının yapılmasını sağlayan adaptördür. NIC'ler, Ethernet ve Token Ring gibi farklı ağ teknolojileri için değişik tiplerde üretilirler. NIC, kullanılan kablo cinsleri için farklı konnektör tipleri sağlar. Kablosuz ağlar için üretilmiş NIC'lerde ise küçük bir anten vardır.



Ağ Mimarisi

Bir ağın mimarisi; topolojisi, kablo erişim metodu, büyüklüğü ve kullanılan iletişim protokolleri tarafından tanımlanır.

Ağ Topolojileri

Bir ağın topolojisini, kablo yerleşiminin bir haritası olarak düşünebiliriz. Topoloji bilgisayarların, nasıl bağlandıklarını tanımlar. En yaygın üç topoloji vardır:

Bus Topoloji: Bütün cihazları birbirine bağlamak için bütün bilgisayarlara uğrayan doğrusal bir kablo ile kurulur.

Star Topoloji: Bilgisayarlar, hub veya switch gibi bir bağlantı cihazı üzerinden birbirlerine bağlanır. En sık kullanılan ve en yüksek performans sağlayan topolojidir.

Ring topoloji: Bu topoloji fiziksel olarak Star'a benzese de veri yolu ağ üzerinde bir döngü oluşturur.

Kablo Erişim Metodu

Geleneksel yerel ağlar, paylaşılan kablo sistemleridir, yani bilgisayarlar aynı kabloya bağlıdır. Aynı anda sadece bir bilgisayar veri iletebilir. Eşzamanlı iletimler, iletimin gerçekleşmemesine sebep olur ve engellenmesi için bir metoda ihtiyaç vardır. Kablo erişim metodları, bir bilgisayarın veriyi kabloya nasıl ileteceğini belirler.

Büyükliklerine Göre Ağlar

Ağlar, büyüklüklerine göre ikiye ayrılır.

LAN (Local Area Network): LAN'lar, yüksek hızlı, güvenilir ve küçük bir alana yayılmış ağlardır.

Örneğin, bir binadaki ağ ya da bir kampus ağı gibi.

WAN (Wide Area Network): Coğrafi olarak birbirlerinden uzak LAN'ların birleştirilmesiyle oluşan büyük ağlardır. Örneğin, bir kaç farklı noktada birimi olan bir şirketin ağı, WAN'dır. LAN'lara göre daha yavaştır.

Open Systems Interconnection (OSI)

1980'li yılların başında şirketler maliyeti düşürmek ve çalışma hızlarını arttırmak amacıyla ağlarını genişletme ve birleştirme ihtiyacı duydular. Birçok ağın farklı yazılım ve donanım özelliklerine sahip olması sonucu uyumsuzluk problemleri yaşandı. ISO (International Organization for Standardization), bu uyumsuzlukları aşmak için üreticilere yardımcı olması amacıyla yeni bir ağ modeli oluşturulması gerektiğine karar verdi ve 1984 yılında OSI (Open Systems Interconnection) Referans Modelini ortaya koydu. Tüm üreticiler yazılımlarını ve donanımlarını OSI Referans Modelinde belirtilen standartlar çerçevesinde geliştirmeye başladılar.

OSI Nedir?

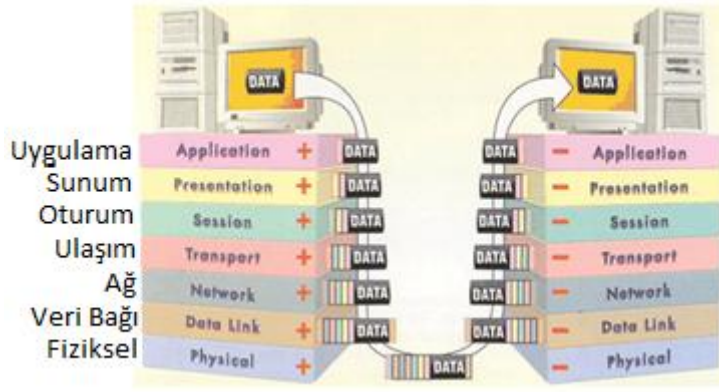
OSI, farklı üreticiler tarafından geliştirilen ağ bileşenlerinin bir arada uyumlu bir şekilde çalışabilmelerini sağlayan kurallar bütünüdür. Ağ bileşenlerinin nasıl haberleştiklerini tanımlayan kavramsal bir yapıdır. Bilginin hazırlanıp ağ ortamından geçerek başka bir bilgisayarda nasıl görüntülendiğini tanımlar. OSI, iletişimi birbirleriyle ilişkili yedi farklı katmanda inceler. Her katmanın ayrı bir fonksiyonu vardır.

Katmanlı modelin avantajları şunlardır:

- Network iletişimini daha küçük daha basit parçalara böler.
- Farklı donanım ve yazılımların haberleşmesini sağlar.
- Herhangi bir katmandaki değişikliğin diğer katmaları etkilemesini engeller dolayısıyla daha çabuk geliştirebilmelerini sağlar.
- Farklı platformların iletişimini sağlar. (örn: Unix ve Windows)
- Her katman diğer katmanları etkilemeden geliştirilebilir.
- Bilginin bir bilgisayardan diğerine ulaştırılması sorunu yedi daha küçük daha kolay çözülebilir soruna bölünmüştür.
- Her sorun ilgili OSI katmanı tarafından çözülmüştür.

OSI nin yedi katmanı;

1. Application
2. Presentation
3. Session
4. Transport
5. Network
6. Data Link
7. Physical



Application Katmanı

Kullanıcıya en yakın katmandır. Kullanıcı uygulamalarına e-posta, FTP, WWW(World Wide Web) gibi ağ servisleri sunar. Ayrıca uygulamaların birbirleriyle iletişimini kontrol eder.

Presentation Katmanı

Veriyi, alıcı cihaz tarafından okunabilir hale getirmekten sorumlu olan katmandır. Gönderilen verinin, alıcı cihaz tarafından nasıl okunacağını belirtir. Daha iyi anlaşılabilmesi için şu benzetmeyi yapabiliriz. Nasıl ki farklı dil konuşan iki insanın anlaşabilmesi için bir çevirmene ihtiyaç vardır, iki ağ cihazının haberleşebilmesi için de verilerin birbirlerini anlayabileceği biçime sokulması gerekir.

Bu işlemi yapan katman Presentation katmanıdır. Başlıca üç öreği vardır.

1. Verinin biçimlendirilmesi
2. Verinin şifrelenmesi
3. Verinin sıkıştırılması

Session Katmanı

Session katmanının görevi, iletişimdeki senkronizasyonu sağlamaktır. Uygulamalar arasındaki oturumları başlatır, sonlandırır ve yönetir. Şöyle bir benzetme yapabiliriz. Bir arkadaşınızla IRC ortamında tartıştığınızı düşünün. İki problemle karşılaşabilirsiniz. Birincisi, ikinizin de aynı anda mesaj yollama olasılığınız vardır. İkincisi, sürekli önceki mesajlara bakmak zorunda kalırsınız. Bu iki sorunu çözmek için mesajlaşmaya başlamadan önce mesajınızın sonunda bittiğini belirtmek, sırayla mesaj yazmak gibi bir dizi kurallar koymanız gerekir. Durum iki ağ cihazı için de aynıdır.

Transport Katmanı

Birincil görevi, gönderici ve alıcı arasındaki veri akışının kontrolü ve verinin alıcıya ulaştığından emin olmaktır. Alıcı cihazın veriyi almaya hazır olup olmadığı ve veri gönderildikten sonra alıp almadığı gibi kontrollerin yapıldığı katmandır. Yeni bir yabancı dil öğrenen bir öğrencinin öğrendiği dilin konuşulduğu ülkeye gittiğinde söylenen her şeyi tekrarlatması (verinin ulaştığından emin olmak) ve yavaş konuşulmasını istemesi (veri akışının kontrolü) iyi bir benzetme olacaktır. Transport katmanında başlıca iki protokol çalışır.

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

Network Katmanı

OSI Referans Modelinin en önemli katmanıdır. Gönderilen verinin hedefine ulaşması için rota seçiminin yapıldığı katmandır. Gönderilen bir mektubun alıcıya ulaşabilmesi için üzerine alıcının adresini yazarsınız. Bu adres sayesinde postaneler ve postacılar mektubunuzu alıcısına belirli bir rota izleyerek ulaştırırlar. İki ağ cihazı da birbirlerine veri yollarken verinin üzerine bir takım adresler yazarlar. Bu adresler "Router" denilen cihazlar tarafından okunup uygun yollardan hedefine ulaştırılır. Verinin üzerine yazılan adres IP (Internet Protocol) adresi denilen mantıksal bir adrestir.

Data Link Katmanı

Gönderilecek verinin elektronik sinyallere dönüştürülüp kabloya iletilmesini ve kablodan gelen elektronik sinyallerin veriye dönüştürülmesini sağlayan katmandır. Bu dönüştürme işlemi kullanılan ağ teknolojisine göre değişiklik gösterebilir. Elektronik sinyallerin kablo üzerinde sorunsuz bir şekilde ilerleyip ilerleyemediğinin kontrolü bu katmanda yapılır. Ayrıca bu katmanda fiziksel adresleme yapılır.

Bu katmanın Media Access Control (MAC) ve Logical Link Control (LLC) diye iki alt katmanı vardır.

- LLC
- MAC

Physical Katman

Data Link Katmanı tarafından elektronik sinyallere dönüştürülen verinin taşınmasından sorumludur. Basit olarak ağ kablosudur.

Data Encapsulation

Ağda gönderilen veri parçasına paket denir. Veriler bir bilgisayardan başkasına yollanmadan önce gönderici bilgisayar tarafından paketlenmelidirler. Bu işleme encapsulation denir. Encapsulation, yollanan verinin hedefine ulaşabilmesini ve hedef bilgisayar tarafından okunabilmesini sağlar.

Encapsulation, veriye ilgili protokol bilgilerinin iliştilmesi ile gerçekleşir. OSI'nin her katmanında veriye bir header (başlık) eklenir. Bu başlıklar verinin hedefine ulaşmasını sağlayan, ağ cihazları ve alıcı bilgisayar tarafından okunan, bilgiler içerir.

Encapsulation işleminin tam tersi alıcı bilgisayar tarafından gerçekleştirilir. Encapsulation'da eklenen başlıklar kontrol edilip veri elde edilir. Bu işleme de-encapsulation denir.

OSI Katmanları ve Cihazlar

Ağ cihazları ve teknolojileri yaptıkları işlere göre bir OSI katmanı ile ilişkilendirilirler.

Physical katmanda çalışan cihazlar: Hub ve Repeater sadece elektronik sinyalleri ileten ve güçlendiren cihazlardır.

Data-Link katmanında çalışan cihazlar: Switch ve Bridge gibi cihazlar kendilerine bağlı olan makinelerin fiziksel adreslerini hafızalarında tutarlar. Veriyi sadece alıcı makineye yönlendirirler.

Network katmanında çalışan cihazlar: Router, farklı ağları ve bu ağlara nasıl ulaşılacağını bilir ve veriyi bu bilgi ışığında hedefine yönlendirir.

TCP/IP Protokol Takımı: TCP/IP protokol takımı, internet ve günümüz ağ sistemlerinin hemen hepsinde kullanılan iletişim protokolüdür.

OSI referans modeline benzer katmanlı bir modeli vardır. TCP/IP protokol takımı dört katmandan oluşmaktadır.

Application Katmanı: Üst seviye protokolleri içerir. Veri sunumu ve kodlama işlevlerini yerine getirir.

Transport Katmanı: Akış denetimi, hata kontrolü ve hata düzeltme işlevlerini yerine getirir.

Internet Katmanı: Gönderilen paketin hedefine ulaşmasını sağlar. Bir adresleme katmanıdır.

Network Access Katmanı: Ağ teknolojileri ve fiziksel adresleme konularını içerir.

TCP/IP Protokol Takımı

TCP/IP, DARPA (Defense Advanced Research Projects Agency) tarafından geliştirilmiş bir dizi protokolden oluşan bir protokol takımıdır. Günümüzde ağlar arası iletişimde ve internette kullanılan standart ağ protokolüdür.

TCP/IP Nedir?

DARPA tarafından geliştirilen TCP/IP, sadece DARPA tarafından kullanılmak üzere tasarlanmış olup, "Berkeley Software Distribution of UNIX" sistemlerinde kullanılmasıyla başlayan gelişme sürecinin sonunda, en yaygın ağ protokolü olmuştur.

Günümüzde ağlar arası iletişimde ve internette kullanılan standart ağ protokolü TCP/IP'dir.

Her türlü ağ altyapısında kullanılabilecek esnek ve yönetilebilir bir yapıya sahiptir. Her üretici tarafından kullanılabilen, geliştirilebilen açık bir protokoldür.

TCP/IP bu özellikleri sonucunda günümüz ağlarında kullanılan tek protokol olmuştur.

Kullanım Alanları

TCP/IP (Transmission Control Protocol/Internet Protocol) endüstri standardı olan bir iletişim protokolüdür.

TCP/IP, yerel ağlar (LAN) ve geniş alan ağları (WAN) için geliştirilmiştir. Standart olarak routable (yönlendirilebilir) olan TCP/IP protokolü, özellikle internet ve intranet ortamlarının temelidir.

TCP/IP'nin bazı tasarım özellikleri:

- Hata düzeltme olanakları.
- Alt ağlara (subnet) bağlanma.
- Belli bir sahibi olmaması.
- Minimum veri kullanımı.

TCP/IP Protokolünün Temel Yapısı ve OSI ile İlişkisi

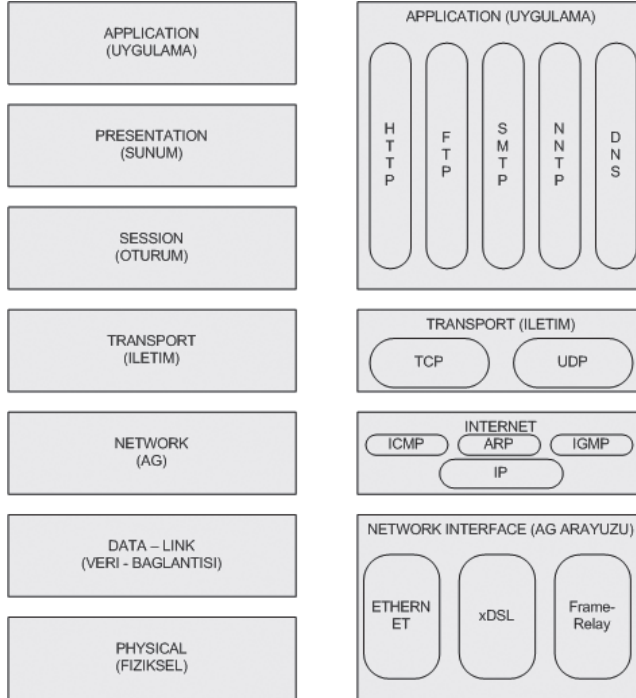
TCP/IP protokol takımı, OSI Referans Modeline benzer katmanlı bir yapıya sahiptir.

OSI ve TCP/IP

TCP/IP'nin görevi, bir ağ cihazından bir başkasına bilgileri taşımaktır. Bu görevi yerine getirirken OSI Referans Modeline uygun şekilde çalışır. Bütün "Physical" ve "Data-Link" katmanı protokollerini destekler.

TCP/IP Katmanları

TCP/IP protokol takımı, ağ iletişimini katmanlara bölerek açıklar. İletişim esnasında yapılan işlemler belirli protokoller aracılığı ile gerçekleştirilir. Her protokol belirli bir TCP/IP katmanında çalışır. Gönderilen verilere, alıcı bilgisayarın veriyi doğru işleyebilmesi için, kullanılan protokoller tarafından bir başlık (Header) eklenir. Örneğin, gönderilecek veriye, alıcı bilgisayara ulaşabilmesi ve alıcı bilgisayarın cevap verebilmesi için, IP protokolü tarafından adres bilgileri eklenir.



TCP/IP protokol takımının dört katmanı vardır.

Application: OSI Referans Modelinin Application, Presentation ve Session katmanlarını kapsar.

Transport: İşlevi OSI'nin Transport katmanı ile aynıdır.

Internet: OSI'nin Network katmanına denk gelir.

Network Interface: OSI'nin Data-Link ve Physical katmanlarını kapsar.

Application

Ağ yönetimi, dosya transferi ve e-posta gibi servisler sağlar.

- DNS (Domain Name System), internette kullanılan isimleri IP adreslerine dönüştüren sistemdir.
- WINS (Windows Internet Naming Service), Microsoft tarafından geliştirilen ve Windows NT ağlarında kullanılan, isimleri IP adreslerine dönüştüren servistir.
- SMTP (Simple Mail Transfer Protocol), e-posta mesajlarını taşıyan protokoldür.
- SNMP (Simple Network Management Protocol), ağ cihazlarının izlenmesi ve kontrolü için kullanılan protokoldür.
- FTP (File Transfer Protocol), ağda bir noktadan başka bir noktaya dosya transferi için kullanılan “güvenilir” bir protokoldür. Transport protokolü olarak TCP kullanır.
- TFTP (Trivial File Transfer Protocol), dosya transferi için kullanılan bir başka protokoldür.
- Transport protokolü olarak UDP kullanır.
- HTTP (HyperText Transfer Protocol), World Wide Web ortamında text, grafik ve video aktarımı için kullanılır.
- Telnet, uzaktaki bir cihazı yönetmek için kullanılır.

Transport

Veriyi segmentlere bölerek kontrollü bir şekilde iletimini ve alıcı cihazda tekrar birleştirilmesini sağlar.

TCP (Transmission Control Protocol), bağlantı-temelli, güvenilir bir iletim protokolüdür. Veri iletime başlamadan önce gönderici ve alıcı arasında bağlantı kurar. Alıcıya ulaşamayan veriyi tekrar yollar.

UDP (User Datagram Protocol), bağlantısız ve güvenilir olmayan bir iletim protokolüdür. Akış kontrolü özelliği olmadığı için daha hızlı iletim sağlar.

TCP

TCP ile yapılan veri iletimlerinde, iletim başlamadan önce “Three-Way Handshake” yöntemiyle bir bağlantı kurulur. Veri, bağlantı kurulduktan sonra kontrollü bir şekilde iletilir.

Three-Way Handshake

Bağlantının kurulabilmesi için cihazlar birbirlerinin sıra numaralarını senkronize ederler. Sıra numaraları gönderilen mesajların gönderilme sıralarının tespiti için kullanılır.

A → B SYN Sıra numaram X

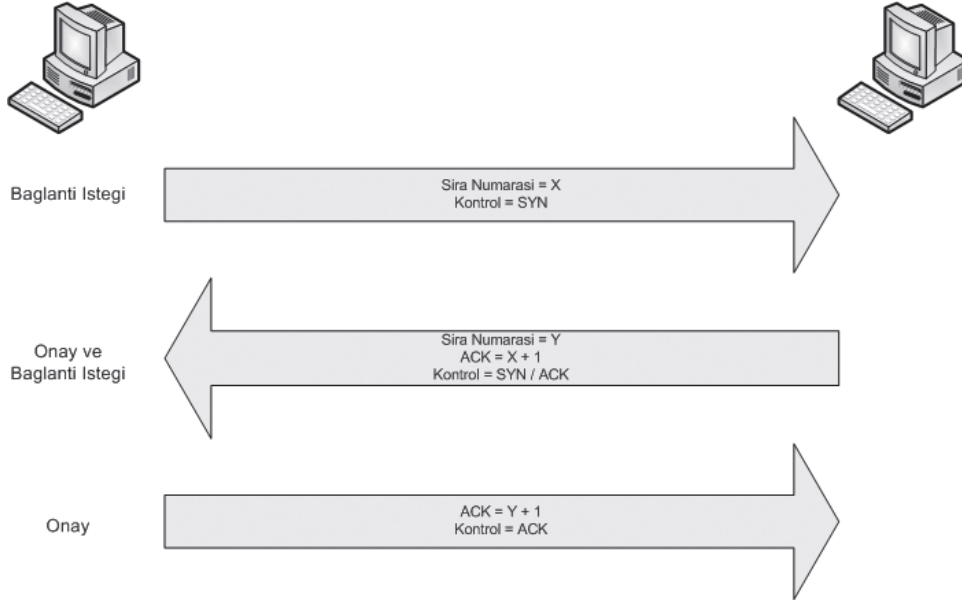
A ← B ACK Sıra numaran X

A ← B SYN Sıra numaram Y

A → B ACK Sıra numaran Y

Bu mesajların sonunda bağlantı kurulur ve veri iletimi başlar. Veri, segmentlere bölünür ve sırayla gönderilir. Alıcı cihaz, veri ulaştıktan sonra sıradakini ister. Eğer veri ulaşmazsa tekrar istenir.

Akış kontrolü bu şekilde sağlanır.

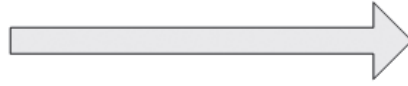
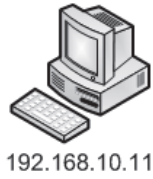


Gönderen cihaz, veriyi gruplara ayırıp sırayla yollar. Alıcı cihaz, verinin ulaştığını ve sıradakinin yollanması isteğini ACK (Acknowledgement) mesajlarıyla gönderene bildirir. Eğer veri, alıcıya ulaşmazsa alıcı ACK mesajıyla verinin gelmediğini bildirir ve tekrar yollanmasını ister. TCP ile yapılan iletimlerde verinin karşı tarafa ulaşacağına emin olabilirsiniz. İşte bu yüzden TCP'ye güvenilir bir protokoldür denir.

UDP

TCP protokolü gibi kontrol mekanizmaları içermez ve bağlantı temelli değildir. Verinin hedefe ulaşacağını garanti etmez ancak hızlıdır. Tek bir IP paketi ile yollanabilecek kadar küçük veriler yollanırken, broadcast ve multicast gibi birçok bilgisayara aynı anda veri yollanırken ya da VoIP (Voice over IP: IP üzerinden ses taşıma teknolojisi) gibi hızın güvenilirlikten daha önemli olduğu iletişim tiplerinde tercih edilir.

UDP	TCP
Bağlanma olmadan verilen hizmet; ana bilgisayarlar arasında oturum açılmaz.	Bağlanarak verilen hizmet; ana bilgisayarlar arasında oturum açılır.
UDP verilerin sırasını veya teslimini garanti etmez veya doğrulamaz.	TCP, doğrulamayla verinin hedefe ulaşmasını ve verilerin sıralı teslimini garanti altına alır.
UDP kullanan programlar verilerin taşınması için gerekli güvenilirliği kendileri sağlamak zorundadır.	TCP kullanan programlara güvenli veri taşıma garantisi sağlanır.
UDP hızlıdır, ek yükü azdır, noktadan noktaya ve noktadan birden çok noktaya iletişimi destekleyebilir.	TCP daha yavaştır, ek yükü fazladır ve yalnızca noktadan noktaya iletişimi destekler.



Port Numaraları

Port numaraları bir bilgisayara giriş kapıları olarak düşünülebilir. TCP ve UDP, veriyi üst katmanlara taşımak ve ilgili uygulama ya da servise iletmek için port numaraları kullanır. Port numaraları, aynı anda yapılan farklı iletişimleri ayırd etmek için kullanılır. Her application katmanı servisi belirli bir port'tan sunulur. Örneğin bir web sunucuya gelen istek paketinin HTTP servisine iletebilmesi için, paketin HTTP servisinin kullandığı port olan TCP 80'e yollanması gerekir. Cevap verecek olan web sunucu da paketi, istek yapan bilgisayarın çıkış portuna yollamalıdır.

Bir bilgisayarda 65536 adet port vardır. Bunlardan ilk 1024 tanesi "well-known" port numaraları olarak adlandırılır ve belirli servisler için ayrılmıştır.

		TCP	UDP
HTTP	80	✓	✓
FTP	20 - 21	✓	✓
TFTP	69		✓
Telnet	23	✓	✓
SMTP	25	✓	✓
POP	110	✓	
DNS	53	✓	✓
DHCP	67 - 68		✓

Kullanılan port numarası gerektiğinde deęiştirilebilir.

Internet

OSI referans modelinin network katmanına denk gelir. Bu katmanın başlıca görevi veriyi, hedefine ulaştırmak için gerekli uygun yolu tespit etmek ve yönlendirmektir. Bunun yanında ağ bağlantısını test etmek için de birkaç araç sunar.

IP (Internet Protocol), hedef cihazın ağ üzerinde yerinin belirlenmesi için kullanılan adresleme protokolüdür. Bir ağdaki bütün makinelerin bir IP adresi olmak zorundadır.

ICMP (Internet Control Message Protocol), ağ iletişiminin kontrol edilebilmesi için gerekli servisleri sunar.

ARP (Address Resolution Protocol), bilinen IP adresleri için Data-Link adreslerini bulmak için kullanılır.

RARP (Reverse Address Resolution Protocol), bilinen Data-Link adresleri için IP adreslerini bulmak için kullanılır.

ARP

Ağ cihazlarının iki adresi vardır.

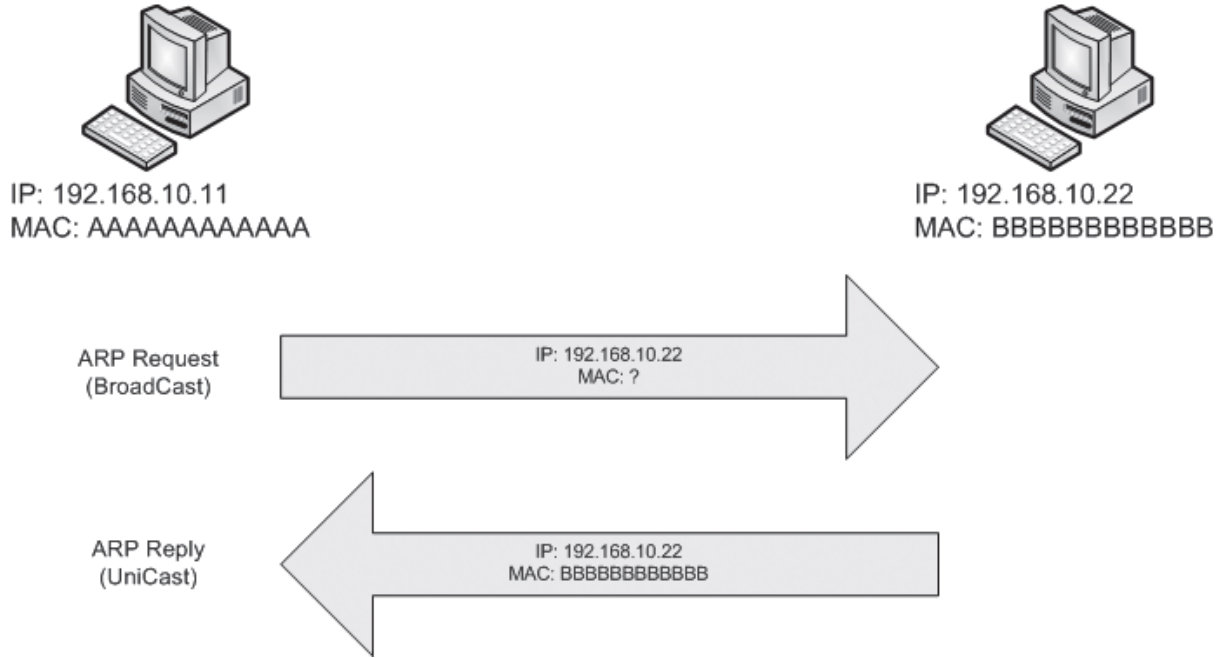
MAC (Media Access Control) adresi: Fiziksel adrestir. Ağ kartlarının ROM belleğine üreticisi tarafından yazılan 48Bit'lik hexadecimal bir sayıdır. Örn: 02-00-4C-4F-4F-50

IP (Internet Protocol) adresi: Mantıksal adrestir. Cihazlara yöneticiler tarafından atanan 32Bit'lik binary bir sayıdır. Örn: 11000000 10101000 00001010 11001000. Böyle bir sayıyı hatırlamak ve yazmak zor olduğu için her sekizli grup decimal'e çevrilmiştir. Adres artık 192.168.10.200 görünümündedir.

Verinin gönderilebilmesi için gönderen cihaz, alıcı cihazın her iki adresini de bilmek zorundadır. Eğer bilmiyorsa ARP Request denilen bir mesaj yayınlayarak öğrenebilir.

Veri göndermek isteyen makine önce alıcının MAC adresini öğrenmek zorundadır. Bunun için, "IP adresi 172.16.3.2 olan cihazın MAC adresi nedir" mesajını (ARP Request) yayınlar. Bu mesaj ağdaki tüm cihazlara gider. Bu mesaja sadece 172.16.3.2 IP adresli cihaz yani alıcı cevap verir.

Artık gönderen, alıcının her iki adresini de öğrenmiştir ve veri iletimine başlayabilir.



ICMP

ICMP, sorun gidermek için ve hata tespiti için kullanılan bir protokoldür. Bir router, paketi hedef ağa ulaştıramıyorsa, bunu ICMP mesajı ile kaynağa sebebi ile birlikte bildirir. Sebep yoğunluk ya da hedef ağın erişilemez olması olabilir.

ICMP, kullanıcı için kontrol fonksiyonları da sunmaktadır. Kaynak ile hedef bilgisayar arasındaki iletişimin, küçük mesajlar ileterek, denetlenmesini sağlayabilir. Yine kaynak ile hedef arasında, paketlerin hangi yolu izlediğini gösterebilir.

Ping Komutu: Kaynaktan hedefe 32Byte'lık küçük bir mesaj gönderilir (Echo Request). Mesajı alan bilgisayar yine ICMP ile cevap verir (Echo Reply). Mesajın hedefe ulaşması ve cevap verilmesi zamanlarını (Round Trip Time) gösterir.

```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping 10.10.0.100
Pinging 10.10.0.100 with 32 bytes of data:
Reply from 10.10.0.100: bytes=32 time=7ms TTL=255
Reply from 10.10.0.100: bytes=32 time=2ms TTL=255
Reply from 10.10.0.100: bytes=32 time=2ms TTL=255
Reply from 10.10.0.100: bytes=32 time=2ms TTL=255
Ping statistics for 10.10.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 3ms
C:\>
```

Tracert Komutu: Kaynaktan hedefe giden yolun izlenmesini sağlar.

```
C:\WINDOWS\system32\cmd.exe
C:\>tracert 192.168.20.2

Tracing route to MAUNAKEA [192.168.20.2]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    SERVER02 [192.168.10.1]
  1  <1 ms    <1 ms    <1 ms    SERVER03 [100.100.100.2]
  2  <5 ms    <1 ms    <1 ms    SERVER04 [200.200.200.1]
  3  <1 ms    <1 ms    <1 ms    MAUNAKEA [192.168.20.2]

Trace complete.

C:\>_
```

Network Interface

OSI referans modeli'nin Data-Link ve Physical katmanlarını kapsar. Verinin, iletim ortamına nasıl iletileceği ve fiziksel adresleme işlemlerini tanımlar. Ağ teknolojileri ve kabloları, Network Interface katmanının ilgi alanındadır.

TCP/IP Protokülünde İletişim Nasıl Kurulur?

TCP/IP, kullanılan ağlarda her bilgisayarın bir IP adresi vardır. Bu adresler paketlerin hedeflerine ulaşmasını sağlar. Her TCP/IP paketine, hedefe ulaştırılabilmesi için, alıcının IP adresi ve geri paket yollanabilmesi için göndericinin adresi yazılır. Yazılan adresler, gönderici ile alıcı bilgisayar arasındaki olası router cihazları tarafından okunup hedefine doğru yönlendirilir.

Paketlerin Ağa Yönlendirilmesi

Her TCP/IP cihazı bir IP adresi ile tanımlanır. Bu adres Network Katmanı adresidir ve Data-link adresinden bağımsızdır. IP adresi internetwork'te eşsiz olmak zorundadır. Bir IP adresi cihazın internetwork'teki yerini belirtir. Bir internetwork, birbirlerinden "Router" cihazları ile ayrılmış farklı IP ağlarından oluşur. IP adresi cihazın hangi ağda olduğunu ve bu ağdaki kimliğini belirtir. IP adresleri iki kısımdan oluşur.

Network ID: Internetwork'ü oluşturan her ağın eşsiz bir ID'si vardır. Bu ID cihazların hangi ağda olduğunu gösterir. Aynı ağda olan cihazların Network ID'leri aynı olmak zorundadır.

Host ID: Cihazın bulunduğu ağda kendisini tanımlayan kısımdır. Aynı ağda olan cihazların Host ID'leri farklı olmak zorundadır.

IP Adreslerinin Ağda Tanımlanması

IP adresi 32Bit'lik binary bir sayıdır. Örneğin, 11000000101010000110010011001000 gibi. Fakat bu sayıyı hatırlamak ve yazmak zordur. Kolaylaştırmak için önce 4 parçaya bölünür ve 11000000.10101000.01100100.11001000 şeklini alır. Her parçaya "oktet" denir. Son olarak her oktet decimal'e çevrilir. Artık IP adresi, 192.168.100.200 şeklindedir. Bilgisayarlar için IP adresi hala binary'dir fakat biz kolay yönetebilmek için decimal'e çeviririz. Bu gösterime "Dotted Decimal" denir. Her oktet minimum 0 (00000000), maksimum 255 (11111111) değerini alabilir. IP adresinin Network ID'si ve Host ID' sinden oluştuğunu söylemiştik. Peki, bu iki kısmı belirten şey nedir?

Subnet Mask

Subnet Mask da IP adresi gibi 32Bit'lik binary bir sayıdır. Her IP adresinin bir subnet mask'ı olmak zorundadır. Subnet mask'ın binary yazılımında, 1'ler Network ID'sini, 0'lar Host ID'sini

gösterir. Subnet mask'ta 1'ler ve 0'lar sıralı olmak zorundadır. 1'lerin arasında 0'lar olamaz. Örneğin 11111111111111111111111111000000000000 gibi. Decimal'e çevirirsek 255.255.240.0 elde ederiz. IP adresi ile Subnet Mask bit'lerini birebir "AND" işlemine tabi tutarsak Network ID 'sini elde ederiz.

1 AND 1 = 1
 1 AND 0 = 0
 0 AND 0 = 0

	BIN	DEC
IP	11.000.000.101.010.000.000.000.000.000	192.168.100.200
SM	11.111.111.111.111.100.000.000.000.000	255.255.240.0
NetID	11.000.000.101.010.000.000.000.000.000	192.168.96.0

Şekilde kullandığımız Subnet Mask, IP adresinin ilk 20 bit'inin network kısmı, son 12 bit'inin host kısmı olduğunu gösteriyor. Bu durumda 192.168.100.200 IP adresli cihazın haberleşebileceği cihazların IP adreslerinin ilk 20 bit'leri 11000000.10101000.0110 olmak zorundadır. Yani hepsinin 192.168.96.0 ağında olmaları gerekir. Aksi halde router kullanmak zorunda kalırız.

IP Adresi Sınıfları

IP adresleri 5 sınıfa ayrılmıştır; A, B, C, D ve E sınıfı. IP adresi sınıfları network ve host kısımları ve başlangıç bit'leri ile birbirlerinden ayrılırlar.

A sınıfı: 1. okteti 1 ile 126 arasındadır. Binary yazılımda ilk bit her zaman "0" dir.

B sınıfı: 1. okteti 128 ile 191 arasındadır. Binary yazılımda ilk bitleri "10" dir.

C sınıfı: 1. okteti 192 ile 223 arasındadır. Binary yazılımda ilk bitleri "110" dir

Tablo 2.3

SINIF	1. Oktet Decimal Aralık	1. Octet İlk Bit'ler	Network /Host ID	Varsayılan Subnet Mask	Ağ Sayısı	Host Sayısı (kullanılabilir adresler)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 (27 – 2)	16,777,214 (2 ²⁴ – 2)
B	128 – 191	1 0	N.N.H.H	255.255.0.0	16,382 (2 ¹⁴ – 2)	65,534 (2 ¹⁶ – 2)
C	192 – 223	1 1 0	N.N.N.H	255.255.255.0	2,097,150 (2 ²¹ – 2)	254 (2 ⁸ – 2)
D	224 – 239	1 1 1 0	Multicast için ayrılmıştır			
E	240 – 254	1 1 1 1 0	Deneme amaçlı kullanılır			

IP Adresi Kuralları

127 ile başlayan IP adresleri test ve sorun giderme amacı ile kullanılırlar. Cihazlara verilemezler. Bu IP adreslerine "Loopback IP Adresleri" denir.

IP adresinin host kısmındaki bitlerin hepsi "0" olamaz. Bu adres network id'sidir.

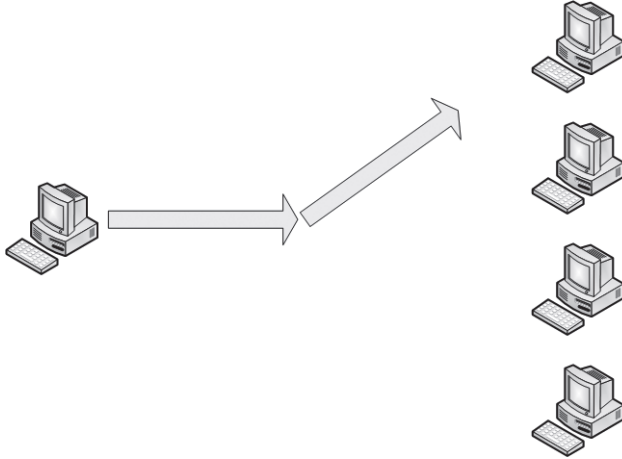
IP adresinin host kısmındaki bitlerin hepsi "1" olamaz. Bu adres "Broadcast" adresidir. Broadcast adresi ağıdaki tüm cihazlara veri gönderilirken kullanılır.

İlk oktet, 223'ten büyük olamaz. Bu adresler Multicast için kullanılır.

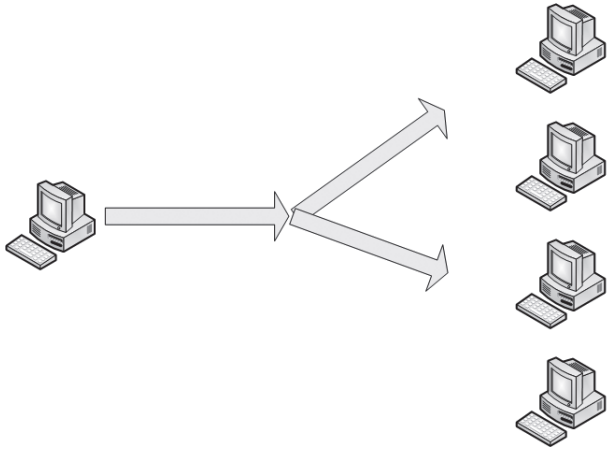
Haberleşme Biçimleri

Bir ağda 3 çeşit haberleşme vardır.

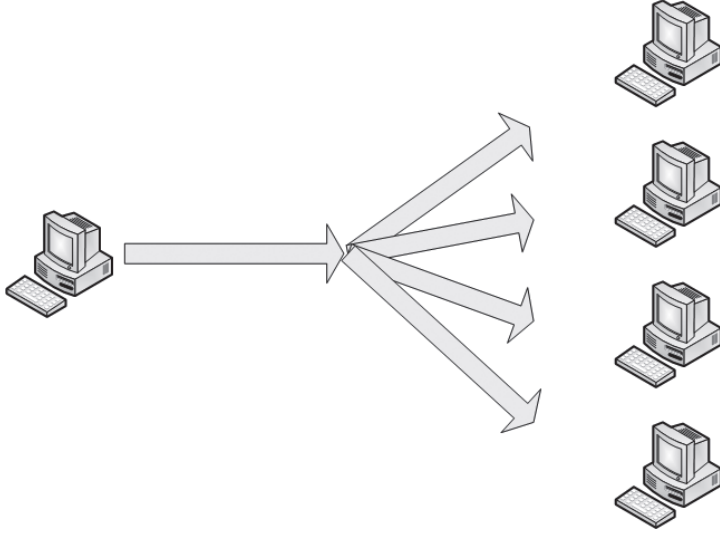
Unicast: Bir cihazdan sadece bir cihaza yapılan iletim.



Multicast: Bir cihazdan belirli bir grup cihaza yapılan iletim.



Broadcast: Bir cihazdan diğerk tüm cihazlara yapılan iletim.



Ağ Cihazları

İki bilgisayarı birbirine bağlayarak küçük bir ağ oluşturulmaya çalışıldığında ihtiyaçlar; her iki bilgisayar için ağ adaptörü ve bunları birbirine bağlayacak bir kablo ile sınırlıdır. Ancak ağ genişlemeye başladığında bir bilgisayara takılacak ağ adaptörü sayısı gibi bazı kısıtlamalar ortaya çıkar. Bu tür de kısıtlamalar hub, switch ve router gibi farklı amaçlar için kullanılan ağ cihazları sayesinde aşılr.

Repeater

Ağda kullanılan kabloların, elektronik sinyalleri iletebilecekleri maksimum uzaklıklar vardır. Örneğin UTP kablolar sinyali 100 metre taşıyabilirler. Daha uzağa veri taşınması gerekiyorsa "Repeater" cihazı kullanılır. Repeater, azalan sinyal seviyesini yükselterek daha uzun mesafelere verinin taşınmasını sağlar.



Hub

Hub'ın görevi sinyalleri güçlendirip, kabloya iletmektir. Bu tanımla repeater'a çok benzemektedir.

Hub'ın repeater'dan farkı, daha çok portu olması ve daha çok bilgisayarın iletişimini sağlamasıdır. Bu yüzden hub'a "Çok Portlu Repeater" da denir.



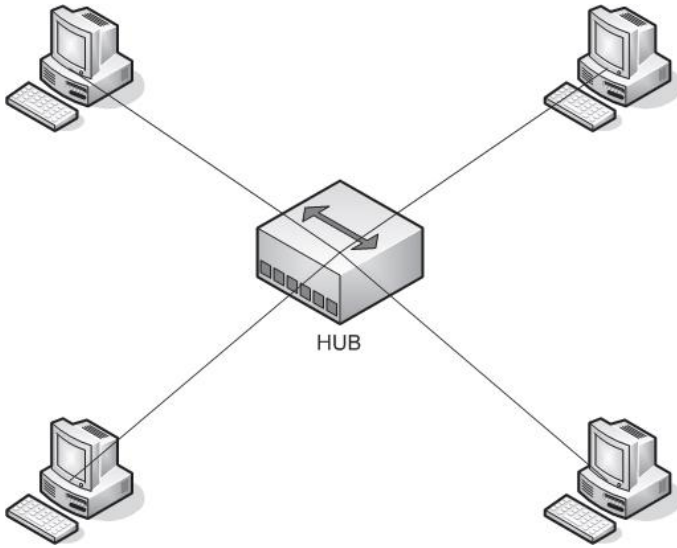
Hub, star topoloji kullanılan ağlarda tüm bilgisayarların bağlı olduğu merkezi cihazdır. Hublar, her bilgisayar için bir porta sahiptir, dolayısıyla port sayısı, bağlayabileceği bilgisayar sayısını belirler. Ancak hub'lar başka hub'lara bağlanarak ağ genişletilebilir.

Hub'ın dezavantajı, kendisine gelen sinyali tüm portlarına iletmesidir. Bu durum gereksiz ağ trafiği oluşturur ve güvenlik açıklarına sebep olur.

Hublar "Active" ve "Passive" olmak üzere ikiye ayrılır.

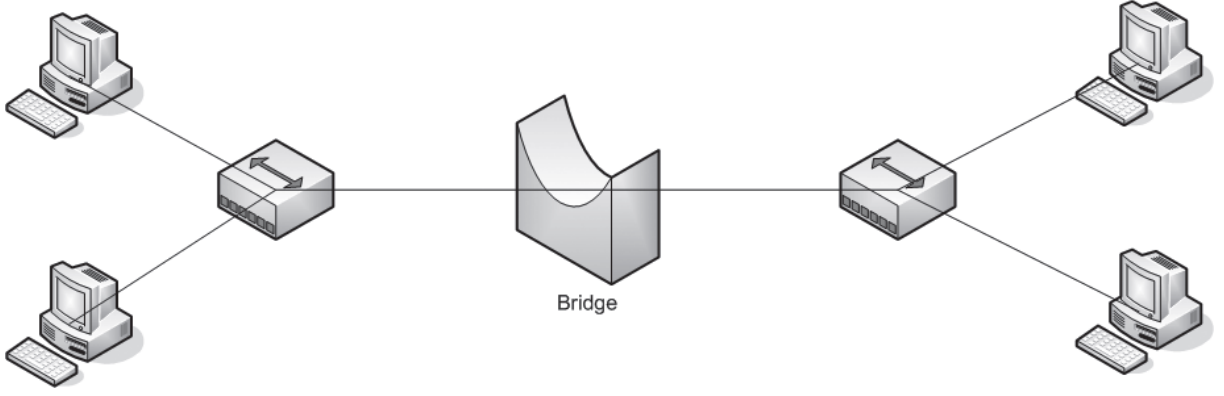
Active Hub: Sinyalleri güçlendirebilen hub'lardır. Enerjilerini bir güç kaynağından alırlar. Piyasada kullanılan hub'ların hemen hepsi "active"dir.

Passive Hub: Sinyalleri güçlendiremeyen hub'lardır. Sadece bir kaç bilgisayarı bağlamak için kullanılabilirler.



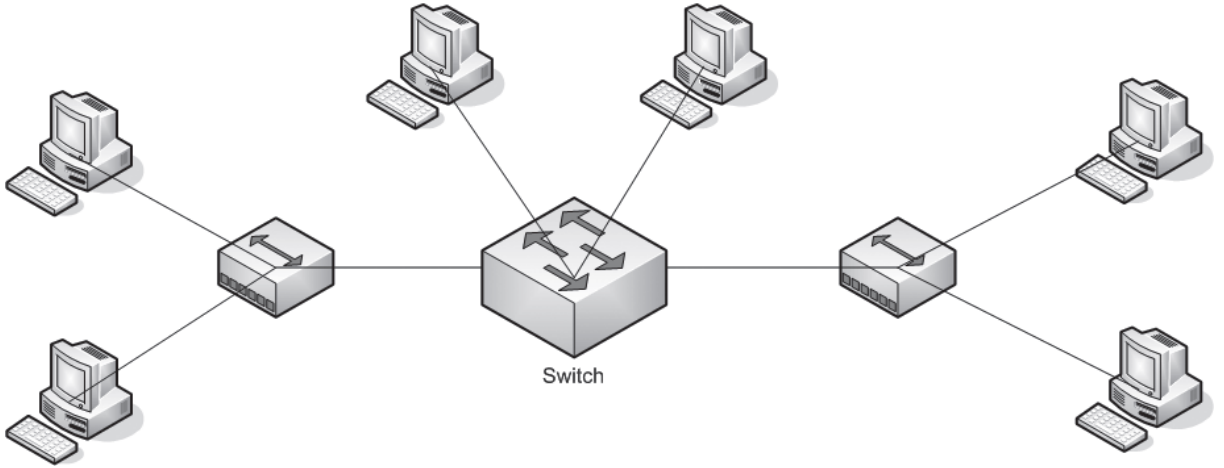
Bridge

Bridge'ler iki LAN segmentini birbirine bağlayan L2 cihazlardır. İki LAN arasındaki gereksiz trafiği filtrelerler. Bridge, her iki tarafındaki bilgisayarların MAC adreslerini hafızasında saklar. Bu da bridge'in, veriyi alacak olan bilgisayarın ne tarafta olduğunu bilmesini sağlar. Günümüz ağlarında bridge'ler önemini yitirmiştir. Bridge yerine switch ya da router kullanılmaktadır.



Switch

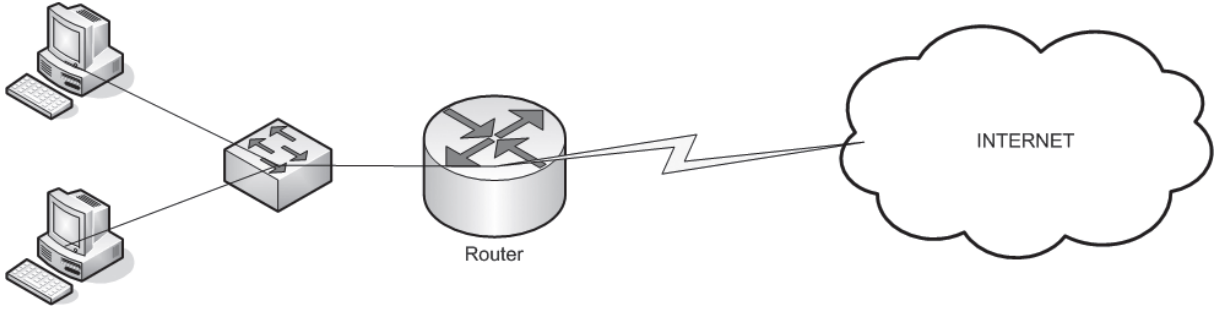
Bridge'ler gibi L2 cihazlardır. Kendisine bağı olan bilgisayarların MAC adreslerini bilir ve buna göre anahtarlama yapar. Bridge'den farkı, daha çok portunun olması ve kullanım alanıdır. Switch sadece ağ segmentlerini değil, doğrudan bilgisayarları bağlamak için de kullanılabilir. Star topoloji kullanan ağlarda merkezi cihazdır. Fakat hub gibi, sinyali tüm portlarına değil de sadece ilgili bilgisayara iletir. Gereksiz ağ trafiği oluşturmadığı için hemen her ağda tercih edilir.





Router

OSI Referans Modelinin 3. katmanında çalışırlar. Sadece MAC adreslerine göre değil, aynı zamanda IP ağlarına göre de anahtarlama yaparlar. Router'ın ağdaki rolü, bir IP paketini, bir IP ağından bir başkasına yönlendirmektir. Bu yüzden router'lar geniş ağlar ve internet için vazgeçilmez cihazlardır. Yaptıkları yönlendirme işlemi sayesinde farklı IP ağlarının haberleşebilmesini sağlarlar.

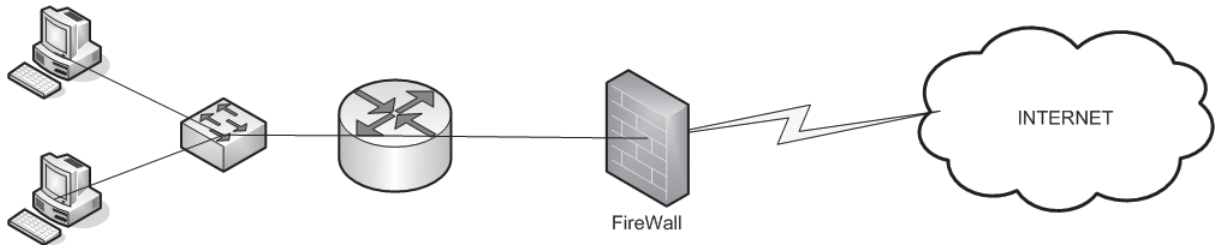




Router'ın işi, kendisine gelen IP paketlerini inceleyip, hedeflerine en kısa sürede ulaşabilmeleri için gerekli yolun seçimini yapmaktır. İnternet erişimi sağlamak ve uzak noktalardaki LAN'ları haberleştirmek için kullanılırlar.

Firewall

Ağı, internetten gelme ihtimali olan zararlı verilere karşı korur. Aynı router cihazları gibi IP paketlerini yönlendirme işlemi yapar. Bu yönlendirme işlemi sırasında paketin tamamını inceleyerek zararlı olup olmadığını kontrol eder. Firewall'lar bu inceleme işlemini yöneticisinin yapılandırması doğrultusunda yapar. Yazılımsal ve donanımsal olmak üzere iki şekilde edinilebilir. Güvenliğin çok önemli olduğu günümüz bilgisayar ağları için vazgeçilmez cihazlardan biridir.

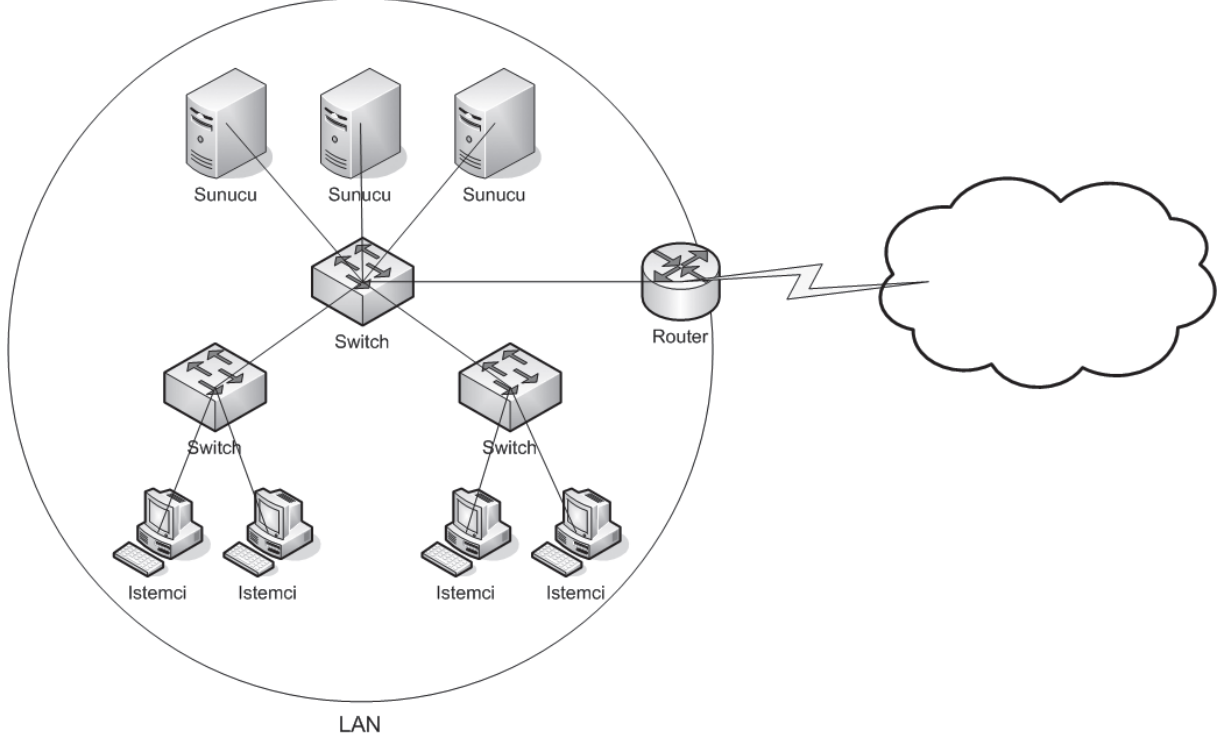


Ağ Tipleri

Bilgisayar ağları, kullandıkları teknolojilere, büyüklüklerine ve amaçlarına göre farklılık gösterirler.

Local Area Network (LAN)

Küçük bir coğrafi alana yayılmış, bilgisayarları ve yazıcı gibi çevre birimlerini bağlamak için kullanılan ağ modelidir. Yüksek hızlı ve düşük hatalı veri iletimi sağlayan ağlardır. Örneğin, bir binadaki bilgisayar ağı ya da bir kampüs ağı gibi.



Ethernet LAN'lar, en yaygın LAN tipleridir ve günümüzde tüm LAN'ları ifade etmek için kullanılabilir.

Ethernet ilk üretildiği 20 sene öncesinden bu zamana kadar, günün hız ihtiyaçlarını karşılayabilmek için sürekli geliştirilmiştir. Ethernet, FastEthernet ve GigabitEthernet gibi değişik hızlarda çalışan tipleri vardır.

OSI Referans Modelindeki Data-Link ve Physical katmanlarında, kablolama ve sinyallemeyi belirler.

Bazı LAN standartları:

IEEE 802.3: OSI'nin Physical ve Data-Link'in alt katmanı olan Media Access Control (MAC) katmanlarını kapsayan teknolojileri ifade eder.

IEEE 802.3u: FastEthernet. 100Mbps hızda çalışan standartları ifade eder. Örneğin, 100BaseTX, 100BaseFX ve 100BaseT4 gibi.

IEEE 802.3z: GigabitEthernet. Fiber kablo üzerinden 1000Mbps hızda çalışan standartları ifade eder. Örneğin, 1000BaseX.

IEEE 802.3ab: GigabitEthernet. Twisted kablo üzerinden 1000Mbps hızda çalışan standartları ifade eder. Örneğin, 1000BaseT.

IEEE 802.3an: 10 GigabitEthernet. Twisted kablo üzerinden 10Gbps hızda çalışan standartları ifade eder. Örneğin, 10GBaseT.

IEEE 802.3ae: 10 GigabitEthernet. Fiber kablo üzerinde 10Gbps hızda çalışan standartları ifade eder. Örneğin, 10GBaseSR.

CSMA/CD

Ethernet ağlarında, bilgisayarlar arası iletişim, belirli bir zamanda hangi bilgisayarın veri iletteceğini belirleyen, bir takım kurallar çerçevesinde gerçekleşir.

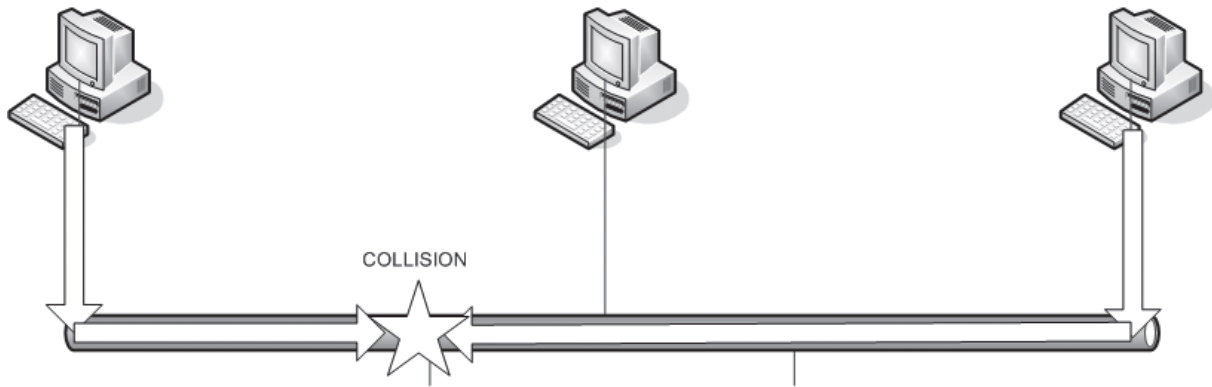
Bu kuralları tanımlayan, Carrier Sense (CS), Multiple Access (MA) ve Collision Detection (CD) isimli üç ayrı fonksiyonu bulunan CSMA/CD teknolojisidir.

CS: Bilgisayarların veri iletmeden önce kabloyu dinleyerek hattın boş olup olmadığına bakması.

MA: Birçok bilgisayarın aynı kabloları kullanması ve kablo erişiminde birbirlerine göre önceliklerinin bulunmaması.

CD: Bir collision oluştuğunda anlaşılabilmesi.

Ethernet ağlarında bilgisayarlar veri iletmeden önce kabloyu dinler. Eğer hat boş ise veriyi gönderir. Hattın boş olması, o anda başka bir cihazın veri göndermiyor olması demektir. Eğer aynı anda iki bilgisayar kablunun boş olduğunu görüp veri iletirse, bu veri sinyalleri çarpışıp birbirlerini bozacaklardır. Bu duruma Collision denir. Collision oluştuğunda, bilgisayarlar collision'ı belirtmek için JAM sinyalleri ile birbirlerini uyarır. Kısa bir süre iletişim olmaz, sonra normal süreç devam eder.



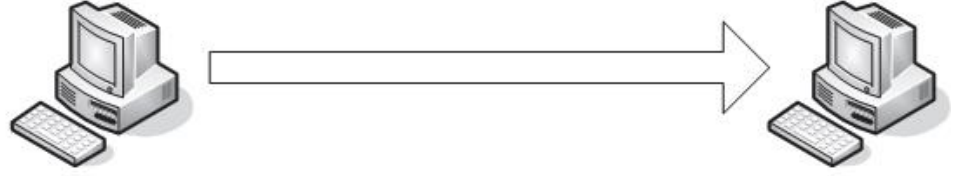
Half Duplex / Full Duplex

Duplex, iki cihazın birbirleri ile karşılıklı iletişim yapabilmesidir. Ethernet ağları iki farklı duplex modunda çalışabilir.

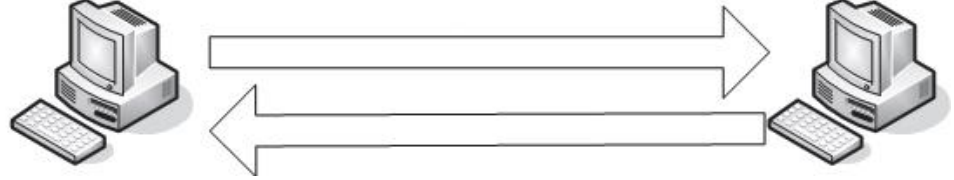
Half Duplex: Karşılıklı iletişim vardır ancak aynı anda sadece tek yöne doğru iletişim kurulabilir. Bu modda, bir bilgisayar veri alırken veri yollayamaz. Hub kullanılan LAN'lar Half-Duplex çalışır.

Full-Duplex: Bu modda, bilgisayarlar aynı anda veri alabilir ve yollayabilir. 100Mbps ve daha yüksek hızlarda switch kullanılan LAN'lar full-duplex çalışabilir. Bu modda twisted kablunun bir perisi veri yollamak için başka bir perisi de veri almak için kullanılır. Full-Duplex moddaki LAN'larda collision oluşmaz.

HALF DUPLEX



FULL DUPLEX



Ethernet Protokolleri

Günümüzde çeşitli hızlarda çalışan farklı ethernet protokolleri vardır.

Ethernet: 10Mbps hızda, coaxial ya da twisted kablo üzerinde çalışır. Ethernet – II olarak da adlandırılır.

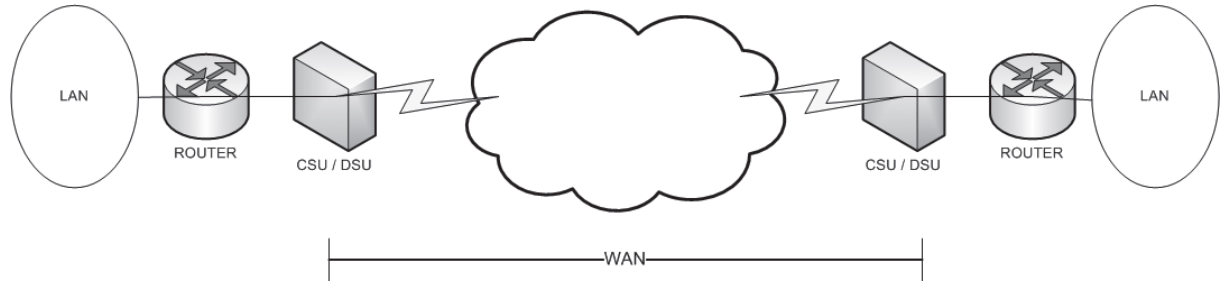
FastEthernet: 10Mbps hızın üzerindeki hızları ifade eder. Kablo altyapısında çok az bir değişiklik ile hızı 10'dan 100Mbps'a yükseltir. Günümüz yerel ağlarında istemci bilgisayarların ağ bağlantısında kullanılır.

GigabitEthernet: Farklı kablo kullanır ve hızı 1000Mbps'a çıkarır. Günümüz yerel ağlarında sunucu sistemlerin bağlantısı için kullanılır.

10GigabitEthernet: Hızı 10Gbps'a kadar çıkarır ve genellikle network backbone (ağ omurgası) bağlantılarında kullanılır.

Wide Area Network (WAN)

WAN'lar geniş coğrafi alanlara yayılmış, düşük hızlı, büyük ağlardır. Çeşitli coğrafi bölgelerdeki yerel ağlar arasında bağlantı sağlamak için kullanılırlar. Örneğin, dünya çapında yayılmış şirketlerin ağları ve internet gibi. İnternet en çok sayıda LAN'i bağlayan en büyük WAN'dır.



WAN'lar Telekom gibi bir servis sağlayıcının tahsis ettiği hatlar üzerinden kurulur ve karşılığında belirli bir ücret ödenir. Servis sağlayıcı, bağlanacak LAN'ler arası iletişim için sağladığı hatların devamlılığı ve hızından sorumludur.

Bir WAN geniş alanlar üzerinde veriyi taşımak için servis sağlayıcılar tarafından sağlanan ISDN, Frame-Relay ve xDSL gibi Data-Link katmanı teknolojilerini kullanır. Veri, video ve ses gibi çeşitli trafik türlerini taşıyabilir.

WAN teknolojileri, OSI'nin 3. katmanı altındaki katmanlarda tanımlanır.

WAN Bağlantı Tipleri

WAN bağlantı teknolojileri üç farklı kategoride incelenebilir.

Packet-Switched (Paket-Anahtarlama): Bu tip WAN'larda, servis sağlayıcı kaynakları birçok kullanıcı tarafından paylaşılır. Her bir kullanıcıya belirli bir miktar hız garanti edilir. Hatlar kalıcıdır ve her zaman açıktır. Frame-Relay, bir packet-switched WAN tipidir.

Circuit-Switched (Devre-Anahtarlama): Bu tip WAN'larda, veri hatları gerektiğinde açılır ve iletişim bitince kapatılır. Genellikle yedek bağlantı hattı olarak kullanılır. PSTN¹, ISDN² ve DSL³ circuit-switched WAN'lara örnektir.

Point-to-Point (Noktadan Noktaya): Bağlantı, önceden kurulmuş, sabit hızlı ve kalıcıdır. Leased Line (Kiralık Hat) olarak da adlandırılır. Diğerlerine göre daha pahalıdır ancak daha kararlı ve hızlıdır. Ücreti hıza ve mesafeye göre değişir.

WAN Cihazları

WAN'larda, kullanıcı tarafında ve servis sağlayıcı tarafında çeşitli cihazlar kullanılır.

Router

Kullanıcı tarafında da servis sağlayıcı tarafında da bulunan cihazlardır. Network katmanı servislerini uygulayan cihazlardır. Kullanılan hattın tipine göre çeşitli bağlantı arayüzleri sunarlar. Örneğin Frame-Relay ve Leased Line hatları için Serial bağlantı arayüzleri kullanılır.

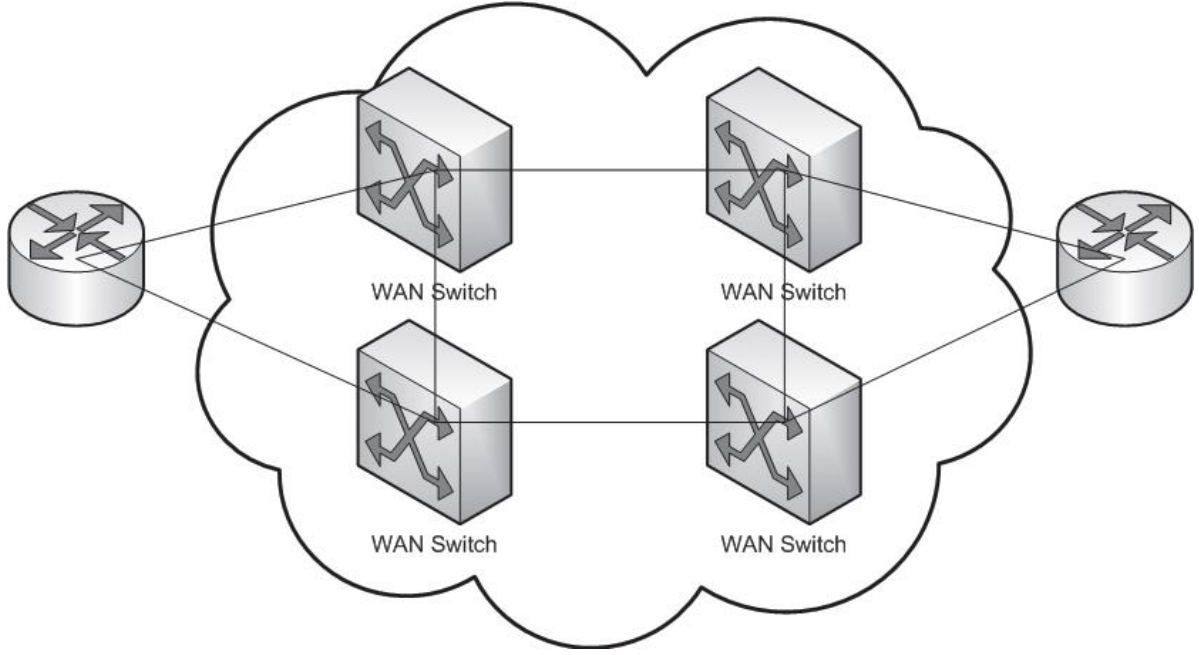
WAN Switch

Birbirinden uzak noktalarda bulunan router cihazları arasında bağlantı sağlar. WAN trafiğini 2.katman teknolojileri kullanarak hedefine doğru anahtarlayan çok portlu cihazlardır. Bağladıkları router'lar arası fiziksel bir bağlantı olmadığı için oluşturdukları devreye virtual-circuit (sanal-devre) denir. Her router bir WAN switch'ine doğrudan bağlıdır. Servis sağlayıcının ağındaki WAN switchleri, kendi aralarında sanal bir devre oluşturup router'ların birbirleri ile iletişim kurabilmelerini sağlar.

¹ **PSTN** yani Public Switched Telephone Network (Genel aktarmalı telefon şebekesi)'dir. PSTN, dünya genelinde kullanılan devre aktarmalı telefon ağıdır. Analog telefon santrali.

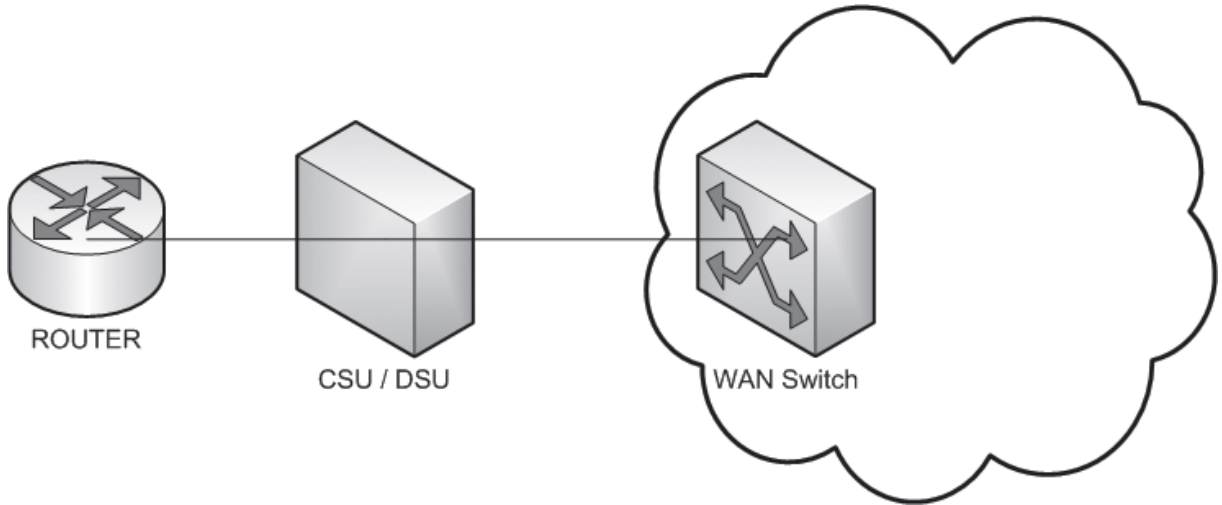
² **ISDN**, Integrated Services Digital Network sözcüklerinin baş harflerinden oluşmuştur ve *Bütünleştirilmiş sayısal ağ hizmetleri* olarak Türkçeleştirilmiştir. ISDN, mevcut analog telefon şebekesinin sayısal alternatifidir. Dijital telefon santrali. Hem ses hemde data aktarmaya yarar.

³ **DSL** (Digital Subscriber Line) dijital abone hattı anlamına gelmekte olup, ADSL de dahil olmak üzere tüm DSL teknolojisini kapsar. ADSL (Asymmetric Digital Subscriber Line), VDSL (Very-High Bitrate Digital Subscriber Line), SHDSL (Symmetric Digital Subscriber Line)



Modem

Modem, PSTN hatlarda kullanılır ve PSTN ağına erişimi sağlar. Dijital-analog dönüşümü sağlar. Bilgisayardan gelen dijital sinyal modem tarafından analog sinyale dönüştürülür ve iletim için uygun hale getirilip WAN hattına gönderilir. Hedefte, gelen analog sinyal modem tarafında dijitale dönüştürülür ve bilgisayarın anlayabileceği hale getirilip bilgisayara iletilir.



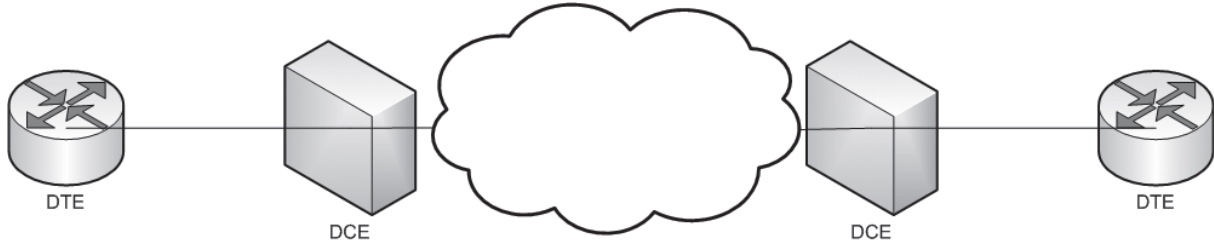
Channel Service Unit / Data Service Unit (CSU/DSU)

Dijital modem olarak da adlandırılabilen CSU/DSU cihazı dijital-dijital çevrimi yapar. Router'dan gelen dijital sinyali WAN hattı üzerinde hareket edebilecek hale getirip iletir. Router ile WAN switch arasındaki fiziksel bağlantıyı sağlar.

Data Terminal Equipment / Data Circuit-Terminating Equipment (DTE/DCE)

WAN iletişimi, DTE cihazları birbirine bağlamak için kullanılır. Genellikle DTE cihazlar router'lardır. Router'lar WAN servislerini doğrudan kullanamazlar. Kullanabilmelerini sağlayan cihazlar, DCE cihazlardır. Modemler ve CSU/DSU cihazları DCE cihazlardır. DTE cihazlar WAN servislerini DCE cihazlar aracılığı ile kullanırlar. DTE/DCE cihazlar, kullanıcının

sorumluluğunun bitip servis sağlayıcının sorumluluğunun başladığı noktadır. Kullanıcı için WAN, DTE ve DCE arasındaki link, channel ya da line denen hattır.



WAN Terminolojisi

Customer Premises Equipment (CPE): Kullanıcının binasında bulunan, kullanıcıya ait ya da servis sağlayıcı tarafından kullanıcıya kiralanılan cihazlardır. DTE/DCE cihazları içerir.

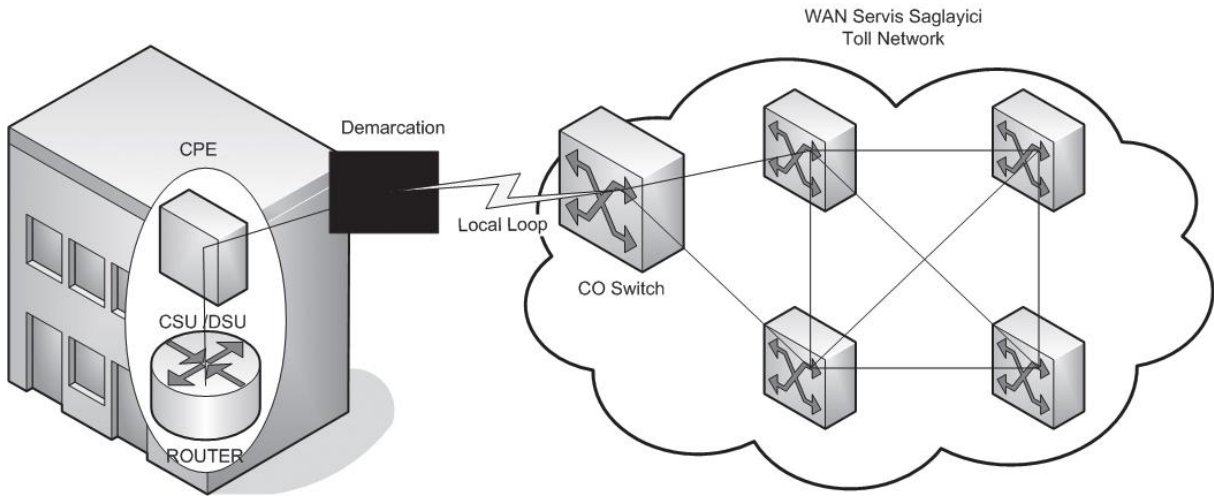
Demarcation: CPE'nin bittiği ve servis sağlayıcısına ait olan local-loop'un başladığı noktadır. Genellikle POP'tur.

Local Loop: POP'dan servis sağlayıcının merkezine yapılan kablolamadır.

CO Switch: Servis sağlayıcının, WAN servisi için en yakın POP'u sağlayan switch'idir.

Point of Presence (POP): Servis sağlayıcının cihazlarının bulunduğu noktadır.

Toll Network: Servis sağlayıcısına ait ağ bulutudur.



Metropolitan Area Network (MAN)

Büyük bir coğrafi alanda, birden fazla LAN'ı birbirine bağlamak için kullanılır. WAN ile aynı teknolojileri kullandığı için aynı özelliktedir.

Aynı şehirde bulunan LAN birimlerinden oluşan WAN'dır.

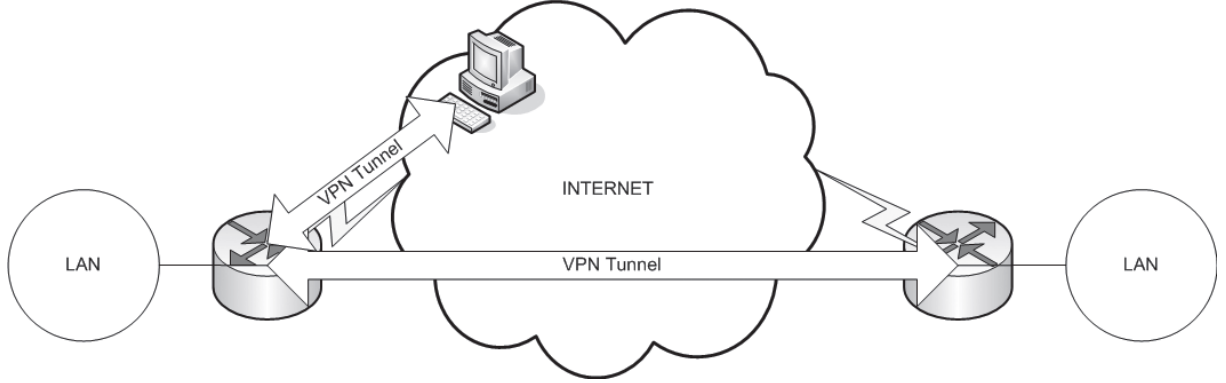
Bağlantı için genellikle leased line, optik ya da kablosuz teknolojileri kullanılır.

Virtual Private Network (VPN)

İnternet gibi halka açık ağlar üzerinden oluşturulan uzak bağlantı ağlarıdır. Halka açık ağlar kullanıldığı için birçok güvenlik teknolojisi içerir.

Bağlanan birimler arası WAN servisi kiralınmadığı için maliyeti daha düşüktür. Kiralanan hatların sadece internet bağlantısı sağlaması yeterlidir. İnternete bir şekilde erişen, LAN'lar arası VPN teknolojileri kullanarak sağlanan bağlantıdır.

Birimler arası bağlantıda ve ev kullanıcıların şirket ağına bağlanmasında kullanılabilir.



Ağ Topolojileri

Ağ topolojileri; bilgisayarların birbirlerine nasıl bağlandıklarını ve nasıl iletişim kurduklarını gösteren yapılarıdır. Mantıksal topolojiler ve fiziksel topolojiler olarak ikiye ayrılırlar. Fiziksel topoloji; bilgisayarların fiziksel olarak birbirlerine nasıl bağlandıklarını gösterir. Mantıksal topoloji ise fiziksel bağlantının nasıl kullanılarak iletişim kurulduğunu gösterir. Buna göre fiziksel olarak "Star" topoloji kullanan bir ağ, mantıksal olarak "Bus" topoloji kullanıyor olabilir.

Bus Topoloji

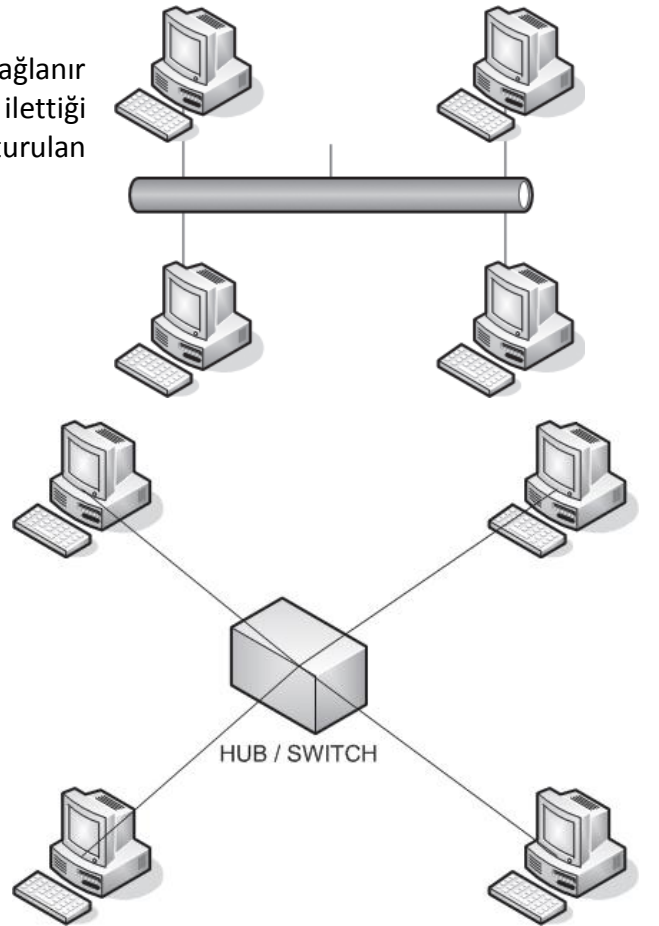
Bus topolojisinde bilgisayarlar, doğrudan bir hatta bağlanır ve aralarında başka bağlantı yoktur. Bir bilgisayarın ilettiği sinyal tüm bilgisayarlara ulaşır. Coaxial kablo ile oluşturulan ethernet ağları, bus topolojisine örnektir.

Avantajları :

- İlave bir cihaza gereksinim duymaz.
- Ucuzdur.

Dezavantajları :

- Kablonun herhangi bir yerindeki kopukluk tüm sistemi etkiler.
- Hata tespiti zordur.
- İletişim yavaştır.



Star Topoloji

Star topolojide tüm bilgisayarlar merkezi bir ilave cihaza bağlanır. Merkezdeki cihaz sinyal iletimini

sağlar. Her bilgisayar kendi kablosu ile merkezdeki cihaza bağlanır.

Hub kullanılarak oluşturulan star topoloji ağları, hub'ın kendisine gelen sinyalleri tüm bilgisayara yollaması yüzünden, fiziksel olarak star olsa da mantıksal olarak bus topolojidir.

Avantajları :

- Kurulumu basittir.
- Yüksek hız sağlayabilir.
- Arıza tespiti kolaydır.
- Herhangi bir kablodaki kopukluk, sadece kablonun bağlı olduğu bilgisayarı etkiler.

Dezavantajları :

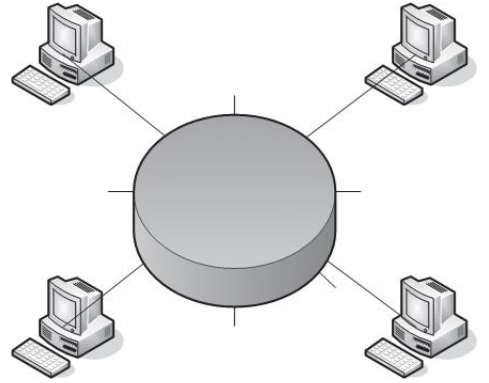
- İlave cihaz gerektirir.

Ring Topoloji

IBM'in geliştirdiği Token-Ring ağlarda ve FDDI⁴ teknolojisinde kullanılan topolojidir.

Bilgisayarlar, merkezdeki MSAU (Multi Service Access Unit) denilen cihaza, ayrı kablolar ile bağlanırlar ancak aralarındaki iletişim tek yönlü ve halka biçiminde olması sebebiyle adı Ring topolojidir. Genişlemeye açık değildir ve yüksek hızlara ulaşamaz.

IBM'in Token-Ring ağları, fiziksel olarak star ancak mantıksal olarak bus topolojidir. FDDI teknolojisi kullanan ağlar, fiziksel olarak da mantıksal olarak da ring topoloji kullanır.



Mesh Topoloji

Bu topolojide tüm bilgisayarlar diğer tüm bilgisayarlara bağlıdır. Bir noktadan diğerine sadece bir yol yoktur. Bu topoloji, çok yüksek hata toleransı gerektiren iletişimlerde kullanılır. Genelde WAN'larda kullanılırlar.

Avantajları :

- Herhangi bir kablonun kopması, alternatif yollar olması sebebiyle, iletişimi engellemez.
- Yüksek bağlantı hızı sağlayabilir.

Dezavantajları :

- Yüksek maliyetlidir.
- Bilgisayar sayısı arttıkça kablolama imkansız hale gelebilir.

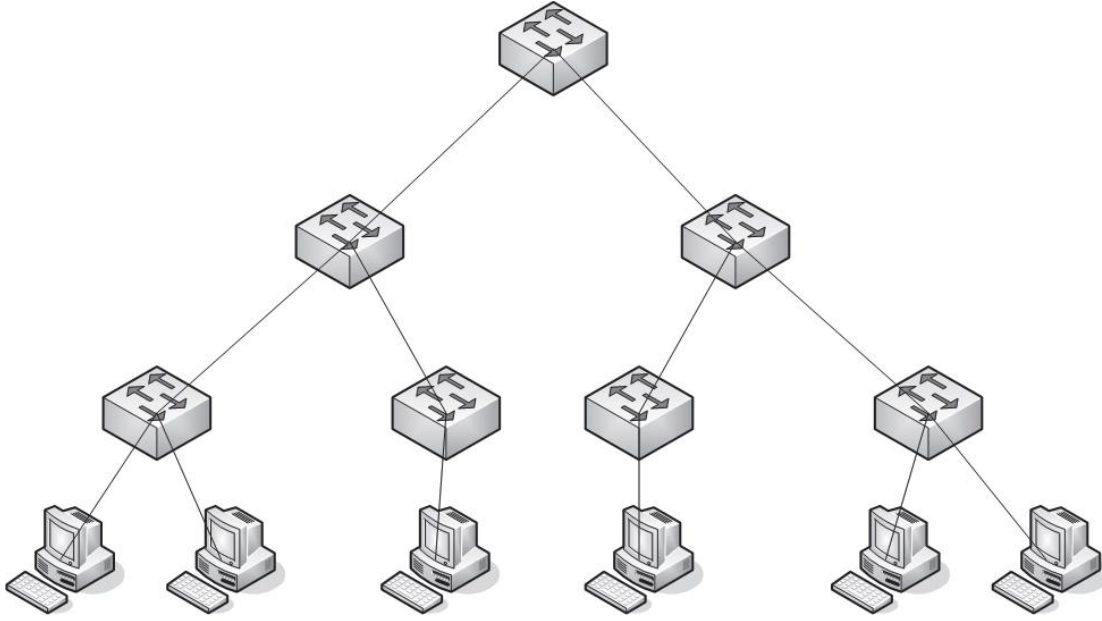
Hybrid Topoloji

Hybrid topolojiler, bir kaç farklı topolojinin birleşmesi ile oluşan topolojilerdir. Star-Bus, Star-Ring örnek olarak gösterilebilir.

⁴ FDDI (Fiber Distributed Data Interface) OSI'nin 1. ve 2. katmanında çalışan yine Ethernet gibi LAN ve WAN ağlarına erişmek için kullanılan, günümüzde pek yaygın olarak kullanılmayan bir standarttır. Daha çok omurga kablolamada ve çok yüksek hız gerektiren yerlerde kullanılır.

Extended Star

Star topolojinin genişletilmiş halidir. Hiyerarşik LAN'lerde kullanılırlar. Günümüz yerel ağlarının hemen hepsi extended star'dır.



Ağ Kabloları

Bir bilgisayar ağında, cihazların yolladıkları sinyallerin hareket edebileceği ortama ihtiyaç vardır. Kablosuz ağlarda, sinyaller elektromanyetik dalgalara dönüştürülerek iletilirken, kablolu ağlarda, elektrik akımına ya da ışık sinyaline dönüştürülür.

Kullanılan kablonun kendi iç direnci ve yapısı, veriyi ne kadar uzağa götürebileceğini ve saniyede ne kadar veri taşıyabileceğini belirler.

Piyasada kullanılacak birçok kablo çeşidi bulunmaktadır. Kullanılacak kablo, hız ve mesafe ihtiyaçlarına göre belirlenir.

Twisted Pair Kablolar

Bir yerel ağda, bilgisayarlar ile switch bağlantısında ve telefon bağlantılarında kullanılabilirler. Twisted kablolar, birbirine ikili (pair) olarak sarılmış kablolardan oluşur. Bu sargılar, bir kablo içerisindeki akımın bir diğerindekini etkilemesini (crosstalk) engelleme amaçlıdır.

Kullanım kolaylığı, sürekli geliştirilmesi ve günümüz hız ve mesafe ihtiyaçlarını karşılayabildiği için yerel ağlarda en çok tercih edilen kablo tipidir.

Unshielded Twisted Pair

UTP kablolarında pair'lerin etrafında bir koruyucu kalkan yoktur. Kalkan olmayışı daha esnek olmasını ve kolay uygulanabilmesini sağlar. Diğer twisted kablolarına göre daha ucuzdurlar. Ortamdaki elektromanyetik alandan etkilenebilirler.

Günümüz bilgisayar ağlarında en çok tercih edilen kablo tipidir.



UTP kabloların özellikleri:

- Veriyi 100 metre taşıyabilir.
- 10/100/1000/10000Mbps hızlarında çalışabilir.
- Elektromanyetik alandan etkilenebilir.
- RJ 45 konnektör kullanılır.

Shielded Twisted Pair

Kablo içerisindeki elektromagnetik alandan korunmak için her pair'in etrafında ve dış ortamdaki elektromanyetik alandan korunmak için de tüm pair'lerin etrafında metal bir koruyucu kalkan bulunur. IBM Token Ring ağlarında kullanılmışlardır. Günümüz ethernet ağlarında pek yaygın değildir.



STP kabloların özellikleri:

- Veriyi 100 metre taşıyabilir.
- 10/100/1000/10000Mbps hızlarında çalışabilir.
- Elektromanyetik alandan etkilenmez.
- STP konnektör kullanılır.

Screened Twisted Pair

- Tüm pair'lerin etrafında koruyucu bir kalkan bulunur.
- ScTP kablo özellikleri:
- Veriyi 100 metre taşıyabilir.
- 10/100/1000/10000Mbps hızlarında çalışabilir.
- Elektromanyetik alandan etkilenmez.
- STP konnektör kullanılır.

Kategoriler

Twisted kablolar, çeşitli iletişim tiplerinde kullanılmak üzere farklı kategorilerde üretilmişlerdir.

Cat1: Telefon hatlarında kullanılmışlardır.

Cat2: 4Mbps Token ağlarında kullanılmışlardır.

Cat3: 10Mbps ethernet ağlarında kullanılmışlardır.

Cat4: 16Mbps token ağlarda kullanılmışlardır.

Cat5: 4 pair'den oluşur. 1000Mbps ethernet ağlarında kullanılabilir olmasına rağmen daha çok 100Mbps ağlarda kullanılırlar. RJ 45 konnektörler ile bağlantı sağlanır.

Cat5e: 4 pair'den oluşur. CAT5'in geliştirilmiş halidir. 1000Mbps ethernet ağlarında kullanılır. Crosstalk daha az gerçekleşir. RJ 45 konnektörler ile bağlantı sağlanır.

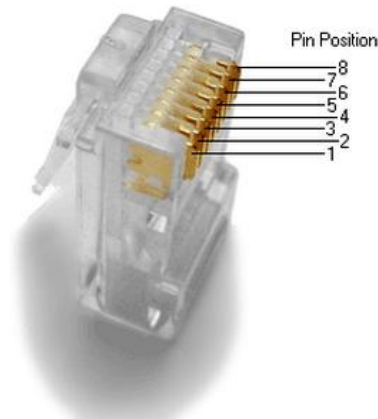
Cat6: 4 pair'den oluşur. Daha çok 1000Mbps ethernet ağlarında kullanılıyor olmasına rağmen 10000Mbps ethernet ağlarında da çalışabilir. Crosstalk, Cat5 ve Cat5e'ye göre çok daha düşüktür. 8P8C(RJ48) konnektörler ile bağlantı sağlanır. 8P8C konnektörlerin görüntüsü RJ 45 konnektörler ile aynıdır.

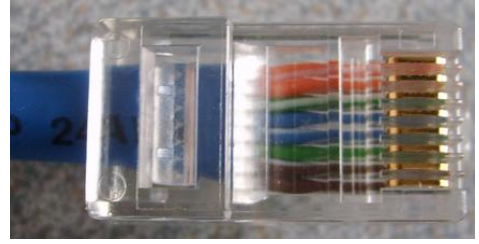
RJ 45	RJ 48
RJ 45 uses pin 1,2,3,6 for receiving and transmitting.	RJ 48 uses pin 1,2,4,5 for receiving and transmitting.
RJ 45 is commonly used in LAN environment in short distance	RJ 48 is used in WAN links such as T1 and E1 leased lines.
RJ 45 uses UTP cables.	RJ 48 used STP cables.
RJ 45 is always single line	RJ 48 can be multiline and flush mount

Cat7: 4 pair'den oluşur. Crosstalk'u engellemek için kalkan kullanılır. 10000Mbps Ethernet ağları için üretilmiştir.

Bağlantı Tipleri

Twisted kablolar, crosstalk'u minimuma indirmek için özel bir bağlantı şekli gerektirir. 4 pair'den oluşan bir twisted kabloda, her biri farklı renkte 8 kablo vardır. Bu 8 renk, 4 ana renkten ve bunların beyazlı olanlarından oluşur. 4 ana renk turuncu, yeşil, mavi ve kahverengidir.





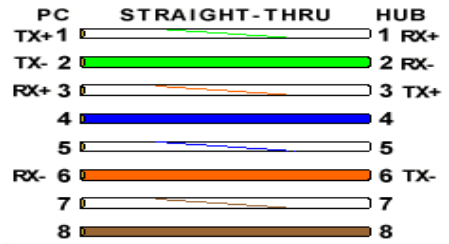
Twisted kablolar bağlantı için genelde RJ 45 konnektör kullanılır. Renk kodlarına göre uygun sıraya sokulduktan sonra kablo RJ 45 konnektöre bağlanılır.

Düz (Straight) Kablo

Kablonun her iki ucu da aynı renk kodu sırasına göre bağlanmış kablodur. Bilgisayar – Switch, Switch – Router bağlantılarında kullanılır.

İki farklı renk sırası kullanılabilir.

- 568A: 1.YB – 2.Y – 3.TB. – 4.M. – 5.MB. – 6.T – 7.KB – 8.K
- 568B: 1.TB – 2.T – 3.YB – 4.M – 5.MB – 6.Y – 7.KB – 8.K



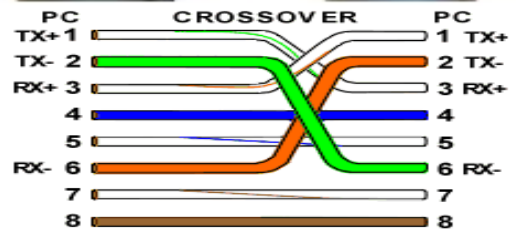
Çapraz (Crossover) Kablo

Twisted kablo kullanan ağ cihazlarında, 100Mbps hızda, RJ 45 konnektörün bağlandığı soketteki 8 pin'den; 1, 2, 3 ve 6 numaralı pin'ler kullanılır. 1. ve 2. pinler veri göndermek için, 3. ve 6. Pinler veri almak için kullanılır. Böyle iki cihaz arasında, switch gibi bir anahtarıcı cihaz kullanılmazsa, her iki cihazın aynı iş için kullanılan pin'lerini bağladığı için straight kablo çalışmayacaktır.

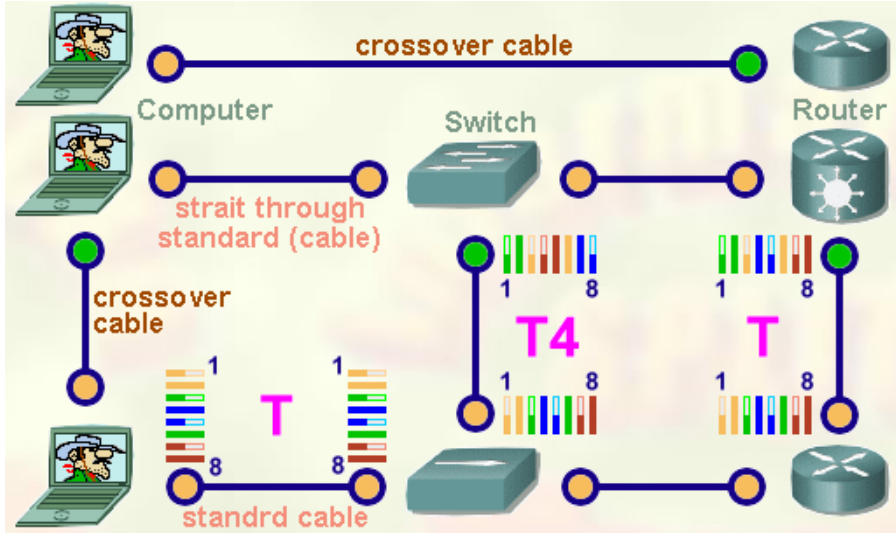
Cross kablunun uçları, bir tarafın veri gönderici pin'lerini diğer tarafın veri alıcı pinlerine bağlamalıdır.

Bilgisayar – bilgisayar, router – router, switch – switch bağlantılarında kullanılır.

100Mbps hız için cross kablunun bir ucu 568A diğer ucu 568B renk sırasına göre bağlanır



100Mbps hızda çalışan ağlarda 4 pair de kullanıldığı için, cross kablo renk sırası farklıdır.



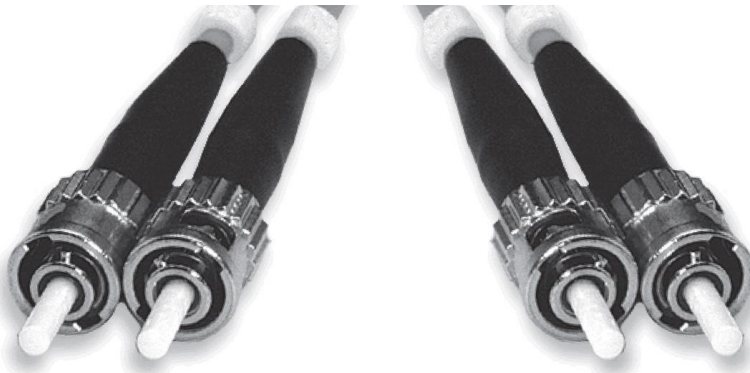
Fiber Optik Kablolar

Veri hareketini, cam ya da plastik fiber üzerinden ışık sinyalleri ile sağlar. Kabloda koruyucu ve sinyalin dışarıya yansımalarını engelleyici birçok katman vardır. Sinyal en içteki "core" katman üzerinde hareket eder. Işık sinyalleri çevredeki elektromanyetik alandan etkilenmez. Bakır kablolardan çok daha uzak mesafelere iletim yapabilirler.



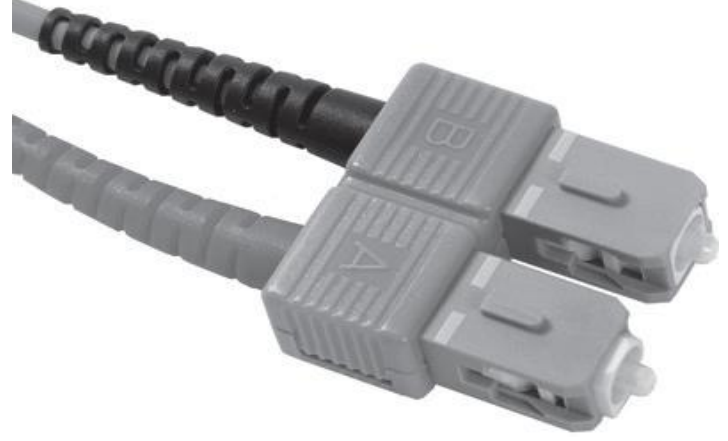
Single Mode Fiber

- Core tabaka incedir.
- Aynı anda bir ışık sinyali taşır.
- Işık kaynağı genelde lazerdir.
- Çok uzak mesafelere (100km maksimum) veri taşıyabilir.
- Bağlantı için Straight Tip (ST) konnektörler kullanılır.



Multi Mode Fiber

- Core tabaka kalındır.
- Aynı anda birçok ışık sinyali taşıyabilir.
- Işık kaynağı LED'dir. Single Mode'a göre daha ucuzdur ancak, Single Mode kadar uzak mesafelere (2km maksimum) veri taşıyamaz.
- Bağlantı için Subscriber Connector (SC) konnektörler kullanılır.
- Her iki mode fiber için Lucent Connector (LC) kullanılabilir.



Ethernet Kablo Standartları

Kullanılan kablo, mesafe ve hızı belirler. Bazı standartlar:

10Base2 (Thinnet):

- 10Mbps
- 50Ohm dirençli Coaxial kablo
- Sinyali 185m uzağa taşıyabilir.
- Bir segmentte en fazla 30 bilgisayar destekler.
- BNC konnektörler kullanılarak bağlantı sağlanır.

10Base5 (Thicknet):

- 10Mbps
- 50Ohm dirençli Coaxial kablo
- Sinyali 500m uzağa taşıyabilir.
- Bir segmentte en fazla 100 bilgisayar destekler.
- N-Style konnektör kullanılır.

10BaseT: Twisted (Sargılı kablo)

- 10Mbps
- 100Ohm dirençli
- UTP ya da STP kablo
- 100m mesafe
- RJ-45 konnektör kullanılır.

100BaseTX

- 100Mbps
- 100Ohm dirençli
- UTP ya da STP CAT5 kablo
- 100m mesafe
- RJ-45 konnektör

1000BaseT

- 1Gbps
- 100ohm dirençli
- UTP ya da STP CAT5e ya da CAT6 kablo

- 100m mesafe
- RJ-45 konnektör

1000BaseSX

- 1Gbps,
- MultiMode fiber kablo,
- 220-550m mesafe,
- SC konektör

1000BaseLX

- 1Gbps,
- MultiMode ya da SingleMode,
- fiber kablo,
- 550-5000m mesafe,
- SC konektör

Ağ Teknolojileri

Günümüz bilgisayar ağlarında, ihtiyaca ve mesafeye göre değişik ağ teknolojileri kullanılır. Ağ teknolojileri, OSI'nin Data-Link ve Physical katmanlarında tanımlanır. Bilgisayarların ağ ortamına nasıl erişeceklerini, hangi kurallara göre iletişim kuracaklarını ve sinyalizasyonu belirler. Temel olarak LAN ve WAN olmak üzere iki tip ağ vardır. Her ikisinde de farklı teknolojiler kullanılabilir.

LAN Teknolojileri

Küçük bir coğrafi alana yayılmış olan, yüksek hız ve düşük hata olasılığı sağlayan ağlara LAN denir. Günümüz LAN'larında sadece ethernet kullanımına rağmen değişik teknolojiler mevcuttur.

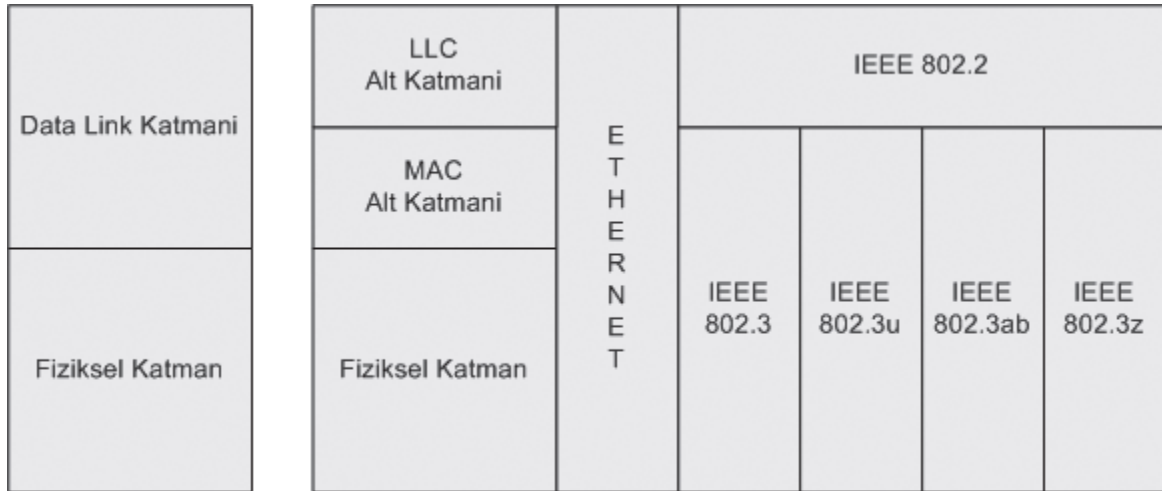
Ethernet

En popüler LAN teknolojisidir. Düşük maliyetlerle yüksek hız sağladığı için sürekli geliştirilen ve kullanılan teknoloji olmuştur.

1970'li yılların başlarında geliştirilen ilk ethernet ağlarında, 75Ohm dirençli Coaxial kablo kullanılarak 3Mbps hıza ulaşılabildi. Daha sonra Xerox ve DEC tarafından geliştirilen ethernet, 1985 yılında IEEE tarafından yeniden derlendi ve IEEE 802.3 ismi ile piyasaya çıktı.

Günümüzde ethernet teknolojisi 10Mbps'den 10Gbps hızına ulaşabilmektedir. 100Gbps hız geliştirilmektedir ve yakın zamanda piyasaya çıkması beklenmektedir. Ethernet teknolojisi kablo erişim metodu olarak "CSMA/CD" (Carrier Sense Multiple Access/ Collision Detection) tekniğini kullanır.

IEEE, OSI'nin Data-Link katmanını MAC ve LLC olmak üzere iki alt katmana böler.



Logical Link Control (LLC) Altkatmanı

LLC alt katmanı, IEEE tarafından Data-Link teknolojilerinin bağımsız olarak çalışabilmesi için geliştirildi. Bu katman, üzerindeki Network katmanı protokollerine esneklik sağlar. Bunun yanında L1 teknolojileri ve MAC'in versiyonları ile etkili bir iletişim kurar.

LLC Header'ı, Data-Link katmanına pakete ne yapılması gerektiğini söyler. Örneğin paketi alan bilgisayar LLC Header'a bakarak, paketin IP protokolüne gönderildiğini anlar.

LLC, Ethernet'in ilk sürümlerinde kullanılmıyordu, bunun yerine pakete "Type" bilgisi giriliyordu.

Media Access Control (MAC) Altkatmanı

Kabloya erişimin nasıl yapılacağını belirler ve fiziksel adresleme yapar. Ethernet ağındaki her bilgisayarın, dünyada unique bir MAC adresi vardır. Bu adres, bilgisayara takılan ethernet kartı üzerine üreticisi tarafından fiziksel olarak girilir. 48Bit'lik MAC adresinin ilk 24Bit'i üreticisini tanımlar.

Son 24Bit'i ise kartın seri numarası olarak düşünülebilir. MAC adresi "ipconfig /all" komutu ile görülebilir. Komut çıktısındaki Physical Address kısmı, MAC adresini verir.

İlk 24Bit, Organizationally Unique Identifier (OUI) adı verilen, her üreticinin edindiği sabit ve unique bir değerdir. Bir üreticide birden fazla OUI bulunabilir. Örneğin 00-01-42 ve 00-01-43 Cisco Systems şirketine ait yüzlerce OUI numarasından iki tanesidir.

Switching

Ethernet, temel olarak paylaşılan ortam üzerinden veri iletimini tanımlayan bir teknolojidir. Her bilgisayarın aynı kabloyu kullanması, aynı anda sadece bir bilgisayarın veri iletebilmesine, kablo hızının bilgisayarlar arasında paylaşılmasına ve veri iletim hızının büyük oranda düşmesine sebep olur. Ayrıca collision olma olasılığı bilgisayar sayısı ile doğru orantılıdır. Bu sebepler ile eski ethernet teknolojisi, çok bilgisayarın bulunduğu bir yerel ağ için uygun değildir. Ancak günümüz ethernet ağları için vazgeçilmez olan switch cihazları ve geliştirilen ethernet teknolojileri, binlerce bilgisayarın aynı yerel ağda hız kaybı olmadan çalışabilmesine olanak sağlar.

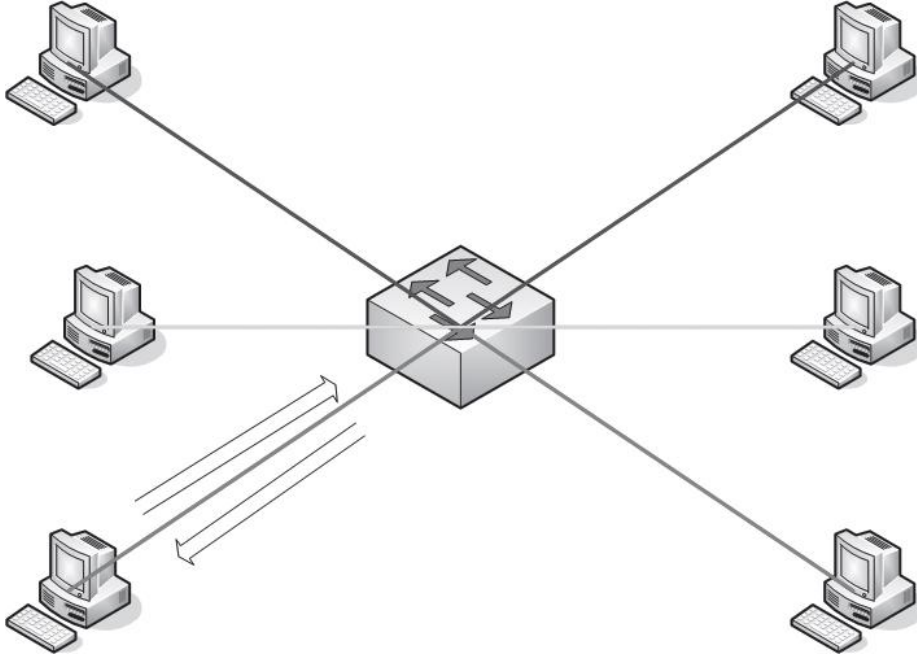
Switching teknolojilerinin sağladıkları:

MicroSegmentation: Switch cihazları iki bilgisayar arasında sabit ve sadece iletişim kuran iki bilgisayarın kullandığı segmentler oluşturur. Bu segmentler, yollanan verilerin sadece ilgili bilgisayara gitmesini ve sadece o bilgisayarın kablosunun meşgul edilmesini sağlar. Aynı anda birçok bilgisayar veri iletimi yapabilir.

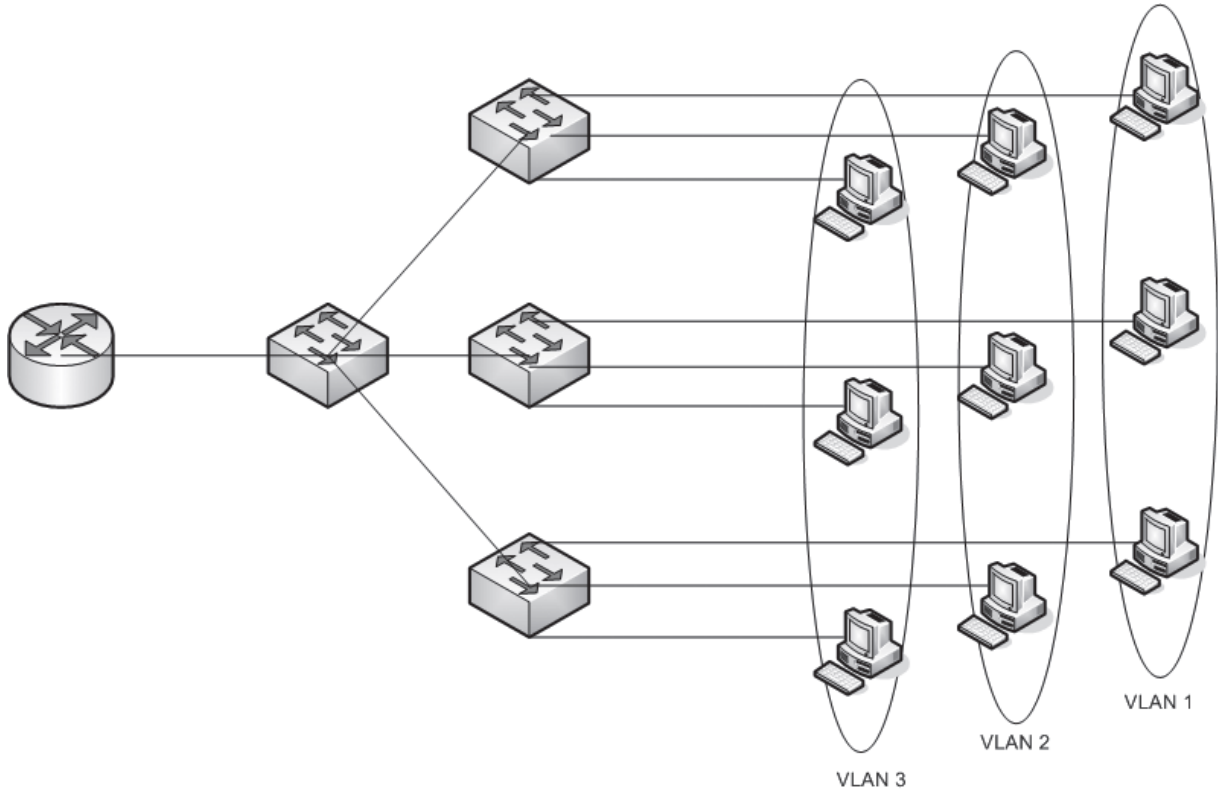
Full-Duplex iletişim sağlayabilir. Bu durumda 100Mbps bağlantı hızı kullanılan bir yerel ağda, 100Mbps veri gönderim hızı ve 100Mbps veri alma hızı olacağı için toplam hız 200Mbps olur. Ayrıca Full-Duplex iletişimde collision oluşmaz.

Virtual LAN (VLAN)

Bu özellikler, bir ethernet yerel ağında sıkça yapılan broadcast iletişiminin sebep olduğu hız kayıplarını engelleyemez. Temel olarak switchler, MAC adreslerine göre anahtarlama yaptıkları için gelen bir broadcast paketini tüm port'larından çıkartarak tüm ağa yayar.



VLAN teknolojisi ile switch portları mantıksal olarak gruplandırılabilir. Her bir grup ayrı VLAN olarak yapılandırılır ve her VLAN farklı bir IP ağını kullanır. Bir VLAN'deki port'a bağlı bir bilgisayarın yolladığı broadcast paketi sadece o VLAN'deki diğer bilgisayarlara iletilir. VLAN'ler arası iletişim ancak routing ile mümkündür. Routing, bir switch tarafından ya da router tarafından yapılır.



VLAN'in sağladıkları:

- LAN'ı broadcast alanlarına böldüğü için veri trafiğini azaltır ve bant genişliği kullanımını artırır.
- VLAN'lar arası iletişim L3 teknikleri kullanılarak denetlenebilir.
- Yönetim ve sorun giderme işlemlerini kolaylaştırır.

Token Ring

IBM tarafından 1970'li yıllarda üretilen Token-Ring teknolojisi, IBM'in hala birinci LAN teknolojisi olmasına karşın, günümüzde pek tercih edilmez. IEEE 802.5 spesifikasyonları ile hemen hemen aynı yapıya sahiptir. Token-Ring ağlarda cihazlar, merkezdeki "MSAU" (Multi Service Access Unit) denilen bir cihaza kendi kabloları ile bağlanmalarına rağmen mantıksal bir ring (halka) oluştururlar. Bu halka kullanılan erişim metodunun bir sonucudur. Token-Ring ağlar, 4-16Mbps hızında çalışır.

Token Passing

Token-Ring ağların kullandığı kablo erişim metodudur. Bu erişim metodunda, ağdaki bilgisayarlara sırayla uğrayan bir "token" üretilir. Token, hangi bilgisayarın veri iletebileceğini belirler. Veri iletmek istemeyen bir bilgisayar token'ı aldığı anda herhangi bir işlem yapmadan sıradaki bilgisayara gönderir. Veri iletmek isteyen bir bilgisayar token'ı aldığı anda, token'a bir işaret koyar ve saklar. Daha sonra veriyi halkadaki bir sonraki bilgisayara iletir. Veri ağda ilerlerken token iletilmez. Bu durumda diğer bilgisayarlar veri iletemez. Özetle, bilgisayarın veri iletebilmesi için token'a ihtiyacı vardır. Token'ı olmayan bilgisayar veri iletemez.

Fiber Distributed Data Interface (FDDI)

1980'lerin ortasında yüksek hız ihtiyacı, ethernet ve token-ring teknolojilerinin sınırlarını zorlamaya başladı. Yüksek hız ihtiyacı karşılanırken güvenilir bir ağ teknolojisine de ihtiyaç vardı.

ANSI X3T9.5 standart komitesi, FDDI ağları geliştirdi. FDDI, ethernet kadar yaygın olmasa da gelişmekte olan bir teknolojidir. Genelde omurga olarak kullanılan FDDI, yerel ağlarda da bilgisayarları yüksek hızla bağlamak için kullanılabilir.

Token Passing

FDDI teknolojisi, Token-Ring gibi Token-Passing erişim metodunu kullanır. Ancak FDDI çift ring kullanır. İkinci ring, birincinin bozulması durumunda otomatik olarak devreye girebilecek şekilde yapılandırılabilir. İstenirse yük dağılımı da yapılabilir. Ayrıca FDDI teknolojisinde yüksek hız sağlayabilen fiber kablolar kullanılır.

Wireless LAN (WLAN)

Adından da anlaşılacağı gibi kablosuz ağlarda ağ kablosu kullanılmaz. Veriler elektromanyetik dalgalar aracılığı ile iletilir. Geleneksel LAN teknolojilerinin (Ethernet, Token-Ring) tüm özelliklerini sağlar. Kablolu ağlar kadar hızlı olmasa da sürekli geliştirilen bir teknolojidir. Kurulum kolaylığı, taşınabilirliği ve ölçeklenebilirliği gibi avantajları nedeniyle tercih edilen bir teknolojidir. Kablosuz LAN'ın gelişimi 1980'li yıllarda 900MHz frekans kullanılarak başladı. Çok az ülke 900MHz frekansına izin verdiği için yaygınlaşamadı. Zaman geçtikçe ortaya çıkan yüksek hız ihtiyacı ve dünya geneline yayılabilmesi için 2.4Ghz frekans kullanılmaya başlandı. IEEE, 1992 yılında 802.11 araştırma grubu ile standartlaştırma çalışmalarına başladı. 1997 yılında, IEEE kurumu tarafından IEEE 802.11 adıyla onaylandı. İlk versiyonları ancak 1-2Mbps hızına ulaşabiliyordu. 1999 yılında daha yüksek hız sağlayan 802.11a ve 802.11b standartları geliştirildi.

Bunları 802.11g takip etti ve sağladığı yüksek hız ile giderek yaygınlaştı. Önümüzdeki yıllarda piyasaya sürülmek üzere hem kapsama alanı daha geniş hemde hızı daha yüksek olan standartlar üzerinde çalışmalar devam ediyor.

WLAN Bileşenleri

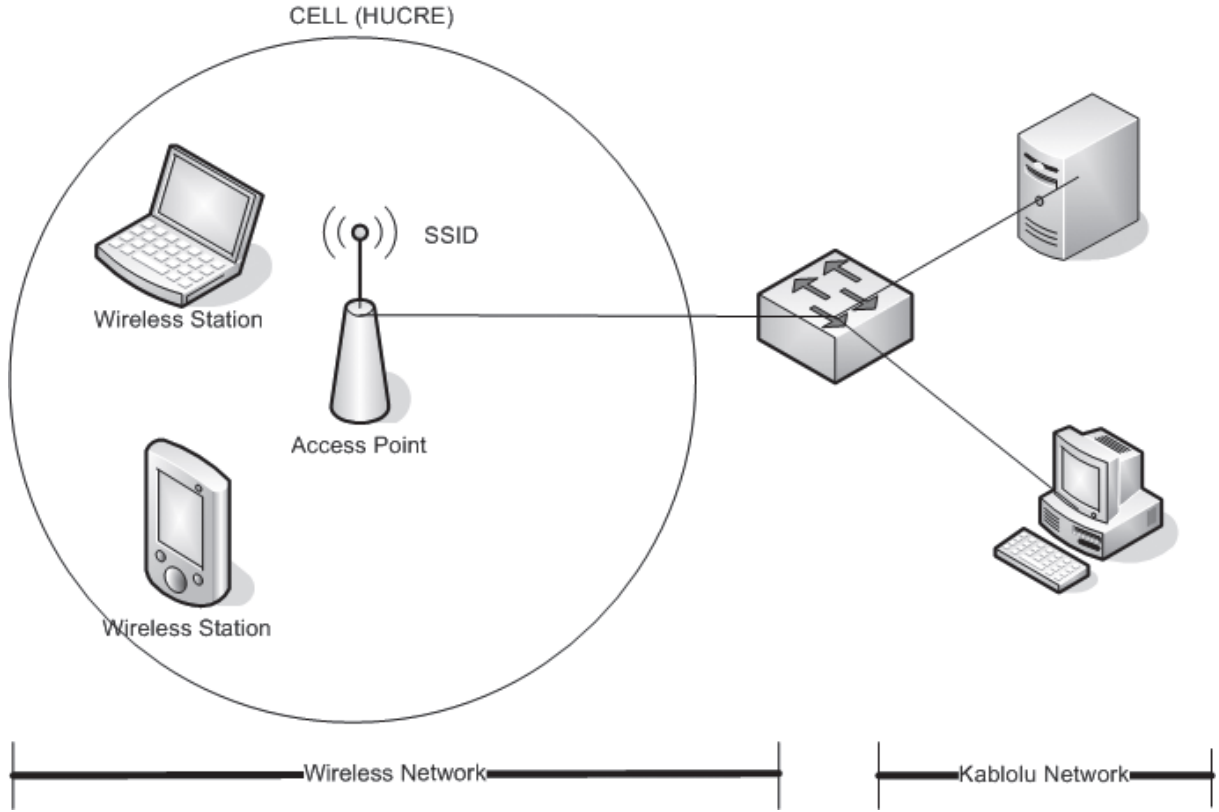
Bir WLAN'de kullanılan bileşenler:

Kablosuz LAN İstasyonu (Wireless LAN Station): IEEE 802.11 standartını kullanabilen ve kablosuz ağlara erişebilecek gerekli donanıma sahip cihazlardır. Örneğin, dizüstü bilgisayarlar gibi.

Erişim Noktası (Access Point - AP): Kablosuz LAN istasyonlarının birbirleri ile bağlantısını sağlar. Ayrıca kablosuz ağ yapısı ile kablolu ağ yapısını sağlar. Her AP'nin, cell denilen belirli bir kapsama alanı vardır. Kapsama alanı dışındaki bilgisayarlar ile iletişim kuramaz.

Kablosuz Yönlendirici (Wireless Router): Temel yönlendirme işlemlerini yapabilen AP'dir.

Service Set Identifiers (SSID): AP'nin oluşturduğu cell'in adıdır. WLAN'ları mantıksal olarak ayırmak için kullanılır. Bilgisayarların bağlanmak istedikleri WLAN'ın SSID'sini bilmeleri gerekir.



WLAN'ler, birçok yönü ile ethernet LAN'lerine benzer. WLAN'ler paylaşılan ağlardır. Aynı anda sadece bir WLAN istasyonu veri iletebilir. Veri iletmek isteyen bilgisayar mevcut veri iletiminin bitmesini beklemek zorundadır. AP'ler ethernet hub'ları gibi çalışırlar. Bu yapısı ile WLAN, coaxiel kablo kullanılan ya da hub kullanılan, half-duplex ethernet LAN'leri ile benzerlik gösterir. WLAN bilgisayarları da MAC adresi kullanır. Kullanıcı açısından ethernet'ten farkı yoktur. Aynı iletişim protokolleri ve servisler kullanılabilir.

Ethernet'ten farklı olarak, collision olmasını engelleyici teknikler içeren Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) erişim metodunu kullanır. Aynı AP'ye bağlı bilgisayarlar arasında collision olma olasılığı yoktur.

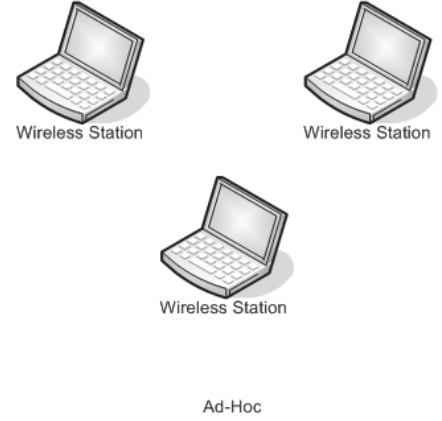
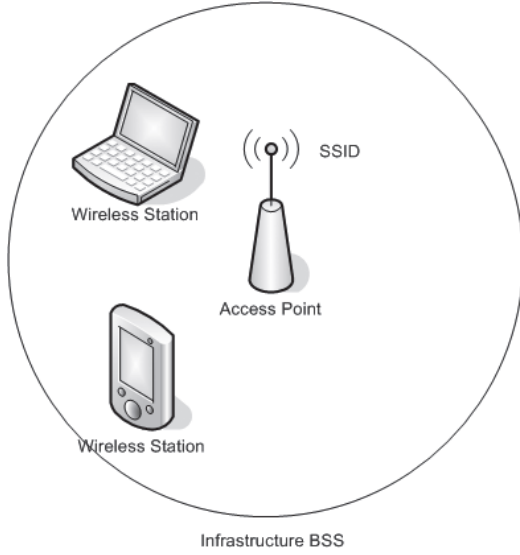
WLAN Topolojileri

Independent Basic Service Set (IBSS): Ad-hoc da denilen bu yapıda bilgisayarlar birbirlerine AP olmadan bağlanırlar.

Infrastructure Basic Service Set: Bu yapıda bilgisayarlar birbirlerine AP aracılığı ile bağlanırlar. İki farklı modu vardır.

Basic Service Set: Bilgisayarlar tek bir AP kullanırlar.

Extended Service Set: BSS'in birçok AP kullanılarak genişletilmiş halidir. Bilgisayarlar hareket ettikçe otomatik olarak bir AP'den diğerine geçebilir. Tüm yapıda ortak SSID kullanılır.



WLAN Teknolojileri

WLAN'ler gün geçtikçe artan mesafe ve hız gereksinimlerini karşılayabilmek için geliştirildiler.

WLAN teknolojileri IEEE tarafından geliştirilir. Geliştirilen WLAN teknolojileri ve cihazları, Wi-Fi Alliance tarafından onaylanır ve kullanıma sunulur. Günümüzde kullanılabilecek 4 farklı WLAN teknolojisi vardır.

IEEE 802.11a:

- 1999 yılında üretilmiştir.
- 5Ghz frekans kullanır.
- 54Mbps hıza ulaşabilir.

IEEE 802.11b:

- 1999 yılında üretilmiştir.
- 2.4Ghz frekans kullanır.
- 11Mbps hıza ulaşabilir.

IEEE 802.11g:

- 2003 yılında üretilmiştir.
- 2.4Ghz frekan kullanır.
- 54Mbps hızına ulaşabilir.

IEEE 802.11n:

- 2009 yılında piyasaya çıkması beklenmektedir.
- 2.4 ve 5Ghz frekansları kullanabilir.
- 248Mbps hızına ulaşabilir.

IEEE 802.11y:

- 2008 yılında piyasaya çıkması beklenmektedir.
- 3.7Ghz frekans kullanır.
- 54Mbps hızına ulaşabilir.

Tablo 2.4

	802.11a	802.11b	802.11g	802.11n	802.11y
Hız	54Mbit/s	11Mbit/s	54Mbit/s	248Mbit/s	54Mbit/s
Frekans	5GHz	2,4GHz	2,4GHz	2,4GHz - 5GHz	3,7GHz
Mesafe	35m - 120m	38m - 140m	38m - 140m	70m - 250m	50m - 5000m

WLAN teknolojilerinde aynı frekansı kullananlar birbirleri ile uyumludur. Bir 802.11g cihaz, 802.11b AP'ye bağlanabilir.

Her teknolojiye kullanılan frekans aralığı vardır. Birbirlerine yakın olan AP'lerin, sinyallerinin bozulmaması için farklı frekans kullanıyor olmaları gerekir.

WLAN'larda, AP ile bilgisayar arasındaki mesafe arttıkça veri iletim hızı düşer. WLAN AP'lerin antenlerine verilen güç arttırılırsa kapsama alanı genişletilebilir.

Diğer WLAN Standartları

IEEE 802.11e: QoS desteği sağlar.

IEEE 802.11f: AP'ler arası bağlantıyı tanımlar.

IEEE 802.11h: 5Ghz frekansta otomatik kanal ve mesafe değişimini tanımlar.

IEEE 802.11i: WLAN güvenliğini tanımlar.

IEEE 802.1x: Kablolu ağlarda da kullanılabilen, ileri seviye güvenlik tekniklerini tanımlar.

WLAN Güvenliği

WLAN'lar, yapıları gereği ortama elektromanyetik ışınım yaptıkları için güvenli değildir. Güvenliğin sağlanabilmesi için her WLAN'ın özelliği olan şifreleme ve kimlik doğrulama teknikleri kullanılabilir.

Service Set Identifier (SSID): Her AP kendisini tanımlamak için bir SSID kullanır. SSID kablosuz ağın adı olarak düşünülebilir. Her istasyon bağlanacağı AP'nin SSID'sini bilmelidir. SSID istasyonların yanlış AP'ye bağlanmalarını önlemek için kullanılır. Aslında bir güvenlik önlemi değildir.

MAC Filtresi: Her AP kendisine bağlanmak isteyen istasyonların MAC adresini kontrol edebilir.

Bu teknik, bağlanma yetkisi olan istasyonların MAC adreslerinin AP'ye girilmesini gerektirir. Yeterli seviyede güvenlik sağlamaz.

Wired Equivalent Privacy (WEP): Şifreleme ve kimlik doğrulama için kullanılan, sabit ve paylaşılan anahtardır. WEP anahtarı hem bilgisayara hem de AP'ye önceden girilmek zorundadır. Yeterli seviyede güvenlik sağlamaz.

WiFi Protected Access (WPA) ve WPA2: WEP'e göre daha güçlüdür. Şifreleme ve anahtar değişimi için TKIP kullanır. Kimlik doğrulama için ya PreShared Key (PSK) ya da IEEE 802.1x kullanır. PSK, hem kullanıcı bilgisayarına hem de AP'ye girilen sabit bir değerdir. WPA2, temel olarak WPA gibi çalışır ancak şifreleme için AES algoritmasını kullanır.

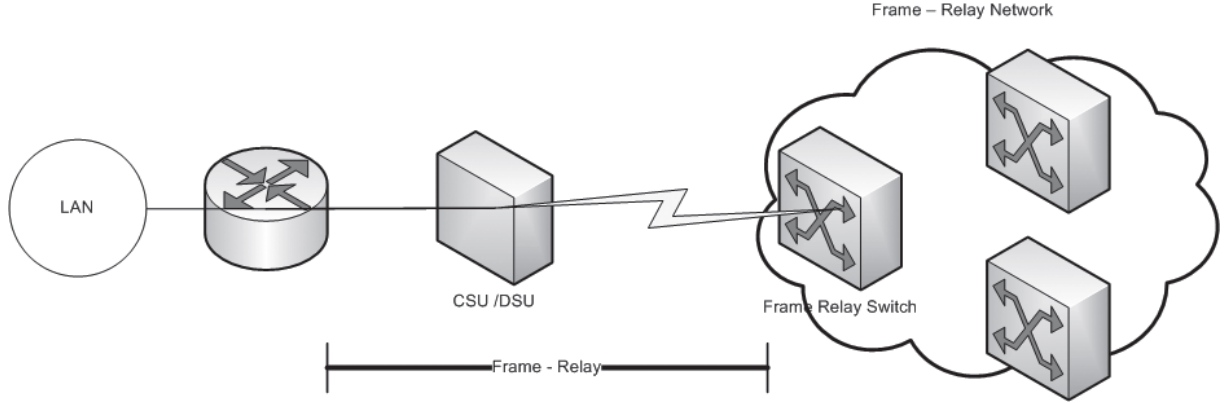
WAN Teknolojileri

WAN'lar, birbirinden uzak noktalardaki LAN'ları heberleştirmek için kullanılırlar. WAN hizmeti, Telekom gibi bir servis sağlayıcısından kiralanır.

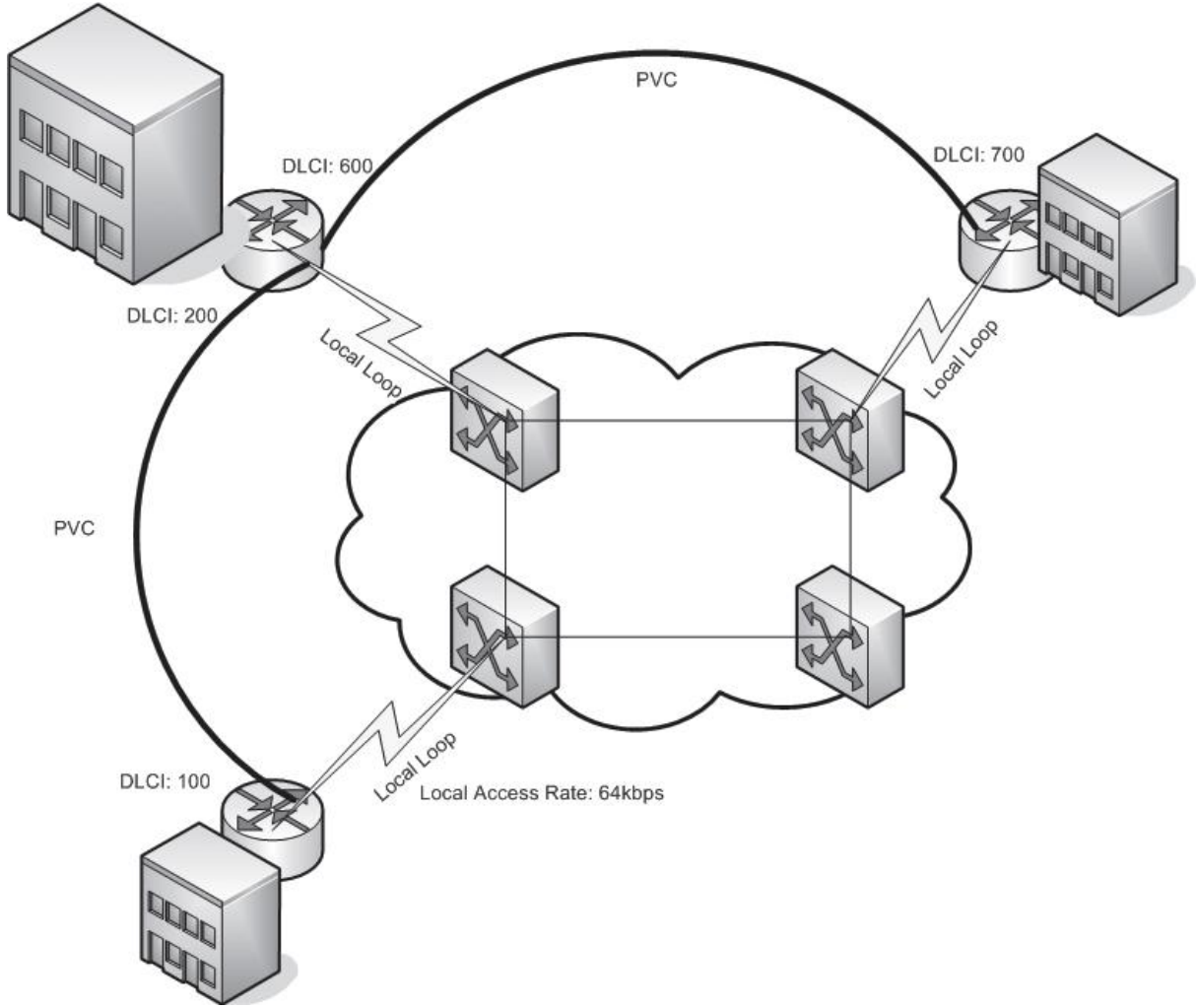
Frame-Relay

Frame-Relay, packet-switching (paket-anahtarlama) metodunu kullanan, yüksek hız sağlayan popüler bir WAN teknolojisidir. OSI'nin 1. ve 2. katmanlarında tanımlanır.

Frame-Relay, router ve servis sağlayıcının yerel switching cihazı arasındaki bağlantıyı tanımlar.



Frame-Relay Terminolojisi



Local Access Rate: Bağlantının port hızıdır.

Virtual Circuit (VC): İki DTE cihaz arasındaki bağlantı kanalını tanımlayan sanal devredir. İki DLCI numarasının eşleşmesi ile oluşur. İki şekli vardır.

Permanent VC (PVC): DTE'ler arasındaki bağlantı kanalı önceden oluşturulmuş ve sabittir. İletişim olmasa da mevcuttur. Genelde PVC kullanılır.

Switched VC (SVC): DTE'ler arasındaki bağlantı kanalı, iletişim gerektiğinde dinamik olarak kurulur ve iletişim bittiğinde kapatılır. Pek yaygın değildir.

Data Link Channel Identifier (DLCI): VC'nin oluşmasını sağlayan ve VC'ler arası ayrımı yapan 10Bit'lik adrestir. İki DTE cihaz arasındaki VC'yi tanımlar.

Committed Information Rate (CIR): Verilerin yollanabileceği maksimum hızdır. CIR değeri, servis sağlayıcı ile kullanıcı arasında belirlenir.

Local Management Interface (LMI): DTE cihaz ile Frame-Relay switch arasındaki sinyalizasyon standartıdır. Her ülkede farklı bir standart kullanılabilir. Türkiye'de ANSI standardı kullanılır.

Frame-Relay ağlarda, her DTE cihaza bir DLCI numarası verilir. Servis sağlayıcı birbirine bağlanması gereken DTE cihazlara verdiği DLCI numaralarını eşleştirerek VC oluşturur. VC oluştuktan sonra bir DLCI'dan çıkan verinin gideceği DLCI, VC'nin diğer ucundakidir.

Digital Subscriber Line (xDSL)

DSL teknolojileri yüksek hızlı ve güvenilir veri hatlarıdır. Farklı mesafe ve hızlarda birçok DSL tipimevcuttur. xDSL tabirindeki "x" değişik DSL tiplerini ifade eder.

Mevcut telefon hatları üzerinde servis sağlayıcı tarafından yapılan küçük değişiklikler sonucu eldeedilebilir. Servis sağlayıcıdan kullanıcıya yeni bir hat çekmek gerekmez. Analog telefon hattı içinkullanılan mevcut Local Loop üzerinden DSL kullanılabilir. DSL'de veri trafiği upstream ve downstream olmak üzere ikiye ayrılır.

Upstream: Kullanıcıdan servis sağlayıcısına yapılan veri akışıdır.

Downstream: Servis sağlayıcıdan kullanıcıya yapılan veri akışıdır.

DSL tipleri downstream ve upstream hızlarına göre iki ana gruba ayrılır.

Simetrik: Upstream ve downstream hızları aynıdır.

Asimetrik: Upstream ve downstream hızları farklıdır. *Downstream hızı her zaman daha yüksektir.*

DSL Tipleri

DSL tipleri hızları, mesafeleri, çalışma şekilleri ve ses iletimi destekleri açısından farklılık gösterir.

Asymmetric DSL: Mevcut analog telefon hatları üzerinden çalışabilir. Asimetrik yapısı dolayısı ile daha çok downstream hızının önemli olduğu iletişim tiplerinde kullanılır. Günümüzde internet bağlantısı için yaygın olarak kullanılmaktadır. Hızı arttırılarak, ADSL2 ve ADSL2+ teknolojileri geliştirilmiştir.

Very-High-Data-Rate DSL (VDSL): Simetrik ya da asimetrik çalışabilir. Aynı anda ses ve veri iletimi sağlayabilir.

ISDN DSL (IDSL): Mevcut ISDN hatları üzerinden veriyi dijital olarak yollar. Ses iletimini desteklemez, sadece veri taşıyabilir.

Symmetric DSL (SDSL): Simetrik yapıya sahiptir ve sadece veri iletiminde kullanılabilir. Standart bir teknoloji değildir.

G.SHDSL: Simetrik bir yapıya sahiptir. Standart bir teknolojidir ve günümüz WAN'lerinde yaygın olarak kullanılmaya başlanmıştır.

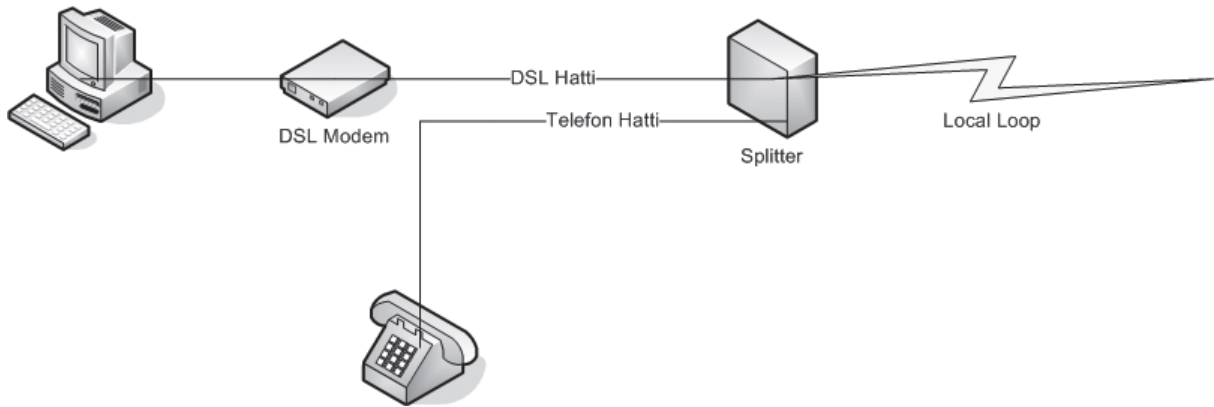
Tüm DSL tiplerinde maksimum hız Local Loop mesafesine bağlıdır. Tablodaki değerler minimum mesafedeki hızlardır. Mesafe arttıkça hız düşer.

ADSL

ADSL, asimetrik yapısı ve ücreti dolayısı ile günümüzde internet bağlantısı için en uygun teknolojidir. Analog telefon hatları için çekilen Local Loop üzerinden çalışabilir. Hat üzerinde

3 kanal oluşturulur. Bir kanal analog ses iletimi için kullanılır, diğer ikisi upstream ve downstream için kullanılır.

ADSL, teknolojisi aynı anda analog ses ve veri iletimini destekler.

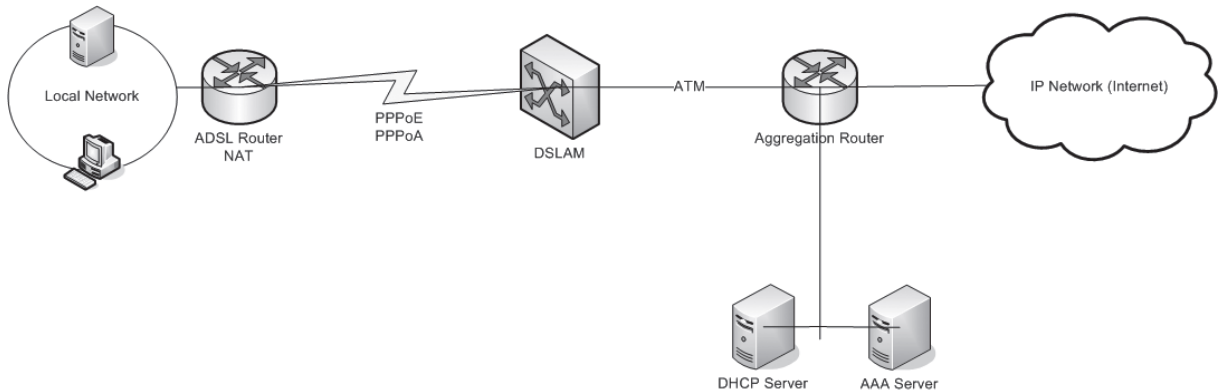


2004 yılında ADSL2 ve ADSL2+ olmak üzere daha yüksek hız sağlayan iki standart geliştirilmiştir.

ADSL Yapısı

ADSL bağlantısında Local Loop, CPE cihazı (Genellikle ADSL Modem) ile servis sağlayıcı cihazı (DSLAM) arasındadır. DSLAM'ın arkasındaki ATM ağ üzerinden, kimlik doğrulaması yapan Aggregation Router'a bağlanılır. ADSL modem ve Aggregation Router arasında oturum başlatılır.

Kimlik doğrulandıktan ve oturum başlatıldıktan sonra internet bağlantısı sağlanır. PVC, ADSL modem ve Aggregation Router arasında oluşturulur. ADSL modem doğru PVC tanımlayıcıları ile yapılandırılmalıdır. Türkiye'de 8/35 kullanılmaktadır.



DSLAM: Üzerinde ADSL modemler bulunan ATM switch'tir. Servis sağlayıcı tarafındadır. ADSL hattın sonlandırıldığı yerdir.

CPE: Kullanıcıya ait donanımdır. Genellikle ADSL Modemdir.

Aggregation Router: CPE'nin internet erişimini sağlayan router cihazıdır. PVC, CPE ile Aggregation Router arasında oluşturulur.

AAA Server: Kullanıcı bilgilerini doğrulayan, bağlantıyı kabul eden ve otomatik IP atayan router cihazıdır.

DHCP Server: Otomatik IP atayan sunucudur. ADSL modem ile DSLAM arasında, servis sağlayıcısının isteğine göre, PPPoE ya da PPPoA encapsulation metodu kullanılabilir. Kullanıcı ADSL modemini uygun encapsulation metoduna göre yapılandırmalıdır.

ATM

ATM, veriyi 53Byte'lık sabit büyüklükteki "Cell" denilen paketlere bölerek hızlı ve güvenilir bir şekilde hedefine ulaştıran bir ağ teknolojisidir. Hem LAN hem de WAN'lerde kullanılabilir. ATM üzerinden ses, görüntü ve veri hızlı bir şekilde iletilebilir. ATM veri iletimini noktadan noktaya yapar.