AĞ TEMELLERİ

HABERLEŞME HAKKINDA GENEL BİLGİLER

VERİ AĞLARI

- Birden çok bilgisayarın birbirine bağlı olduğu donanım ve yazılımların da paylaşılmasına izin veren bilgisayar ağları, veri haberleşmesini veri ağları üzerinden yapmaktadır.

- Bilgi iletimine en güzel örnek evlerimizde kullandığımız telefonlardır. Telefonlarda ses bilgisi kablolar ile santrale gönderilir, santrallerden diğer santrallere ve oradan da hedef telefona çağrı iletilir. Her telefonun kendisine ulaşmakta kullanılan bir numarası bulunmaktadır. Bu sistem incelendiğinde bir ağın nasıl çalıştığı daha kolay anlaşılabilir.

- Sistem bilgisayara uyarlandığında her bilgisayarın bir numarasının bulunduğu, çeşitli kablolama teknolojileri ve ağ elemanlarıyla bilginin hedefe ulaştırıldığı görülecektir.

    - Bilgisayar ağları da bir veri ağıdır. Ağ sistemi ise iki kişisel bilgisayardan oluşabileceği gibi binlerce iş istasyonundan da oluşabilir.

VERİ HABERLEŞMESİ

- Bilgisayar ortamında veri haberleşmesi, sayısal kodlama ile yapılır. Aktarılan veri, 0 ve 1 biçiminde sayısal olarak kodlanarak aktarılır. Böylece, bilgisayar terminolojisinde ***veri haberleşmesi***, sayısal olarak kodlanmış bir bilginin bilgisayarlar arasında değiş tokuşu olarak açıklanabilir.

- Verilerin, bilgisayar ağları üzerinden aktarılabilmesi için bir dizi işlem görmesi ve denetimlerden geçmesi gerekir. Yerine getirilmesi gereken bu işlemler, farklı düzeylerde gerçekleşir ve oldukça karmaşık uygulamalar gerektirebilir. Bu işlemler ve denetimler bütünü, ***veri iletişim sistemini*** oluşturur.

HABERLEŞME HAKKINDA GENEL BİLGİLER

- İletişim terimi bilgiyi elektriksel yollarla göndermeye, almaya, işlemeye karşılık gelir. İletişimin amacı, herhangi bir biçimdeki bilginin zaman ve uzay içinde kaynak olarak adlandırılan bir noktadan, kullanıcı denilen başka bir noktaya aktarılmasıdır.
- İletişim 1840' larda telgraf ile başladı; birkaç "10 yıl" sonra telefonla ve bu yüzyılın başında da radyo ile gelişti.

HABERLEŞME HAKKINDA GENEL BİLGİLER

- Modern bir iletişim sistemi, bilgi göndermeden önce onun sıraya koyulmasıyla, işlenmesiyle ve korunmasıyla ilgilenir. Gerçek anlamda gönderme daha fazla işleme ve gürültünün süzülmesiyle gerçekleşir. Son olarak , kod çözme, mesajı koruma ve bilgi algılama basamaklarından oluşan alma işlemi

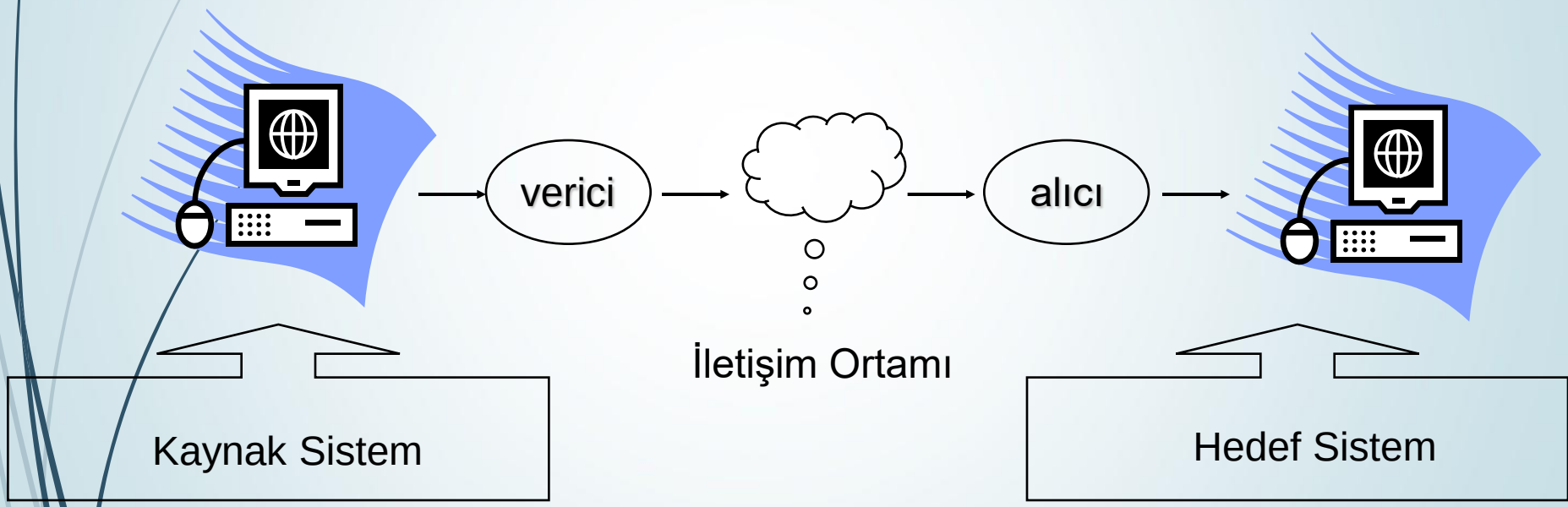
HABERLEŞME HAKKINDA GENEL BİLGİLER

Bir noktadan diğer bir noktaya dijital veya binary bilgilerin iletilmesi işlemine 'veri iletimi' denir. Veri iletim sistemleri, bilgisayar-bilgisayar ve bilgisayar-terminal arasında veri iletimini sağlar. Dijital veya binary hale dönüştürülebilen ses, görüntü gibi analog bilgilerin iletilmesi de veri iletimi ile gerçekleştirilir. Dijital tekniklerin verimliliği yüksek, maliyetleri oldukça düşüktür. Bu nedenle, dijital veri iletim sistemleri oldukça kullanışlıdır.

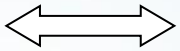
HABERLEŞME HAKKINDA GENEL BİLGİLER

Dijital sinyaller, herbiri bir voltaj seviyesiyle tanımlanan ve birbirinden farklı iki durumdan oluşan binary pals'lerdir. Bu palsler iki seviye arasında değişir. Bu seviyelerden birisi "binary 0" veya "low", diğeri ise "binary 1" veya "high" olarak tanımlanır. Binary bilgilerin bir yerden başka bir yere transferinde iki temel yöntem kullanılır. Bunlar seri ve paralel iletimdir.

VERİ HABERLEŞMESİ



HABERLEŞME HAKKINDA GENEL BİLGİLER



Veri iletişim Ortamı:Bilgisayar ağlarında sinyallerin bir bilgisayardan çıkıp diğerine giderken takip etmek zorunda olduğu yoldur.

Veriler ağ cihazları arasında iki veri iletim yolunu kullanarak hareket eder.

HABERLEŞME HAKKINDA GENEL BİLGİLER

Kılavuzlu iletim: Bilgisayarlar doğrudan kablolarla birbirlerine bağlanırlar. Kullanılan kablolar genellikle iletken tellerdir. Birbirlerine sarılmış çiftli kablolar(twisted pair), koaksiyel kablolar, fiber optik kablolar en çok bilinen kablo çeşitleridir.

Kablosuz İletim Araçları : Bu iletim şeklinde en çok kullanılan araç mikrodalgalardır. Haberleşme iki nokta arasında yüksek frekanslı radyo sinyallerinin iletimi ile sağlanır. Çok uzak noktalar arasında iletim sağlamak için uydular kullanılır.

HABERLEŞME HAKKINDA GENEL BİLGİLER

- **Bant Genişliği** : İletimde olan iki cihaz arasında tek yönde gönderilebilecek en büyük veri miktarıdır. Yan bir veri iletim iletim ortamının birim zamanda taşıyabileceği maksimum veri miktarı (saniyedeki bit sayısı, bps) olarak tanımlanmaktadır.
- b**ps:** Bit per second olarak açılır. Saniyede gönderilen bit sayısıdır.
- **Mbps:** Saniyede 1 milyon bit (Millions of bits per second)

SERİ İLETİM

- Seri iletim bilginin tek bir iletim yolu üzerinden n bit sıra ile aktarılmasıdır. LSB (least significant bit) , en son gönderilen MSB (most significant bit)'dir.
- Bilgisayar ağları üzerindeki iletişim seri iletişimdir.
- Verici ve alıcı senkron olarak çalışabildikleri gibi asenkron olarak ta çalışabilirler. Seri veri iletiminde verinin başlangıç noktasını belirtmek için "start" biti, veri aktarma işlemi sırasında oluşabilecek bozulmaları ortaya çıkarabilmek için veri bitlerinin hemen ardından "parity" biti ve verinin bitiş noktasını belirtmek için "stop" biti kullanılır.

ASENKRON VERİ İLETİMİ

- Klavye, fare ve modem gibi çoğu PC cihazları asenkron (eşzamansız) seri veri iletimi metoduyla veri iletimi yaparlar. Gönderilen sekiz bitlik veri başında start ve stop bitleri bulunduğundan senkron veri iletişimine göre yavaş olmasına rağmen daha az kablo kullanılması en büyük avantajıdır.
- Asenkron iletişimin temel özellikleri şunlardır:
  -Transfer edilecek veriler karakter bazında yazılır
  -Gönderilecek her bir karakter verisinin başlangıcını ve bitişini belirten start ve stop bitleride gönderilir.
  -Karşılıklı olarak haberleşecek cihazların iletişim parametreleri aynı olmalıdır(Hız, Kodlama Seti vb…)
  Asenkron veri iletişiminde alıcı ve vericinin karşılıklı dikkat edileceği en önemli protokolden birisi hızdır. Göndericinin saat frekansı ile alıcının saat frekansı arasındaki farklılık verilerin doğru alınamamasına neden olur.

SENKRON VERİ İLETİMİ

- Senkron veri iletişiminde veri ile birlikte saat palside gönderilir. Bu durum start ve stop bitlerinin gerekliliğini ortadan kaldırır. Aynı zamanda senkron iletişim karakter blokları bazında olduğu için asenkron iletişime göre daha hızlıdır. Ancak daha karmaşık devreler içerdiğinden pahalıdır. Senkron deyimi, alıcı ve vericinin eşzamanlı çalışması anlamına gelir. Saat palsi ihtiyacıda bu durumdan ileri gelir.

SENKRON VERİ İLETİMİ

- Veri iletimine başlamak için önce gönderici taraf belirli bir karakter gönderir. Bu her iki tarafça bilinen iletişime başlama karakteridir. Alıcı taraf bildiği bu karakteri okursa iletişim kurulur. Verici bilgileri gönderir. Transfer işlemi veri bloğu tamamlana yada alıcı verici senkronizasyon kaybolana kadar devam eder.

SENKRON VERİ İLETİMİ

Senkron iletişimin temel özellikleri şunlardır:
-Hata saptama ve koruması yapılır.
-Hız genellikle gönderici tarafından sağlanır.
-Senkron cihazlar asenkron cihazlara göre daha hızlı ve daha pahalıdır.
-Veriler bloklar halinde gönderilir.
-Blok formatları kullanılan protokole göre değişir.

PARALEL İLETİM

Digital olarak kodlanmış bilginin tüm bitleri aynı anda transfer ediliyorsa buna “paralel veri iletimi “ denir. Paralel veri iletiminde iletilecek bilginin her biti için ayrı bir kablo bağlantısı sağlanır.

Paralel veri iletiminde, bir karakterin tüm bitleri aynı anda iletildiği için start -stop bitlerine ihtiyaç yoktur. Dolayısı ile doğruluğu daha yüksektir.

Paralel iletimde aktarılacak veri her Bit ayrı bir iletim yolundan aktarılır. Paralel İletim çoğunlukla aynı kart içerisinde kalan Aktarımlarda veya birbirlerine çok yakın cihazlar arasındaki aktarımlarda kullanılır.(Bilgisayar ile yazıcı arasındaki iletim)

SERİ VS PARALEL İLETİM

- Seri veri iletiminde, bir kerede bir karakterin sadece bir biti iletilir. Alıcı makine, doğru haberleşme için karakter uzunluğunu, start-stop bitlerini ve iletim hızını bilmek zorundadır.
- Paralel veri iletiminde, bir karakterin tüm bitleri aynı anda iletildiği için start-stop bitlerine ihtiyaç yoktur. Dolayısıyla doğruluğu daha yüksektir.
- Paralel veri iletimi, bilginin tüm bitlerinin aynı anda iletimi sebebiyle çok hızlıdır. ASCII kodundaki her bir bitin transferinin 1 mikrosaniyede gerçekleştiğini varsayarsak, seri iletimde 8 bitlik ASCII kodunun iletimi 80, paralel iletimde ise 8 mikrosaniyede gerçekleşir.
- Paralel iletimde çok kablolu hatlar kullanılır. Veri iletiminde kullanılan portlardaki kabloların pahalı olmasından dolayı da paralel veri iletimi kısa mesafelerde tercih edilir. Seri iletişim bağlantılarında ise genellikle ikili hatlar kullanılır. Bu nedenle uzun mesafelerde seri veri iletimi tercih edilir.

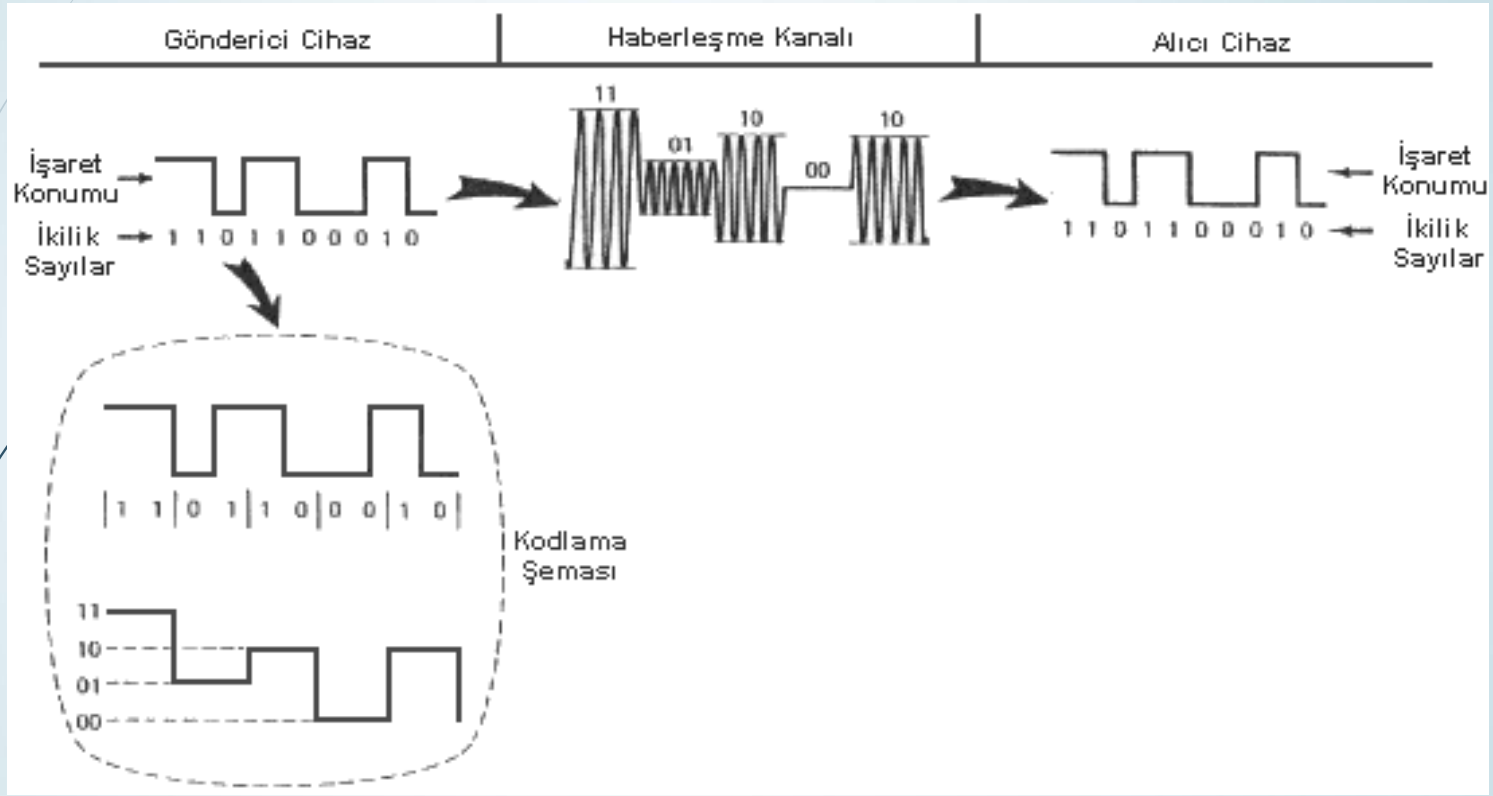
MODÜLASYON

- Sayısal bilgi sinyallerinin, analog taşıyıcı sinyaller üzerine bindirilip uzak mesafelere gönderilmesi işlemine MODULASYON denir. Sayısal bilgi sinyalleri tek başına uzak mesafelere gidemezler. analog sinyaller ise az bir güçle uzak mesafelere gidebilirler. Bu nedenle, taşıyıcı sinyaller hamal olarak kullanılırlar ve sayısal bilgi sinyalleri vericide modülasyon işlemine tabi tutularak, taşıyıcı üzerine bindirilir.

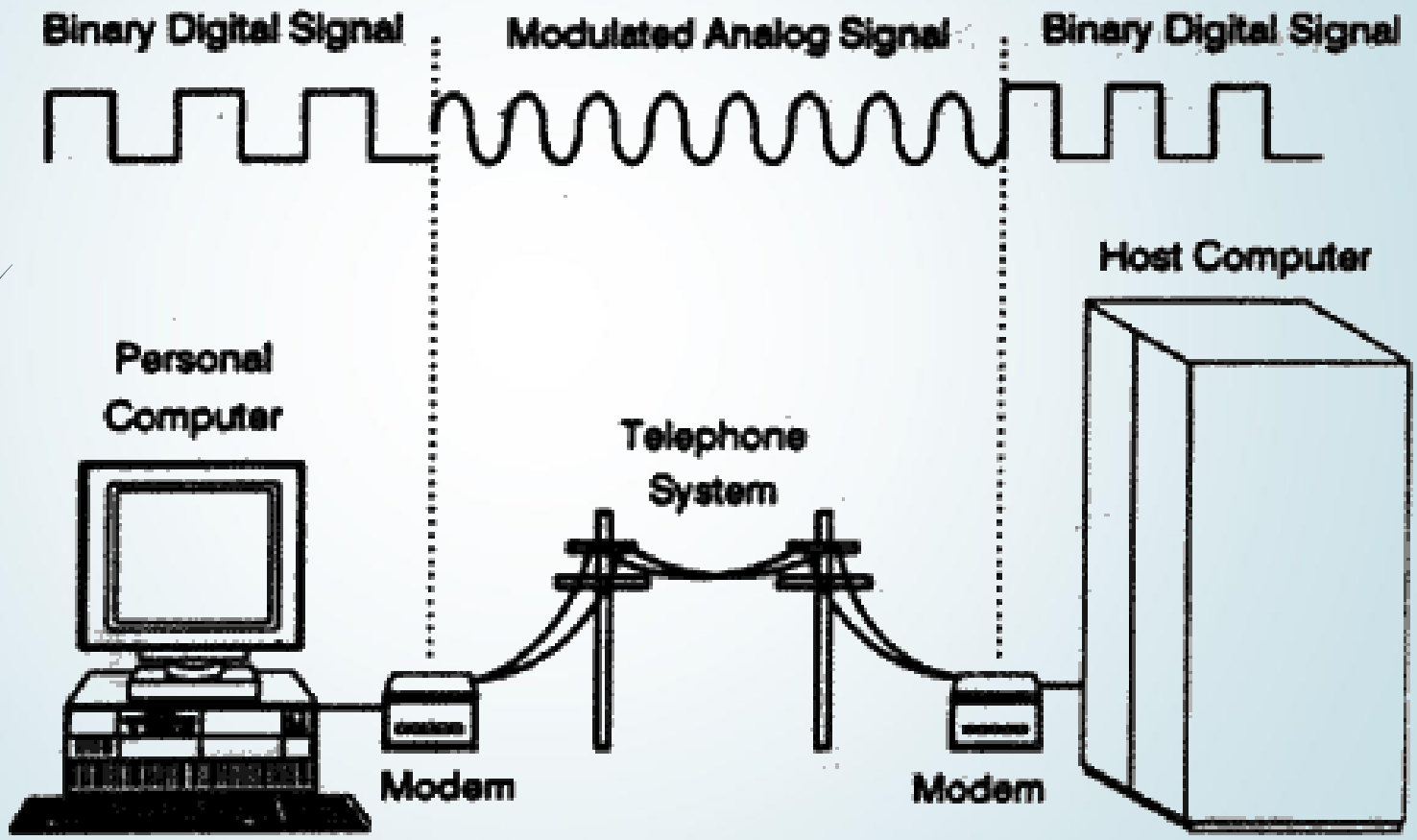
MODÜLASYON

- Genlik Modülasyonu: İşlem, taşıyıcı dalganın genliği değiştirilerek yapılır. Genlik modülasyonunda taşıyıcı dalganın genliği ses dalgasına uygun olarak değiştirilir.
- Frekans Modülasyonu: İşlem frekansı değiştirilerek yapılır. Frekans modülasyonunda ise taşıyıcı dalganın frekansı ses dalgasına uygun olarak değiştirilir.
- Modülasyon vericide gerçekleştirilir.
- Bu işlem modülatör denilen elektronik cihazlar tarafından gerçekleştirilir.
- Demodülasyon alıcıda gerçekleştirilir.
- İkisini birden yapan cihazlar MoDem olarak adlandırılır.

MODÜLASYON


Gönderici Cihaz
Haberleşme Kanalı
Alıcı Cihaz
İşaret Konumu
İkilik Sayılar
1 1 0 1 1 0 0 0 1 0
11
01
10
00
10
İşaret Konumu
İkilik Sayılar
1 1 0 1 1 0 0 0 1 0
1 1 0 1 1 0 0 0 1 0
Kodlama Şeması
11
10
01
00

MODÜLASYON


Binary Digital Signal
Modulated Analog Signal
Binary Digital Signal
Host Computer
Personal Computer
Telephone System
Modem
Modem

AĞ TEMELLERİ

BİLGİSAYAR AĞLARI NEDİR?

AĞLARIN KISA TARİHÇESİ

- 1969 yılında, ABD'de, savunma gayesiyle kurulan bir merkez, ARPANET adıyla bir bilgisayar ağını hazırladı. Bu hususta araştırma yapan strateji uzmanları, bu ağ yardımıyla görüşüp fikir alışverişi yapıyorlardı.

- 1972'de bu ağ, bir konferans aracılığıyla kamuoyuna tanıtıldı.

- 1980 tarihine kadar birçok hususi ağ ortaya çıkmıştı. Bu tarihte farklı ağların birbirleriyle irtibat kurmasına izin veren protokol imzalandı. ABD'de faaliyetler sürerken, Avrupa ve Uzak Doğu'da da, özellikle üniversiteler, araştırma merkezleri stratejik resmi kurumlar arasında bilgisayar ağları teşekkül etmeye başlamıştı.

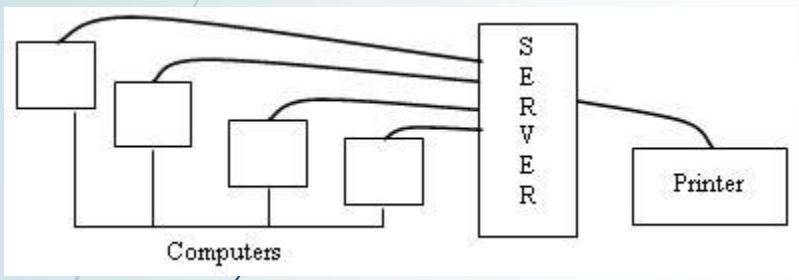
- 1983'de ARPANET, askeri ve sivil iki ağa ayrıldığında ortaya çıkan ferdi ağların bütününü ifade etmek için "**Internet"** ismi teklif edildi.

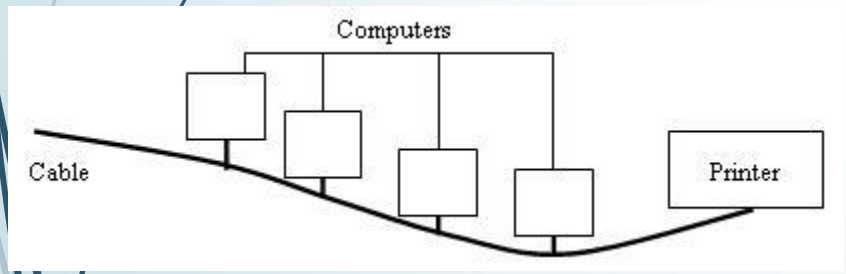
BİLGİSAYAR AĞLARI NEDİR?

Bilgisayar sistemlerinin birbirine bağlanarak herhangi bir donanım kaynağının ya da bilginin paylaşıldığı(verilerin iletildiği) yapılara bilgisayar ağları denmektedir.

Bu bağlantı sadece bakır teller aracılığıyla olmaz: fiber optik kablolar, kızıl ötesi dalgalar, iletişim uyduları, 3G, 4G vs. de kullanılabilir.

BİLGİSAYAR AĞLARI NEDEN VAR?





Veri Paylaşımı?

Bilgisayar Kaynaklarının Paylaşımı?

Haberleşme?

Merkezi Yönetim?

Ortak Çalışma Grupları?

Yüksek İşlem Hızının Sağlanması?

BİLGİSAYAR AĞLARI NEDEN VAR?

Kaynak Paylaşımı

· Ağlar, cihazların yani kaynakların (yazıcı, disk, cd sürücü vs.) paylaşımını olanaklı kılar. Bu sayede kaynak israfını engeller.

Yazılım ve donanım maliyetlerini düşürür.

· Ürün geliştirme maliyetini azaltır

İletişim

Çalışanların kendi aralarında ve dünya ile bir iletişim ortamı kurar bu sayede haberleşmeyi etkinleştirir.

BİLGİSAYAR AĞLARI NEDEN VAR?

Uygulama Paylaşımı

- Uygulamaların yazılımların ve dolayısıyla bilginin paylaşımını olanaklı kılar
- Paylaşılacak programlar server(sunucu) üzerinde olan bir ağ diski üzerinde kurulabilir.
- İlgili dosya paylaşılabilir, okunabilir veya çalıştırılabilir ama silinemez olarak belirlenir ve kullanıma açılır.
- Kullanıcılar sisteme bağlanır(login) ve sonrasında diske erişir, uygulamaları çalıştırabilirler.
- Bu şekilde programların kurulma ve bakim işlemleri kolaylaşır.
- Ağ lisansı ile yazılım maliyeti düşer.

BİLGİSAYAR AĞLARI NEDEN VAR?

Doküman Paylaşımı

- İlgili dosyalar farklı kullanıcılar tarafından tek bir noktadan paylaşılabilir, okunabilir veya çalıştırılabilir
- Ayni dosyaya veya dosyaların farklı bölgelerine farklı kullanıcılar tarafından değişik haklarla iletişim sağlanabilir.
- Bunun için karmaşık - gelişmiş yazılımlar kullanılmalıdır.
- Paylaşılan dokümandaki değişiklik bütün kullanıcılara yansır.

BİLGİSAYAR AĞLARI NEDEN VAR?

· ***Bilgi:***

- Gazetelerden tartışma gruplarına, e-posta'dan elektronik ticarete, video konferans, WWW, ftp (dosya transferi), eğlence gibi birçok ortama internet aracılığıyla ulaşılabilmesi ve bilginin toplanabilmesini sağlar.

Yüksek Güvenilirlik:

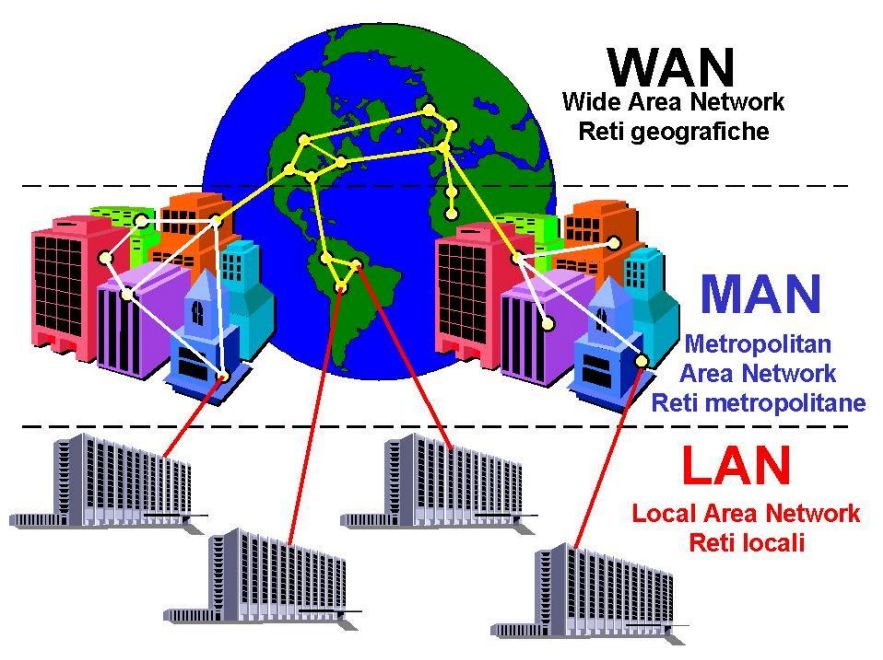
- Önemli dosyaların birkaç makinada yedeklenmesini sağlayarak bilgi güvenliğini sağlar.
- Ayni dosyaya veya dosyaların farklı bölgelerine farklı kullanıcılar tarafından değişik haklarla iletişim sağlanabilir.

Büyüklüklerine Göre Bilgisayar Ağları

Bilgisayar ağları coğrafi yerleşimleri açısından üç temel gruba ayrılırlar

- Yerel alan ağları (**L**ocal **A**rea **N**etwork)
- Geniş Alan Ağları (**W**ide **A**rea **N**etwork)
- Metropol (Kampüs)Alan Ağları (**M**etropolitan **A**rea **N**etwork)

Büyüklüklerine Göre Bilgisayar Ağları



- LAN (Local Area Network)
  - Oda, bina veya binalar arası
- MAN (Metropolitan Area Network)
  - 3-30 mil, bir şehirde
- WAN (Wide Area Network)
  - Tüm dünyada

Yerel Alan Ağları (LAN)

Yerel alan ağları, okullar, şirketler, hastaneler gibi küçük yerleşim bölgelerindeki bilgisayarların birbirlerine bağlanmasıyla oluşurlar. Temel amaç bilgisayarların bazı donanımları paylaşmasını sağlamaktır.

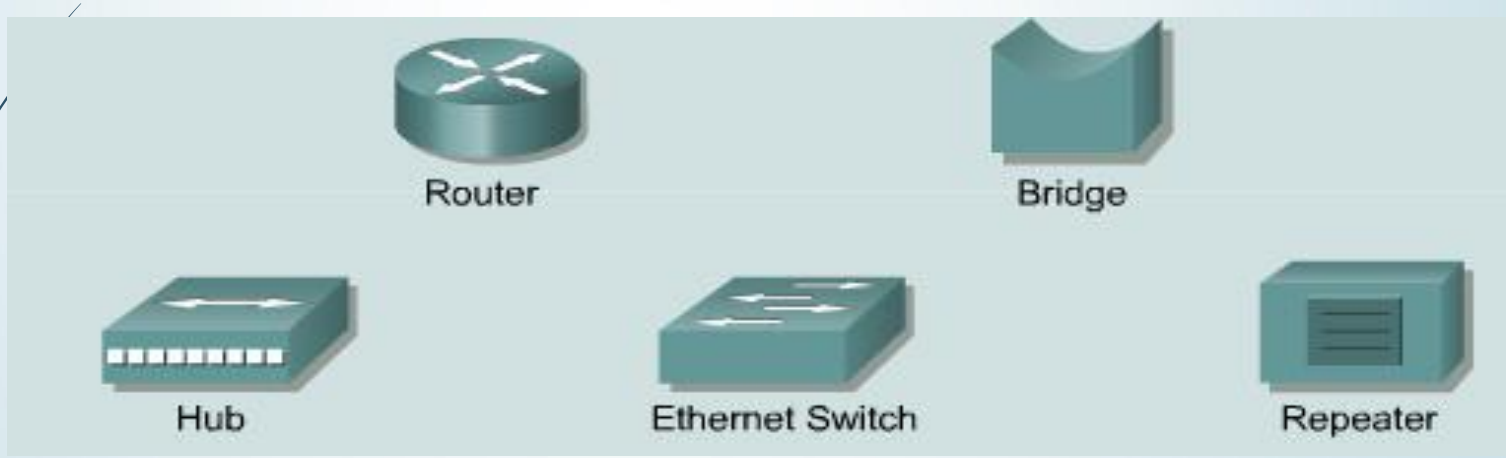
Yerel Alan Ağları (LAN)

Bu tür ağlarda ortalama veri iletim hızı kablosuz Ethernetler kullandığında 1-5 Mbit/s, UTP Ethernetlerle 10-100 Mbit/s civarındadır. Daha yüksek hızlara genelde gerek duyulmasa da, fiber optik altyapı ile bir kaç yüz Mbit/s gibi hızlara erişmek mümkündür. Yerel ağlar için IEEE tarafından belirlenmiş 3 standart yapı mevcuttur:

CSMA/CD (Carrier-Sense Multiple Access/Collision Detection), Token Ring ve Token Bus.

Yerel Alan Ağları (LAN)

LAN'da kullanılan bazı cihazlar



LAN Mimarileri

Ana Makine (MainFrame) Modeli:

- Ana makinenin kendi işlemcisi (CPU), sabit diski (harddisk), ve bunları kumanda etmek için bir ekranı ve klavyesi ve de terminallere bağlı seri portları vardı. Bu aptal terminaller (dumb terminal) sadece ekran ve klavyeden oluşurdu, yani bir deyişle pasif makinelerdi. Terminallerin yerel bir disk alanları da olmadığı için bilgiyi ana makine üzerinde saklarlardı. Tüm yük ana makinenin üzerindeydi ve bu yüzden çok pahalıydı. En büyük dezavantajı tabii ki güvenilir olmaması, yani ana makinede çıkacak bir sorunun tüm sistemi etkilemesi, terminallerin kendi başlarına işlem yapabilme kabiliyetlerinin olmaması idi.

LAN Mimarileri

İstemci-sunucu (Client-server) Modeli:

- İstemci/Sunucu modeli ile pasif terminaller yerine kendi başlarına işlemler yapabilen ve kendi sabit disklerinde programlar saklayabilen makineler geldi. Böylece her istemci kendi başlarına belirli işlemleri yerine getirebilmekte, yetersiz durumda kaldıklarında ise o işe özelleşmiş olan sunuculara başvurmakta idiler. Örneğin her istemcide ofis uygulamaları, masa üstü yayıncılık, oyun programları kullanılması buna rağmen veri tabanı ya da web gibi uygulamalarda bir sunucuya erişilmesi gibi.

LAN Mimarileri

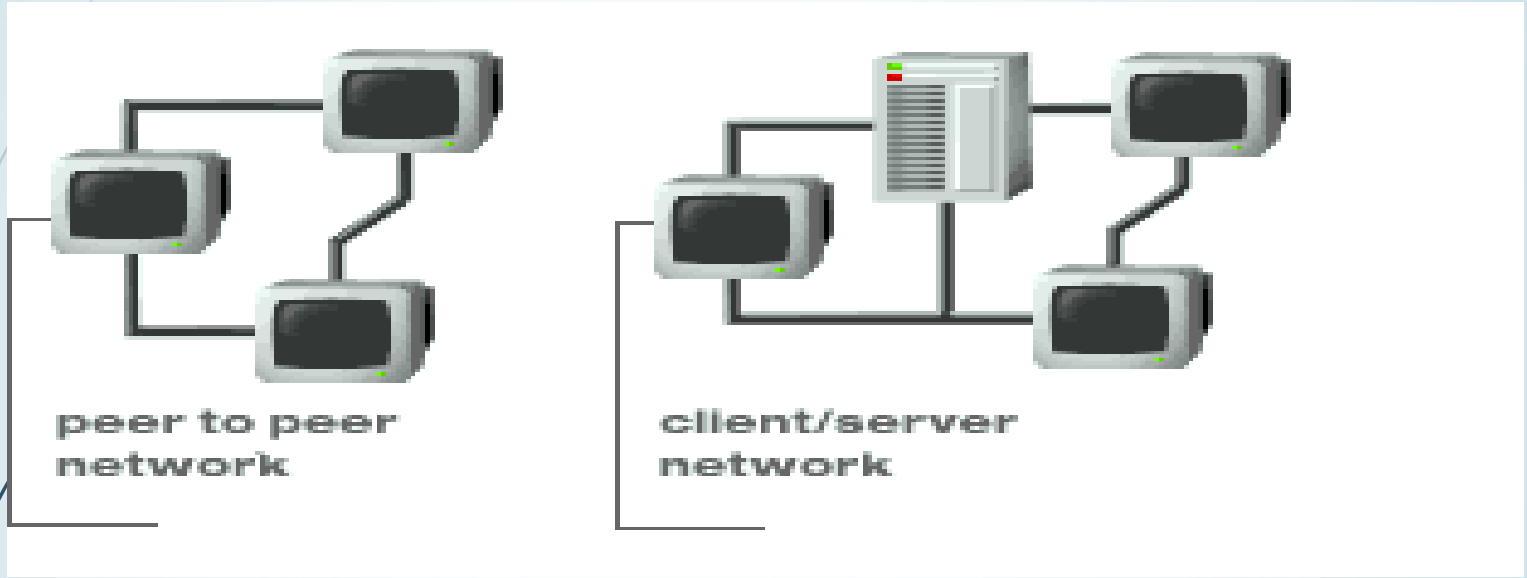
- Her bilgisayarın istemci veya sunucu olmak üzere ayrı bir rolü vardır.
- Sunucularda özel işletim sistemleri bulunur.
- Her sunucu belli bir iş üzerinde uzmanlaşabilir. (Dosya sunucusu, Yazıcı Sunucusu, E-posta sunucusu vb.)
- İstemciler diğer istemcilerle değil yalnızca sunucularla iletişim kurarlar.
- İstemcilerde standart işletim sistemleri ya da özel işletim sistemleri olabilir.

LAN Mimarileri

Türdeş (Peer to peer) Modeli:

- Bu ağ yapısında server kullanılmaz, her bir istemci kendi hard diskine sahiptir. Her bilgisayar birbiri ile konuşabilir ve istediği bilgi veya servisi alabilir. İstemciler diğer istemcilerin kullanımına açmak istedikleri veri veya servisi paylaştırırlar.
- Her bilgisayar eşittir ve erişim hakları onaylanmış ağdaki diğer bilgisayarlarla iletişim kurabilirler.
- Eşler arası ağda her bilgisayar hem istemci hem sunucu olarak görev alır.

LAN Mimarileri



Geniş Alan Ağları (WAN)

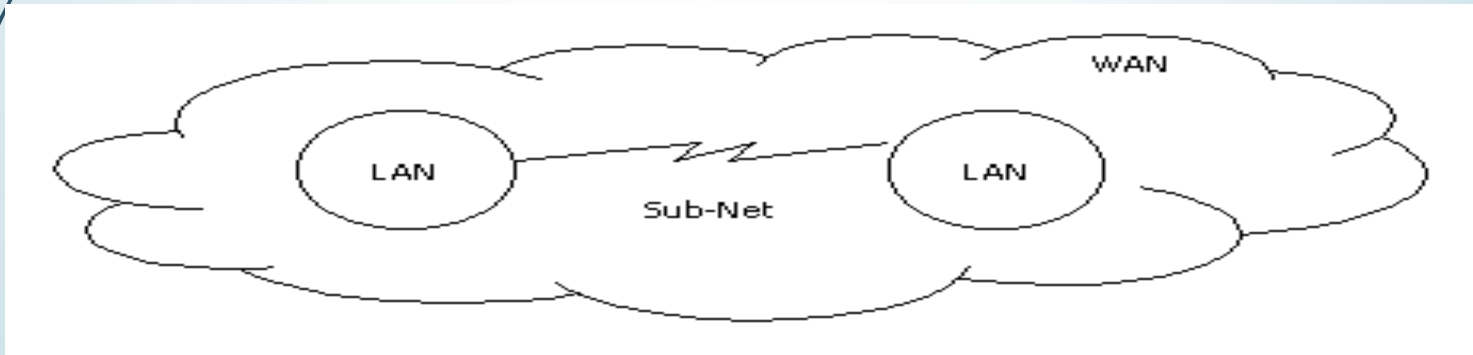
Bir ülke ya da dünya çapında yüzlerce veya binlerce kilometre mesafeler arasında iletişimi sağlayan ağlardır. Coğrafi olarak birbirinden uzak yerlerdeki (şehirlerarası/ülkelerarası) bilgisayar sistemlerinin veya yerel bilgisayar ağlarının (LAN) birbirleri ile bağlanmasıyla oluşturulur..

Geniş Alan Ağları (WAN)

- Temel özellik mesafenin uzak olması ve aradaki iletişim ortamının bir Telekom (örneğin Türk Telekom) şirketinden kiralanmasıdır. İletişim ortamının band genişliğinin sınırlı olması ve band genişliğine göre ücret ödendiği için bu ortam en iyi şekilde değerlendirilmelidir. Dolayısıyla WAN bağlantılarda en önemli anahtar sözcükler band genişliği , maliyet ve bağlantı servis kalitesidir.
- WAN bağlantısı için Telekom'dan alınacak hizmetlere örnek verecek olursak , Analog Modem ile bağlantı, Kiralık Hat bağlantısı, FR (Frame Relay), X25, SDSL gibi WAN bağlantısı teknolojileridir.

Geniş Alan Ağları (WAN)

WAN'da kullanılan bazı cihazlar



Metropol Alan Ağları (MAN)

MAN’lar bir şehir içindeki farklı bölgelerdeki LAN’ları bağlamak için kullanılır. LAN’ın kapsadığı alandan daha geniş, fakat WAN’ın kapsadığından daha dar mesafeler arası iletişimi sağlayan ağlardır. Genellikle şehir ya da kampüs içi bilgisayar sistemlerinin birbirleriyle bağlanmasıyla oluşturulur. Günümüzde LAN teknolojilerinin gelişmesi ile gündemden düşmüştür.

Ağ Topolojileri

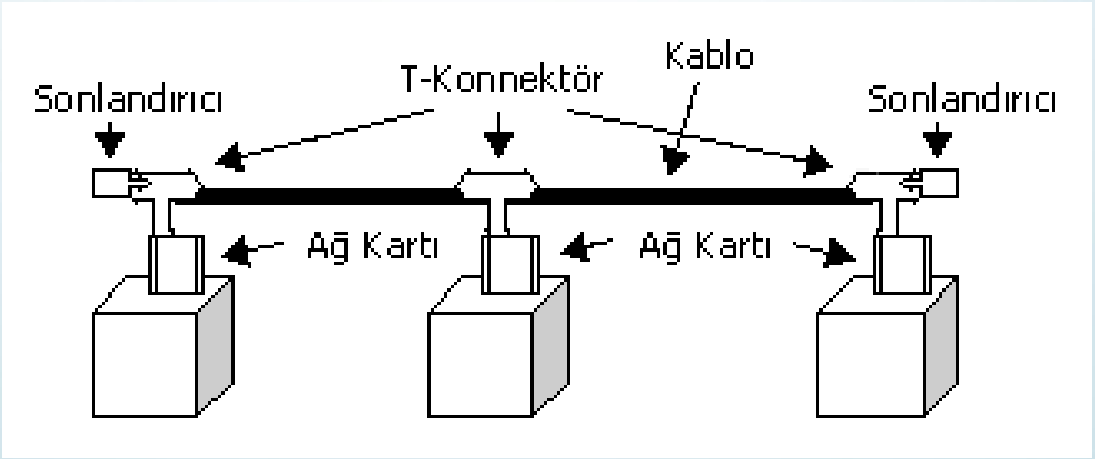
- Bir ağdaki bilgisayarların nasıl yerleşeceğini, nasıl bağlanacağını, veri iletiminin nasıl olacağını belirleyen genel yapıdır.
- Fiziksel topoloji: Ağın fiziksel olarak nasıl görüneceğini belirler (Fiziksel katman)
- Mantıksal topoloji: Bir ağdaki veri akışının nasıl olacağını belirler (Veri iletim katmanı)

Ağ Topolojileri

- Doğrusal (Bus Topology)
- Halka (Ring Topology)
  - Star-wired ring
- Yıldız (Star Topology)
  - Star-wired bus
- Ağaç (Tree Topology)
- Karmaşık (Mesh Topology)

Doğrusal (Bus) Topoloji

- Bir kablo yol olarak düşünülürse, bu yol üzerindeki her bir durak ağda bir düğümü (node-terminali/cihazı) temsil etmektedir.
- Bu tek kabloya; bölüm (segment), omurga (backbone), trunk denilebilir.
- Ağ bağlantısı tek bir koaksiyel kablo ile yapılır. İnce koaksiyelde azami menzil 185 mt, kalın koaksiyelde 500 mt.dir.



Doğrusal Topoloji - (Avantaj ve Dezavantajları)

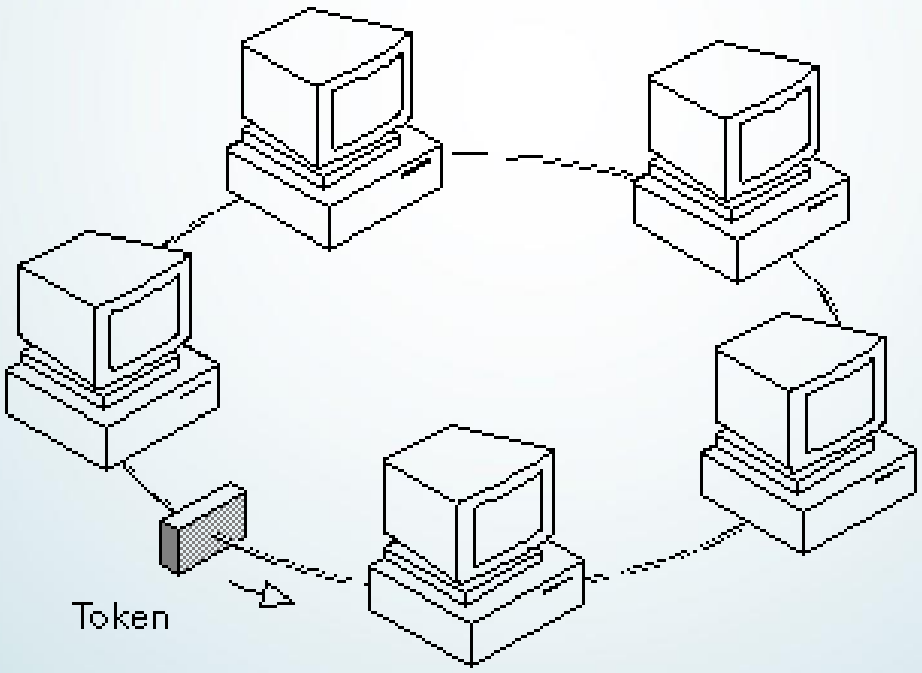
- Avantajları:
  - Ağa bir bilgisayarı bağlamak oldukça kolaydır.
  - Hub veya benzeri merkezi ağ ekipmanı gerektirmez.
  - Daha az uzunlukta kablo gerektirir.
- Dezavantajları
  - Omurga kabloda bir bozulma veya kesilme olursa tüm ağ bağlantısı kesilir.
  - Maksimum 30 bilgisayar. (Çarpışma)
  - Ağda sorun olduğunda sorunun nerden kaynaklandığını bulmak zaman alıcı olabilir.
  - Tek başına tüm bir binanın ağ çözümü için genellikle kullanılmamaktadır.

HALKA (RING) TOPOLOJİSİ

- Bu topolojide her istasyon bir halkanın elemanıdır ve halkada oluşan bilgi bütün istasyonlara ulaşır. Her istasyon halkada oluşan bilgiyi ve hedef adresi alır. Hedef adres kendi adresi ise kabul eder. Aksi halde gelen bilgi işlem dışı kalır.
- Halkadaki bilgi akışı tek yönlüdür. Yani halkaya dahil olan bilgisayarlar gelen bilgiyi iletmekle görevlidir. Ancak günümüzde pek çok halka ağı iki halka kullanmakta ve çift yönlü bilgi akışı elde etmektedir. Herhangi bir sonlandırmaya gerek duyulmaz.

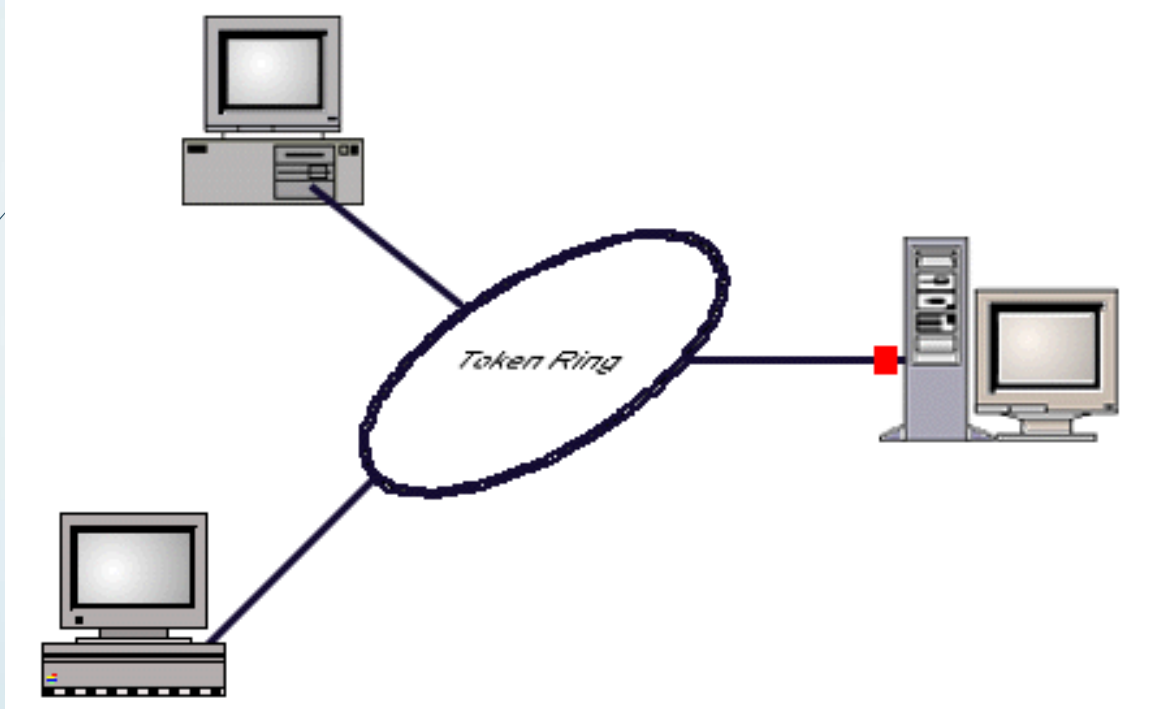
Halka (Ring) Topoloji

- IBM tarafından geliştirilmiştir. (Token Ring, 4/16 Mbps)
- Mantıksal olarak bir daire şeklinde tüm düğümlerin birbirine bağlanması.

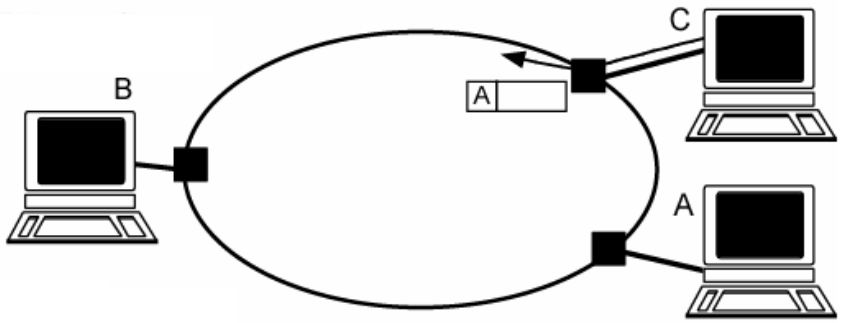


Halka(Token Ring) Topoloji

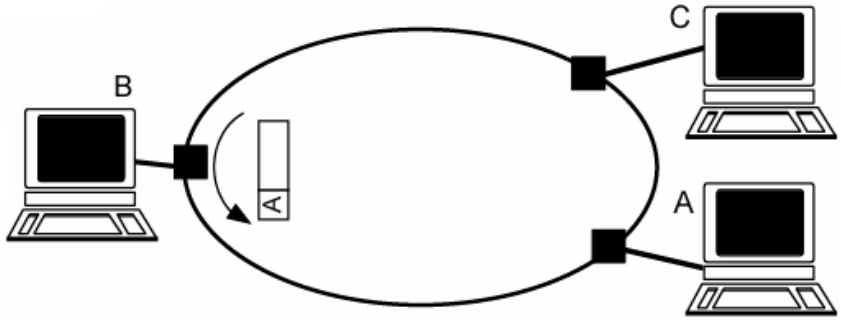
- Token (Jeton) (3 byte'lık) bu düğümler arasında dolaşan bilgidir.



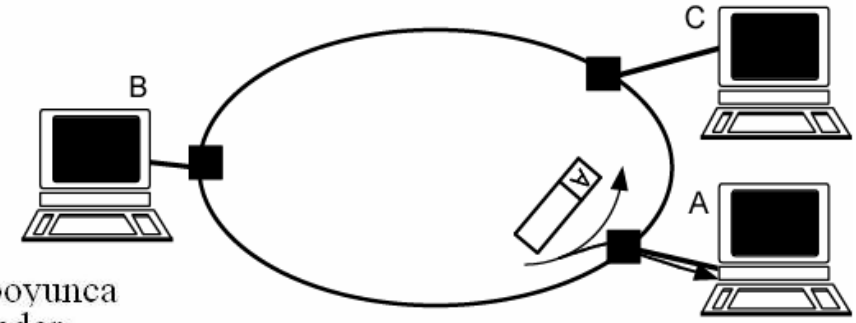
(a) C bir çerçeveyi A bilgisayarına gönderir



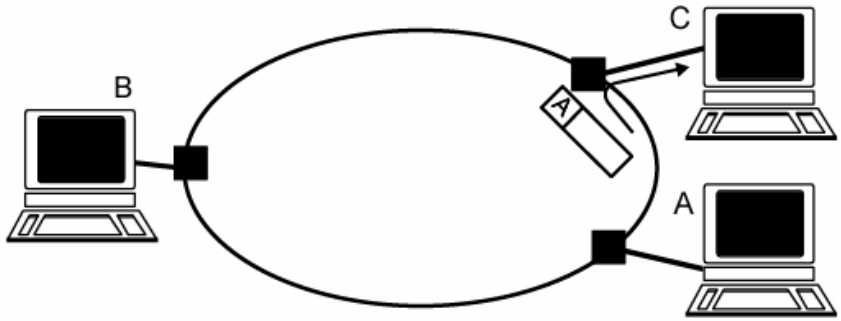
(b) Çerçevenin adresi B olmadığından, B bunu dikkate almaz

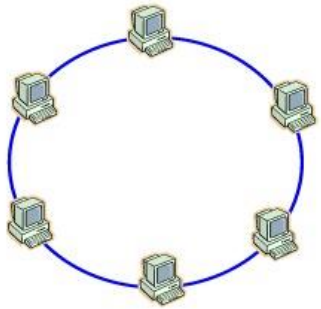


(c) A, çerçevenin kendine ait olduğunu anlar ve bunu alır, çerçeve kablo boyunca yoluna devam eder.



(d) C geri dönen çerçeveyi alır.





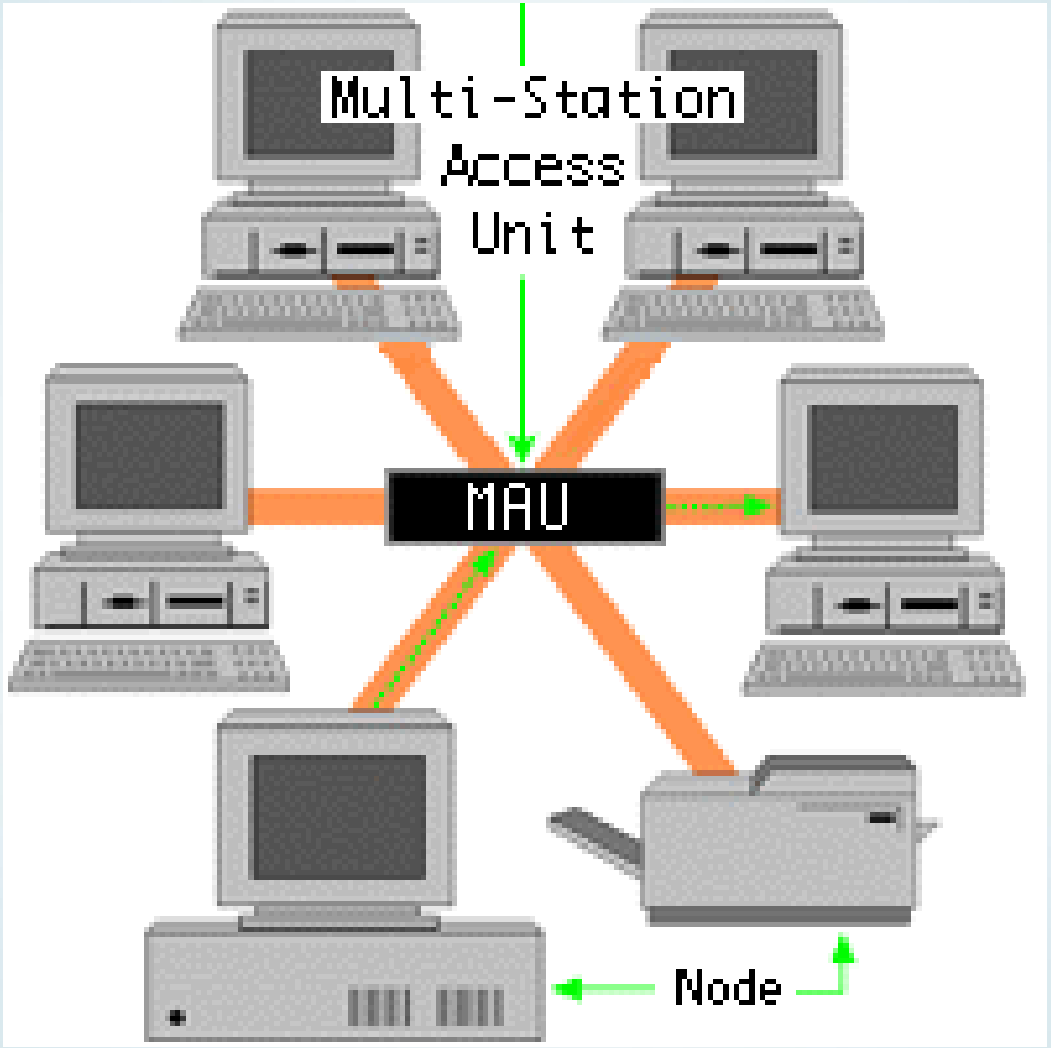
Halka Topoloji

- Halka içersindeki bir bilgisayar bozulursa tüm ağ bağlantısı kesilir.
- Çarpışma olasılığı düşüktür.
- Şu anda halka topolojilerde UTP, STP kablo kullanılmaktadır.
- İlk halka topolojiler; 4 Mbps (CAT3 UTP), daha sonra 16 Mbps(CAT4 ve üstü veya STP Tip 4) çalışmaktadır.
  - Halka topolojiye uygun ethernet kartları; 4 veya 16 Mbps'da çalışır.

Halka Topoloji ➔ Star-Wired Ring

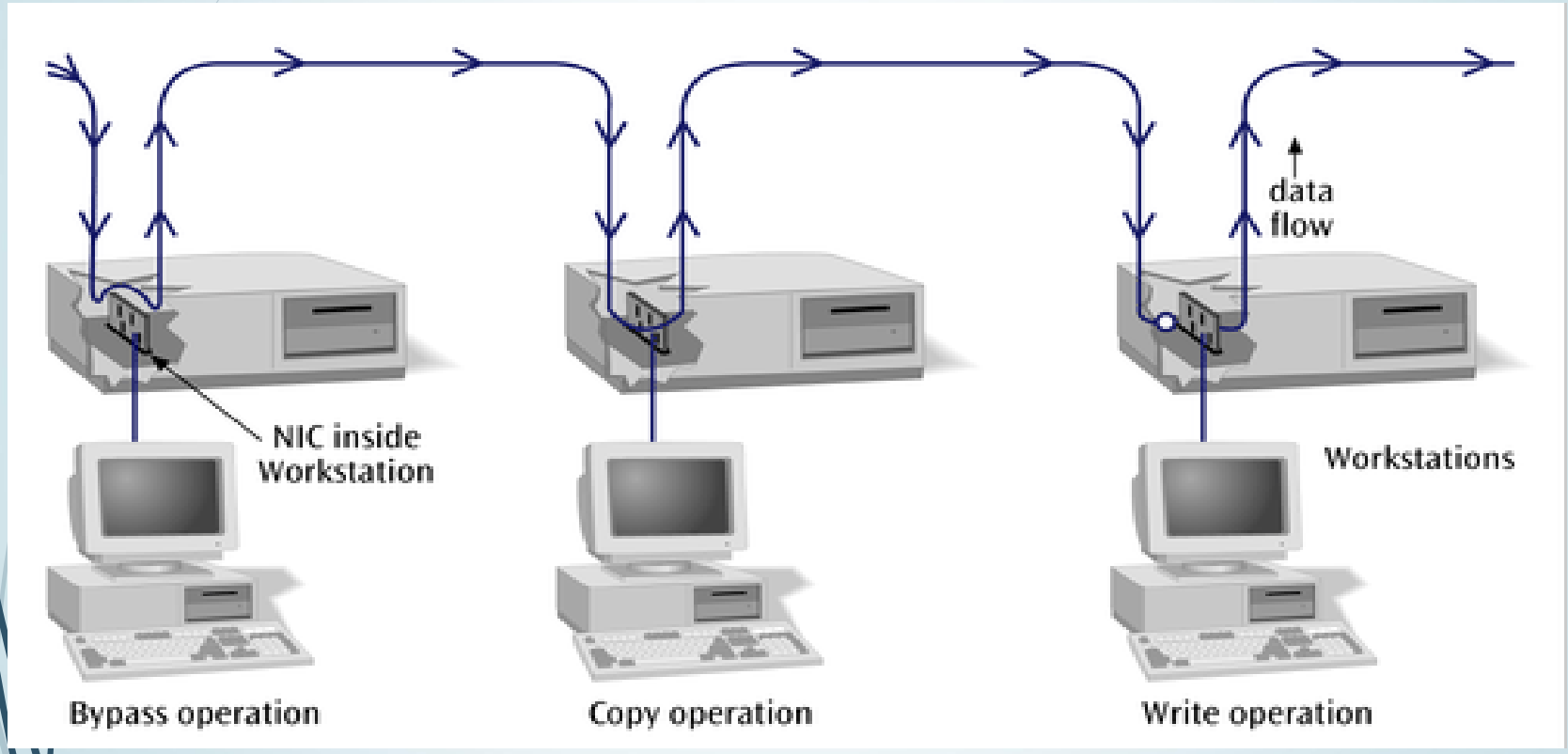
- Star-wired ring'de denilebilir.
  - Yerleşim fiziksel olarak yıldız olarak görünür ancak mantıksal olarak jetonlar dairesel olarak ağda ilerler.
  - Yıldız topolojisindeki Hub yerine burada MAU (Multistation Access Unit) veya MSAU (Multistation Access Unit) kullanılır.
  - Bu MAU'da veriler dairesel olarak gider.
    - Hub kendisine gelen bütün sinyalleri tüm düğümlere iletirken MAU gelen sinyali bir halka şeklinde sadece bir yönde iletir.
    - Böylece ağdaki tüm düğümler jetonu alır.

Halka Topoloji ➔ Star-Wired Ring



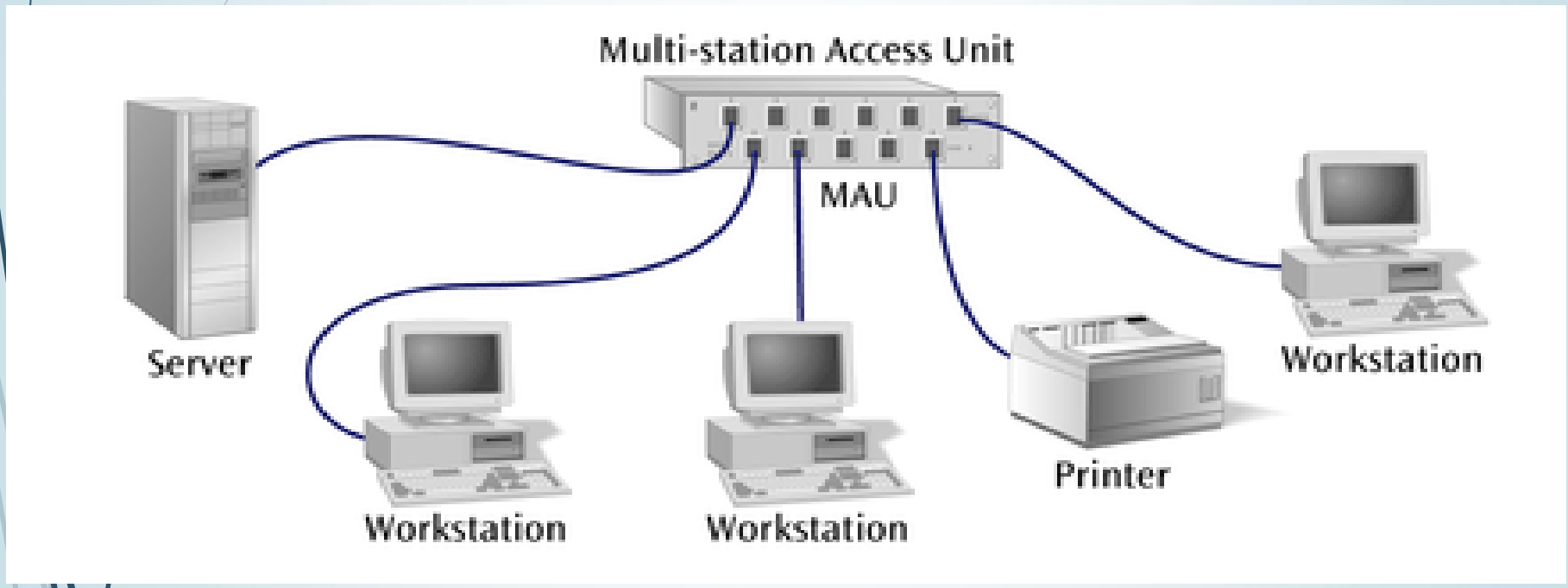
Halka Topoloji ➔ Star-Wired Ring

Klasik Halka topolojisi

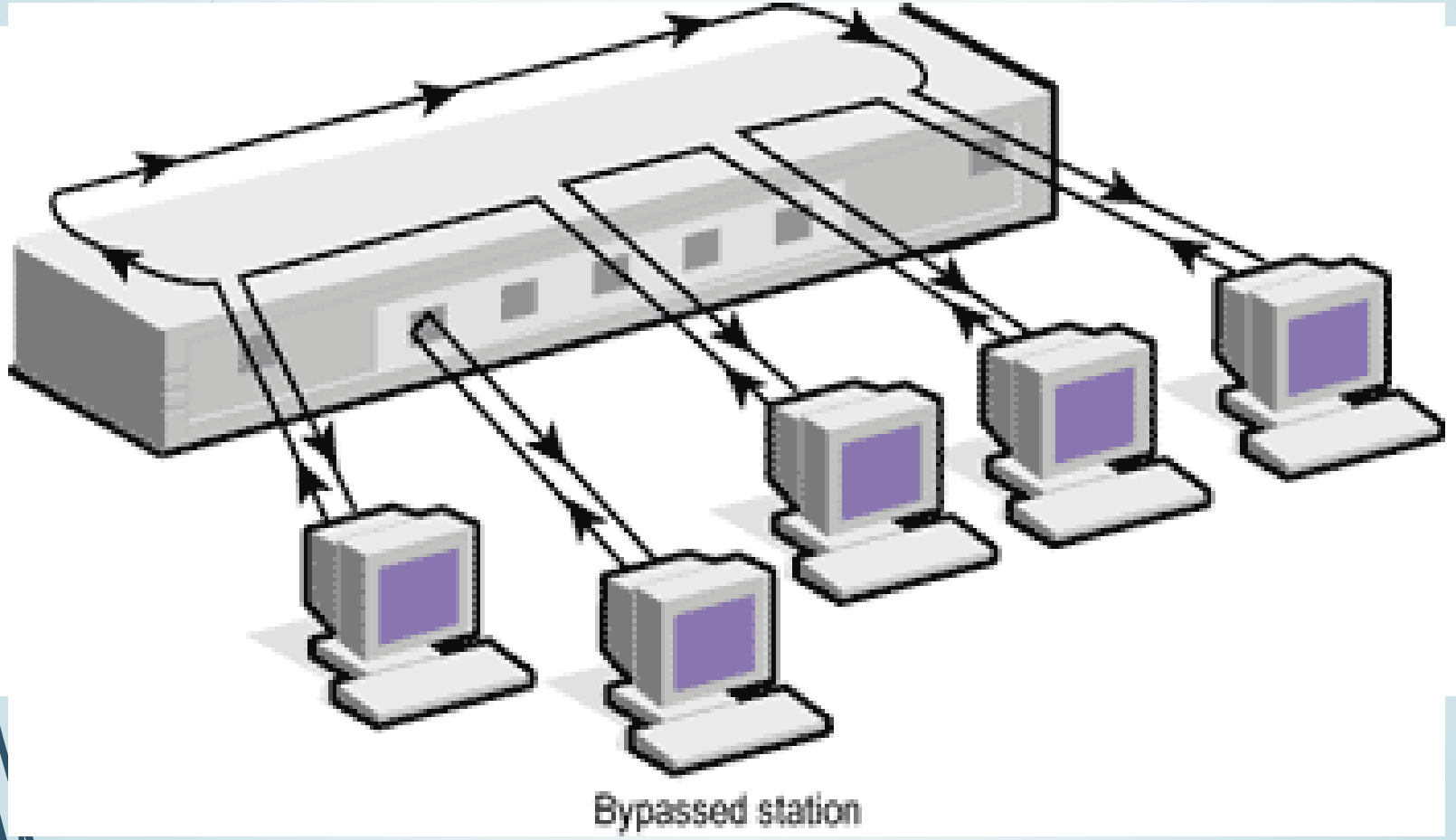


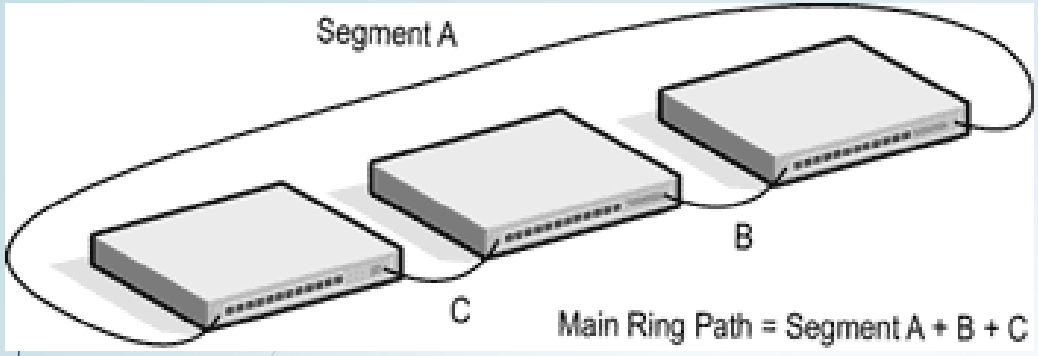
Halka Topoloji ➔ Star-Wired Ring

Star-Wired Ring topoloji

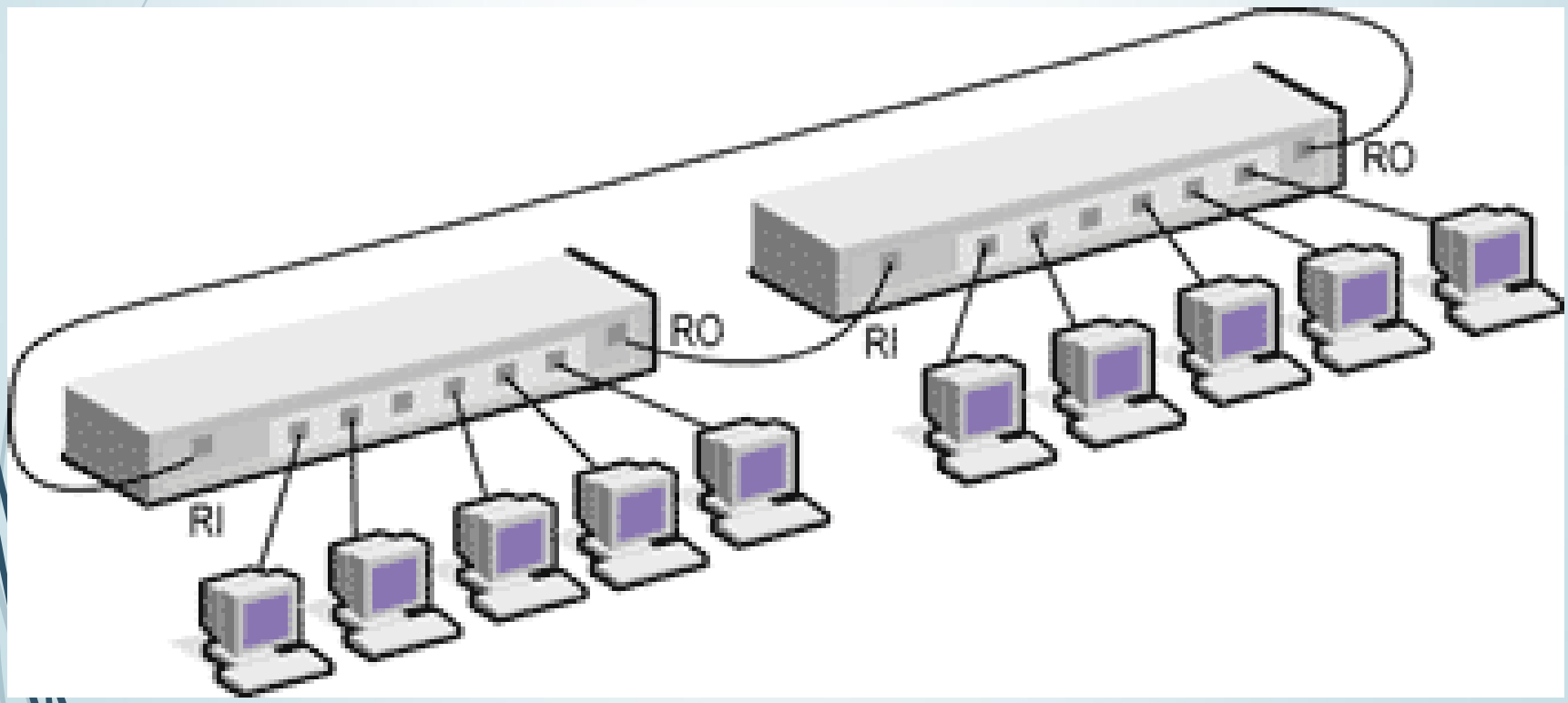


MAU





İki MAU bağlanması için MAU'daki RI (Ring In) ve RO (Ring Out portları kullanılır.



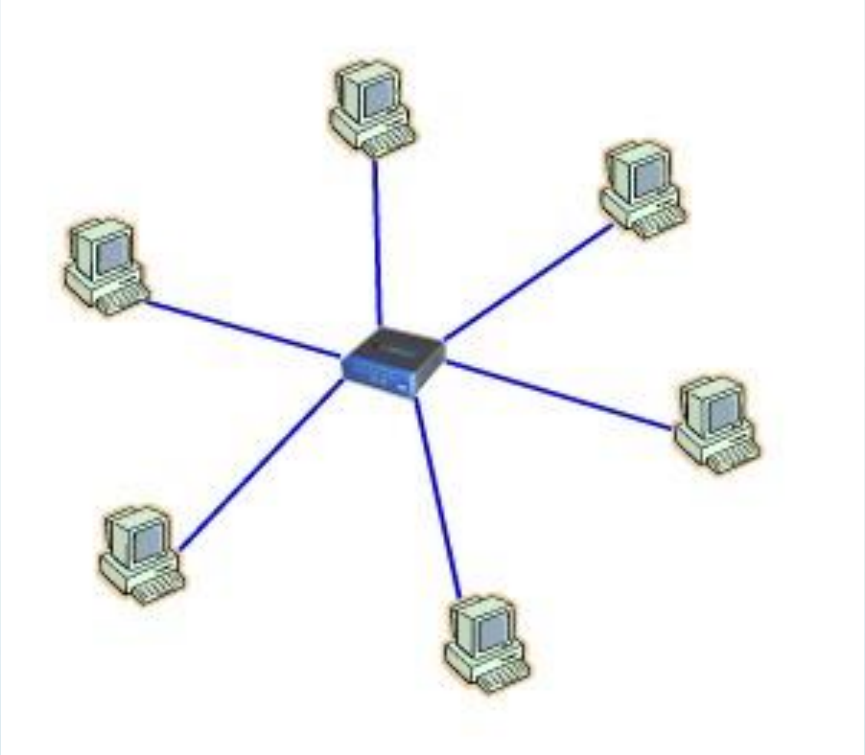
YILDIZ TOPOLOJİSİ

- Bu topolojide ağdaki iletişimin gerçekleşmesi için merkezi birim bulunur ve bütün istasyonlar bu merkezi birime bağlanır. Ortak yol topolojisine göre performansı daha yüksektir, güvenilirdir fakat daha pahalı çözümler sunar.
- Bir istasyondan diğerine gönderilen bilgi önce bu merkez birime gelir, buradan hedefe yönlendirilir. Ağ trafiğini düzenleme yeteneğine sahip bu merkezi birim, hub ve anahtar (switch) olarak adlandırılır.

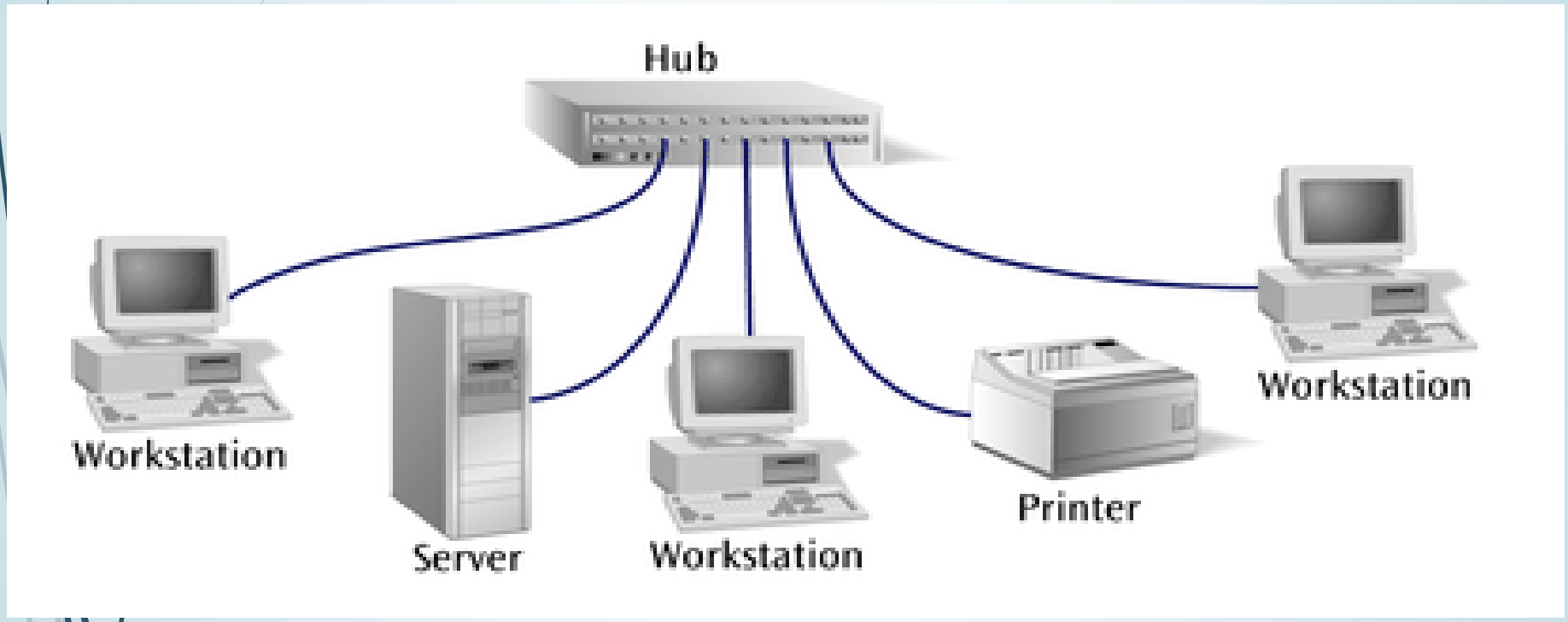
YILDIZ (STAR) TOPOLOJİSİ

- Bu topolojiye dayalı bir sistem kurulurken korumasız çift bükümlü UTP (Unshieded Twisted Pair) veya korumalı çift bükümlü STP (Shielded Twisted Pair) kablo kullanılır.
- İstasyonların merkezi birime (hub) olan uzaklığı maximum 100 metredir. Kullanılan ağ kartına veya kabloya göre ağ farklı hızlarda çalışabilir.

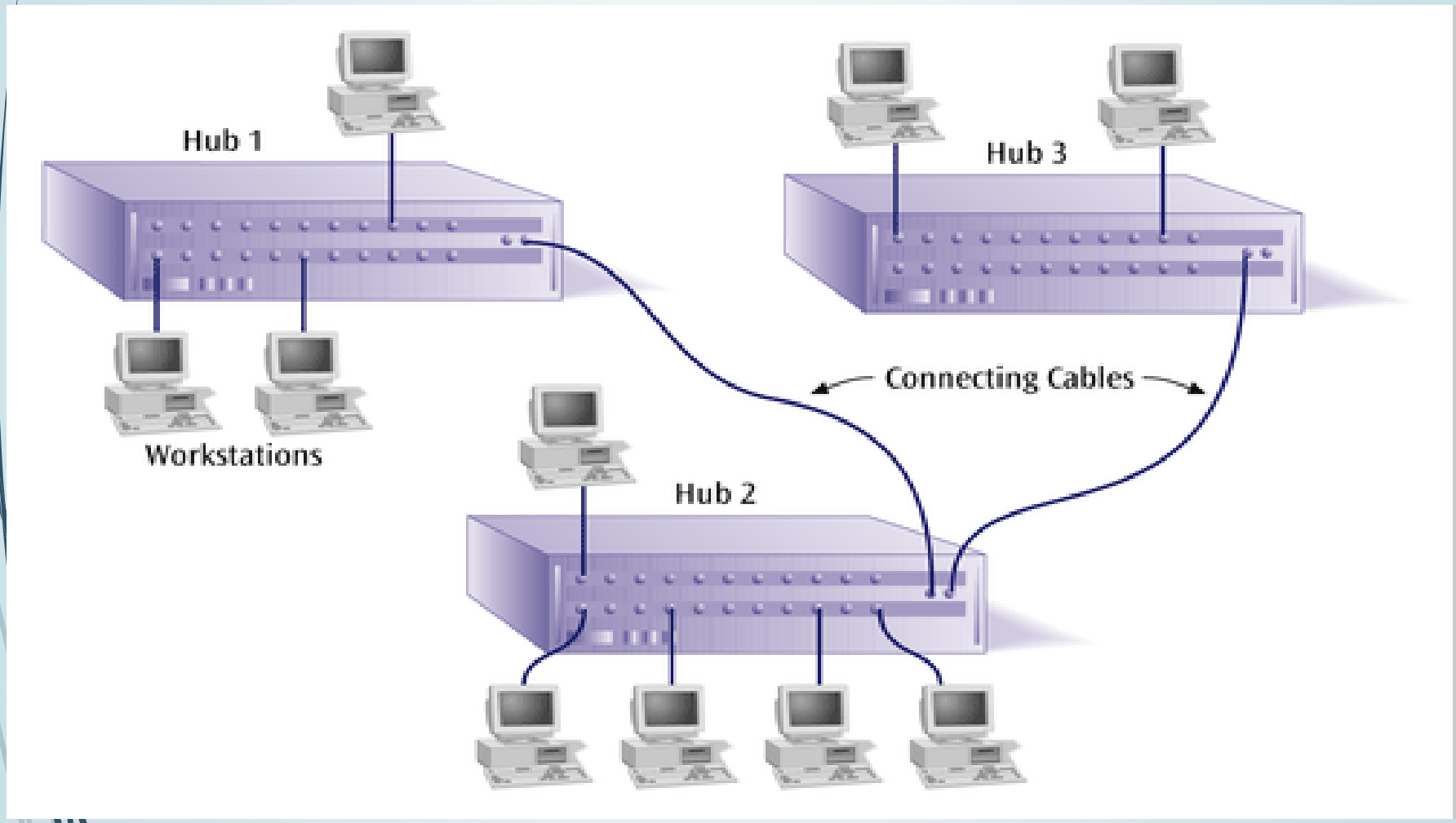
Yıldız (Star) Topoloji



Yıldız (Star) Topoloji



Star-wired bus ~ Yıldız Topoloji



Yıldız Topoloji (Avantaj ve Dezavantajları)

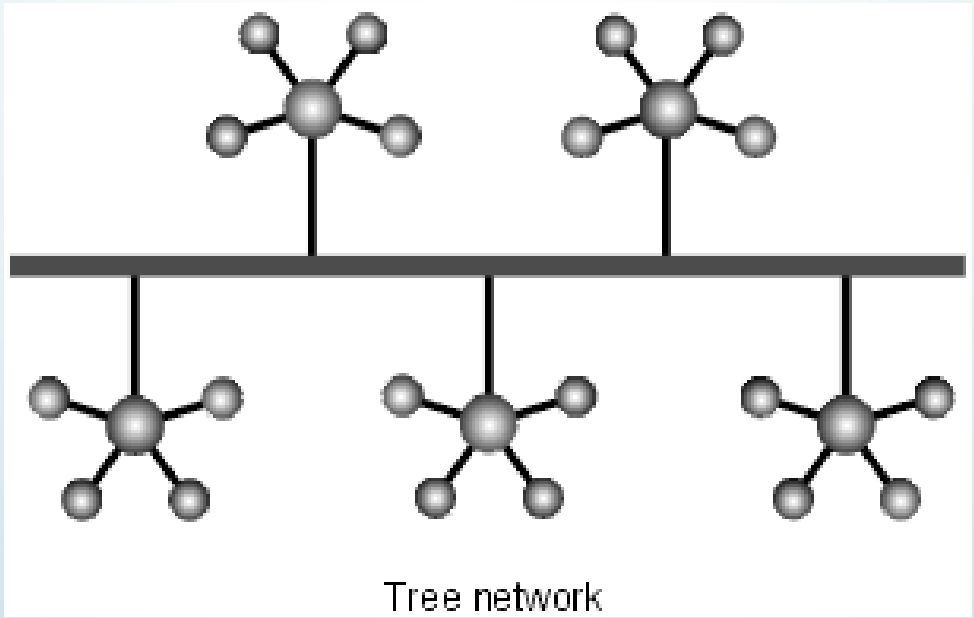
- Avantajları:
  - Ağı kurmak kolaydır
  - Bir bilgisayara bağlı kablo bozulduğunda ağın çalışması etkilenmez.
  - Ağdaki sorunları tespit etmek kolaydır.
- Dezavantajları
  - Hub kullanıldığında ağ trafiği artar.
  - Doğrusala göre daha fazla uzunlukta kablo gerektirir.
  - Hub veya Switch bozulduğunda tüm ağ çalışmaz hale gelir.
  - Hub ve Switch gibi cihazlar nedeniyle doğrusala göre kurulumu daha pahalıdır.

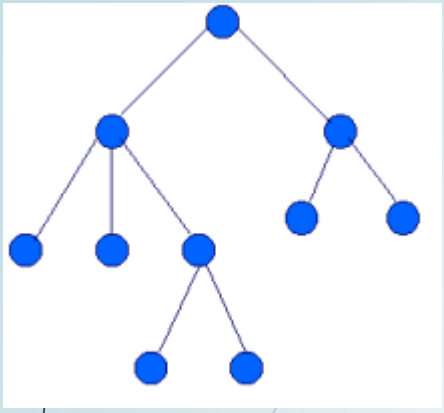
AĞAÇ (TREE) TOPOLOJİSİ

- Ağaç topolojisinin diğer adı hiyerarşik topolojidir.
- Ağacın merkezinde sorumluluğu en fazla olan bilgisayar bulunur. Dallanma başladıkça sorumluluğu daha az olan bilgisayarlara ulaşılır.
- Bu topoloji çok büyük ağların ana omurgalarını oluşturmakta kullanılır.

Ağaç (Tree) Topoloji

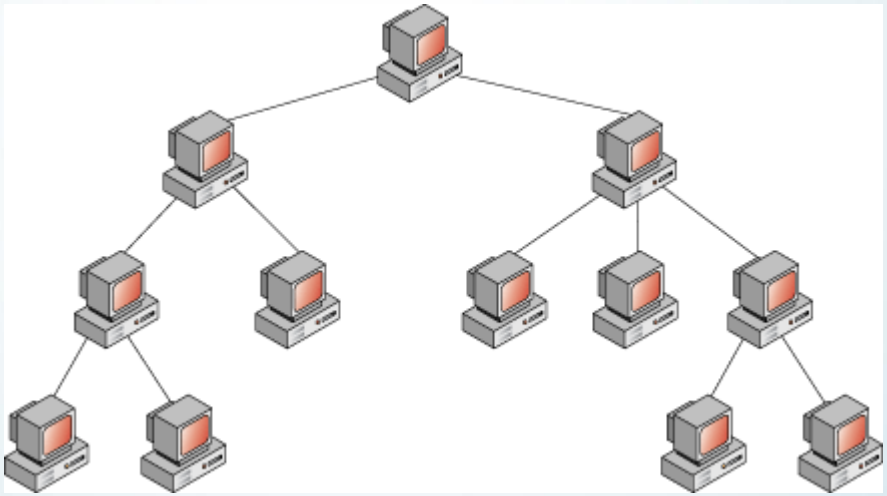
- Genellikle yıldız topolojisindeki ağları birbirine bağlamak için kullanılır. Böylece ağlar büyütülebilir.
- Bir ağacın dalları farklı topolojilerdeki ağları temsil eder, ağacın gövdesi ile de bunlar birbirine bağlanabilir.



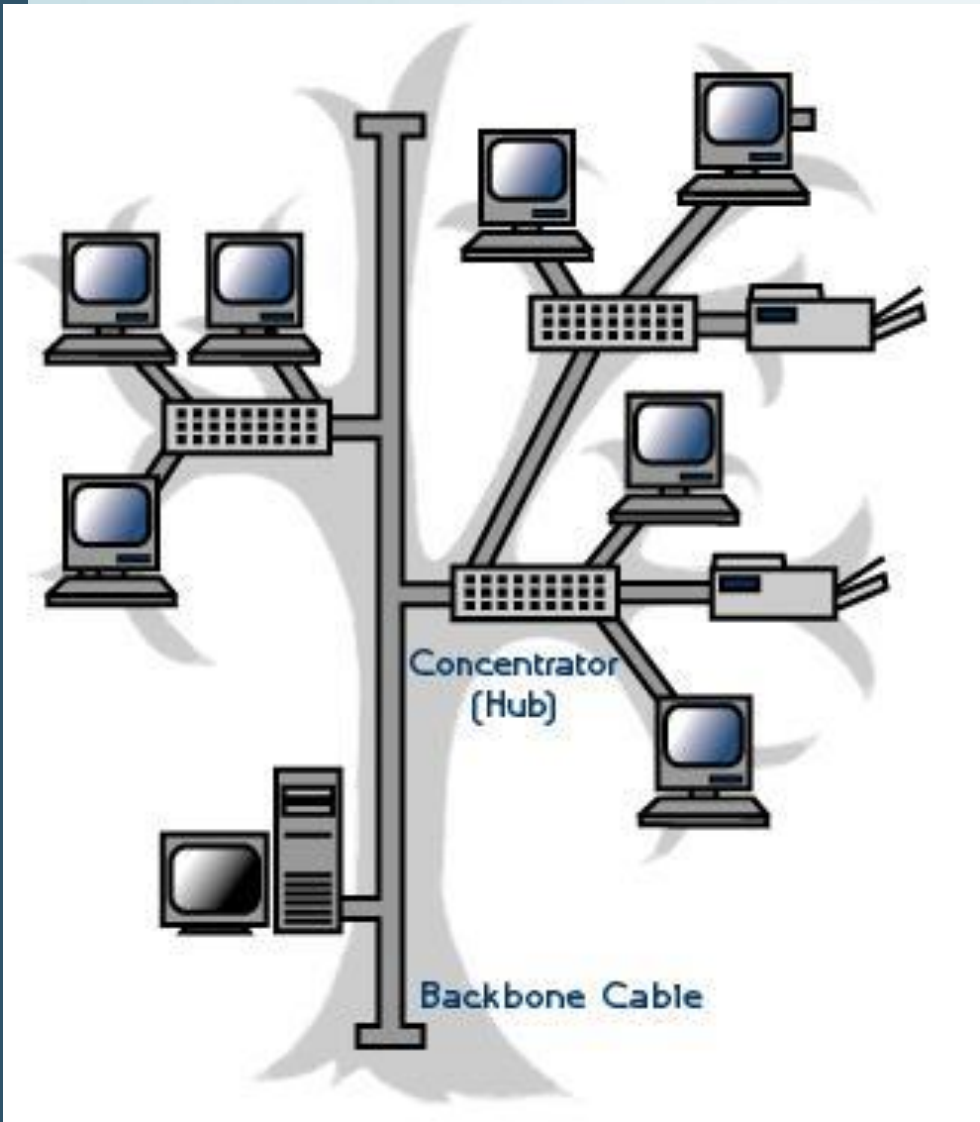


Ağaç (Tree) Topoloji

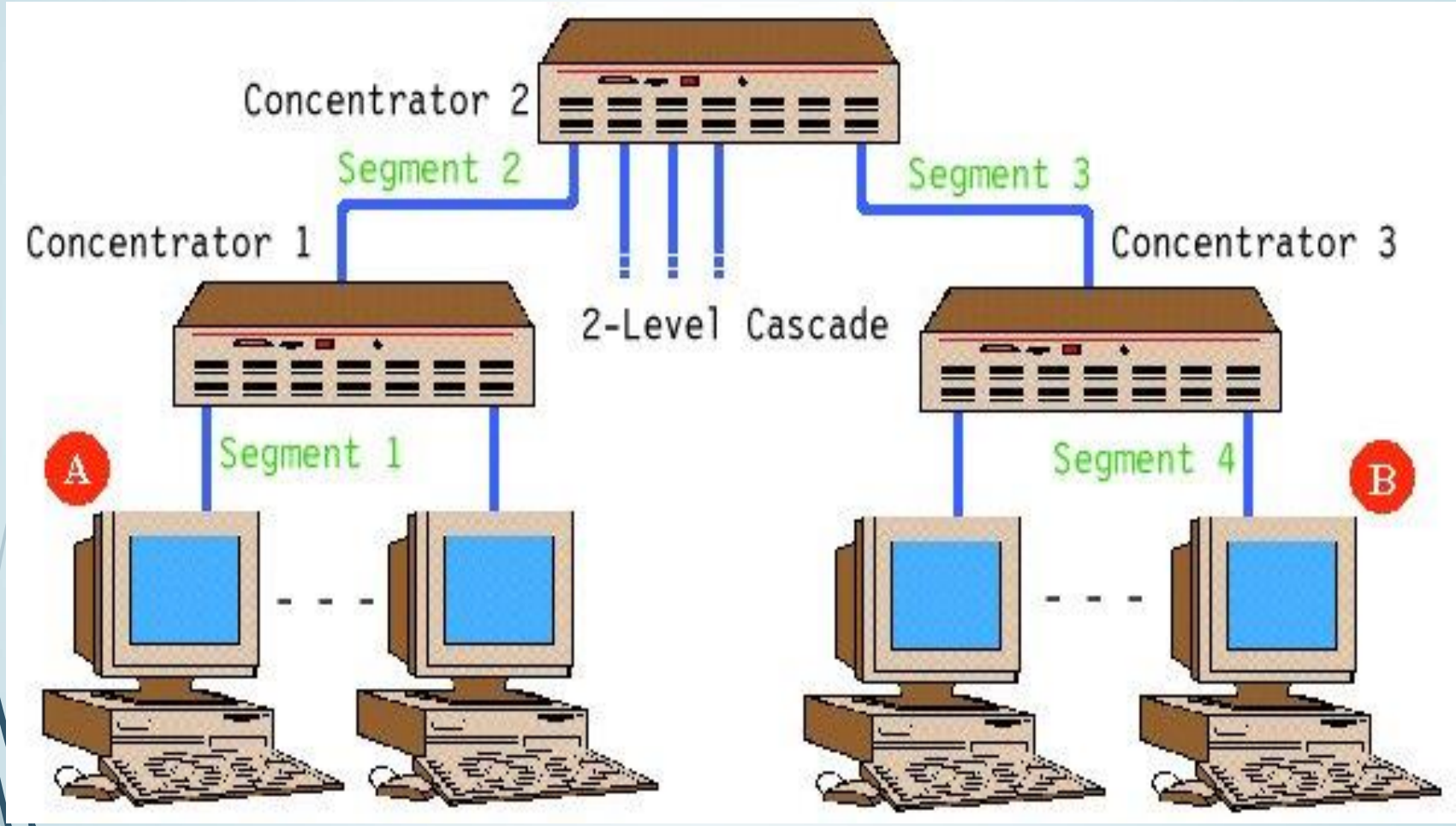
- Hiyerarşik yapıdaki ağlar için kullanılır.



Ağaç Topoloji - (Avantaj ve Dezavantajları)



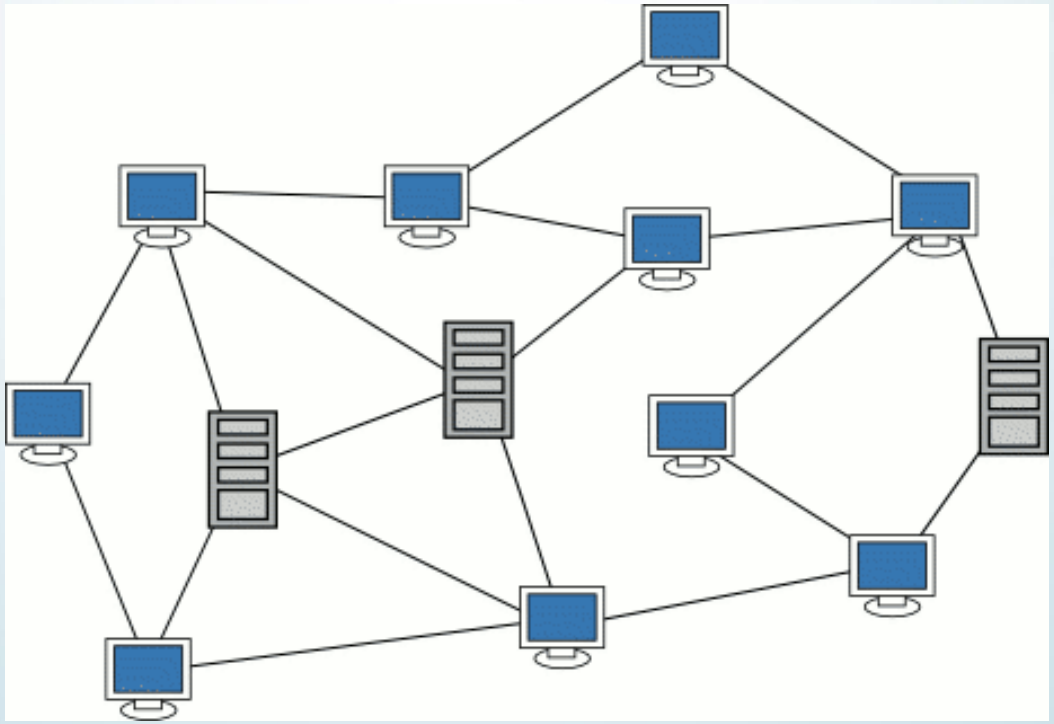
- Avantajları:
  - Her bir bölüme (segment) ulaşmak kolaydır
  - Bir çok çalışma grubu bir araya getirilebilir.
- Dezavantajları
  - Her bir bölümün uzunluğu kullanılan kablo ile sınırlıdır.
  - Omurga kablosu bozulduğunda bölümlerdeki ağ trafiği etkilenir.
  - Kurulumu ve düzenlenmesi daha zordur.


Concentrator 2
Segment 2
Segment 3
Concentrator 1
Concentrator 3
2-Level Cascade
Segment 1
Segment 4
A
B

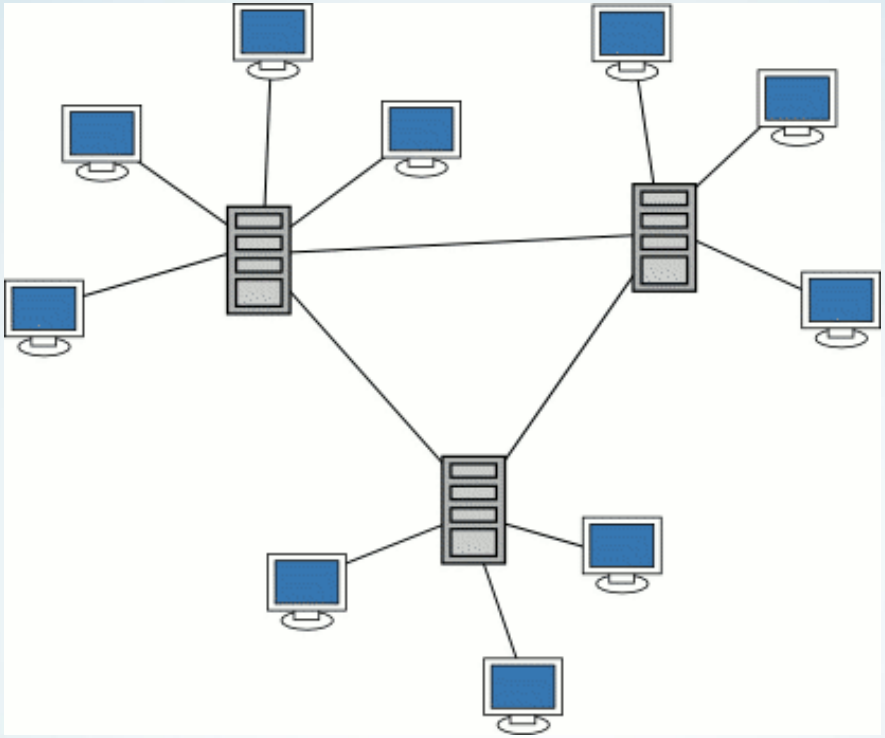
Örgü (Mesh) Topoloji

- Gerçek Mesh topolojide tüm düğümler ağ içerisinde birbirine bağlıdır.
- Daha çok WAN'da kullanılır.
- LAN'da kullanıldığında tüm düğümlerin birbirine mutlaka bağlı olması gerekmez.

Gerçek Mesh topoloji

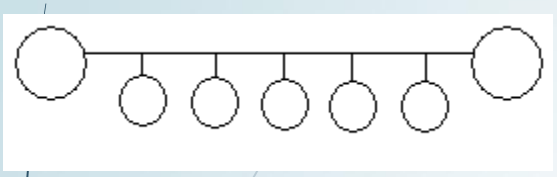


Örgü(Mesh) Topoloji

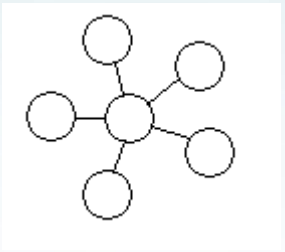


- Hybrid mesh topoloji, karmaşık ağlarda (veritabanı sunucularının uzak mesafeler arası bağlantıları vb.) kullanılır.

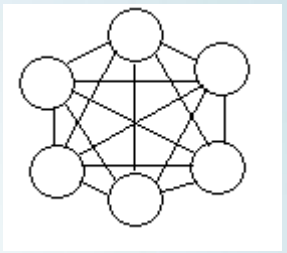
Doğrusal
(Bus)



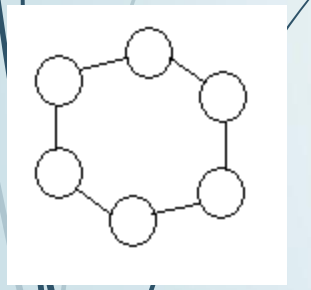
Yıldız
(Star)



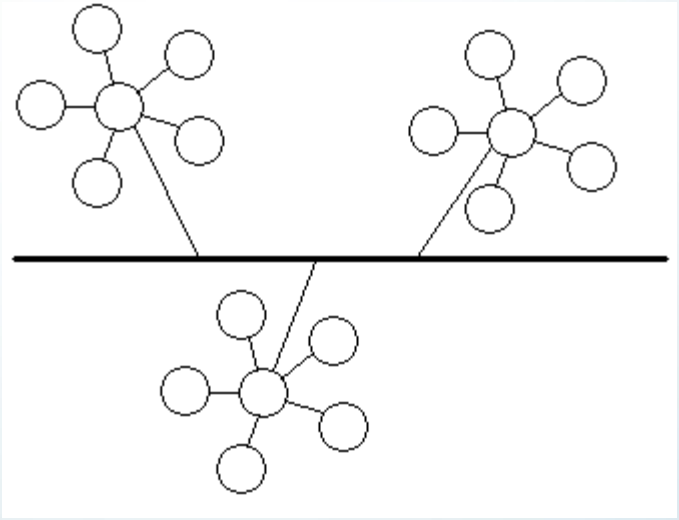
Örgü
(Mesh)



Halka
(Ring)



Ağaç
(Tree)



Topoloji	Kurulum	Düzenleme	Sorun çözme	Veri aktarımında problem
Doğrusal	Çok kolay	Kısmen zor	Zor	Tek bir kablo, kabloda problem veri aktarımını etkiler
Halka	Kısmen Kolay	Kısmen zor	Kolay	Halkadaki bozukluk veri aktarımını etkiler
Yıldız	Kolay, ancak zaman alıcı	Kolay	Kolay	Tek bir kablodaki bozukluk bir pc'yi etkiler
Ağaç	Zor	Zor	Kolay	Oldukça az
Örgü	Zor	Zor	Kolay	Oldukça az

Ağ Bağlantı Tipleri

Kablolu

Kablosuz

AĞ TEMELLERİ

OSI Referans Modeli

ISO

- ISO (International Standards Organization - Uluslararası Standartlar Örgütü)
- ISO Teknik konularla ilgili en büyük standartlaştırma örgütüdür. Mekanik, elektrik, kimya, petrol ürünleri, uzay ve havacılık gibi çok çeşitli konularda çalışan 214 adet teknik komitesi bulunmaktadır. ISO standartları, ilgili teknik komite tarafından en az beş yılda bir gözden geçirilmekte, gerekirse değiştirilmektedir.

Protokol ve ITU

- **Protokol**: İki bilgisayar arasındaki iletişimi sağlamak amacıyla verileri düzenlemeye yarayan, standart olarak kabul edilmiş kurallar dizisidir. İki cihaz arasındaki haberleşme için ortak bir iletişim yöntemidir.
- **ITU –International Telecommunication Union** : Veri haberleşmesi konusunda standartlar belirler

IEEE

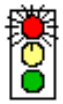
- IEEE –Instute of Electrical and Electronics Institute : IEEE'nin açılımı Elektrik ve Elektronik Mühendisleri Enstitüsü'dür. IEEE'nin misyonu, elektro ve bilgi teknolojilerinde ve bilimlerde mühendisliğin yaratma, geliştirme, paylaşma ve bilgiyi uygulama süreçlerini insanlığın ve mesleğin yararı için güçlendirmektir. Komiteler halinde çalışırlar ve bilgisayar ağları ile ilgili standartlar geliştirirler. Her komite farklı bir konuda çalışır ,802.3 , 802.11b ,802.4 gibi..

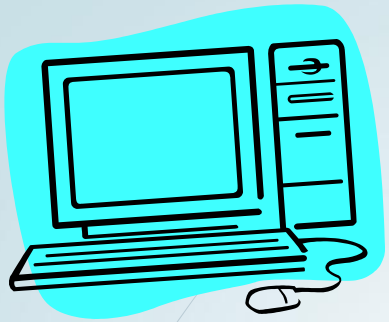
OSI Referans Modeli

Bilgisayar ağları kullanılmaya başlandığı ilk zamanlarda sadece aynı üreticinin ürettiği cihazlar birbirleriyle iletişim kurabiliyordu. Bu da şirketleri tüm cihazlarını sadece bir üreticiden almalarını zorunlu kılıyordu. 1970'lerin sonlarına doğru ISO (International Organization for Standardization) tarafında, OSI (Open System Interconnection) modeli tanımlanarak bu kısıtlamanın önüne geçildi. Böylece farklı üreticilerden alınan cihazlar aynı ağ ortamında birbirleriyle haberleşebileceklerdi.

OSI Modeli

- Farklı bilgisayarların ve standartların gelişmesi ile sorunların ortaya çıkması nedeniyle
- ISO (International Organization for Standardization), OSI (Open Systems Interconnection) modelini 1984'te geliştirdi.
- 7 Katmandan oluşmakta ve karmaşıklığı azaltmak ve standartlar geliştirmek amacıyla geliştirilmiştir.
- OSI modeli bir kullanıcının bilgisayarındaki bir uygulama tarafından gönderilen verinin iletim ortamı üzerinden diğer bilgisayardaki uygulama yada uygulamalara nasıl iletileceğini tanımlar.

OSI MODEL			TCP / IP
7		**Application Layer** Type of communication: E-mail file transfer, client/server.	**FTP,** **SMTP,** **DNS,** **Telnet**
6		**Presentation Layer** Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.	
5		**Session Layer** Starts, stops session. Maintains order.	
4		**Transport Layer** Ensures delivery of entire file or message.	**TCP,** **UDP**
3		**Network Layer** Routes data to different LANs and WANs based on network address.	**IP** (ICMP, ARP, RARP)
2		**Data Link (MAC) Layer** Transmits packets from node to node based on station address.	
1		**Physical Layer** Electrical signals and cabling.	



Terminal A

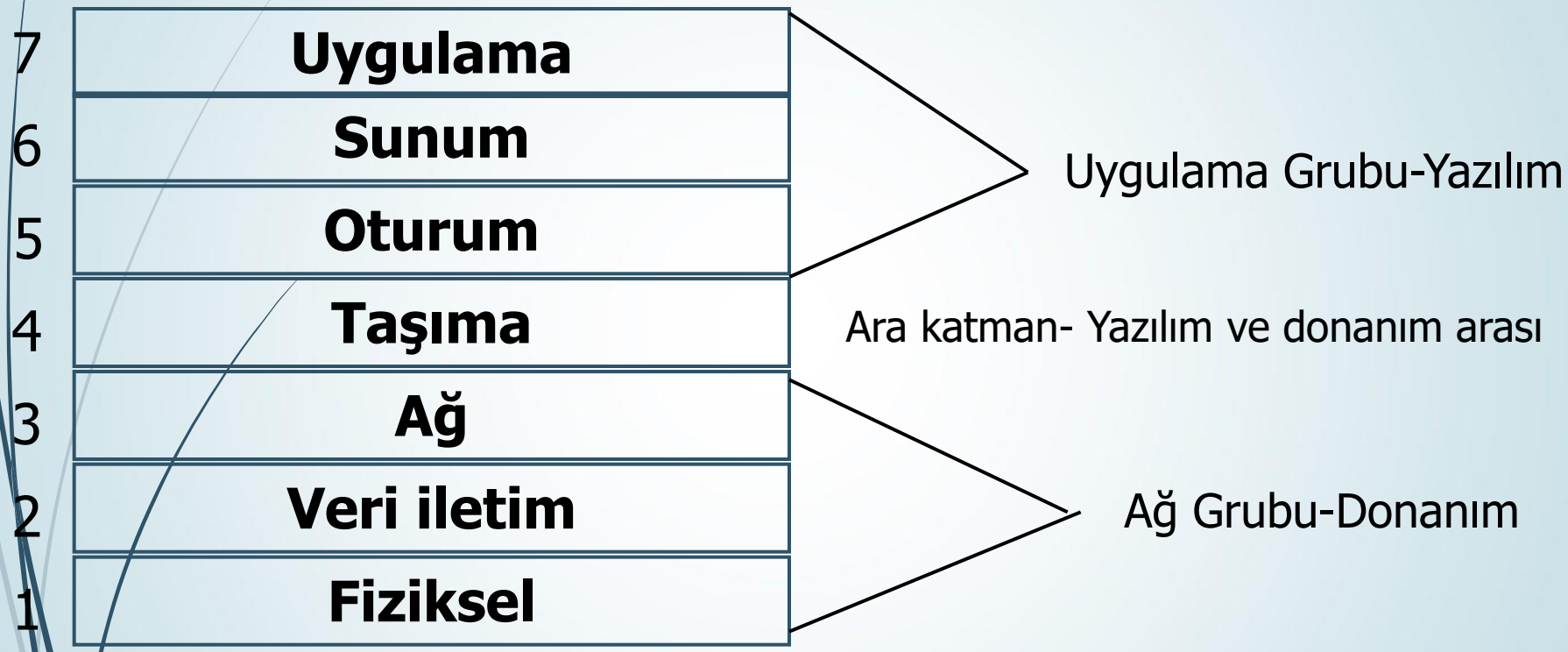
Terminal B

7	**Uygulama**	7	**Uygulama**
6	**Sunum**	6	**Sunum**
5	**Oturum**	5	**Oturum**
4	**Taşıma**	4	**Taşıma**
3	**Ağ**	3	**Ağ**
2	**Veri iletim**	2	**Veri iletim**
1	**Fiziksel**	1	**Fiziksel**

OSI Faydaları

- Karmaşık network işlemlerini katmanlara bölerek yönetimi kolaylaştırır
- Bir katmanda yapılan değişiklik bir başka katmanda değişiklik yapılmasını gerektirmez
- Farklı üreticilere ait iletişim cihazlarının ve yazılımların bir arada çalışmasını sağlar.

OSI Modelinin Katmanları



OSI Katmanları

- Üst katmanlar
  - 7. Application Layer (uygulama katmanı)
  - 6. Presentation Layer (sunum katmanı)
  - 5. Session Layer (oturum katmanı)
- Ara katman
  - 4. Transport Layer (taşıma katmanı)
- Alt katmanlar
  - 3. Network Layer (ağ katmanı)
  - 2. Datalink Layer (veri bağıkatmanı)
  - 1. Physical Layer (fiziksel katmanı)

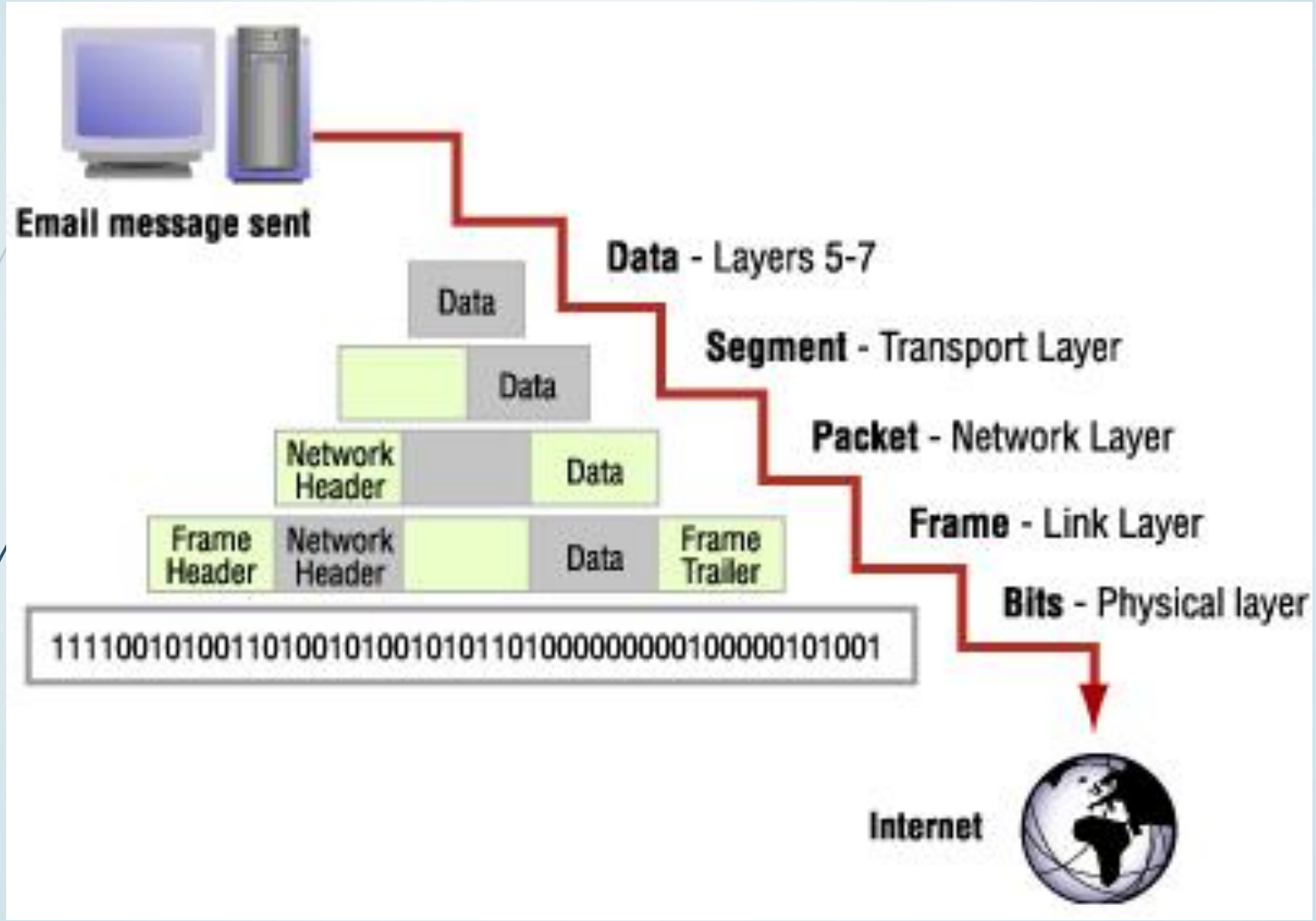
Katman	Görevi
7.) Uygulama	Kullanıcının uygulamaları
6.) Sunum	Aynı dilin konuşulması; veri formatlama, şifreleme
5.) Oturum	Bağlantının kurulması ve yönetilmesi
4.) Taşıma	Verinin bölümlere ayrılarak karşı tarafa gitmesinin kontrol edilmesi
3.) Ağ	Veri bölümlerinin paketlere ayrılması, ağ adreslerinin fiziksel adreslere çevrimi
2.) Veri bağı	Ağ paketlerinin çerçevelere ayrılması
1.) Fiziksel	Fiziksel veri aktarımı

Katman	PDU (Protocol Data Unit) Adı
7.) Uygulama	HTTP, FTP, SMTP
6.) Sunum	ASCII, JPEG, PGP
5.) Oturum	NetBIOS, DHCP
4.) Taşıma	TCP, UDP, SPX
3.) Ağ	IP, IPX
2.) Veri bağı	Ethernet, Frame Relay, ISDN
1.) Fiziksel	Bit, Kablo, Konnektör

OSI'de Verilerin Adı

Katman	Kullanılan Veri Adı
7.) Uygulama	Data (Veri)
6.) Sunum	Data
5.) Oturum	Data
4.) Taşıma	Segment (Bölüm)
3.) Ağ	Packet (Paket)
2.) Veri bağı	Frame (Çerçeve)
1.) Fiziksel	Bits (Bit)

Sarma (*encapsulation)*



OSI Katmanları Arasında Veri Aktarımı

7. Uygulama (Application) Katmanı

- Kullanıcı tarafından çalıştırılan tüm uygulamalar burada tanımlıdır. Örneğin;
  - HTTP
  - WWW
  - FTP
  - SMTP – E-mail (Simple Mail Transfer Protocol)

6. Sunum (Presentation) Katmanı

- Bu katman verileri, uygulama katmanına sunarken veri üzerinde kodlama ve dönüştürme işlemlerini yapar.
- Ayrıca bu katmanda;
  - veriyi sıkıştırma/açma,
  - şifreleme/şifre çözme,
  - EBCDIC'den ASCII'ye veya tam tersi yönde bir dönüşüm işlemlerini de yerine getirir.
- Bu katmanda tanımlanan bazı standartlar;
  - PICT ,TIFF ,JPEG ,MIDI ,MPEG, HTML.

EBCDIC (**E**xtended **B**inary **C**oded **D**ecimal **I**nterchange **C**ode = Genişletilmiş İkilik Kodlu Ondalık Değişim Kodu

- IBM tarafından kullanılan bir karakter kümesidir.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
4_			â	ä	à	á	ã	å	ç	ñ	[	.	<	(	+	!	4_ ($4_{hex} = 0100_{bin}$)
5_	&	é	ê	ë	è	í	î	ï	ì	ß	]	$	*	)	;	^	5_ ($5_{hex} = 0101_{bin}$)
6_	-	/	Â	Ä	À	Á	Ã	Å	Ç	Ñ	¦	,	%	_	>	?	6_ ($6_{hex} = 0110_{bin}$)
7_	ø	É	Ê	Ë	È	Í	Î	Ï	Ì	`	:	#	@	'	=	"	7_ ($7_{hex} = 0111_{bin}$)
8_	Ø	a	b	c	d	e	f	g	h	i	«	»	ð	ý	þ	±	8_ ($8_{hex} = 1000_{bin}$)
9_	°	j	k	l	m	n	o	p	q	r	ª	º	æ	¸	Æ	¤	9_ ($9_{hex} = 1001_{bin}$)
A_	µ	~	s	t	u	v	w	x	y	z	¡	¿	Ð	Ý	Þ	®	A_ ($A_{hex} = 1010_{bin}$)
B_	¢	£	¥	·	©	§	¶	¼	½	¾	¬		¯	¨	´	×	B_ ($B_{hex} = 1011_{bin}$)
C_	{	A	B	C	D	E	F	G	H	I		ô	ö	ò	ó		C_ ($C_{hex} = 1100_{bin}$)
D_	}	J	K	L	M	N	O	P	Q	R	¹	û	ü	ù	ú	ÿ	D_ ($D_{hex} = 1101_{bin}$)
E_	\	÷	S	T	U	V	W	X	Y	Z	²	Ô	Ö	Ò	Ó	Õ	E_ ($E_{hex} = 1110_{bin}$)
F_	0	1	2	3	4	5	6	7	8	9	³	Û	Ü	Ù	Ú		F_ ($F_{hex} = 1111_{bin}$)
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	

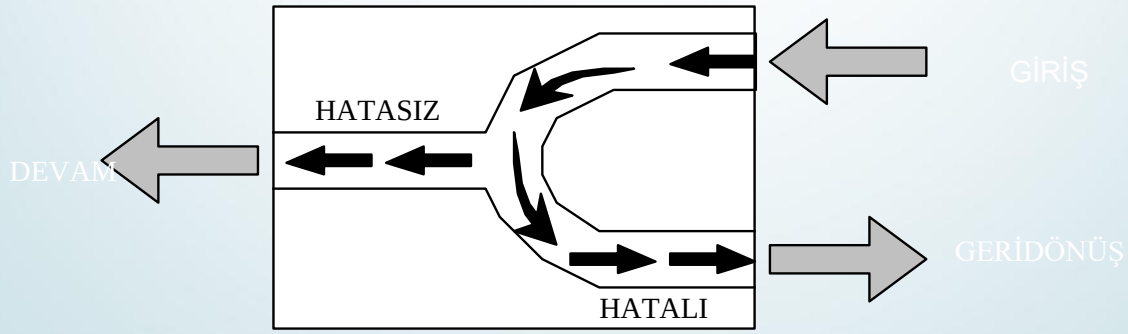
ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange)

- ANSI tarafından sunulan, standartlaşmış karakter kümesidir.
  - 33 tane basılmayan kontrol karakteri (ekranda basılmayan) ve 95 tane ekrana basılan karakter bulunur

	0	1	2	3	4	5	6	7
0	NUL	DLE	SP	0	@	P	`	p
1	SOH	DC1	!	1	A	Q	a	q
2	STX	DC2	"	2	B	R	b	r
3	ETX	DC3	#	3	C	S	c	s
4	EOT	DC4	$	4	D	T	d	t
5	ENQ	NAK	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	'	7	G	W	g	w
8	BS	CAN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[	k	{
C	FF	FS	,	<	L	\	l	|
D	CR	GS	-	=	M	]	m	}
E	SO	RS	.	>	N	^	n	~
F	SI	US	/	?	O	_	o	DEL

5. Oturum (Session) Katmanı

- Oturumun kurulması, yönetilmesi ve sonlandırılmasını sağlar.
- Haberleşmenin organize ve senkronize edilmesini sağlar.
- Eğer veri iletiminde hata oluşmuş ise tekrar gönderilmesine karar verir.

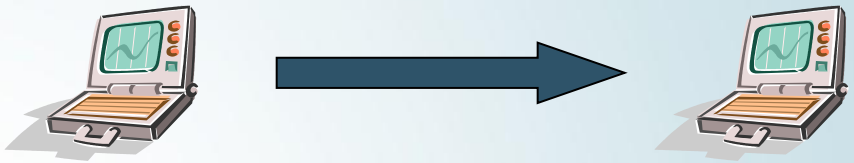


5. Oturum (Session) Katmanı

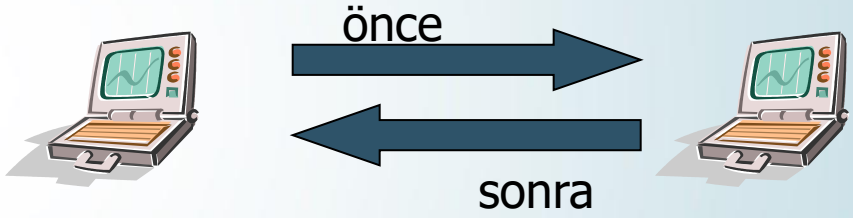
- Verinin güvenliğini sağlar.
- Bu katmanda çalışan protokollere örnek;
  - NFS (Network File System),
  - SQL (Structured Query Language)
  - ASP (AppleTalk Session Protocol)
  - Telnet

5. Oturum (Session) Katmanı İletişim Türleri

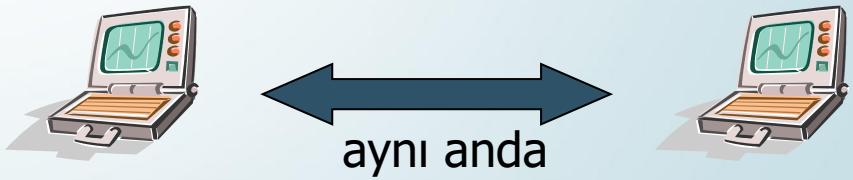
- Tek yönlü (Simplex)



- Yarı çift yönlü (Half-Duplex)



- Çift yönlü (Full-Duplex)



4. Taşıma (Transport) Katmanı

- Bu katman 5-7 ve 1-3 arası katmanlar arası bağlantıyı sağlar.
  - Üst katmandan aldığı verileri bölümlere (segment) ayırarak bir alt katmana iletir,
  - Bir üst katmana bu bölümleri birleştirerek sunar.
- İki düğüm arasında mantıksal bir bağlantının kurulmasını sağlar.

4. Taşıma (Transport) Katmanı

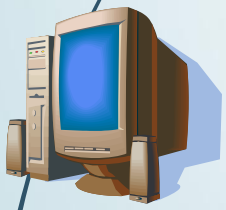
- Aynı zamanda akış kontrolü (flow control) kullanarak karşı tarafa gönderilen verinin yerine ulaşıp ulaşmadığını kontrol eder.
- Karşı tarafa gönderilen bölümlerin gönderilen sırayla birleştirilmesini sağlar.
- Örnek; TCP, UDP (User Datagram Protocol), SPX

4. Taşıma (Transport) Katmanı

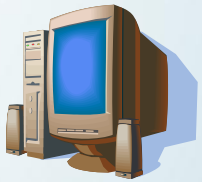
- **Connection Oriented Protokol (Bağlantı temelli protokol) :** Gönderen ve alan taraflar transfer işlemine başlamadan önce anlaşırlar. Gönderen-alana “seninle bir bağlantı kurmak istiyorum” diye istekte bulunur, sonra veri trafiği başlar. Veri aktarımı güvenli ve kayıpsız bir şekilde yapılmak isteniyorsa iletişim bağlantı temelli olarak gerçekleştirilmelidir. TCP bağlantı temelli bir protokoldür. Bu nedenle verinin kayıpsız iletimi önemli ise TCP gibi bir protokol seçilerek ağ yapılandırılmalıdır.

4. Taşıma (Transport) Katmanı

- **Connection Oriented Protokol (Bağlantı temelli protokol) :**



Veri gönderme isteği gönderir



Veri gönderme isteği kabul edilir

Bağlantı kurulur ve iletişim başlar

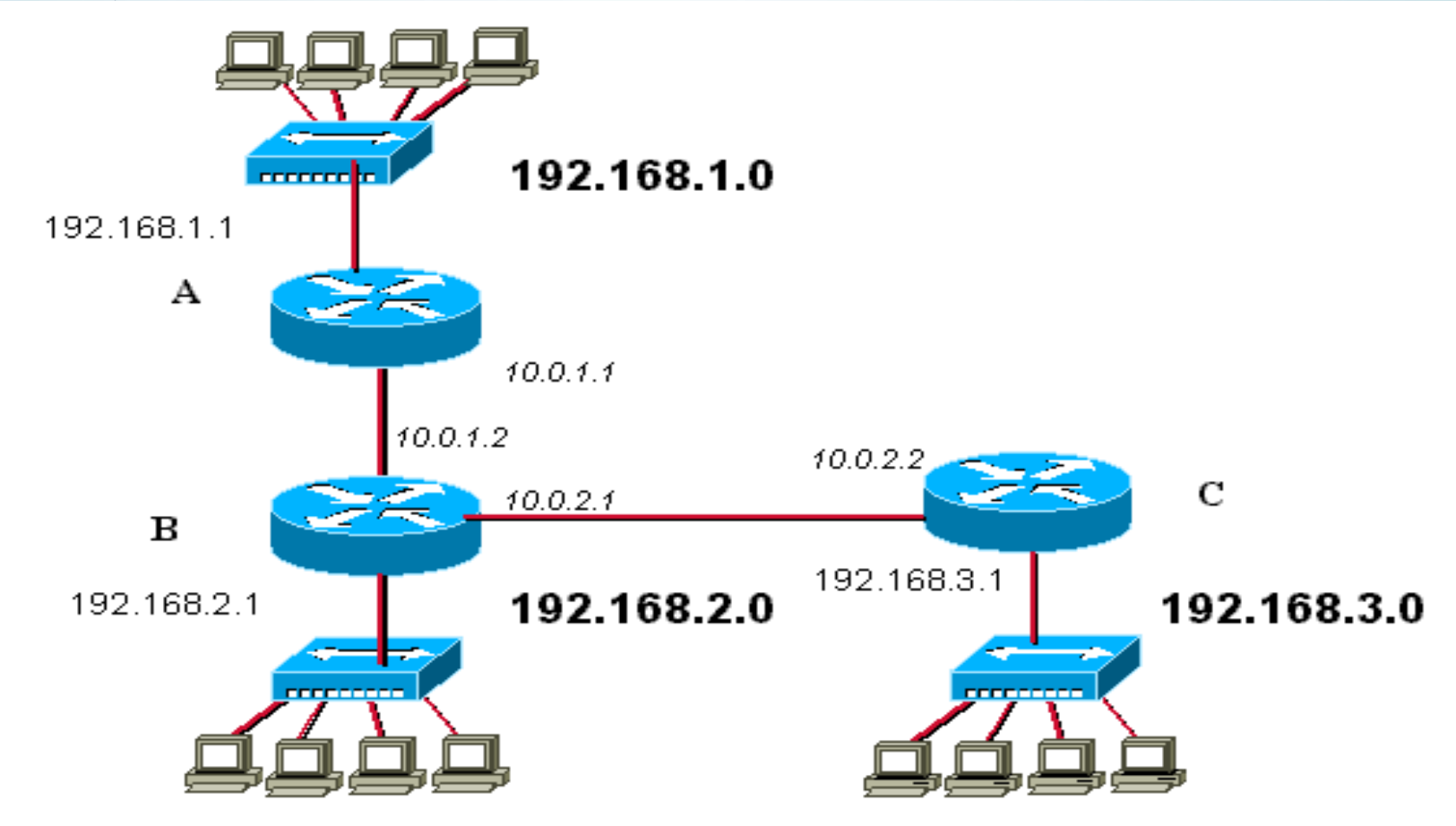
4. Taşıma (Transport) Katmanı

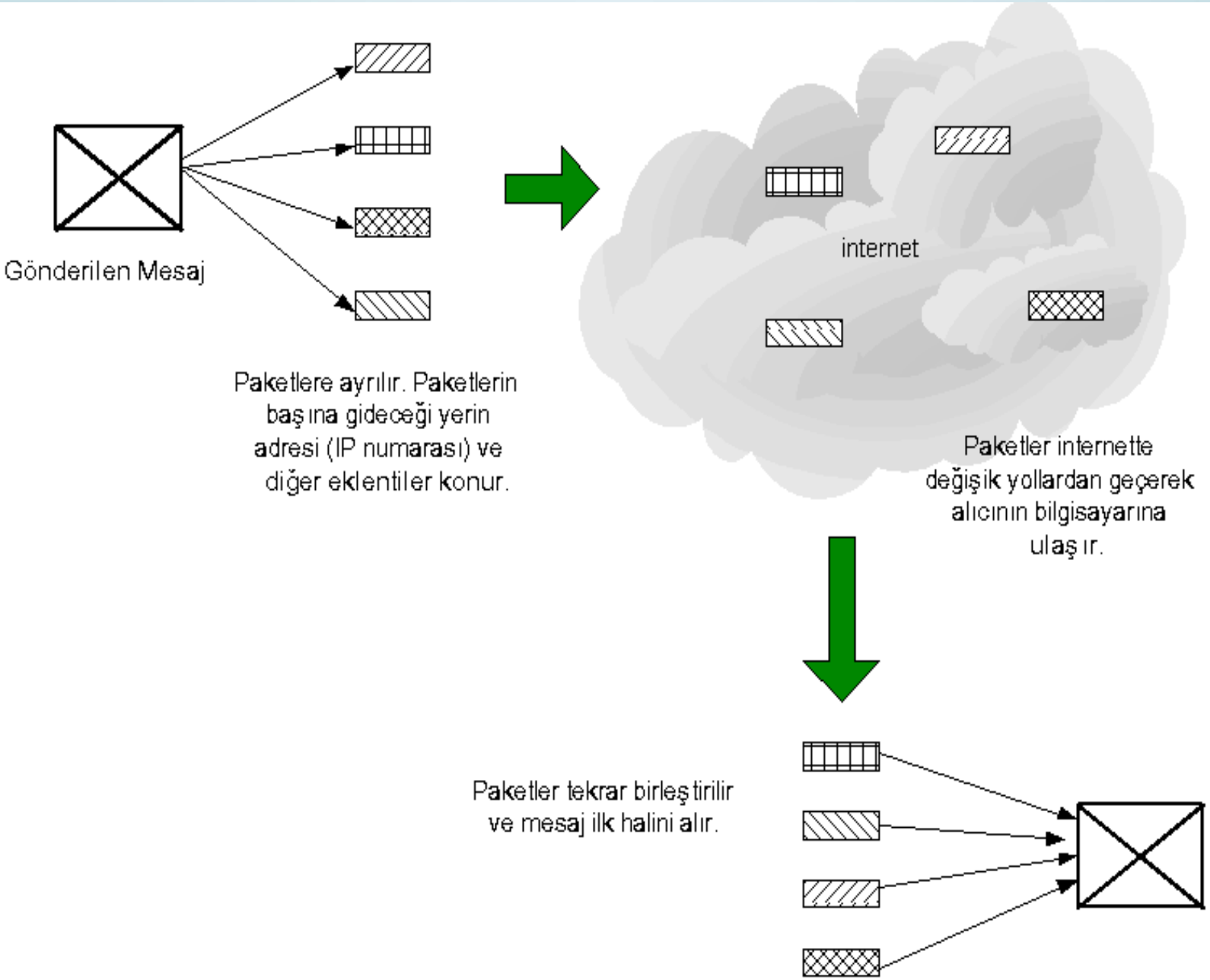
- **Connectionless Protokoller (Bağlantı temelli olmayan protokoller) :** Gönderen sadece veriyi gönderir. Verilerin gönderilip gönderilmediğini hiç kontrol etmez. Bu nedenle verinin kayıpsız bir şekilde gidip gitmemesiyle ilgilenmez. UDP böyle bir protokoldür. Genelde multiplayer oyunlar bu tip bir protokol ile iki bilgisayar arasındaki iletişimi sağlar. Verilerin güvenli gidip gitmediği kontrol edilmediği için TCP gibi bağlantı temelli bir protokole göre daha hızlı çalışır.

3. Ağ (Network) Katmanı

- Bu katmanda iletilen veri blokları paket olarak adlandırılır.
- Bu katman, veri paketlerinin ağ adreslerini kullanarak bu paketleri uygun ağlara yönlendirme işini yapar.
- Adresleme işlemlerini (Mantıksal adres ve fiziksel adres çevrimleri) yürütür.
- Yönlendiriciler (Router) bu katmanda tanımlıdırlar.
- Örnek; IP ve IPX.

3. Ağ (Network) Katmanı

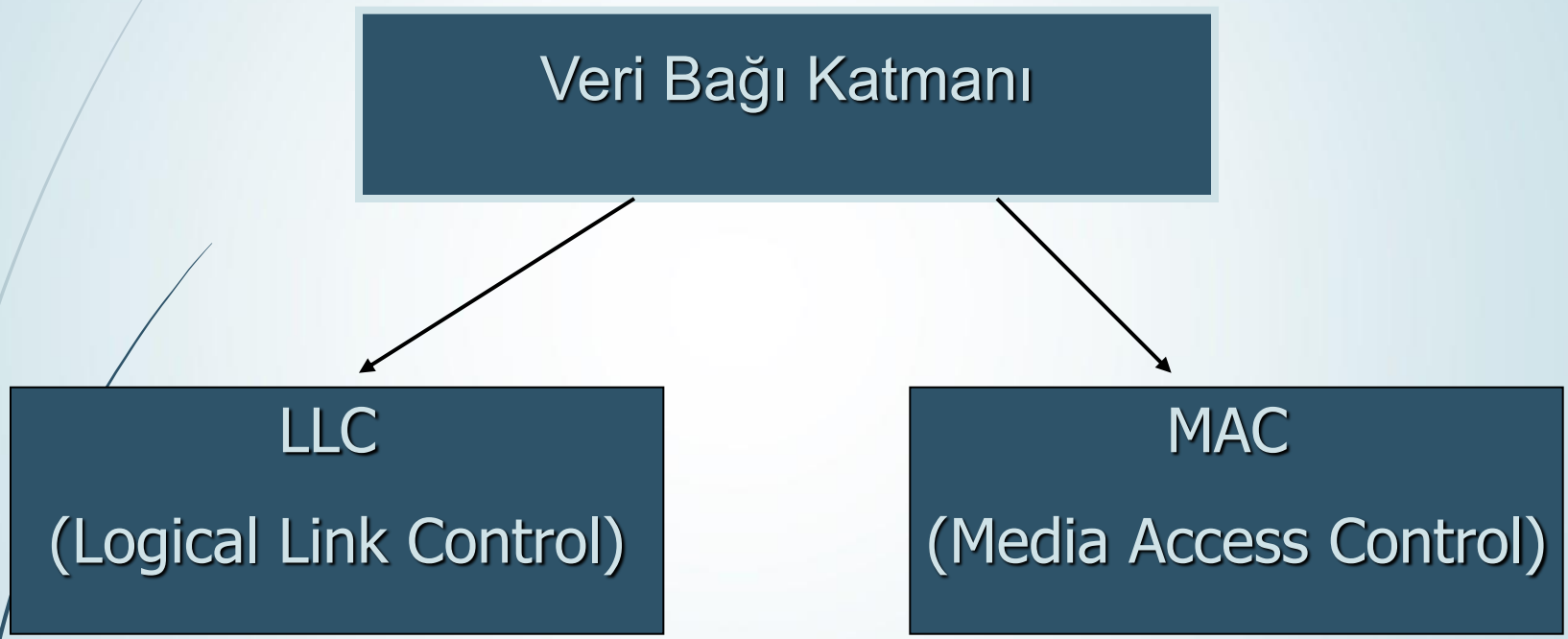



Gönderilen Mesaj
Paketlere ayrılır. Paketlerin başına gideceği yerin adresi (IP numarası) ve diğer eklentiler konur.
internet
Paketler internette değişik yollardan geçerek alıcının bilgisayarına ulaşır.
Paketler tekrar birleştirilir ve mesaj ilk halini alır.

2. Veri Bağı(Data Link) Katmanı

- Ağ katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek çerçeve (frame) halinde fiziksel katmana iletme işinden sorumludur.
- İletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder, eğer çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlar.
- Ayrıca ağ üzerindeki diğer bilgisayarları tanımlama, kablonun o anda kimin tarafından kullanıldığının tespitini yapar.
- Örn: Ethernet, Frame Relay, ISDN, Switch ve Bridge

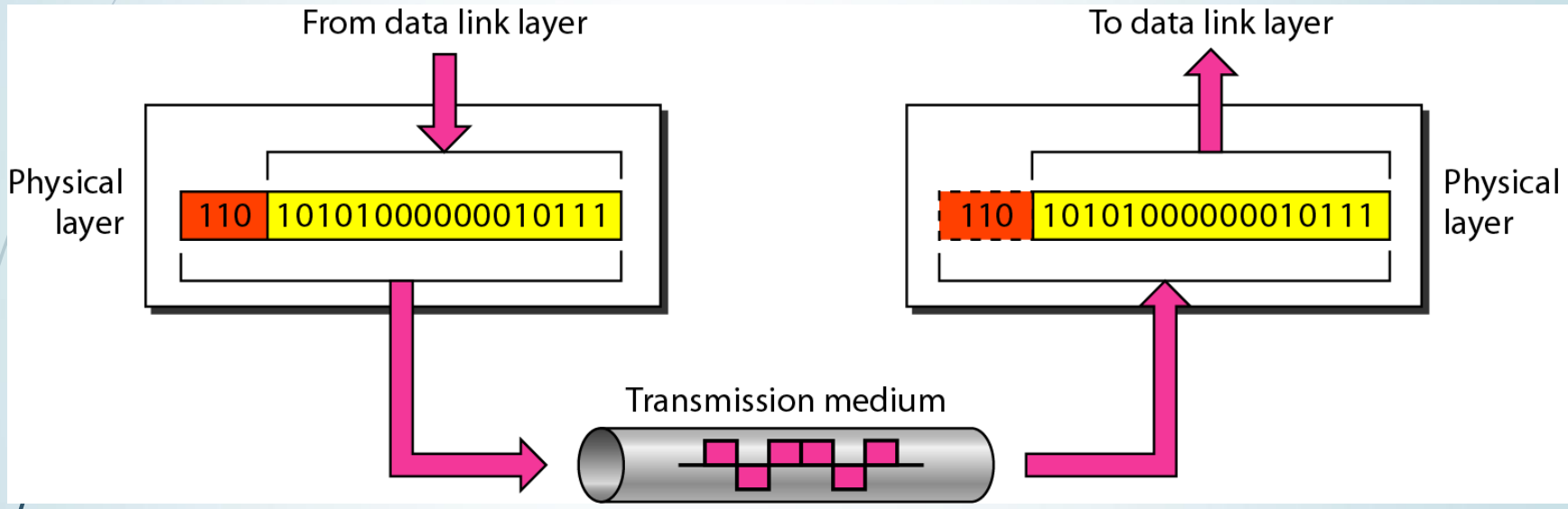
Veri Bağı Katmanı İki Alt Katmandan Oluşur;



- **Media Access Control (MAC)**
  - MAC alt katmanı veriyi hata kontrol kodu (CRC), alıcı ve gönderenin MAC adresleri ile beraber paketler ve fiziksel katmana aktarır.
  - Alıcı tarafta da bu işlemleri tersine yapıp veriyi veri bağlantısı içindeki ikinci alt katman olan LLC'ye aktarmak görevi yine MAC alt katmanına aittir.
- **Logical Link Control (LLC)**
  - LLC alt katmanı bir üst katman olan ağ katmanı için geçiş görevi görür. Protokole özel mantıksal portlar oluşturur (*Service Access Points*, SAP). Böylece kaynak makinada ve hedef makinada aynı protokoller iletişime geçebilir (örneğin TCP/IP).
  - LLC ayrıca veri paketlerinden bozuk gidenlerin (veya karşı taraf için alınanların) tekrar gönderilmesinden sorumludur. *Flow Control* yani alıcının işleyebileğinden fazla veri paketi gönderilerek boğulmasının engellenmesi de LLC'nin görevidir.

1. Fiziksel (Physical) Katmanı

- Verilerin fiziksel olarak gönderilmesi ve alınmasından sorumludur.
- Bu katmanda tanımlanan standartlar taşınan verinin içeriğiyle ilgilenmezler. Daha çok işaretin şekli,fiziksel katmanda kullanılacak konnektör türü, kablo türü gibi elektriksel ve mekanik özelliklerle ilgilenir.
- Hub'lar fiziksel katmanda tanımlıdır.
- 10BaseT, 100BaseT, UTP, RJ-45, IEEE 802.5 (Token Ring) vb. standartlar


From data link layer
To data link layer
Physical layer
110
1010100000010111
110
1010100000010111
Physical layer
Transmission medium

1. Fiziksel (Physical) Katmanı

- **Baseband :** Fiziksel medya (yani kablo) üzerinde komünikasyon sağlamak amacıyla, sadece bir tek band kullanılmasına izin veren haberleşme standardıdır. Yani kablodan aynı anda tek bir sinyal iletilebiliyorsa bu basebanddır.

1. Fiziksel (Physical) Katmanı

- **Broadband :** Baseband networklerin tam tersidir. Burada fiziksel kablo, sanal olarak birçok kanala bölünmüştür. Yani aynı kablodan, aynı anda farklı frekanslar kullanarak birden fazla sinyal iletmek de mümkündür ve bu teknik Broadband olarak anılır.

AĞ TEMELLERİ

VERİ BAĞI KATMANI ve Ethernet

Ethernet İle İlgili Temel Bilgiler

- Günümüzde bir çok LAN teknolojisinden söz edilse de, Ethernet açık ara farkla en yaygın LAN teknolojisidir. Ethernet ilk ortaya çıkışından itibaren teknolojisi ve üretim haklarıyla herkese açıktır. Kullandığı teknolojinin üretimi kolaydır ve ucuza mal edilebilir. Aynı zamanda güvenilir olduğu ve kullanıcıların ihtiyaçlarını karşıladığı için en yaygın yerel ağ teknolojisi haline gelmiştir. En yaygın teknoloji olması ethernetin üreticiler için büyük bir pazar haline gelmesine ve sürekli geliştirilmesine yol açmaktadır.

Ethernetin tarihi

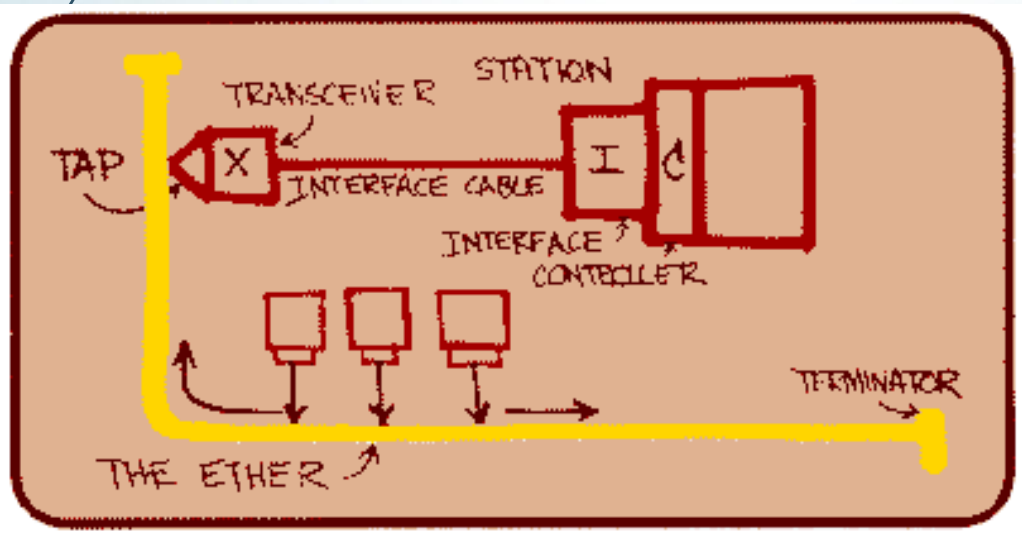
- Ethernet Xerox firmasının Palo Alto araştırma merkezinde 1970'li yıllarda Dr. Robert M. Metcalfe tarafından geliştirildi. Metcalfe "geleceğin ofisi" projesi üzerinde çalışıyordu ve elinin altında dünyanın ilk workstation bilgisayarlarından biri olan Xerox Alto bilgisayarlar bulunuyordu.

Ethernetin tarihi

- 1972 yılının sonlarında, Metcalfe ve Xerox'ta çalışan iş arkadaşları Xerox Alto'ları birbirine bağlamak için deneysel olarak Ethernet'i geliştirdiler. Böylece Alto bilgisayarlar diğer sunucular ve lazer yazılıcılar birbiriyle haberleşebiliyordu. İlk Ethernetin çalışma hızı Alto'larla uyumlu olması için Alto'nun çalışma hızı ile aynı tutulmuş ve sonuçta ağ 2.94 Mega Bit/Saniye hızında çalışmıştır. İlk ethernet tek parça bir koaksiyel kablo kullanıyordu.

Ethernetin tarihi

Tarih	Ethernet
1970	LAN network çalışmaları
1982	IEEE 802.3
1995	Fast Ethernet
1998	Gigabit Ethernet



Ethernetin tarihi

- Bu diyagram...Dr. Robert M. Metcalfe tarafından 1976 yılının haziran ayında National Computer Conferance'da ethernetin doğuşu sırasında çizildi.
- Ethernetin doğuşundan beri bu diyagramdaki temellere dayanan kullanım süregeldi.

Ethernetin tarihi

- Metcalfe önce Alto Aloha Network olan sistemin ismini 1973 yılında "Ethernet" olarak değiştirdi. Böylece sistemin sadece Alto bilgisayarlarda değil tüm bilgisayarlarda çalışabileceğini vurgulamak istiyordu. Ethernet kelimesi bir zamanlar tüm uzayı doldurduğuna ve elektromanyetik sinyallerin aktarımını sağladığına inanılan "ether" den geliyordu. Metcalfe'nin sisteminde de veri bitleri tüm sistemlere ulaştığı için sonuçta "Ethernet" doğmuş oldu.

Ethernetin tarihi

- 1979 yılına kadar sadece Xerox içinde kullanılan Ethernet'in resmi duyurusu 1980 yılında yapıldı. Xerox, DEC(Digital Equipment Corporation) ve Intel firmaları ile beraber, sonradan "DIX Standart" olarak anılan ethernet standardını yayınladı. DIX standardı koaksiyel kablo üzerinden 10 MBs hızında çalışan etherneti tanımlamıştır. Böylece ethernet, firma içi deneysel bir çalışmadan herkese açık gerçek bir ürün haline gelmiş oldu.

Ethernet vs IEEE 802.3

- DIX standardından sonra Ethernet, Institute of Electrical and Electronics Engineers (IEEE)'in 802 kodlu komisyonu tarafından geliştirilmeye devam etti. IEEE 1985 yılında "IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications" şeklinde bir isimle yeni ethernet standardını yayınladı. İzleyen dönemde IEEE standardı International Organization for Standardization (ISO) tarafından yürütülmeye devam etti. ISO günümüzde bilgisayar ağları ile ilgili tüm standarları yürüten kuruluştur.

Ethernet vs IEEE 802.3

- 1985 yılından itibaren üretilen tüm ürünler IEEE 802.3 standardına göre üretilmektedir. Aslında bu ürünleri "IEEE 802.3 CSMA/CD" standardını kullanan ürünler olarak tanımlamak daha doğrudur. Ama dünya çapında hala genel olarak "Ethernet" kelimesi tüm bu ürünler ve dahil oldukları teknolojiyi tanımlamak için kullanılmaktadır.
- Ethernet tek bir ağ teknolojisi olmaktan çok, aynı bus topolojisini, frame yapısını ve network access(ağ erişimi) metodunu kullanan ağ teknolojileri ailesini tanımlar.

Ethernet/IEEE 802 Standartları

- IEEE, 1980 yılı başlarında LAN standartlarını belirlemeye başlamış ve günümüzde yoğun olarak kullanılan standartların temelini atmıştır. IEEE 802.x protokolleri bu çalışmaların sonucu olarak ortaya çıkmıştır. Bu protokole standardında her tanımlamaya 802.3 benzeri bir numara verilmiştir.

Protokol Adı	Açıklama
802.1	Ağlar ve sistem yönetimi hakkında genel tanımlamalar.
802.2	LLC alt katmanını tanımlar.
802.3	Ethernet - CSMA/CD yol erişim yöntemi.
802.3u	100Base-T.
802.3z	Gigabit Ethernet.
802.4	Jetonlu Yol (Token Bus) tanımlaması.
802.5	Jetonlu Halka (Token Ring) tanımlaması.

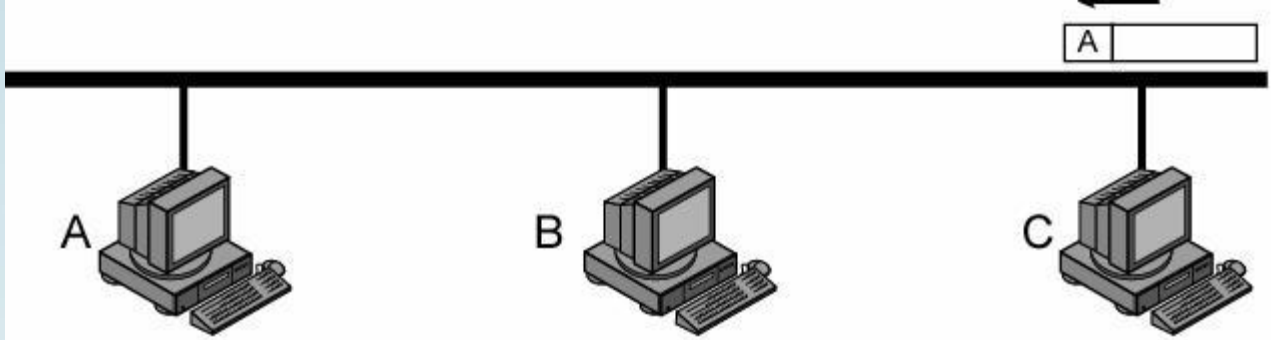
Günümüzde en yaygın kullanılan!

- **100baseT:** Saniyede 100 Mb/S hızında veri taşıyan çift bükümlü kablo kullanan yerel alan ağları için Ethernet standardı.

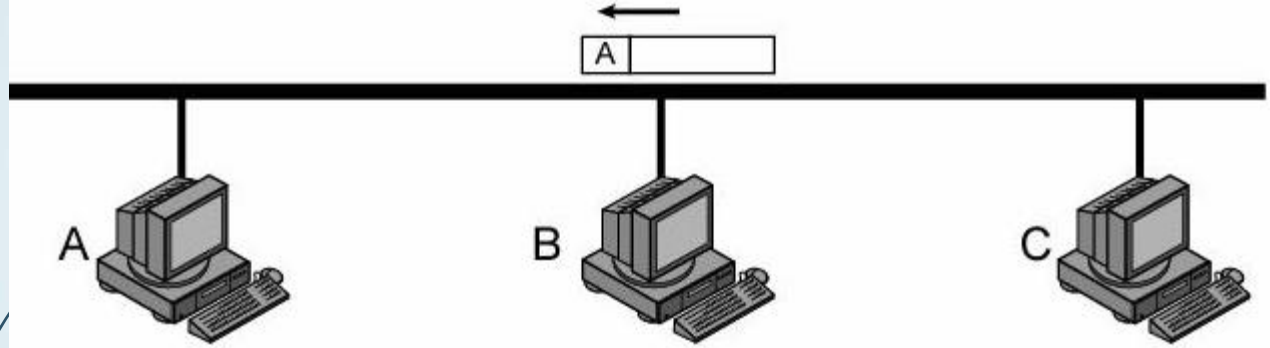
Ethernet nasıl çalışır?

Etherneti geliştiren ekip üç ana problemi çözmek zorundaydılar:

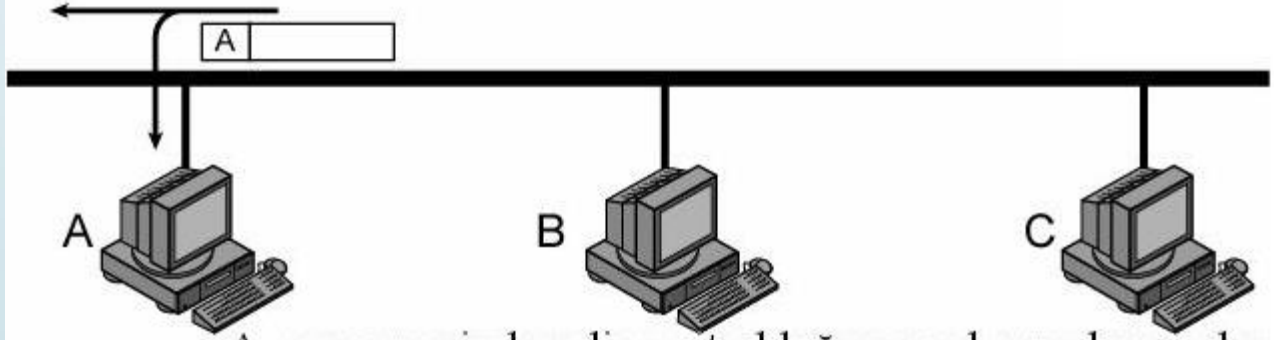
- Kablo üzerinden veri nasıl gönderilecek
- Gönderen ve alıcı bilgisayarlar nasıl tespit edilecek
- Belli bir anda kabloyu kimin kullanılacağına nasıl karar verilecek



C bir çerçeveyi A bilgisayarına gönderir



Çerçevenin adresi B olmadığından, B bunu dikkate almaz



A, çerçevenin kendine ait olduğunu anlar ve bunu alır, çerçeve kablo boyunca yoluna devam eder.

Ethernet'in bu özelliği ciddi bir güvenlik açığına yol açabilir. Packet Sniffer olarak adlandırılan programlar, bilgisayara gelen veri paketlerini MAC adresi ne olursa olsun alıp kullanmaya izin verirler. Bu tip programlar iyi niyetle kullanıldığında problemlerin çözümüne yarayabileceği gibi, yerel ağınızda meraklı bir kullanıcının sizin aslında başka bir makinaya göndermekte olduğunuz her dosyayı izlemesine neden olabilir.

Bir Ethernet kartı networkdeki bütün frameleri yakalar.Ancak eğer hedef adresi kendisi değilse frame ile ilgilenmez.Bu durumdan sistemin haberi olmadığından uygulama programları ve işletim sistemleri (dolayısıyla kullanıcı) hiçbir şekilde etkilenmez.

Ancak frame içindeki hedef adres değeri FF FF FF FF FF FF ise bu bir Genel yayın adresidir ve bu frame tüm Ethernet kartları tarafından alınır ve işlerim sistemine aktarılır.

CSMA/CD (Carrier Sense Multiple Access/Collision Detect)

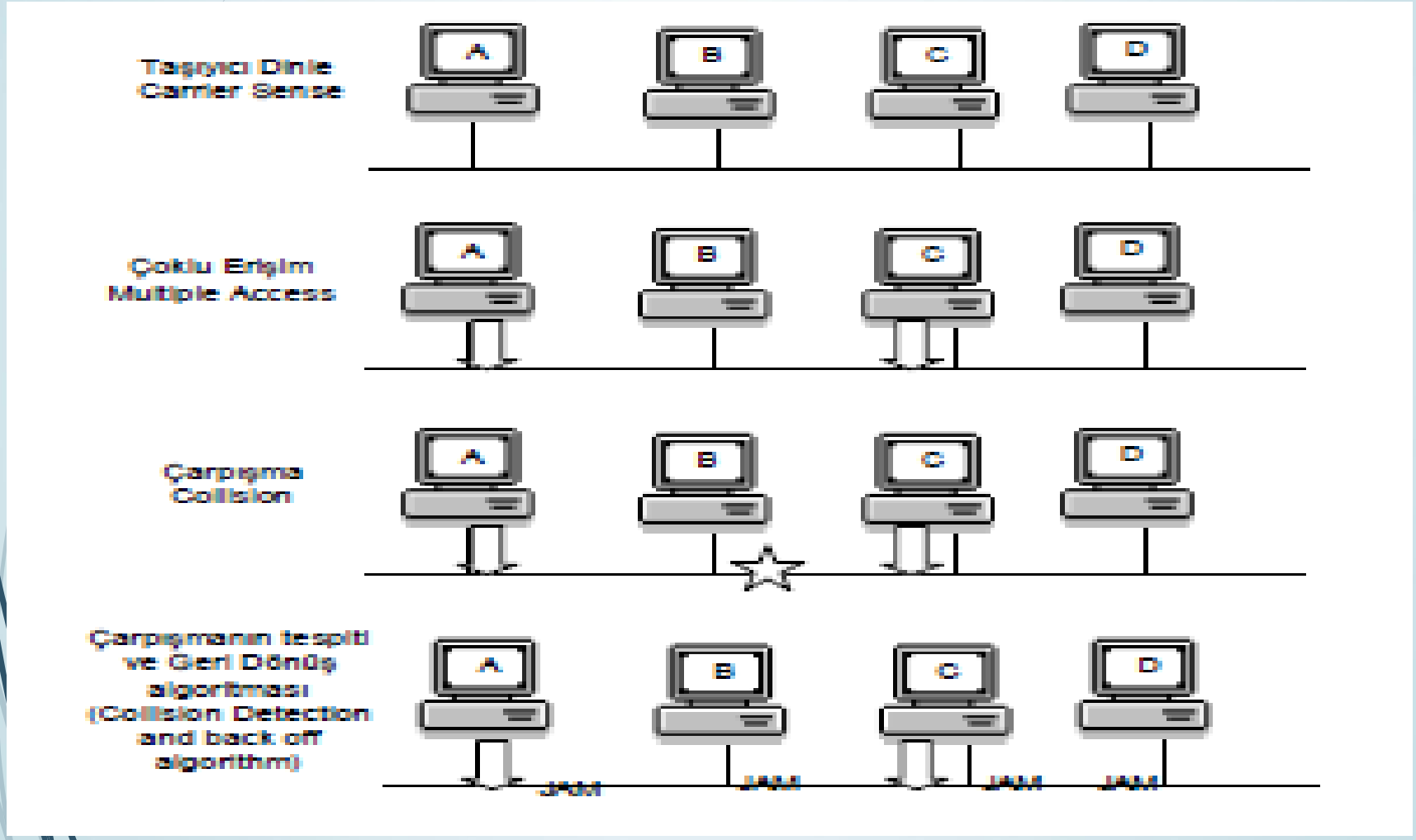
- Ethernet ve IEEE 802.3 standartlarında kullanılan bir protokol.
- Çarpışmayı bulma (Collision Detect)
  - Bir ethernet kartı bilgi göndereceği zaman ağ trafiğini izler.
  - Ağ kablosunda veri yoksa verisini kabloya bırakır.
  - Eğer kabloda veri varsa diğer veri hedefine gidinceye kadar beklenir. Ardından veriyi gönderir.
  - Eğer bu işlemler başarısız olursa çarpışma meydana gelir.

CSMA/CD

CSMA/CD erişim metodunda, listen-before-transmit iletişiminden önce dinle modunda çalışmayla veri network cihazlarına iletilir.

Bunun anlamı cihaz veri iletmek istediği zaman ilk olarak aktarım ortamının meşgul olup olmadığı kontrol etmelidir. Eğer node, ağın meşgul olduğunu tanımlarsa, tekrar denemeden önce rastgele bir süre bekleyecek. Eğer node networkün meşgul olmadığını tanımlarsa node iletme ve dinleyişe başlayacak. Node diğer istasyonlara, aynı anda iletmiyor olduğundan emin olmak için dinler.

Ağ üzerinde çarpışma oluşması



Ağ üzerinde çarpışmanın Önlenmesi

Kablo boşta olduğunda her Ethernet ara yüzüne sahip cihaz eşit hakka sahiptir ve veri aktarımına başlayabilir. Buna Multiple Access denir. Bir ethernet ağında bilgisayar üzerinde çalışan işletim sistemi veya kullanıcısı önemli değildir. Bir DOS makinası ethernetin kabloyu kullanma şansı açısından W2000 server ile aynıdır.

Bazı durumlarda iki sistem kablonun boş olduğunu tespit ederek aynı anda veri aktarımına başlayabilir. Bu durumda iki tarafın yolladığı veri çakışır(Collision). Ethernet kartları çakışmayı hemen tespit ederler(Collision Detection).

Ağ üzerinde çarpışmanın Önlenmesi

Eğer ağ çok yoğun kullanılıyorsa, aynı frame/veri paketi gönderilirken birden fazla çakışma olabilir. Bu durumda sistemler rastgele belirlenen bekleme süresini uzatmaya başlarlar. Burada süre rastgele belirleniyorsa nasıl daha uzun veya kısa olabilir diye bir soru akla gelebilir. Sürenin rastgele olması her iki tarafında aynı süre bekleyip, sonra da yine aynı anda aktarım yapmalarının önüne geçmek için rastgeledir. Örneğin her iki tarafta birden ona kadar bir sayı tutar ve o kadar milisaniye bekler. Ancak süre belirlenirken, aynı paketin gönderiminde üstüste çakışma oluyorsa(ağda yoğun trafik varsa) süre 1-10 arası değil belki 50-100 arasında seçilir.

Ağ üzerinde çarpışmanın Önlenmesi

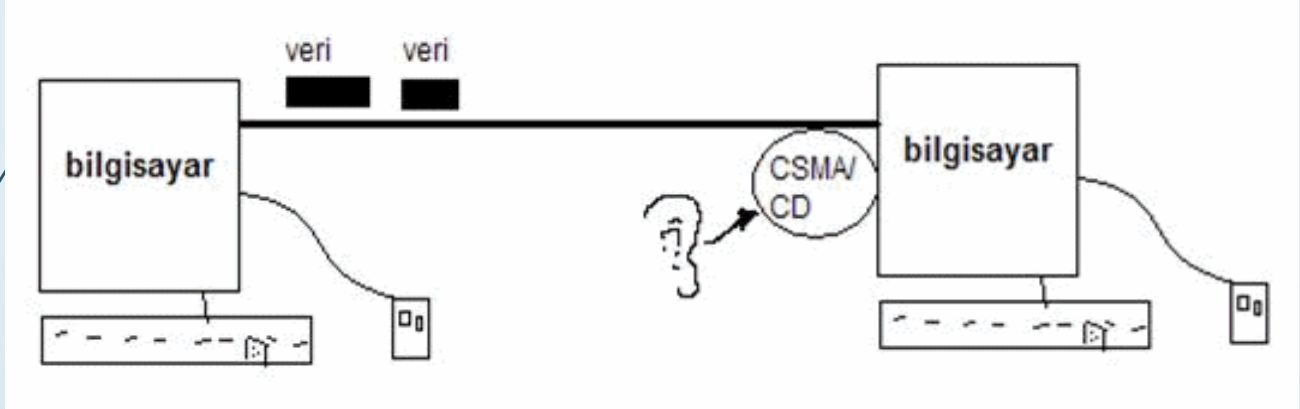
Bu noktada ethernetin diğer ağ teknolojilerinde de olduğu gibi veri aktarımını %100 garanti etmediğini görüyoruz. Bu açık üst katman protokollerinin sağladığı veri kontrolü ile telafi edilir. Bir paket yolda kaybolursa veya 16 denemede de yollanamayıp iptal edilirse, alıcı taraftaki üst katman protokol (TCP/IP kullanılıyorsa; TCP) gönderen taraftaki TCP'ye gelen veride bir eksiklik olduğunu bildirecek ve tekrar yollanmasını isteyecektir.

CSMA/CD

CSMA/CD fiziksel katman topolojisi ilk zamanlar pasif ortak yoldan ibaretti; ancak anahtar (switch) cihazların uygulamada yaygınlaşmasıyla birlikte yıldız-anahtarlamalı yol da kullanılmaktadır. 802.x protokolleri LAN fiziksel katmanlarında çoğunlukla Manchester kodlaması veya 4B5B diye adlandırılan kodlama tekniği kullanılır.

CSMA/CD ve MAC Kavramları

- **CSMA/CD** (Carrier Sense Multiple Access / Collision Detection') protokolü, IEEE Network' ler tarafından kullanılır. İletişim hattına bilgi paketinin nasıl yerleştirileceğini belirler. Bir birim network hattına bilgisini bırakmadan önce, başka bir birimin hatta bilgi bırakıp bırakmadığını anlamak amacıyla, hattı dinler.

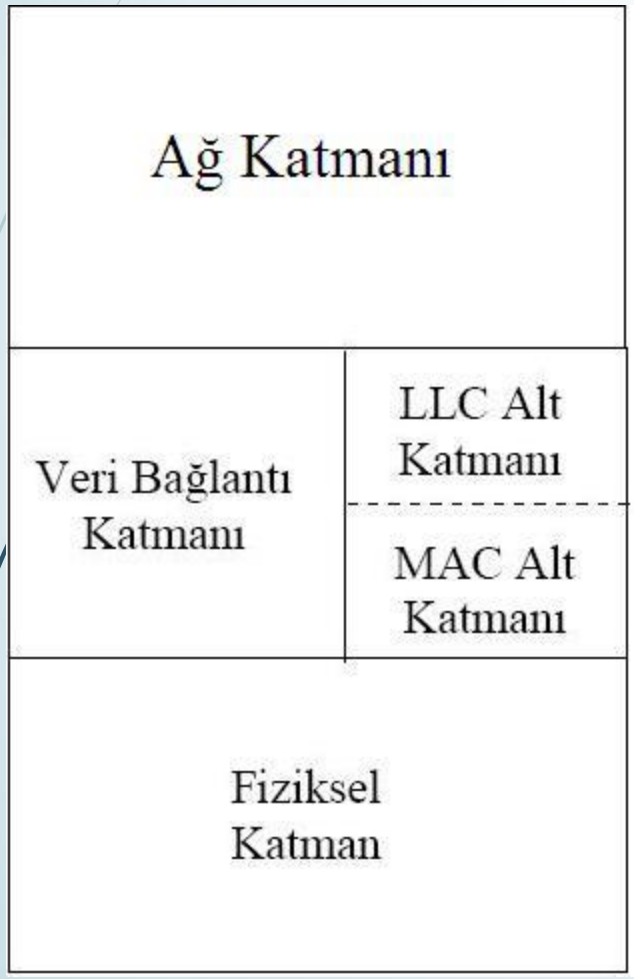


- **MAC Adresi:** Ethernet Network cihazlarına, tanınabilmeleri için, hexadecimal ve dünyada bir eşi daha olmayan seri numarası verilir. Bu numaralar, üretici firmalar tarafından fabrikada verilmektedir.

MAC adresleri

- Her Ethernet kartı ayrı bir MAC adresine sahiptir. MAC adresi 48 bittir. Bunun neticesinde 2^48 adet farklı Ethernet kartı bulunabilir.
- IEEE üreticiye 24 bitlik bir üretici kodu verir. Bu kod Organizationally Unique Identifier(OIU) olarak adlandırılıyor ve her üreticiye farklı bir kod veriliyor. Üretici her ağ kartı için ilk 24 biti kendi OIU numarası, geri kalan 24 biti ise kartın seri numarası(Device ID-başka bir karta daha verilmeyecek) olmak üzere MAC adresi belirleyip, ağ kartının üzerinde programlanabilir bir çipe bu numarayı yazar. Böylece bu kartın dünyada eşi olmayan bir MAC adresi olur.

VERİ BAĞLANTI KATMANI



Fiziksel Adresleme ve ağ ilingesini kullanarak verinin ortam içinde güvenilir bir biçimde aktarımını sağlar.

Veri Bağlantı Katmanı 2 Alt Katmandan oluşmaktadır. Bunlar:

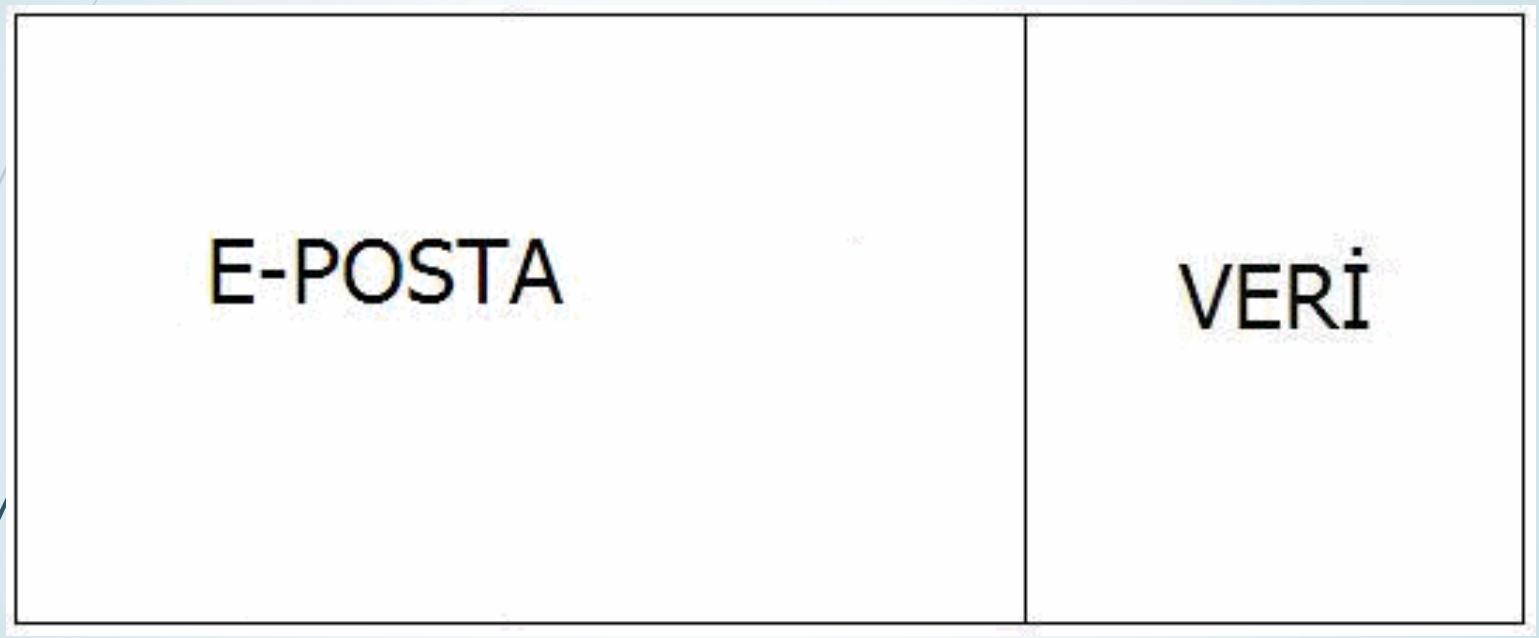
- LLC Alt Katmanı
- MAC Alt Katmanı

Fiziksel Katmandan bir önceki katmandır.

MAC ALT KATMANI

- Ağ katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek çerçeve (frame) halinde fiziksel katmana iletme işinden sorumludur.
- İletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder, eğer çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlar.

MAC ALT KATMANI



E-Posta’nın OSI modeli katmanlardan geçerken meydana gelen dönüşümleri

MAC ALT KATMANI

- MAC alt katmanı veriyi hata kontrol kodu (CRC), alıcı ve gönderenin MAC adresleri ile beraber paketler ve fiziksel katmana aktarır.
- Alıcı tarafta da bu işlemleri tersine yapıp veriyi veri bağlantısı içindeki ikinci alt katman olan LLC'ye aktarmak görevi yine MAC alt katmanına aittir.

LLC VE HATA TESPİTİ

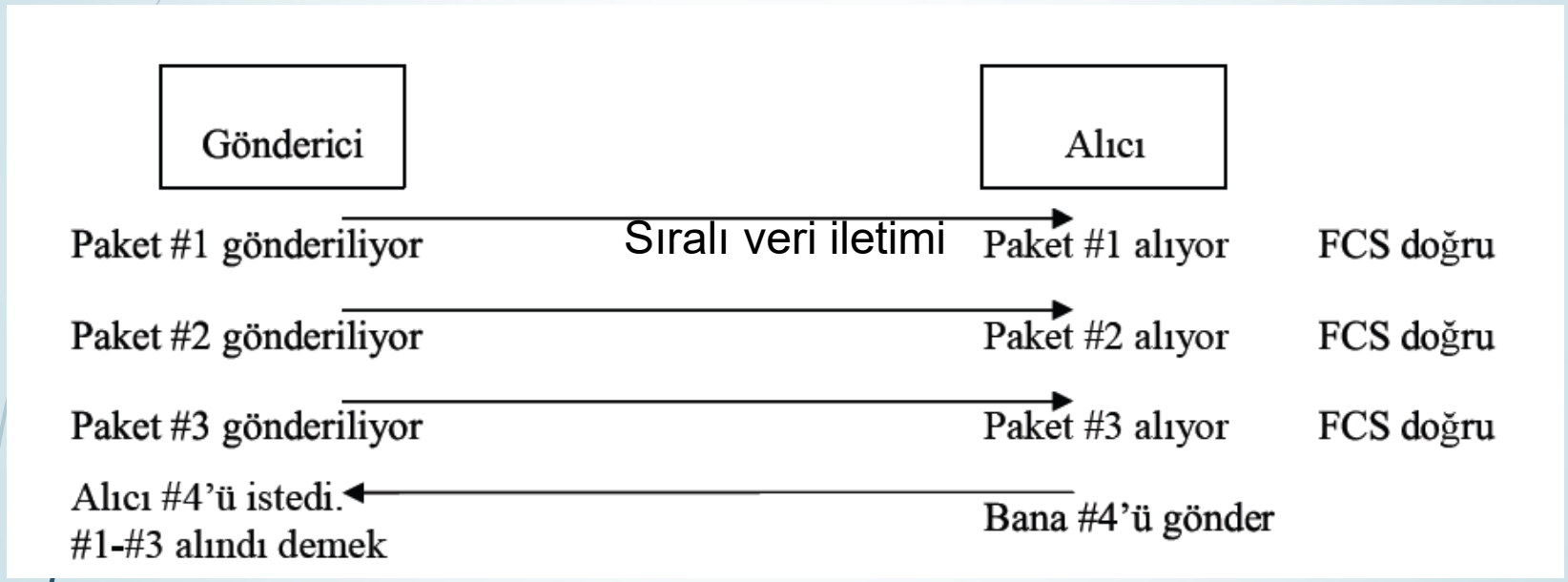
Logical Link Control (LLC)

- LLC alt katmanı bir üst katman olan ağ katmanı için geçiş görevi görür. Protokole özel mantıksal portlar oluşturur(Service Access Points, SAPs). Böylece kaynak makinada ve hedef makinada aynı protokoller iletişime geçebilir(örneğin TCP/IP<-->TCP/IP).

LLC’NİN GÖREVİ

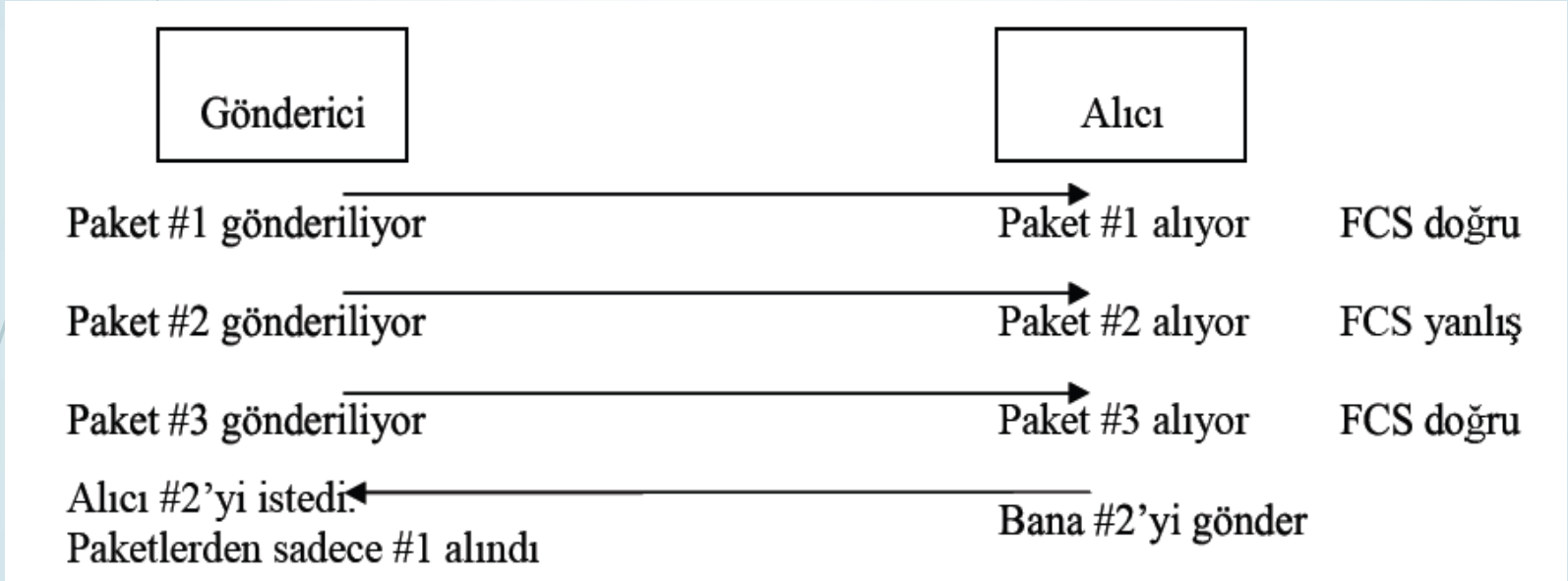
- LLC ayrıca veri paketlerinden bozuk gidenlerin(veya karşı taraf için alınanların) tekrar gönderilmesinden sorumludur. Flow Control yani alıcının işleyebileğinden fazla veri paketi gönderilerek boğulmasının engellenmesi de LLC'nin görevidir.

Hata Tespiti



Sıralı veri iletimi

Hata Tespiti



Hata giderme

CRC (Cydic Redundancy Check)

- Uygulaması kolay ve güvenliği güçlü bir tekniktir. CRC tekniği veri çerçevelerinin koruması için kullanılır.

- 90,69,66,82,65,79,78,69 P=17

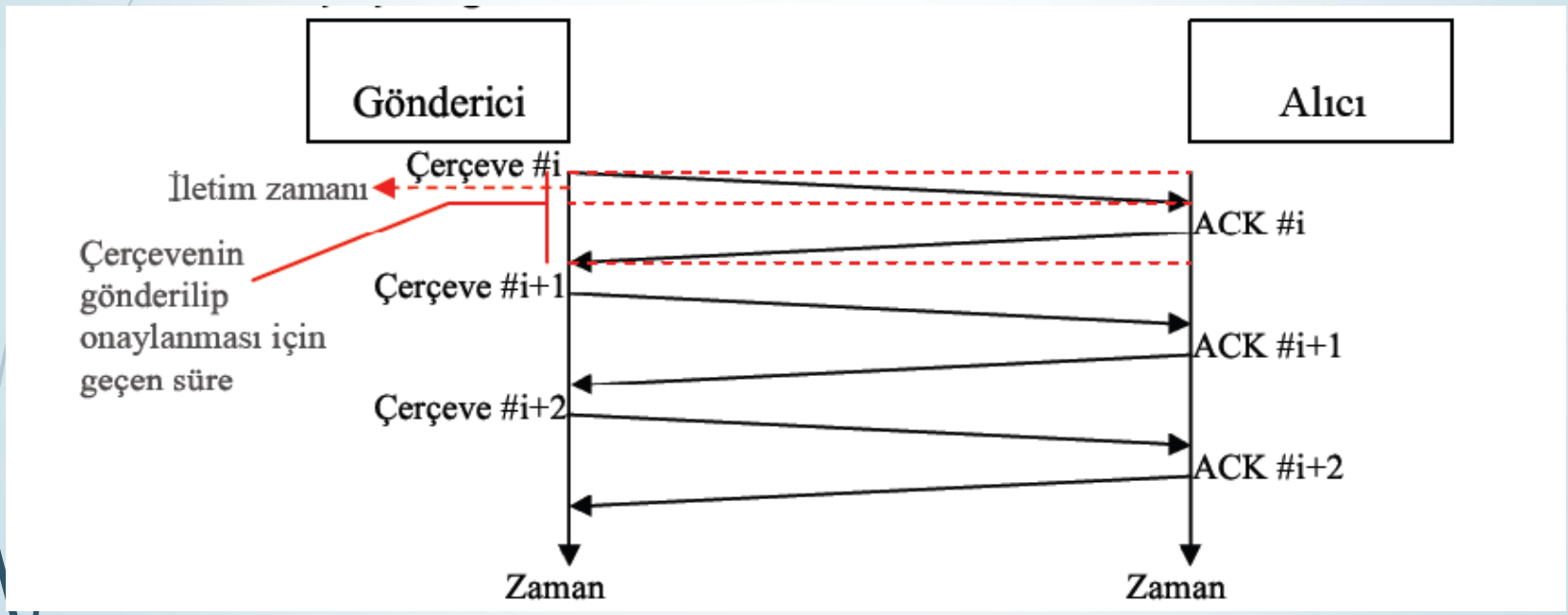
598/17=35, kalan=3

ARQ (Otomatik Tekrar İsteği)

- İletim sırasında verinin bütünlüğü ve doğru bir şekilde iletilmesi için ARQ kullanılır.

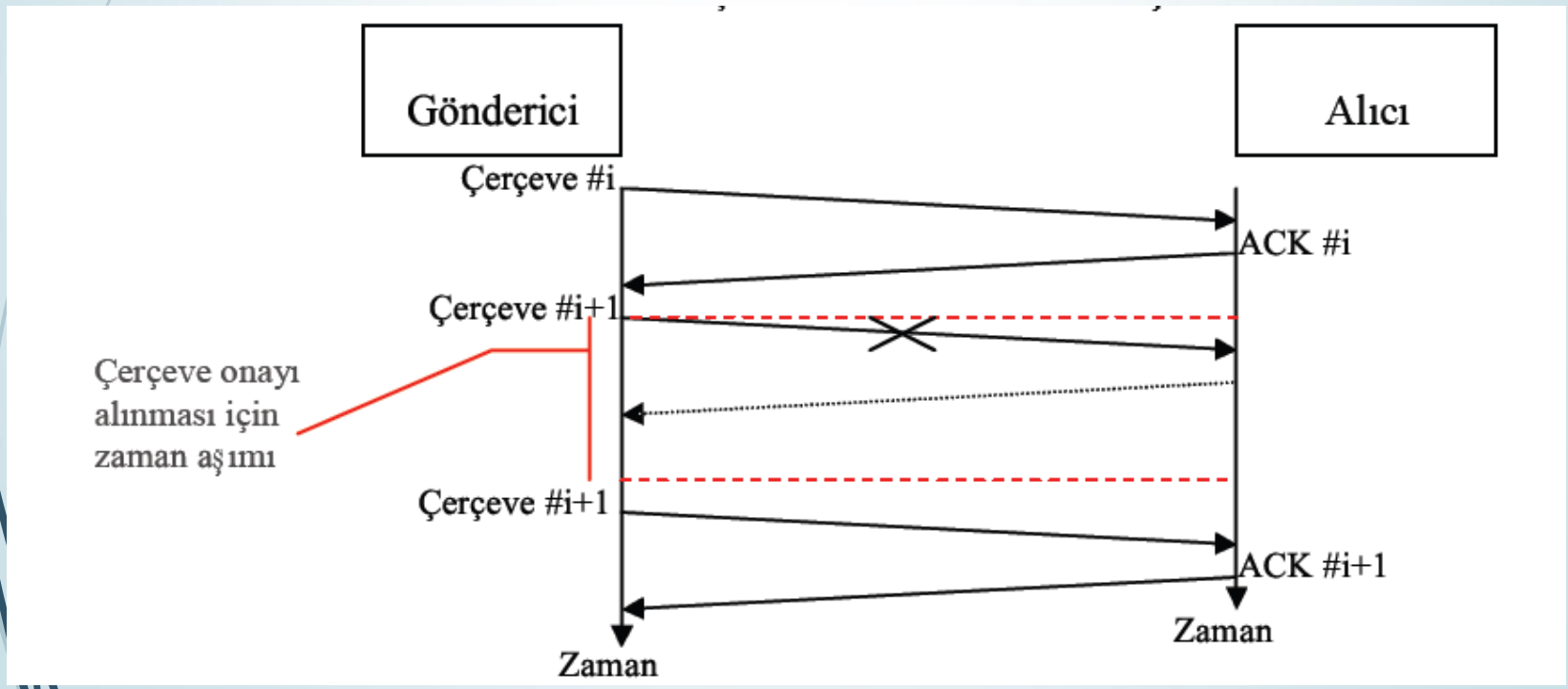
Dur ve Bekle Protokolü

- Normal veri akışı



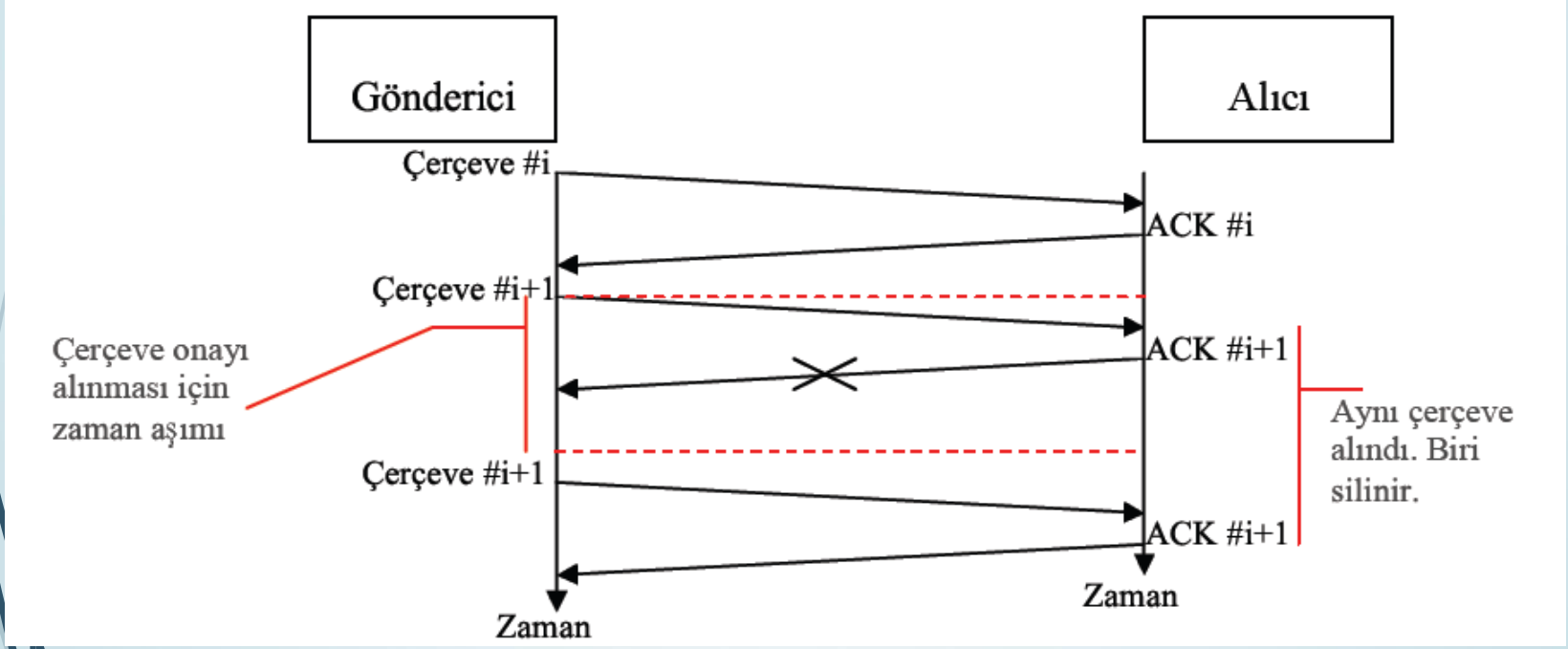
Dur ve Bekle Protokolü

- Gönderilen çerçevenin bozulması



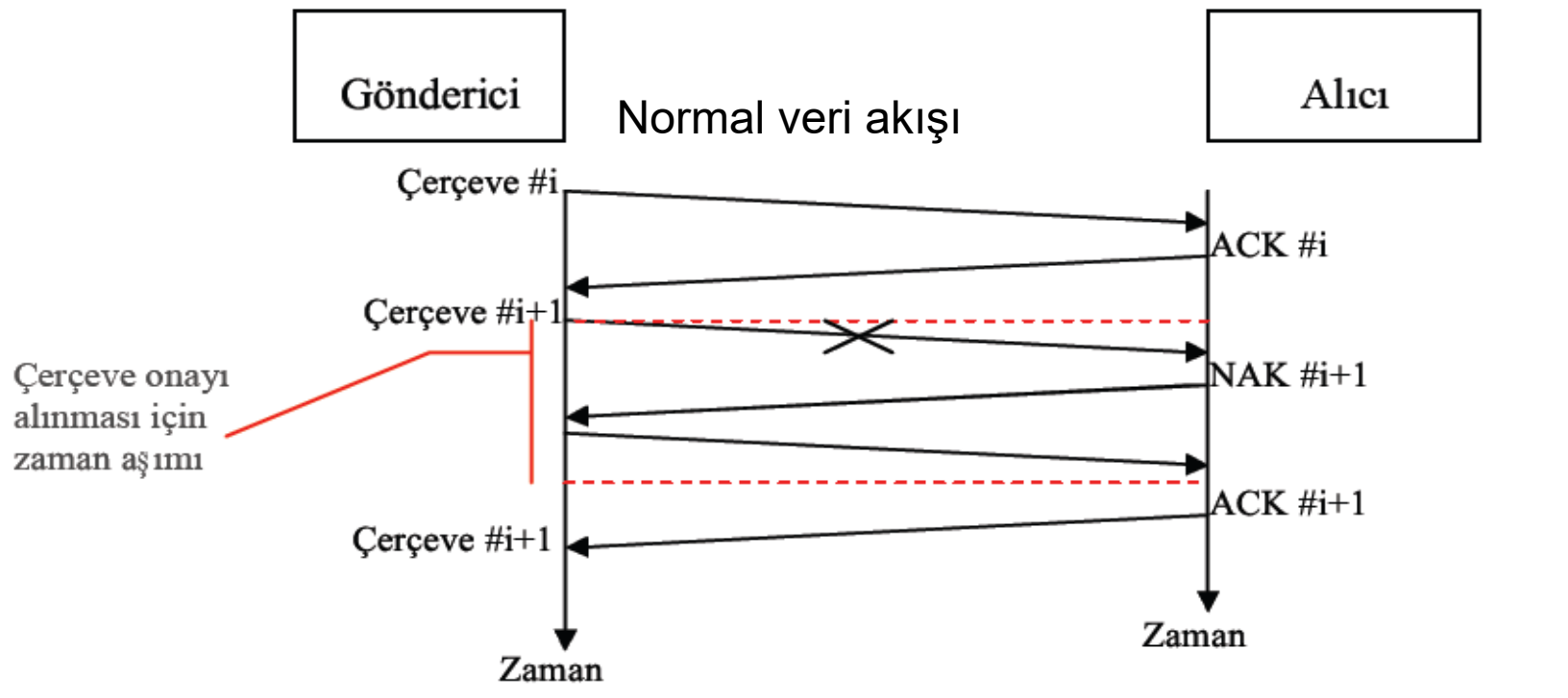
Dur ve Bekle Protokolü

- ACK çerçevesinin bozulması



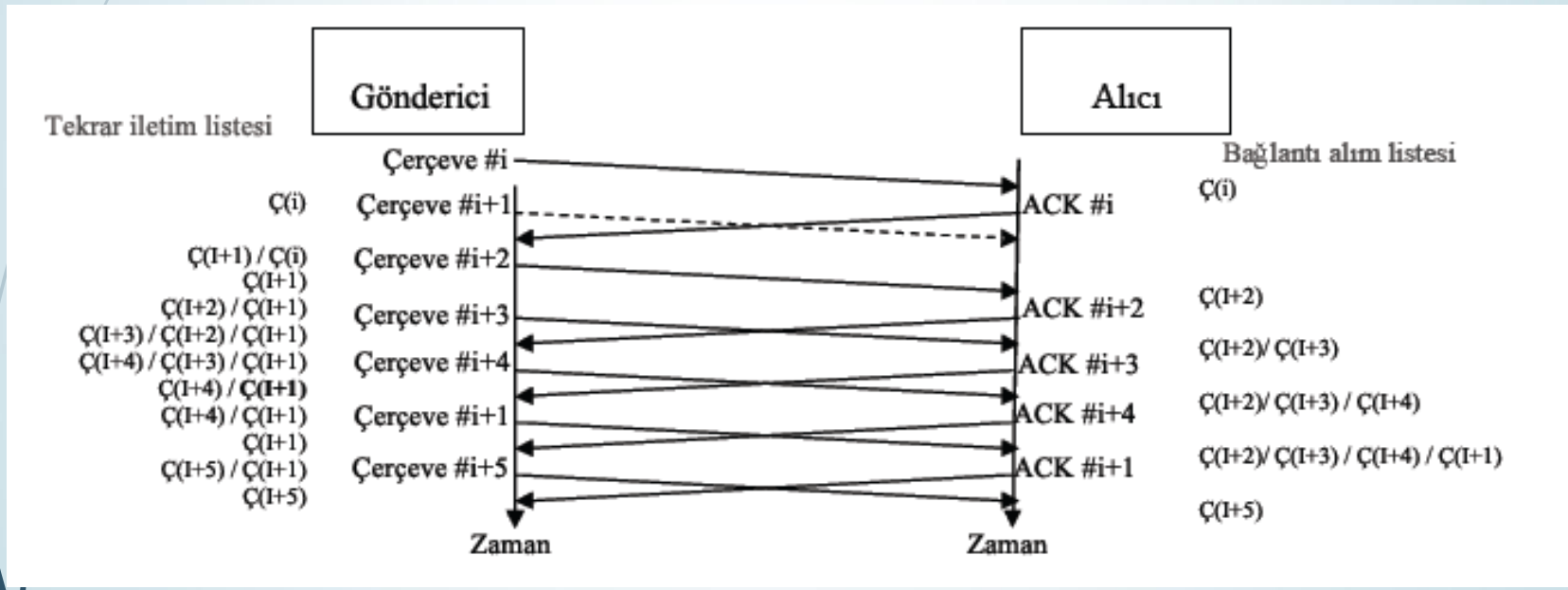
Dur ve Bekle Protokolü

- Gönderilen çerçevenin bozulması ve NAK gönderilmesi



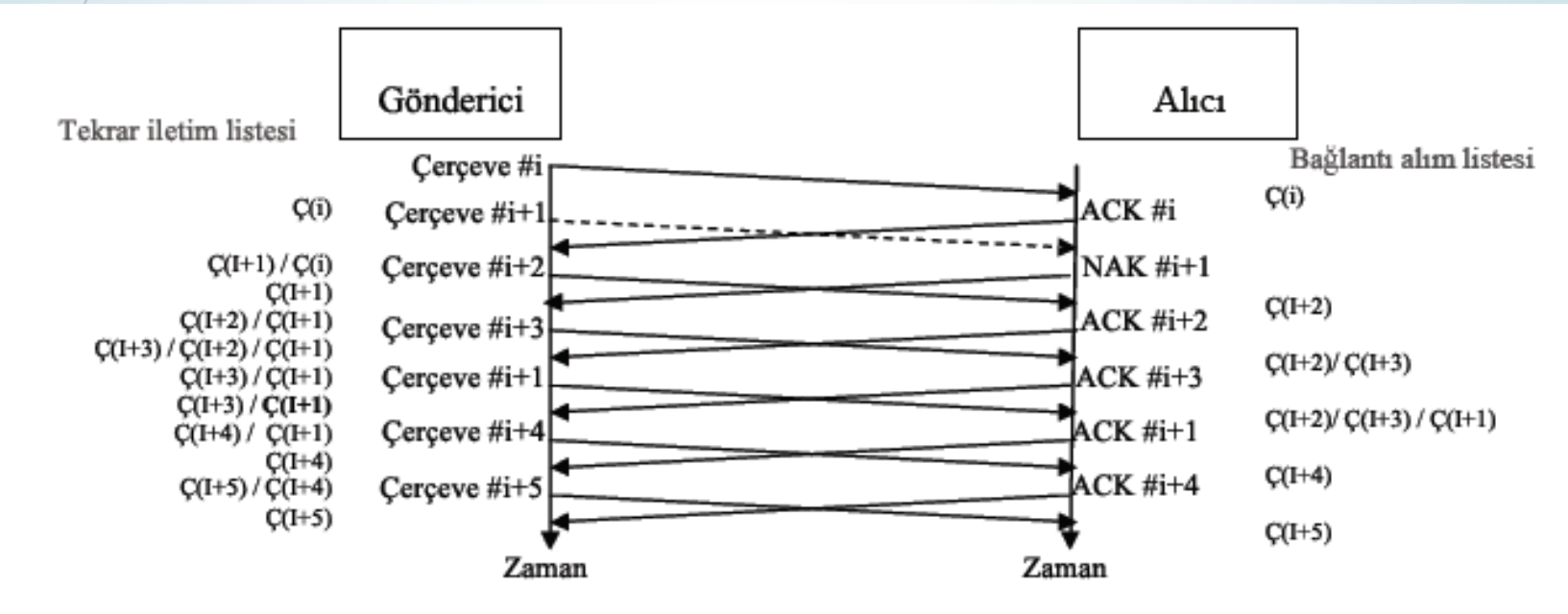
Sürekli Tekrar İstemi

- Çerçevenin bozulma durumu ve tekrar gönderim



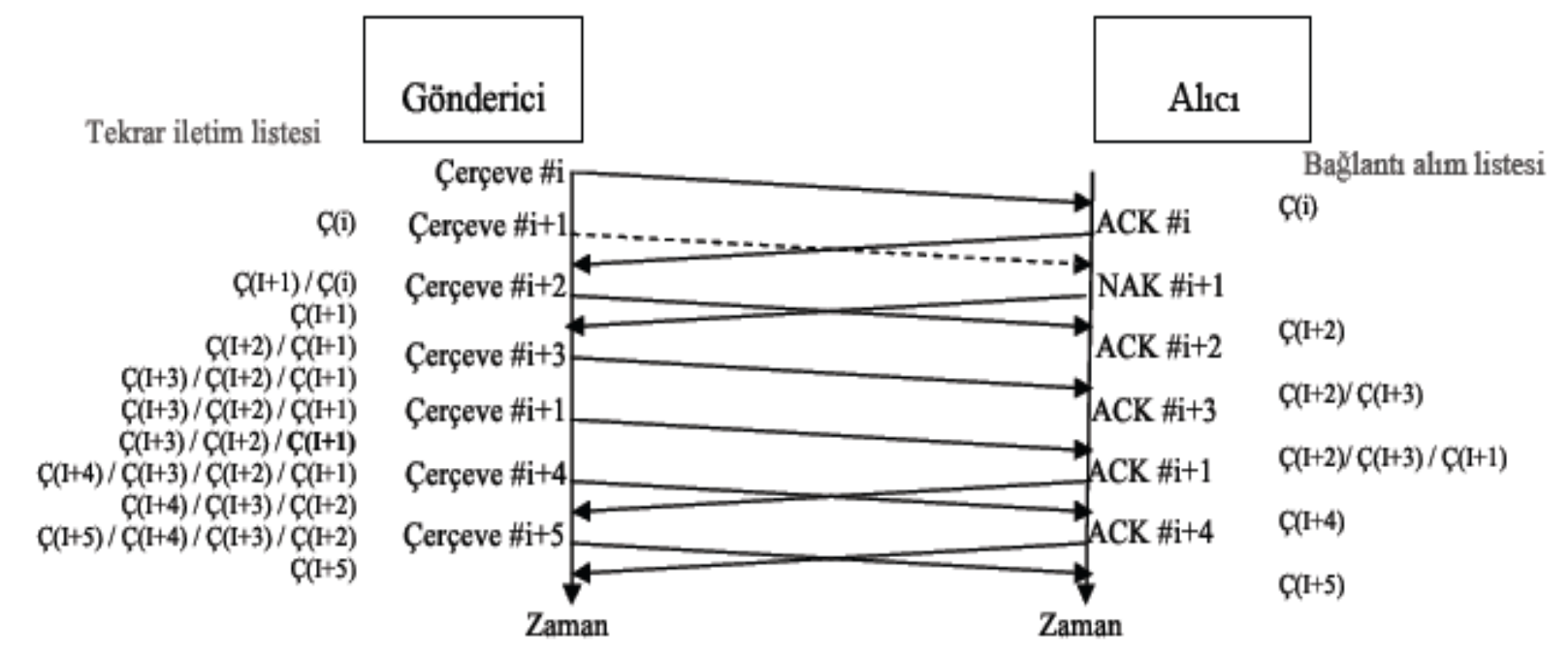
Seçmeli Tekrar

- Çerçevenin bozulma durumu ve belirgin tekrar gönderim



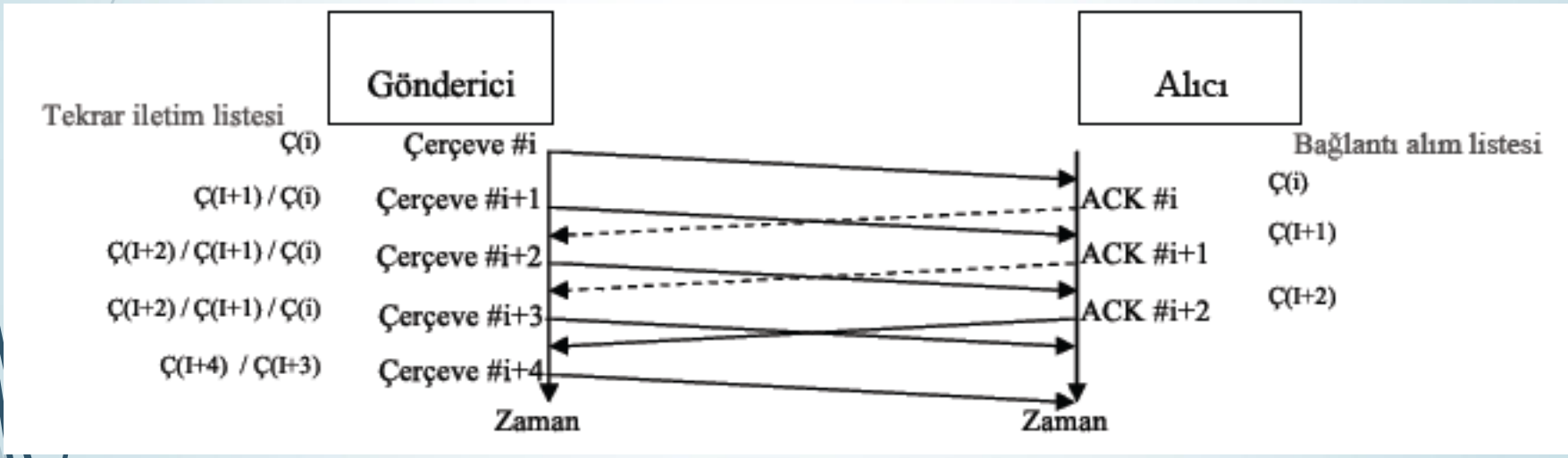
N Çerçeve Gerile

- N çerçeve gerile protokolü ve iletim çerçevesinin bozulması



N Çerçeve Gerile

- N çerçeve gerile protokolü ve eksik doğrulama



IEEE 802.3 Karakteristik Değerleri

- **10base2:** 200 metrelik ince eş eksenli kablo kullanan ve 10 Mb/s hızında veri taşıyan ana bant yerel alan ağları için Ethernet standardı.
- **10base5:** 500 metrelik ince eş eksenli kablo kullanan ve 10 Mb/s hızında veri taşıyan temel bant ve bus topolojisini kullanan ethernet standardıdır.

Karakteristik	Değerler	IEEE 802.3 Değerleri				
		10Base5	10Base2	1Base5	10BaseT	10Broad36
Veri oranı (Mbps)	10	10	10	1	10	10
İşaretleşme metodu	Baseband	Baseband	Baseband	Baseband	Baseband	Broadband
En fazla kablo uzunluğu (m)	500	500	200	250	1800	1800
Topoloji	Bus	Bus	Bus	Star	Star	Bus

IEEE 802.3’ ün Çalışması

- Bilgiler değişken uzunluktaki çerçeveler içerisinde gönderilir, teslim ve denetim bilgileri dışında en çok 1512 baytlık veri taşır. Ethernet standardı (IEEE 802.3), saniyede 10 mega bit (10 milyon) temel bant iletişimi sağlar.

7	1	6	6	2	46-1500
Preamble	S O F	Hedef Adres	Kaynak Adres	Uzunluk	Veri

- IEEE 802.3 çerçeveleri bir ve sıfırların değişen kalıplarıyla başlar. Bu kalıplar preamble olarak adlandırılır.
- IEEE 802.3 çerçevelerinde hedef adresinden önceki byte *start-of-frame (SOF)* ayracıdır. Bu byte art arda gelen “1” bitleri ile biter. Bunlar LAN üzerindeki tüm istasyonların çerçeve karşılama bölümlerinin eşlenmesini sağlar.

IEEE 802.3’ ün Çalışması

- IEEE 802.3 ağlarında preamble bölümünden sonra hedef ve kaynak adresleri sahaları gelir. Adresler IEEE 802.3 arabirim kartlarında bulunur. Adreslerin ilk 3 byte’ ı IEEE tarafından üretici belirteci olarak tanımlanırken, son 3 byte’ i ise Ethernet üreticisi tarafından tanımlanır.

7	1	6	6	2	46-1500
Preamble	S O F	Hedef Adres	Kaynak Adres	Uzunluk	Veri

- IEEE 802.3 çerçevelerinden, kaynak adresini takip eden saha, uzunluk sahasıdır. Bu saha, kaç byte’ lık verinin bu çerçevede yer aldığını belirtir.

IEEE 802.3’ ün Çalışması

- Son olarak ise veri sahasında verinin kendisi bulunur. Veri katmanı ve fiziksel katman işlemleri tamamlanmış olur.
- Veri bir üst katmana ulaşır.

AĞ TEMELLERİ

AĞ CİHAZLARI

Ağ Kartı (NIC- Network Interface Kart)

- Bilgisayarları ve diğer cihazları ağa bağlamada kullanılan kartlardır. Ağ kartı NIC (Network Interface Card) olarak da adlandırılır.
- Veriler bilgisayarda ikilik sistemde işlenirler. Ağ kartları bu verileri elektrik, ışık veya radyo sinyalleri ile diğer bilgisayarlara iletir.
- Ağ kartları hız ve bağlantı yolları bakımından da farklılık gösterir. ISA, PCI, USB, PCMCIA gibi bağlantı yuvalarını kullanan ağ kartları vardır. Günümüzde en çok kullanan ağ kartları pci bağlantı yuvalarını kullanmaktadır.

Ağ Kartı (NIC- Network Interface Kart)

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

Protokol	Kablo	Hız	Topoloji
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

Ağ Kartı (NIC- Network Interface Kart)

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 etmiştir.

Ağ Kartı (NIC- Network Interface Kart)

Ethernet Çalışma Esası

Ethernet kartı veriyi hatta bırakmadan önce, hattı denetler. Eğer hat başkası tarafından kullanılıyorsa gönderen ve alıcının Mac adreslerini içeren veriyi hatta bırakır.

Ethernet kartı seçimi

Ethernet kartlarında kullanılacak kablolama tipine göre BNC, RJ45 ve AUI konnektörleri olabilir. Bazı Ethernet kartlarında birden fazla konnektör yuvası bulunabilir. Bunlara combo Ethernet kartları denir. Karttaki konnektör yuvası sayısı arttıkça Ethernet kartının fiyatı artar. Ayrıca günümüzde Ethernet o kadar çok yaygınlaşmıştır ki, anakart üreticileri anakart üzerine (onboard) Ethernet kartlarını gömmektedirler. Piyasada artık şu anda en çok UTP kablo ve RJ - 45 birleşimi kullanılmaktadır. BNC kablolama artık yerini UTP kablolamaya bırakmaktadır.

Ağ Kartı (NIC- Network Interface Kart)

10Base-T için	CAT 3,4,5 UTP kablo ile 100 metreye kadar.
10Base-F için	Çok modlu FO kablo ile 2 km'ye kadar.
100Base-TX için	CAT 5 UTP kablo ile 100 metreye kadar.
100Base-T4 için	CAT 3,4,5 UTP kablo ile 100 metreye kadar.
01000Base-T için	CAT 5 UTP kablo ile 100 metreye kadar.
1000Base-LX için	Çok modlu FO kablo ile 550 metreye kadar.

Kart Türü	Hızı(Mbps)	Kablo Türü	Port Konnektörü
10Base-T	10	UTP,STP	RJ45
10Base-F	10	Fiber Optik	ST veya SC
100Base-TX	100	UTP,STP	RJ45
100Base-T4	100	UTP,STP	RJ45
100Base-FX	100	Fiber Optik	ST veya SC
1000Base-SX	1000 (1 G)	Fiber Optik	ST veya SC
1000Base-T	1000 (1 G)	UTP	RJ45

Ağ Kartı (NIC- Network Interface Kart)

İleri Düzey Ethernet Kartlarındaki bazı özellikler :

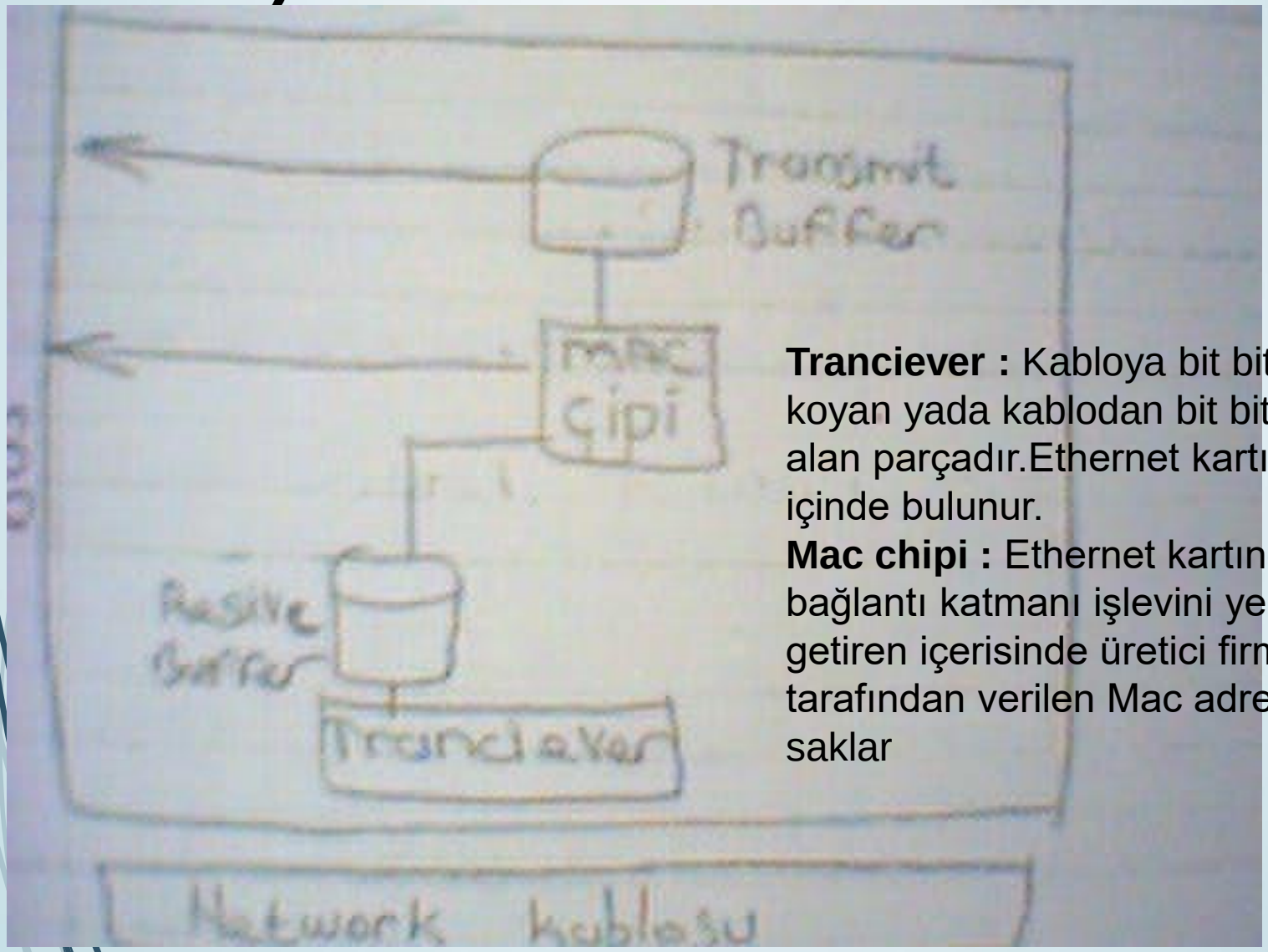
Priority packet Desteği : Priority paketlere öncelik vermek için kullanılır.Bu özelliğe sahip kartlar bazı verilerin geçişi için öncelik sağlayabilir.

Adapter Fault Tolerance desteği (AFT): Server ile switch arasına iki kart takılır.Birinci kart primary (birincil) , ikinci kart backup (yedek) için kullanılır.Herhangi bir şekilde birinci kartın bağlı olduğu hat koparsa ikinci kart otomatik devreye girer.

Automatic Load Balancing (ALB): ALB özelliği AFT özelliğine benzer.Ancak ikinci kart sadece yedek için bekleyeceğine veri akışıda sağlar.Server'a 4 kadar ağ kartı takılarak trafüğü 4 katına çıkarmış olursunuz.

Remote Wake-Up : Bir sistemi uzaktan açabilmek için magic-packet adlı bir sinyal gönderilir.Network kartı bu sinyali tanıyıp sistemi açar.Bunun için network kartından sisteme ayrı bir kablo bağlantısı yapılır

Ağ Kartı (NIC- Network Interface Kart)

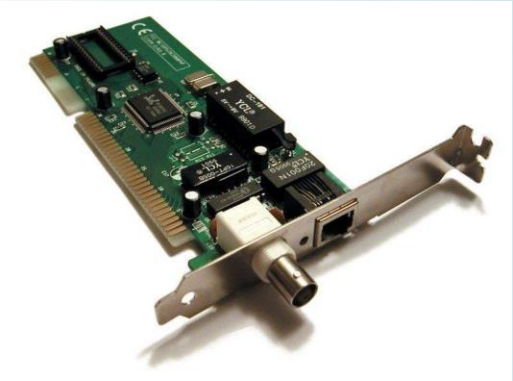


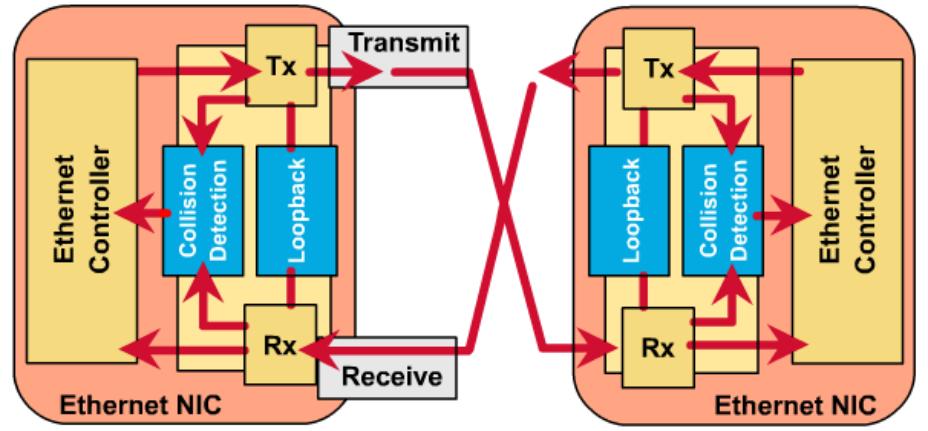
Tranciever : Kabloya bit bit veri koyan yada kablodan bit bit veri alan parçadır.Ethernet kartının içinde bulunur.

Mac chipi : Ethernet kartında, veri bağlantı katmanı işlevini yerine getiren içerisinde üretici firma tarafından verilen Mac adresini saklar

Ağ Kartı (NIC- Network Interface Kart)

- Her LAN teknolojisi (Ethernet, Token Ring, FDDI) için farklı NIC vardır.
- On-board transceiver (Transmitter-Receiver)
  - Kabloya işaret uygulamak ve collision'ları algılamak için

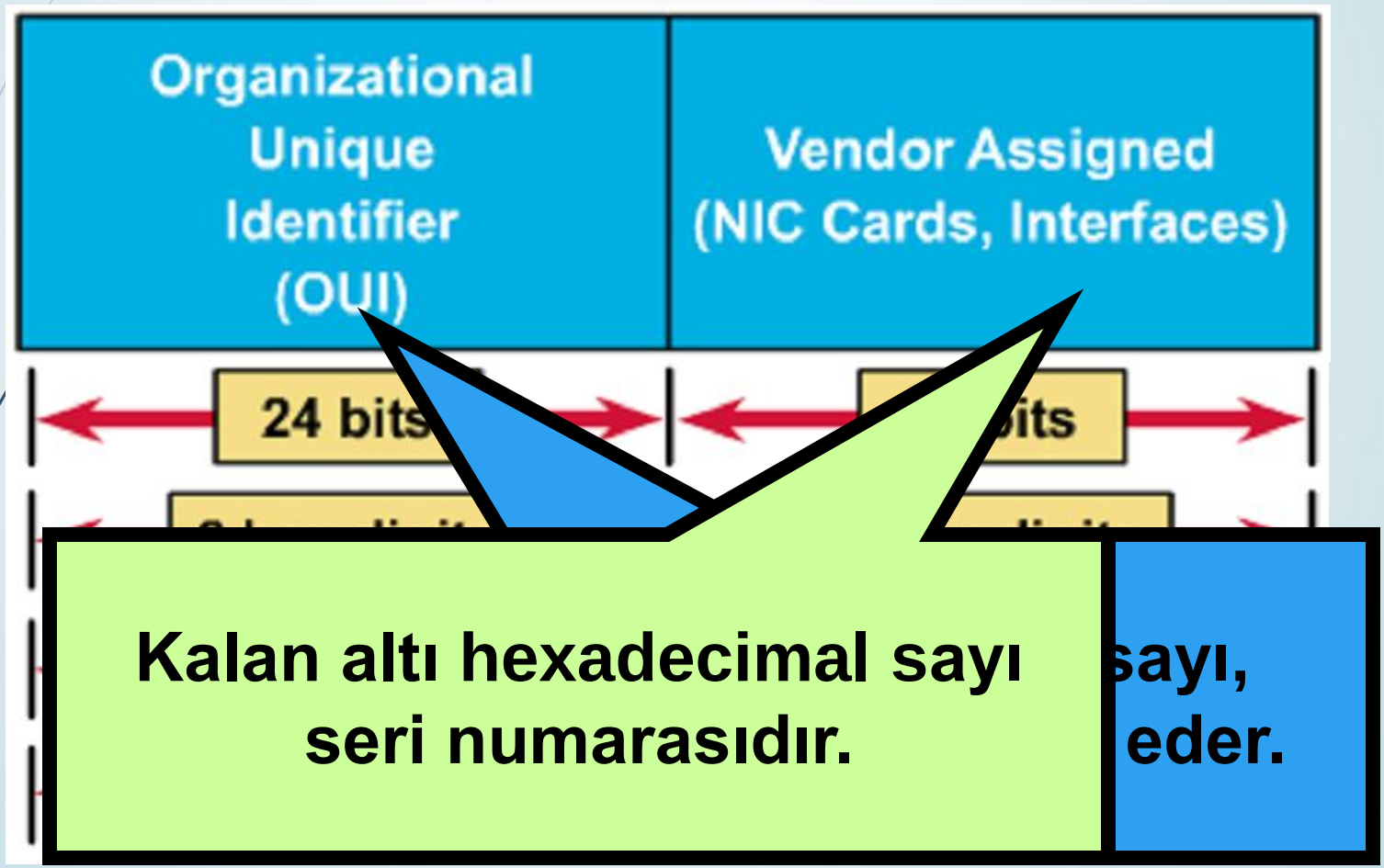




MAC Adresi

- Ağda sistemler birbirini sahip oldukları MAC adresi ile tanırlar.
- Her NIC, dünyada eşi olmayan bir adrese sahiptir.
- Ethernet, 48 bit uzunluğunda ve 12 hexadecimal (onaltılık) sayı sistemiyle ifade edilen MAC adreslerini kullanır.
  - İlk 24 bit ya da 6 hexadecimal dijit, üreticinin kod numarası,
  - Geri kalan 24 bit ya da 6 hexadecimal dijit ise kartın seri numarasıdır.

MAC adres formatı

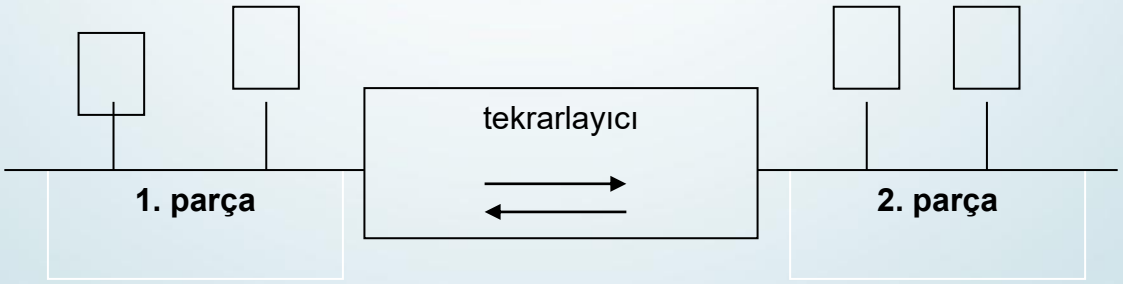


Repeater (Tekrarlayıcı)

Tekrarlayıcı, ağ dilimlerini (Segments) birbirine bağlayarak ağı genişletmek, uzatmak için kullanılır; görevi, iletişim hattının fiziksel uzunluğunu artırmaktır. Şöyle ki, hat, üzerindeki elektriksel işareti iletirken belirli bir zayıflamaya uğratır; bu çok fazla olursa karşı taraf işareti algılayamaz; dolayısıyla iletişim gerçeklenemez. Bu durumda araya zayıflayan işareti kuvvetlendirip karşı tarafa ulaşmasını sağlayan **tekrarlayıcı** koyulur. Küçük boylu, hat uzunluğu belirten sınırlar içinde kalan ağ uygulamalarında tekrarlayıcı gereksinimi olmaz; ancak hat uzunluğu artarsa, araya tekrarlayıcı koyulması gerekir.

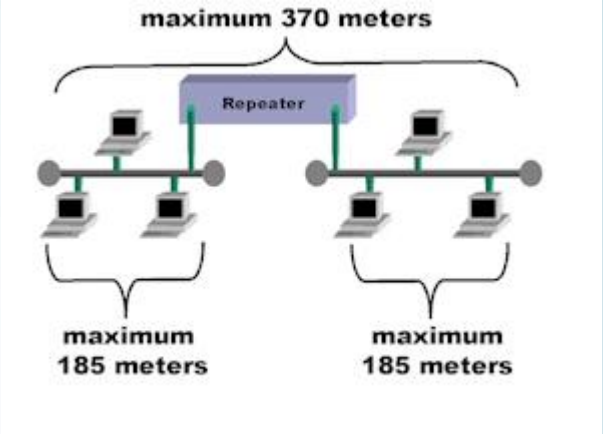
Repeater (Tekrarlayıcı)

Tekrarlayıcılar birden çok ağı birbirine bağlamak için değil de aynı ağa ait parçaları, yani ağ dilimlerini birleştirmek için kullanılır. Çünkü ağ bağlantısı için kullanılan iletişim kuralları ve özellikle bağlantıda kullanılan kabloların iletişim mesafeleri kablo cinsine göre belirlidir ve belirli bir üst sınır vardır. Eğer arada bir kuvvetlendirme yapılmıyorsa, ancak belirli bir mesafeye kadar iletim sağlanır. Daha uzun bir bağlantı için araya bu kuvvetlendirme işini yapacak tekrarlayıcı cihazı koyulması gerekir.



Repeater (Tekrarlayıcı)

Tekrarlayıcı (Repeater) OSI referans modelinin 1. katmanı olan fiziksel katmanda tanımlı görevi yapar; gelen verinin içeriği ile ilgilenmez, ayrıca elektriksel olarak kuvvetlendirip diğer portuna iletir. Kısaca bir tekrarlayıcının temel işlevi, kendisine herhangi bir yönden gelen elektriksel işareti karşıya kuvvetlendirilmiş olarak aktarmaktır.



HUB (Çok portlu Tekrarlayıcı)

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.

HUB (Çok portlu Tekrarlayıcı)

Hub’lar bir portundan gelen frame’leri diğer bütün portlarına gönderir. Hub’lar kendisine gelen verinin içeriği ile ilgilenmezler. Hub için gelen veri sadece bir elektiriksel sinyalden ibarettir. Fakat Hub’lar kendisine gelen bu sinyali güçlendirerek diğer portlarına aktarırlar. Bu nedenle OSI’nın 1.katmanında çalışan cihazlardır. Çünkü Hub ile bir ağı genişletmek, kablo ile genişletmekten çok farklı değildir.

HUB (Çok portlu Tekrarlayıcı)

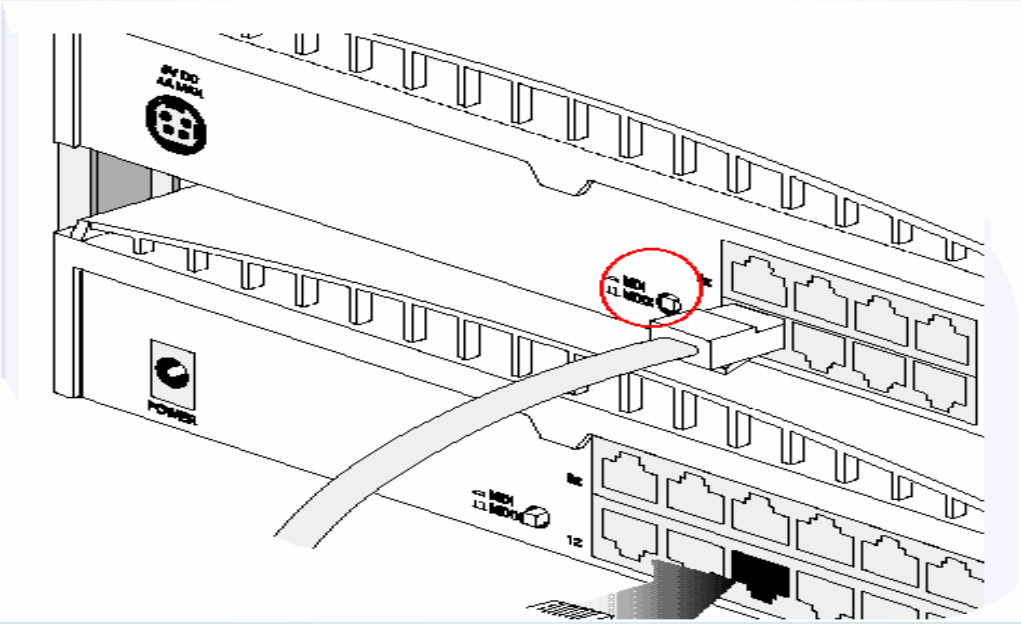
Hublar, 4, 8, 12, 16, 24 portlu olarak üretilirler. Huba UTP kablo ile bağlanılır ve her bir bağlantı 100 metreden daha uzun olamaz. Hub çalışırken herhangi bir portundan kablo çıkartmanız veya takmanız herhangi bir sorun çıkarmaz.

Ağ kuruduktan sonra ortaya çıkan problemlerden biri de ağın genişlemesidir. Ağ genişledikçe mevcut hubın port sayısı yeterli olmayabilir. Böyle durumlarda ya daha çok porta sahip bir hub alınır ya da başka bir hub ile mevcut hub birbirine bağlanır. Hublar birbirine bağlanarak ağın daha da genişlemesi sağlanabilir. Hubların birbirine bağlanması için hubların çoğunluğunda bulunan uplink portu kullanılır.

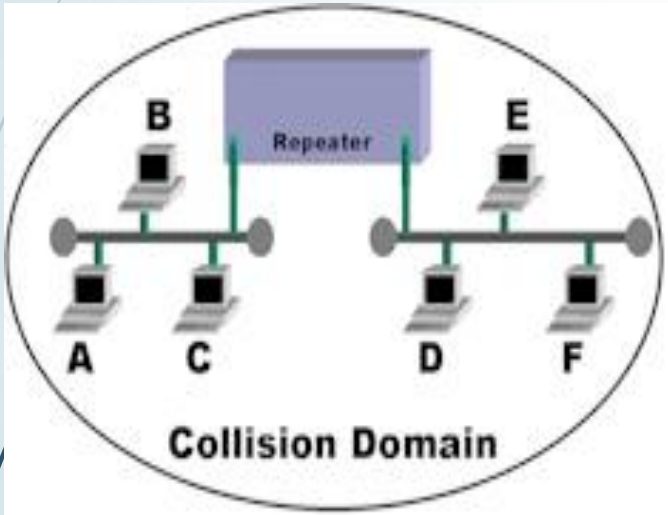
HUB (Çok portlu Tekrarlayıcı)

HUB (Çok portlu Tekrarlayıcı)

Birbirine bağlanacak iki hubdan birinin uplink portuna düz kablonun bir ucunu, diğer hubın ise normal bir portuna kablonun diğer ucunu takın. Ancak daha sonra karıştırmamanız amacıyla birinci porta takmanızı öneririz. Ayrıca uplink portunun yanında bir düğme bulunuyorsa bu düğmeye basılmalıdır.



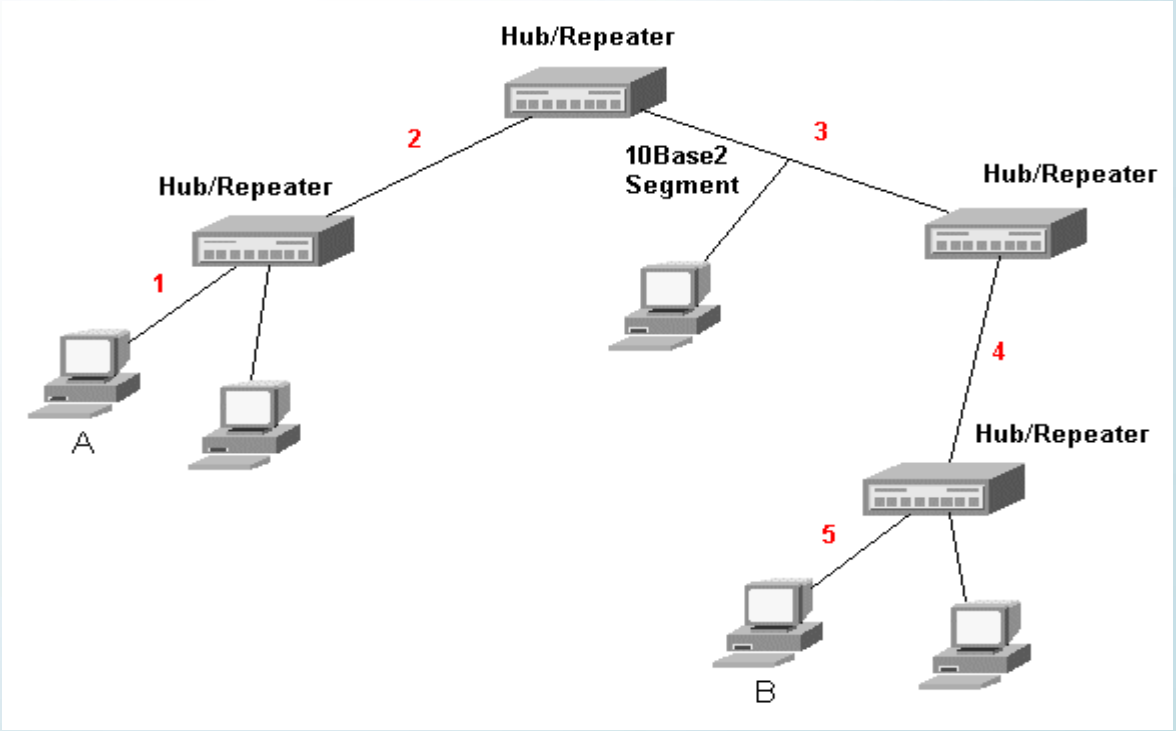
HUB (Çok portlu Tekrarlayıcı)



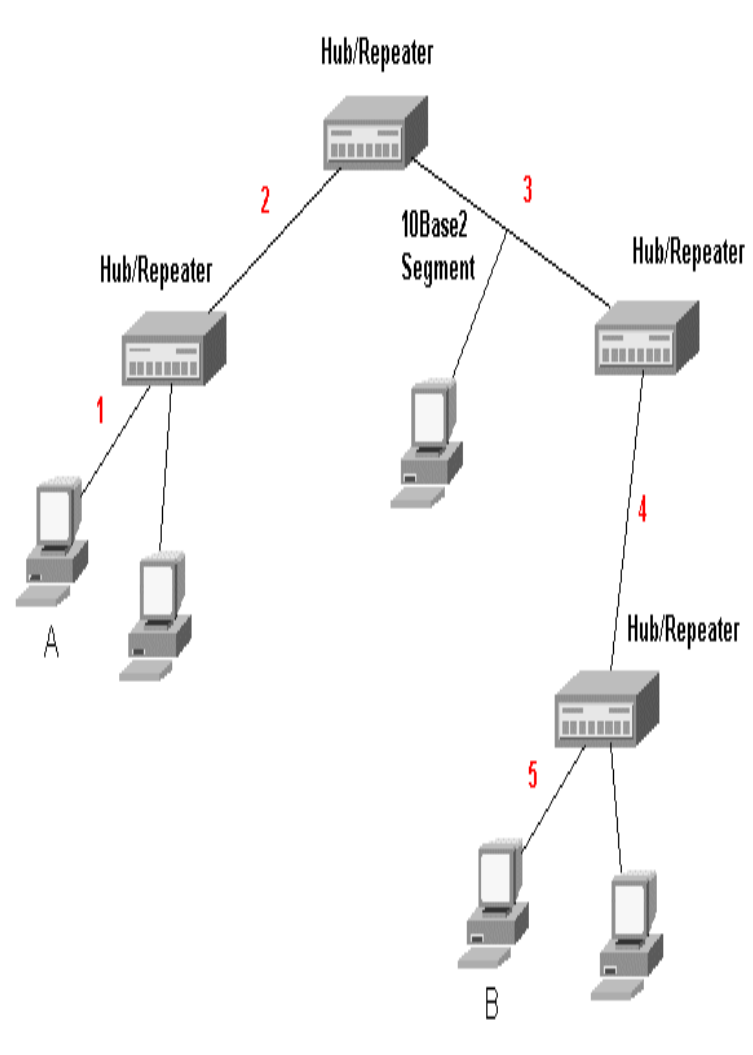
Birden fazla ethernet segmenti repater veya hub ile birbirine bağlanırsa aynı çakışma alanı/collision domain'in üyesi haline gelirler. Çakışma alanı tek bir makinanın ürettiği trafik tümüne yayılan bir veya birden fazla segment manasına gelir. 5-4-3 kuralı denilen bir dizi sınırlandırmalar çakışma alanını olabileceği maksimum büyüklüğü belirler.

HUB (Çok portlu Tekrarlayıcı)

Aynı çakışma alanı içinde iki sistem arasında en fazla;
- 5 Segment
- 4 Repeater
- 3 Populated Segment olabilir.



HUB (Çok portlu Tekrarlayıcı)



en uzak mesafe A ve B için geçerli

Bu örnek 5-4-3 kuralına uyuyor mu?

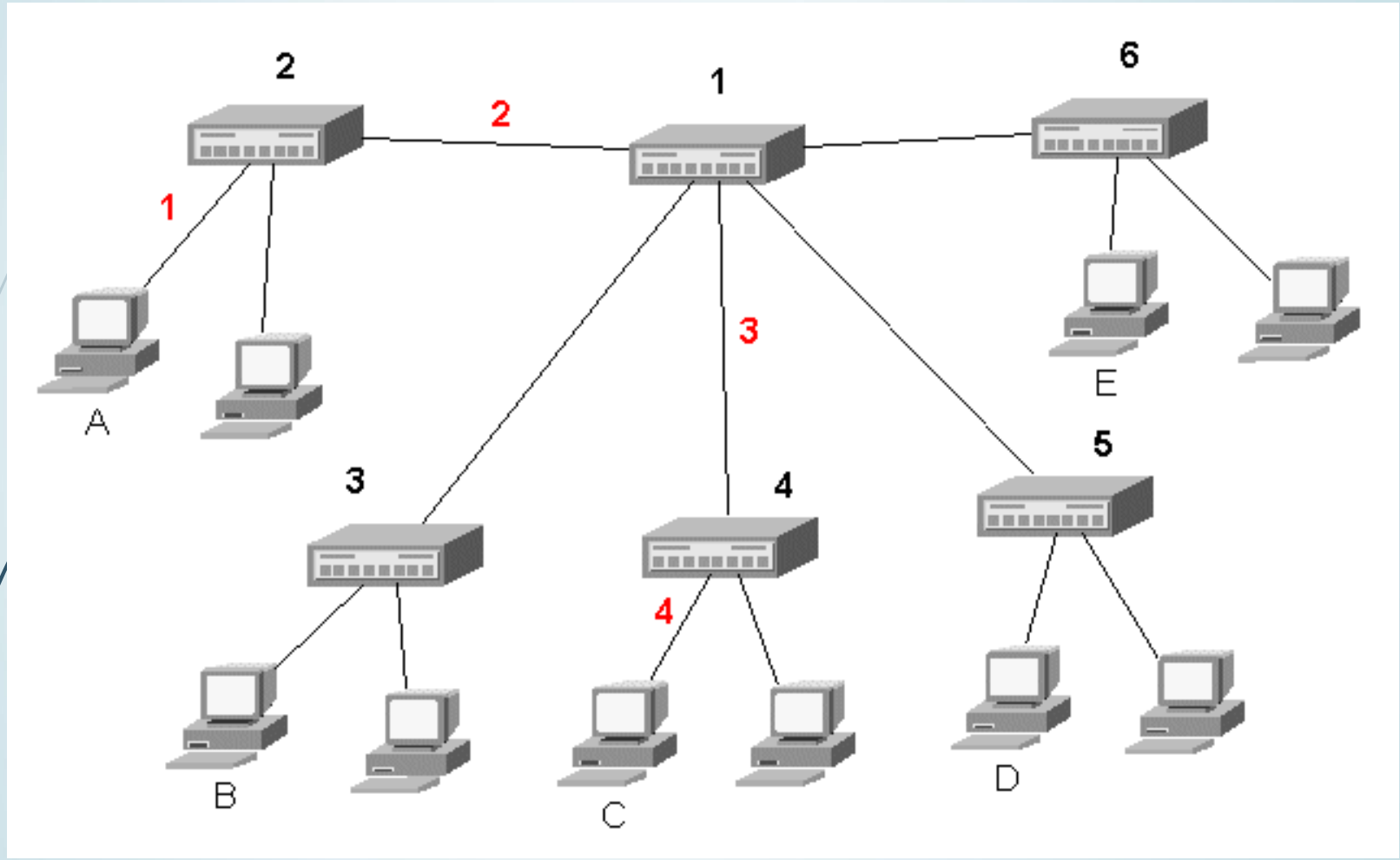
5 Segment (1, 2, 3, 4, 5)

4 Repater veya Hub geçiyor.

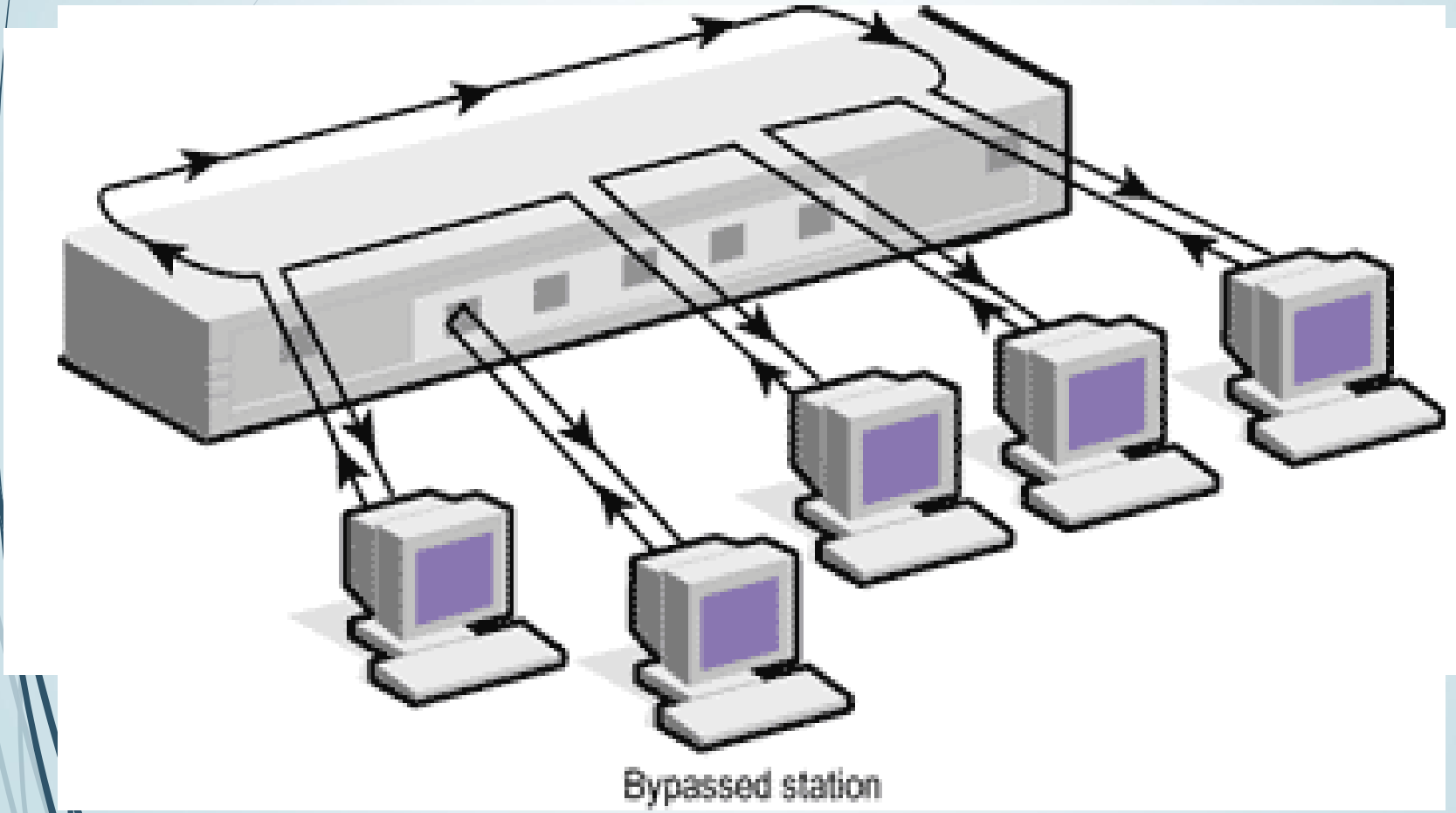
3 Tane populated segment(en az bir terminal bağlı kablo)

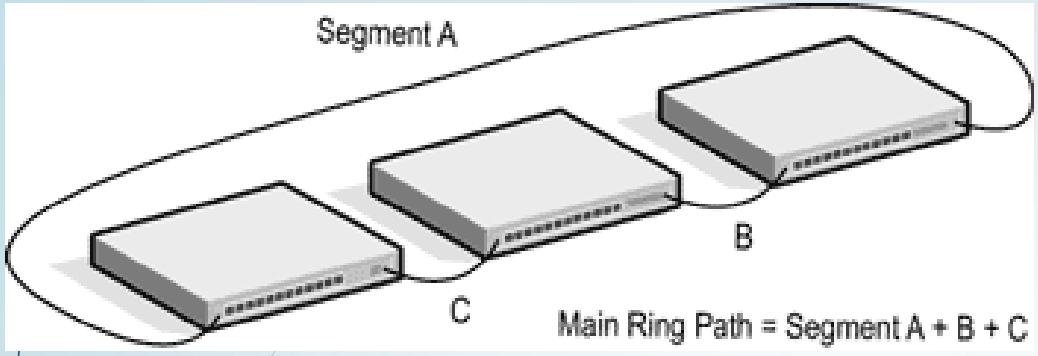
5-4-3 kuralı tüm ağ'da olabilecek hub/repeater veya segment sayısını değil, en uzak durumdaki iki makina arasında olabilecekleri tanımlar.

HUB (Çok portlu Tekrarlayıcı)

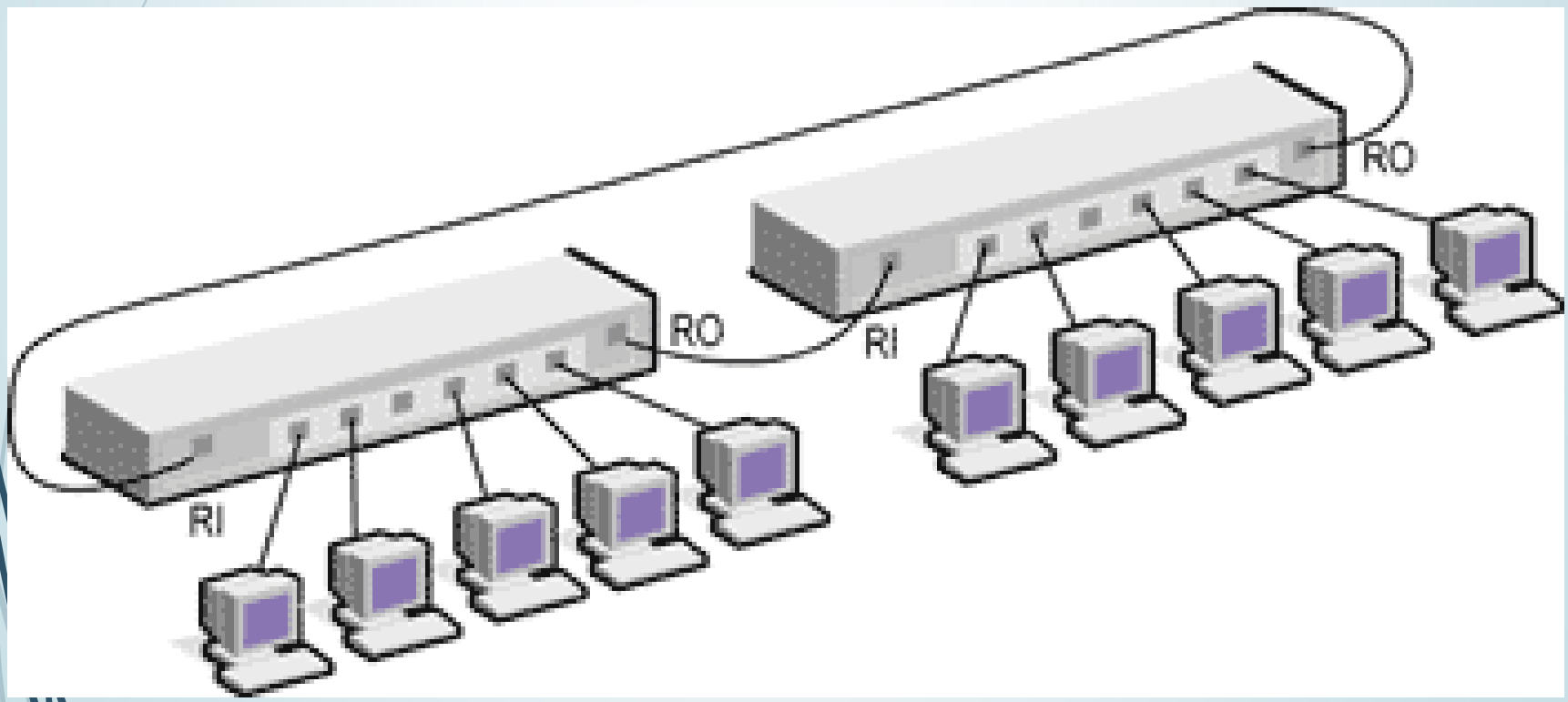


MAU (Multistation Access Unit)





İki MAU bağlanması için MAU'daki RI (Ring In) ve RO (Ring Out portları kullanılır.



Switch (Anahtar)

Anahtar (switch) akıllı bir hub cihazıdır. Hubın yaptığı görevin aynısını yapar, ancak ağı yormaz. Aynı anda birden fazla iletim yapma imkanı sağlar. Böylece aynı anda bir bilgisayar yazıcıyı kullanırken diğer ikisi kendi aralarında dosya transferi yapabilirler.

Switch (Anahtar)

Anahtar, portlarına bağlanan bilgisayarları MAC adreslerine bakarak tanır. Anahtarlama işlemini gerçekleştirmek için MAC adreslerini yapısında bulunan tabloda tutar.
Bu tabloda MAC adresinin hangi porta bağlı olduğu bilgisi bulunur. Kendisine ulaşan veri paketlerinin MAC adreslerini inceler ve her bir porta dağıtmak yerine, sadece hedef MAC adresine sahip olan bilgisayarın bağlı olduğu porta bırakır. Böylelikle veri paketi sadece hedef bilgisayara ait portu ve kabloyu meşgul eder. Çakışmalar engellenmiş olur ve ağ performansı artar.

Switch (Anahtar)

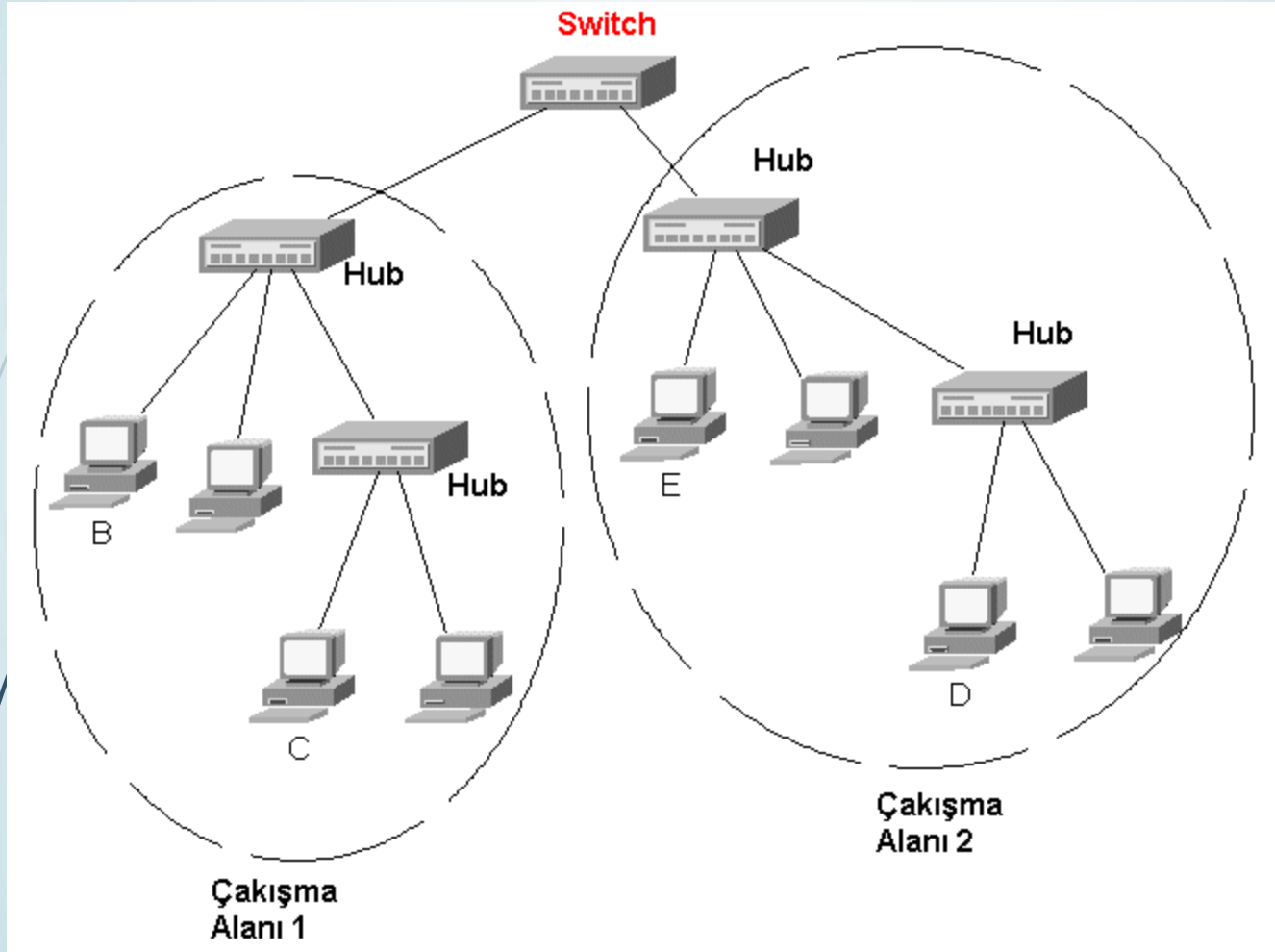
Bir anahtarın MAC adres tablosu

Alıcı MAC Adresi	Bağlı Olduğu Port
08-00-021a-3c-b2	1. port
00-a0-24-1a-3c-b2	5. port
08-00-21-a4-c8-92	7. port
08-00-02-1a-3c-33	8. port
08-00-24-1a-3c-b2	8. port
00-00-02-1a-3c-b2	2. port
00-00-25-1a-3c-ae	4. port
...	
...	

Switch (Anahtar)

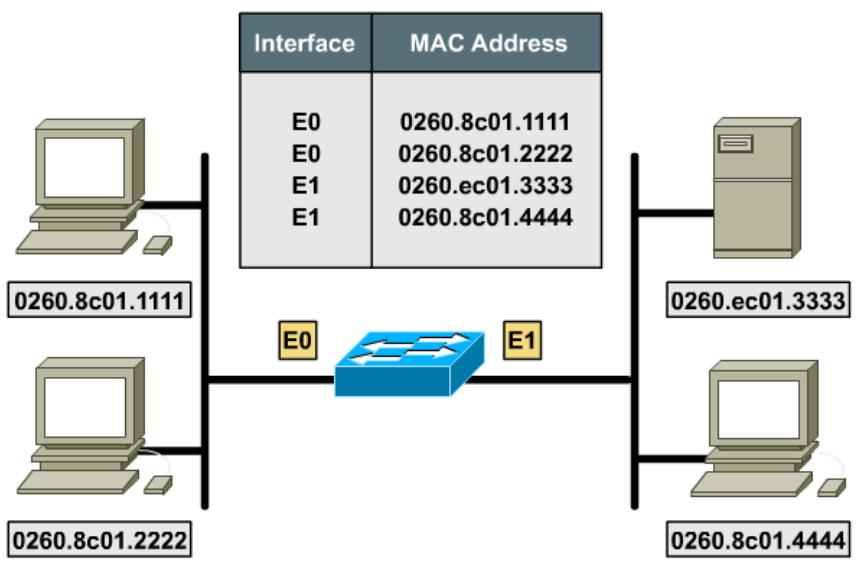
- Anahtarlama işlemi bu tabloya dayanılarak gerçekleştirilir.
- Eğer bir çerçevenin alıcı kısmındaki adres, o andaki tablo içerisinde yoksa, ilgili çerçeve tüm portlara yayın yapılarak aktarılır.
- Tablonun tutacağı MAC adres sayısı sınırlıdır. Ve güncelleme için cep bellek algoritmalarından bir kullanılır (bu adresler görme anında eklenir). Yani, tablo dolarsa yeni MAC adresleri ancak, önceliklerden bir tablodan çıkarılarak eklenebilir. Dolayısıyla bu tablonun boyu küçük olursa ve ağın o kısmında çok fazla sistem varsa, yayın türü aktarım oranı artar ve çok sık olarak cep bellek algoritmasının çalıştırılması gerekir.
- Merkez anahtar (core switch) konumundaki cihazların MAC adres tablolarının yeterince büyük olması istenir.

Switch (Anahtar)



SWITCH

- 2. katman cihazıdır.
- Birden çok uç sistemi bir noktada toplayıp, onlar arasında anahtarlama yöntemiyle bağlantı kurulmasını sağlar
- Çok portlu bridge olarak da tanımlanabilir.
- LAN'larda trafiği azaltıp, band genişliğini artırarak tıkanıklığı azaltır.
- LAN segmentlerini birbirine bağlar.
- Bridge'lerdeki gibi switchler de LAN segmentlerini birbirine bağlarken, MAC Adreslerini içeren tablo kullanır.



Switch (Layer 2 Switch)

- OSI’nin 2. katmanında çalışır.
- Topolojinin merkezinde yer alarak gelen bilgiyi ilgili terminale yollar.
- Aynı anda birden fazla çağrıya cevap verebilir.
- MAC adresler ile çalışır.
- Katman 3 Switche göre daha ucuzdur.

Switch Türleri

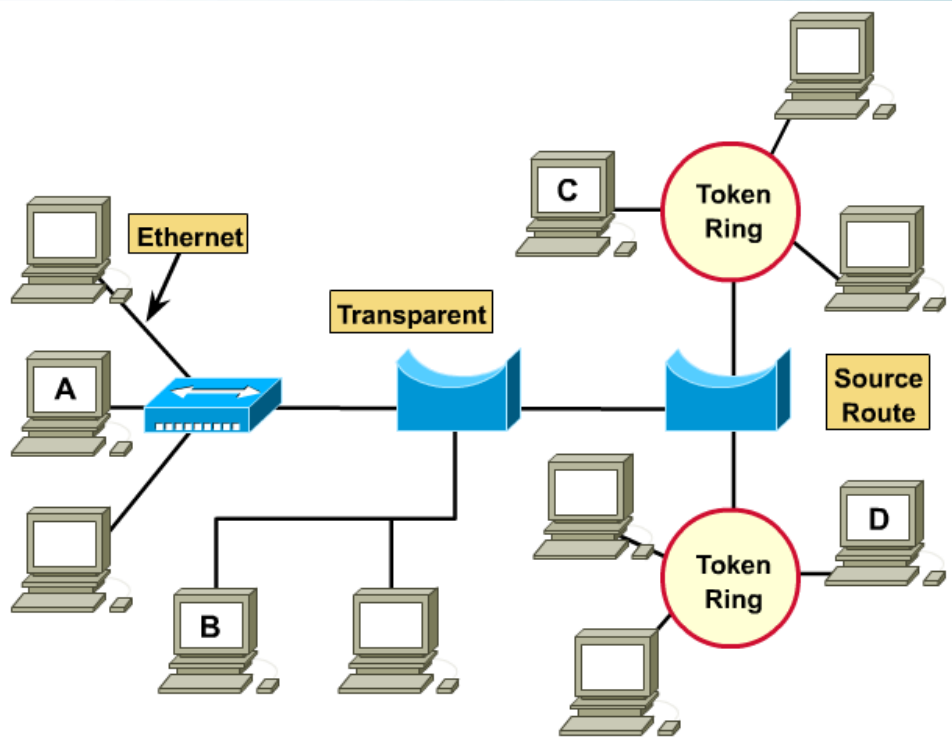
- Store-and-forward switch
  - Paketi giriş portundan aldıktan sonra buffer'a atar.
  - Ardından paketi ilgili çıkış portuna gönderir.
  - Paketteki hataları kontrol etmez, bu nedenle daha hızlıdır.
  - Ancak bozuk paketler ağda ilerler.
- Cut-through switch
  - Paketi iletmeden önce hedef adresi belirler. Ardından adresin çıkış portuna bu paketi iletir.
  - Pakette hata olup olmadığını kontrol eder. Hatalıysa iletmez.

KÖPRÜ (BRIDGE)

- OSI Veri İletim katmanında çalışır.
  - MAC adreslerini kullanarak paketleri iletir.
- Köprüler bağımsız çalışma gruplarını birbirine bağlamak için kullanılır.
  - Birbiri ile aynı topolojide veya farklı topolojide olabilir.
  - Örneğin bir yıldız ve bir halka topolojisinde ağları birbirine bağlayarak tek bir ağ gibi gösterir.
- Veri yönlendirme işlemi yapar.
- 10 Mbps ve 100 Mbps ağları birbirine bağlayabilir

BRIDGE (KÖPRÜ)

- 2. katmanda çalışır.
- Network segmentlerini birleştirir.
  - Farklı Layer 2 teknolojilerini birbirlerine bağlayabilir.
    - Ethernet, Token Ring, FDDI
- Gereksiz trafiği azaltır.
- Üzerinde yerleşik MAC Adres tabloları vardır.



BRIDGE

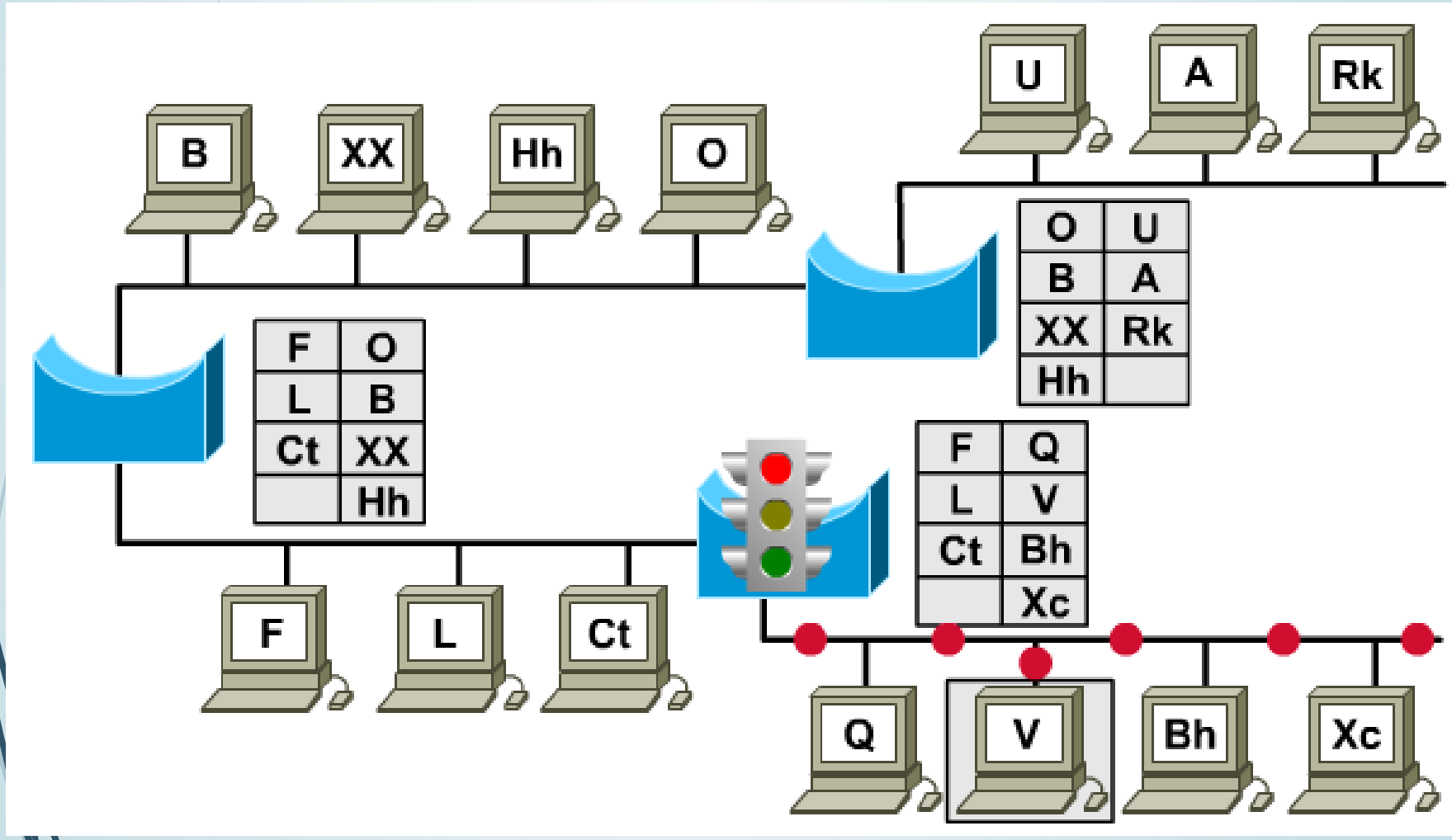
İki bağımsız network arasına bir bridge, her iki tarafa da aktarılmak istenen paketleri inceler.

- Eğer paket, karşı tarafta bulunan bir hostu adresliyorsa, o paketi diğer networke aktarır.
- Eğer paket aynı network içinde bir hostu adresliyorsa, karşı tarafın trafiğini artırmamak için, orayı adreslemeyen paketleri süzer.

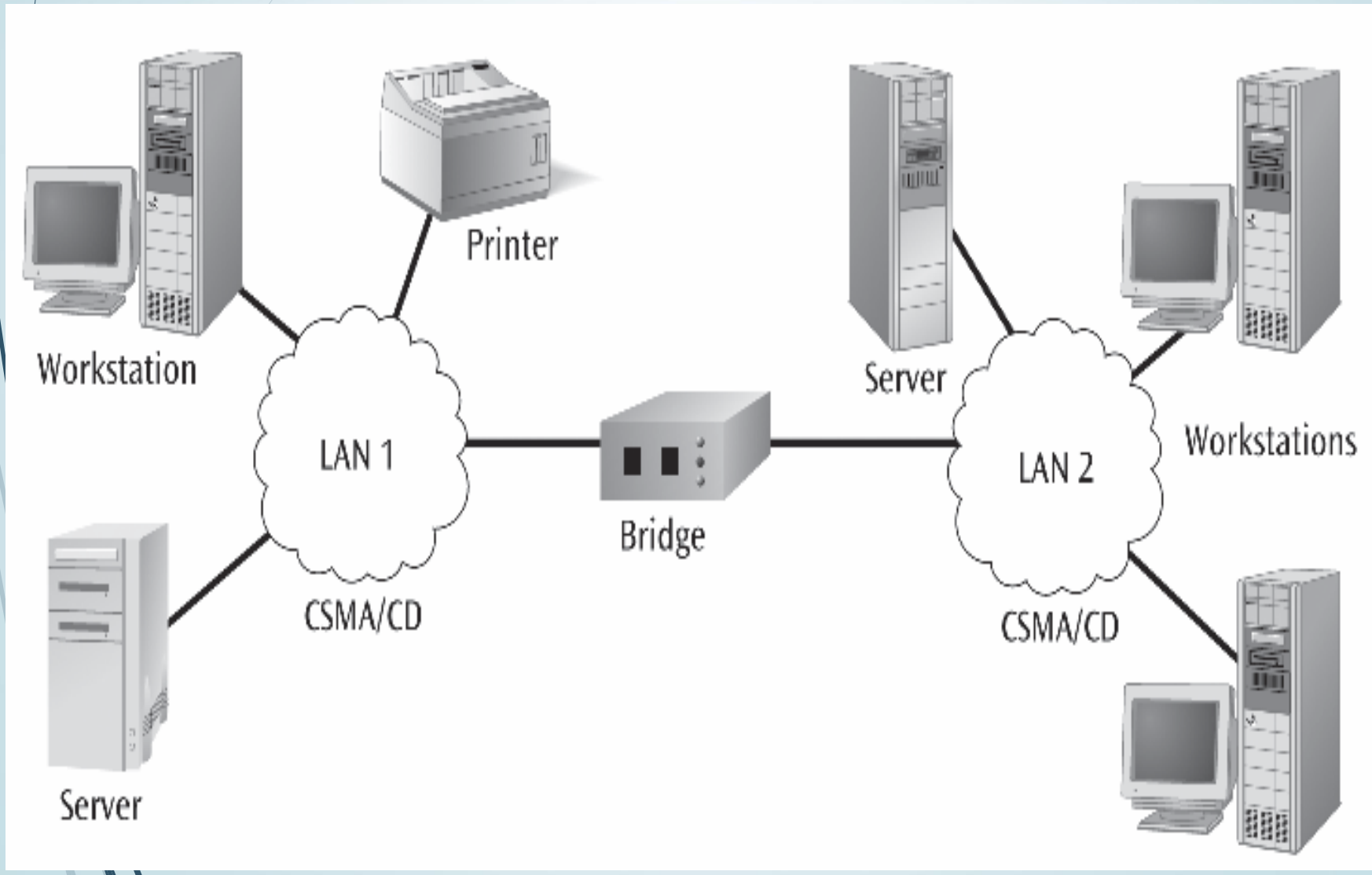
Bridge bünyesinde, adreslerin hangi networke ait olduklarını içeren tablolar bulunur.

- Bridge, depola-ve-gönder mantığı ile çalışan bir cihaz olduğu için network iletimini yavaşlattır. Bu da gecikmeye neden olur.
- Bridge'ler, bir networkteki gecikmeyi %10-30 artırırlar.

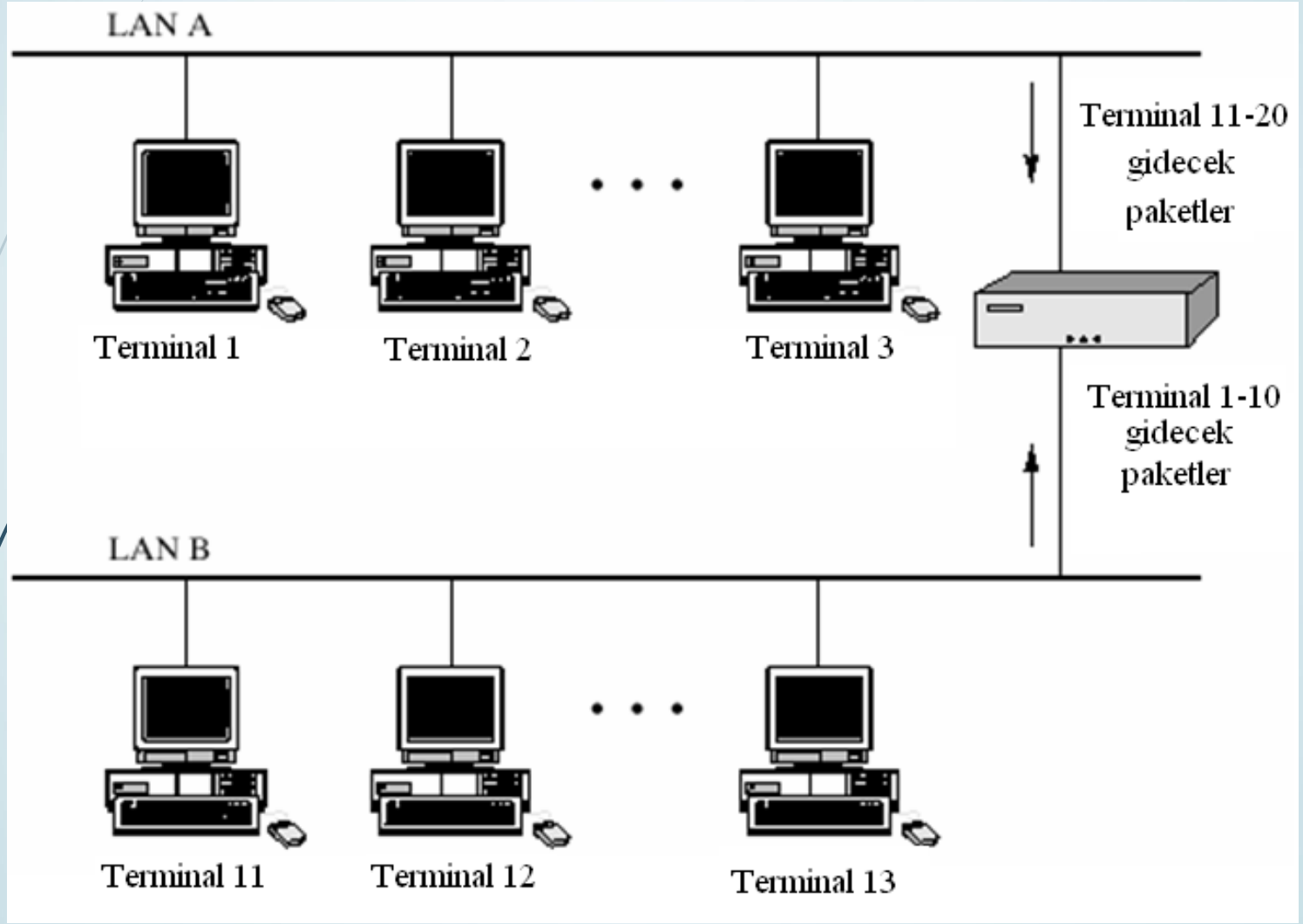
Bridge Nasıl Çalışır?



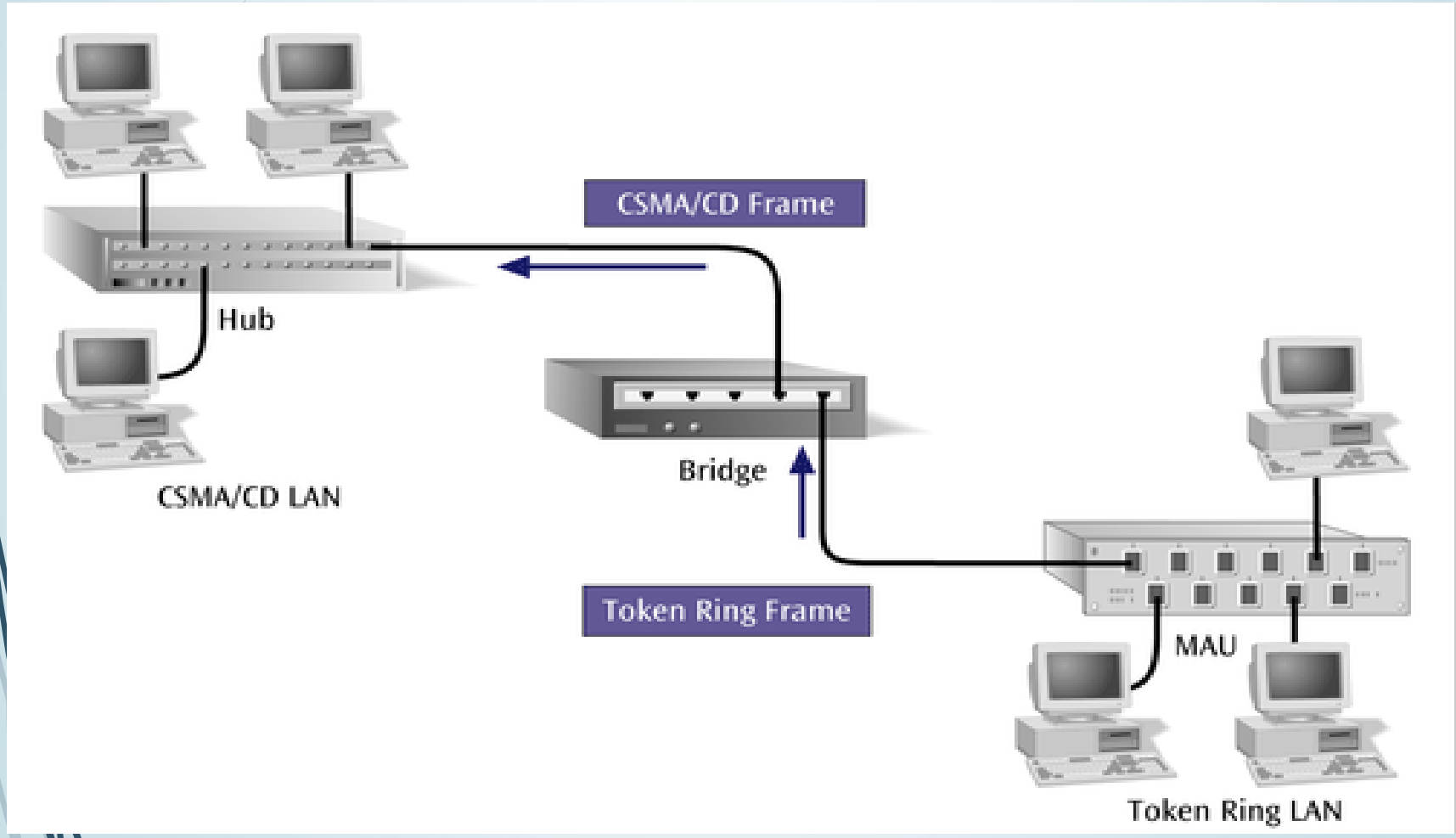
KÖPRÜ (BRIDGE)



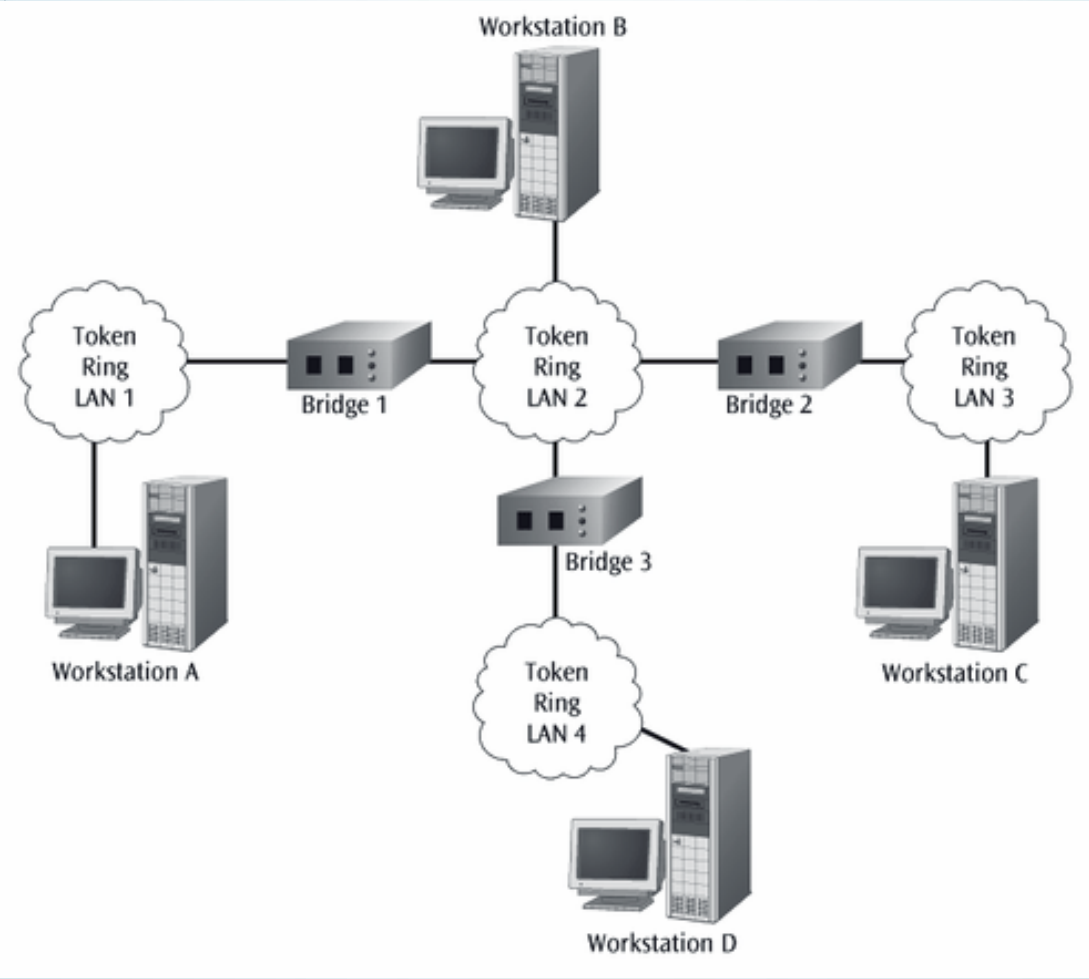
Bridge Operation



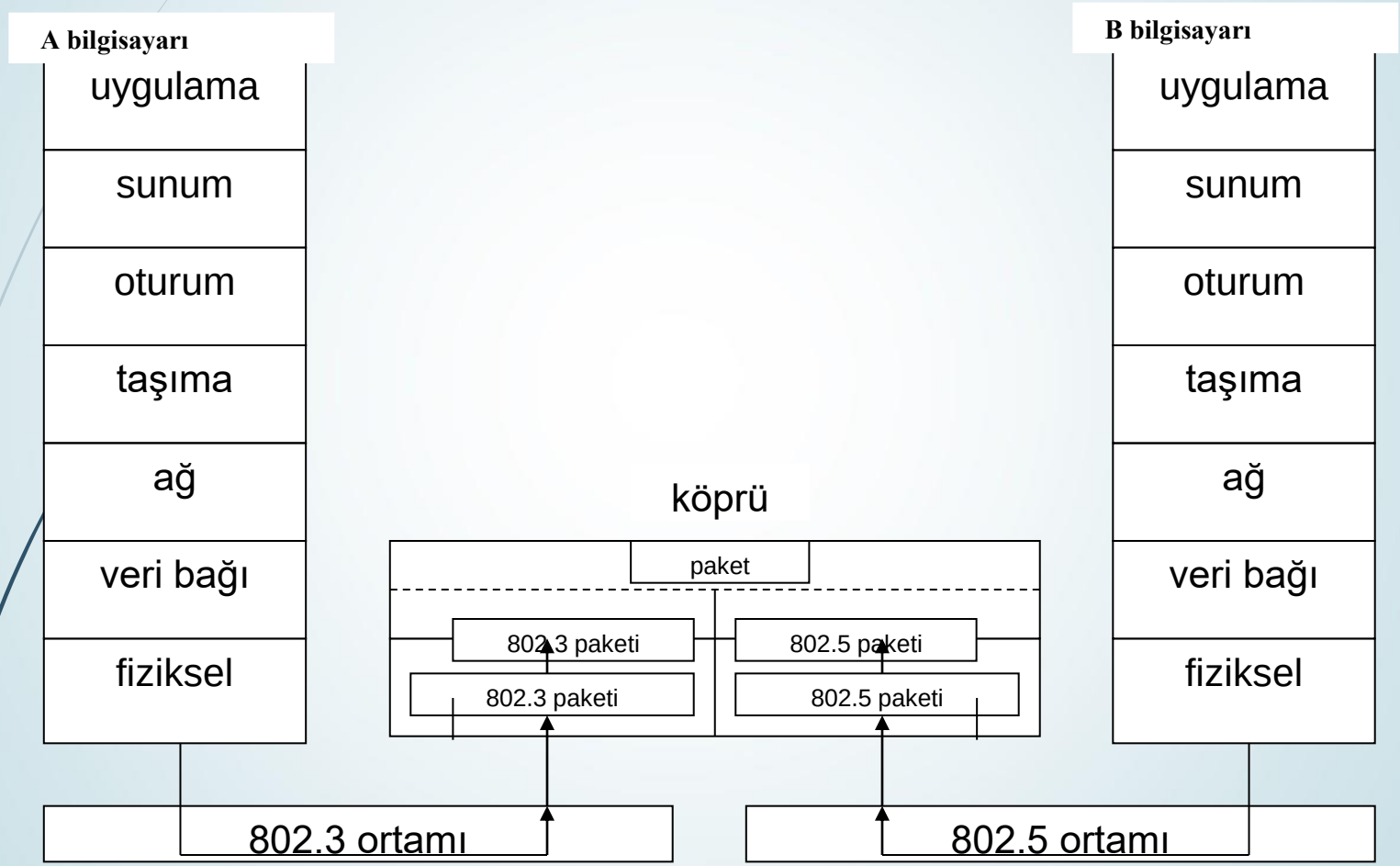
İki farklı ağ ve köprü



Halka topolojide köprü



Şekil - IEEE 802.3 - IEEE 802.5 ağları arasında köprüleme işleminin gerçekleştirilmesi



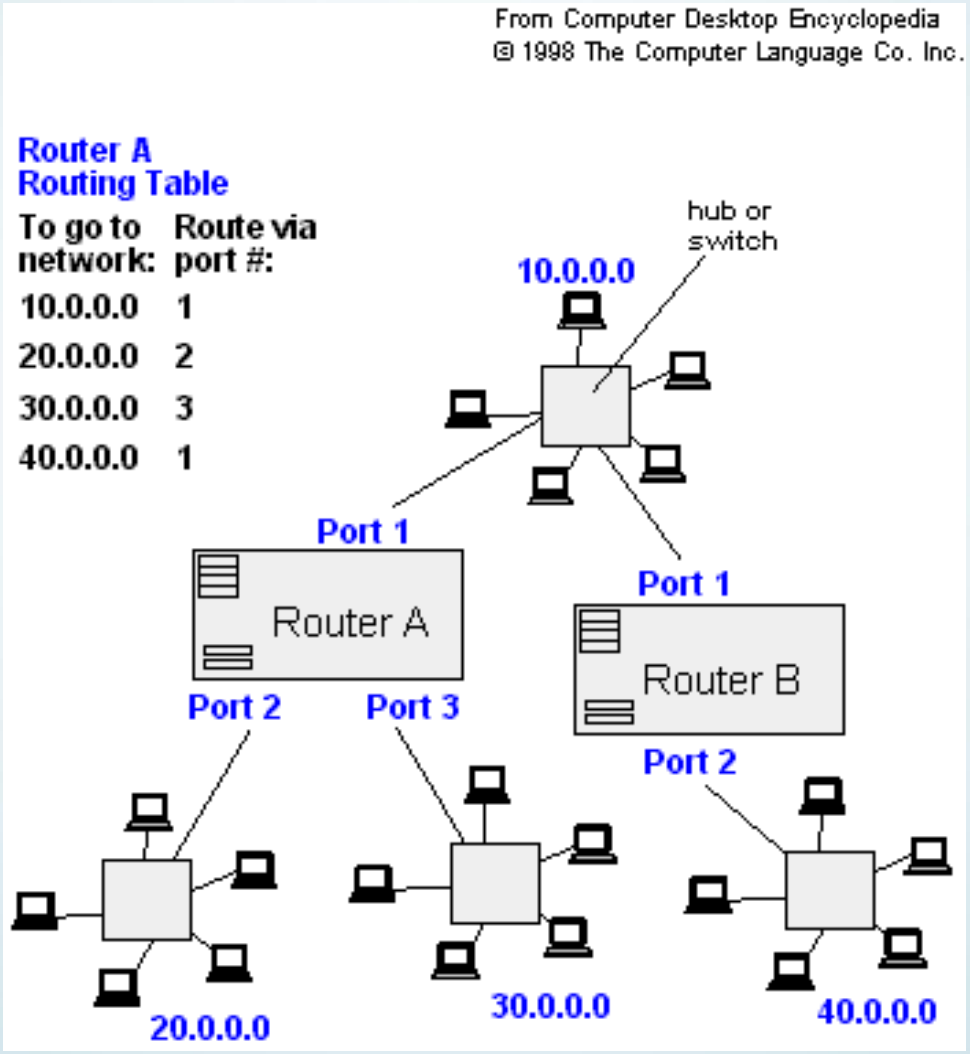
Yönlendirici (Router)

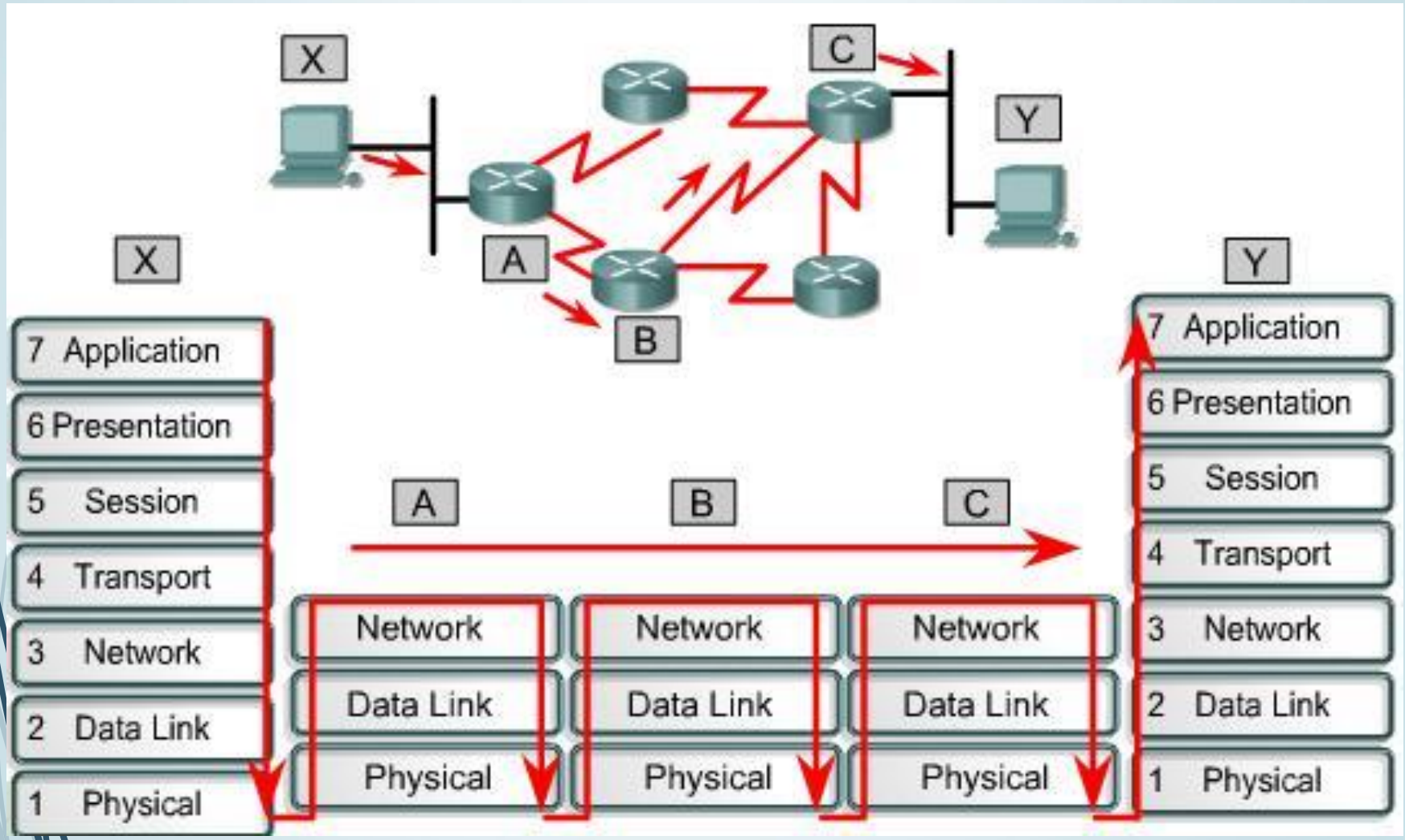
OSI başvuru modelinin ilk üç katmanına sahip aktif ağ cihazlarıdır. Temel olarak yönlendirme görevi yapar. LAN lar arasında bağlantı kurmak amacıyla kullanılır. Yönlendiricinin üzerinde LAN ve WAN bağlantıları için ayrı ayrı portlar bulunur. Bu portlar ile iki ağ arasında bağlantı sağlanır.

YÖNLENDİRİCİ (ROUTER)

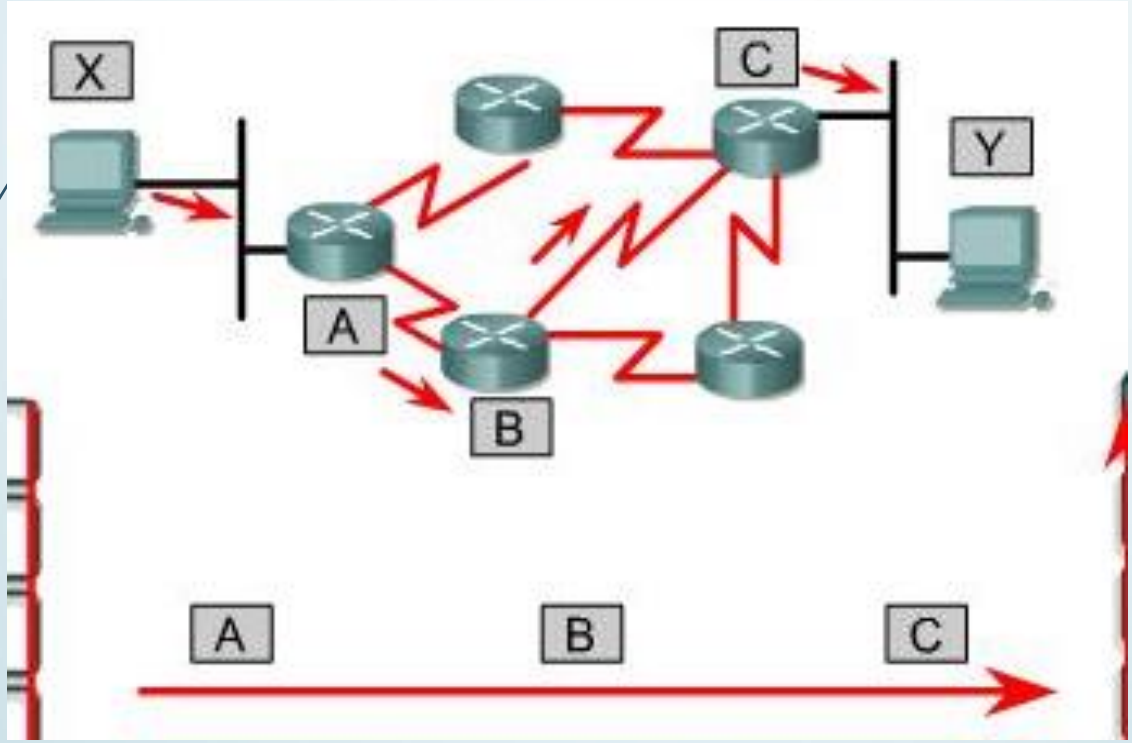
- Routerin bir işlemcisi, epromu ve üzerinde bir işletim sistemi IOS (Internal Operating System) vardır.

Paket yönlendirme




X
C
Y
A
B
X
Y
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
A
B
C
Network
Data Link
Physical
Network
Data Link
Physical
Network
Data Link
Physical
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

Statik ve Dinamik Yönlendirme :



Statik Yönlendirme :

Örneğin X bilgisayarı Y bilgisayarına ulaşmak istesin.Bu durumda X ile Y bilgisayarı arasında olası bir çok yol vardır.Eğer X bilgisayarını dışarıdaki ağa çıkartan A router'ına Eğer X bilgisayarı Y bilgisayarına gitmek isterse her zaman önce B router'ına git, sonrada B routerina C router'ı üzerinden git gibi bir ayarlama yapılmış ise bu statick yönlendirme işlemdir.

Dinamik Yönlendirme :

X ile Y arasında iletişim kurabilmek için birden fazla olasılık vardır. Bu durumda biz router'ları dinamik(adaptif) yönlendirme algoritmaları çalışacak şekilde konfigüre edersek Router'lar kendi aralarında sürekli konuşarak hangi yolun en iyi olacağına karar vererek verileri istenilen hedefe o şekilde ulaştırırlar. Artık X ile Y bilgisayarı arasında bir veri alışverişi olacağı zaman A ile B arasındaki hat kopsa dahi iletişim diğer olası hatlar üzerinden devam edecektir.

Routerler verileri internet ortamında yada iki LAN arasında yönlendirirken bir takım akıllı algoritmalar kullanırlar.

Bu tür algoritmalar, en iyi yolun belirlenmesinde kullanılacak parametrelerin tutulduğu bir yönlendirme tablosuna (routing table) sahiptirler. Yönlendirme tablosu, algoritma uyarınca ağ sürekli sorgulanarak güncellenir. En uygun yolun belirlenmesi için birçok algoritma vardır ve bu algoritmalar en uygun yolu belirleyebilmek için yol uzunluğu (path length), güvenirlik (reliability), gecikme (delay), yolun band genişliği (bandwidth), trafik yoğunluğu (load) ve iletişim maliyeti (communication cost) gibi parametrelerden bir veya birkaçını kullanarak bir metrik değer hesaplar. Bu metrik değere göre paketler yönlendirilir.

Metrikler:

1-) Yol uzunluğu : En yaygın olarak kullanılan metrik, yol uzunluğudur. Bazı ağ protokolleri, ağ yöneticilerinin her ağ bağlantısına bir değer atanmasına izin verir. Diğer yönlendirme protokolleri, geçilen noktaların toplamını yol uzunluğu olarak alır. Burada da geçilen ağ elemanlarının sayısı önemlidir.

2-) Güvenlilik : Güvenlilik, her ağ bağlantısının güvenli olmasıdır. Güvenlilik oranı genellikle ağ yöneticileri tarafından belirlenir. Bu oranlar genellikle keyfi sayısal değerlerdir.

3-) Gecikme : Yönlendirme gecikmesi, bir paketin kaynaktan hedefe ağ üzerinden ulaşması için geçen zamandır. Gecikme, ağ bağlantılarının bant genişliği, yol boyunca her yönlendiricideki port kuyruğu, tüm ara ağların trafik durumu ve fiziksel uzaklık gibi çeşitli etmenlere bağlıdır. Gecikme, yaygın ve yararlı bir metriktir.

Metrikler:

4-) Bant genişliği : Bant genişliği, bir hattın trafik kapasitesini belirler. 10 Mbps Ethernet bağlantısı, hattaki diğer tüm şartlar eşit olmak koşuluyla 64 kbps kiralık hatta tercih edilir. Bant genişliği, bir hattaki maksimum taşıma oranı olmasına rağmen daha büyük bant genişliğine sahip hatlar, daha iyi bağlantı sağlamazlar. Örneğin daha hızlı bir hat çok daha fazla meşguldür, dolayısıyla hızlı hatlar üzerinden bir paket gönderilmesi için gereken zaman daha fazla olabilir.

5-) Yükleme : Yükleme bir ağ biriminin meşguliyet derecesini belirler. Yükleme, CPU kullanımına ve her saniye işlenen paketlerin sayısına göre hesaplanır.

6-) İletişim masrafı : Bazı şirketler, maliyetler kadar performansa önem vermezler. Örneğin genel hatlar kiralık özel hatlara göre daha yavaştır; fakat çok daha ucuzdur.

Paketlerin ömrü

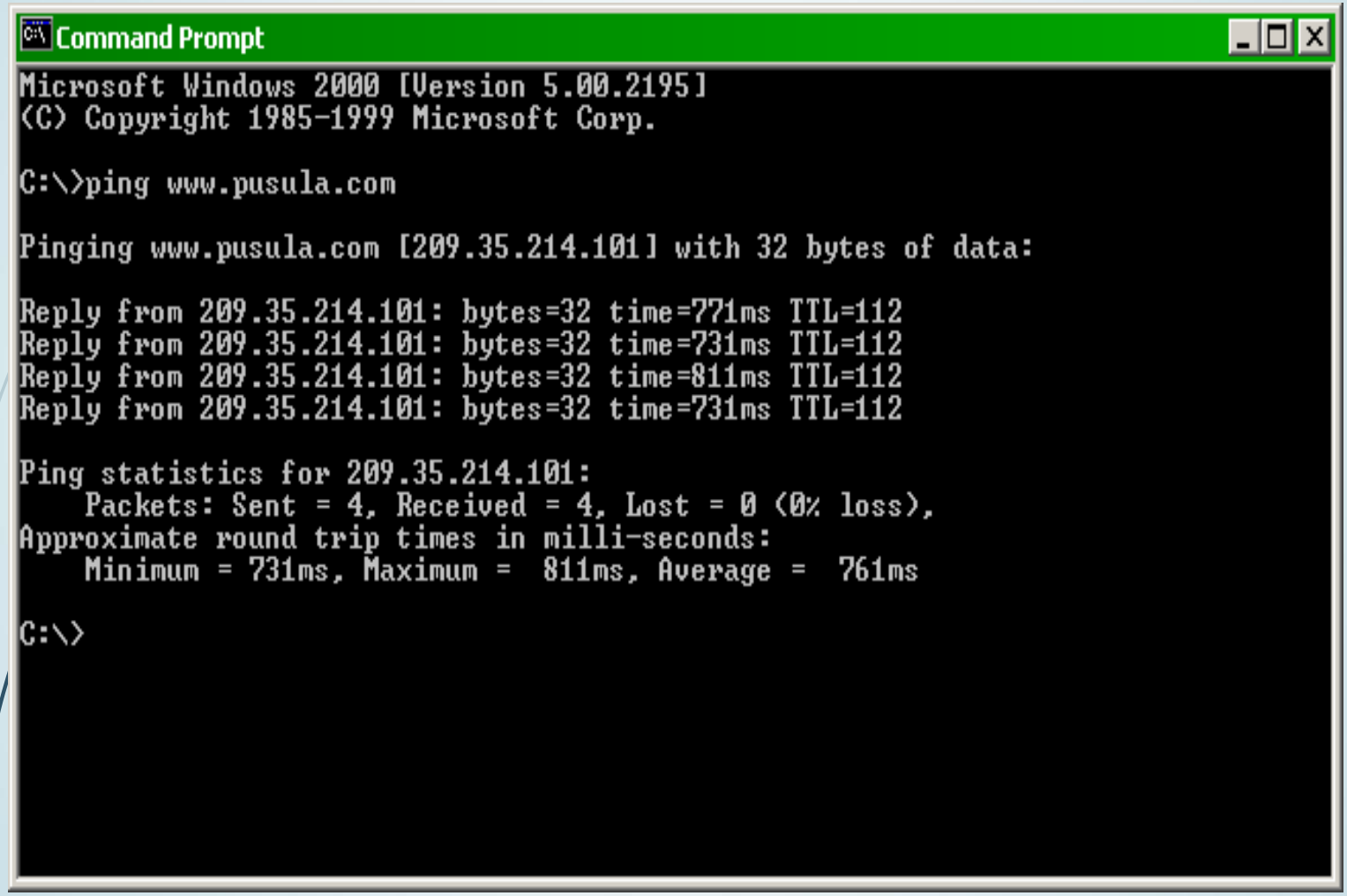
ya adres bilgisi yanlış yazılmışsa?

Veri paketleri, sonsuza kadar router dan routera yönlendirilmez mi? Bu durumda internette aşırı bir trafiğe yol açmaz mı?

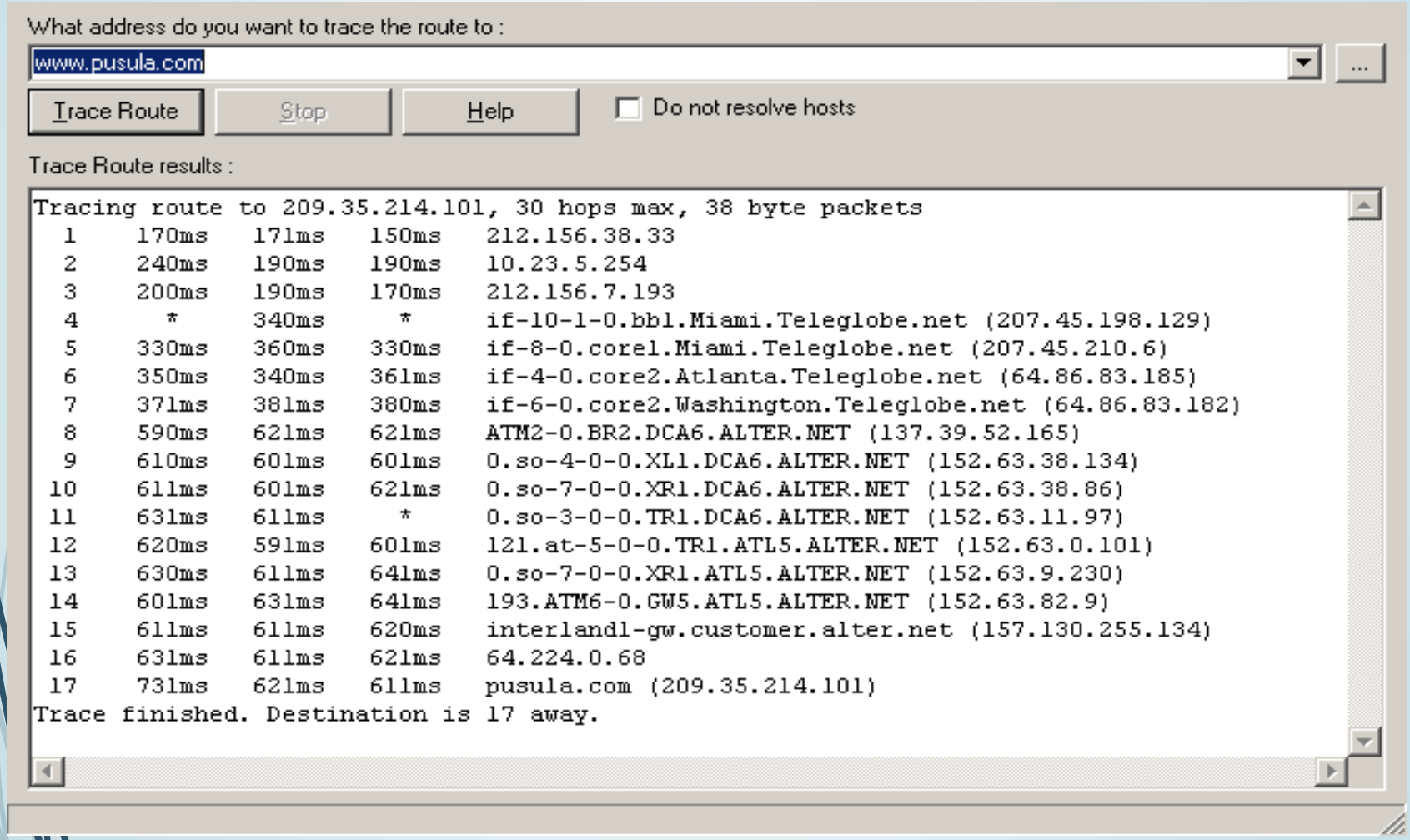
Evet bu çok doğru bir soru ve tespit. Bu durumu önlemek için TCP/IP veri paketlerinde TTL (Time-To-Live) tanımı vardır. TTL nümerik bir değer alır ve genellikle 128 olarak atanır. Veri paketinin ömrü bu değerin sıfır olması ile sona erer.

Bu TCP/IP nin bir özelliğidir.

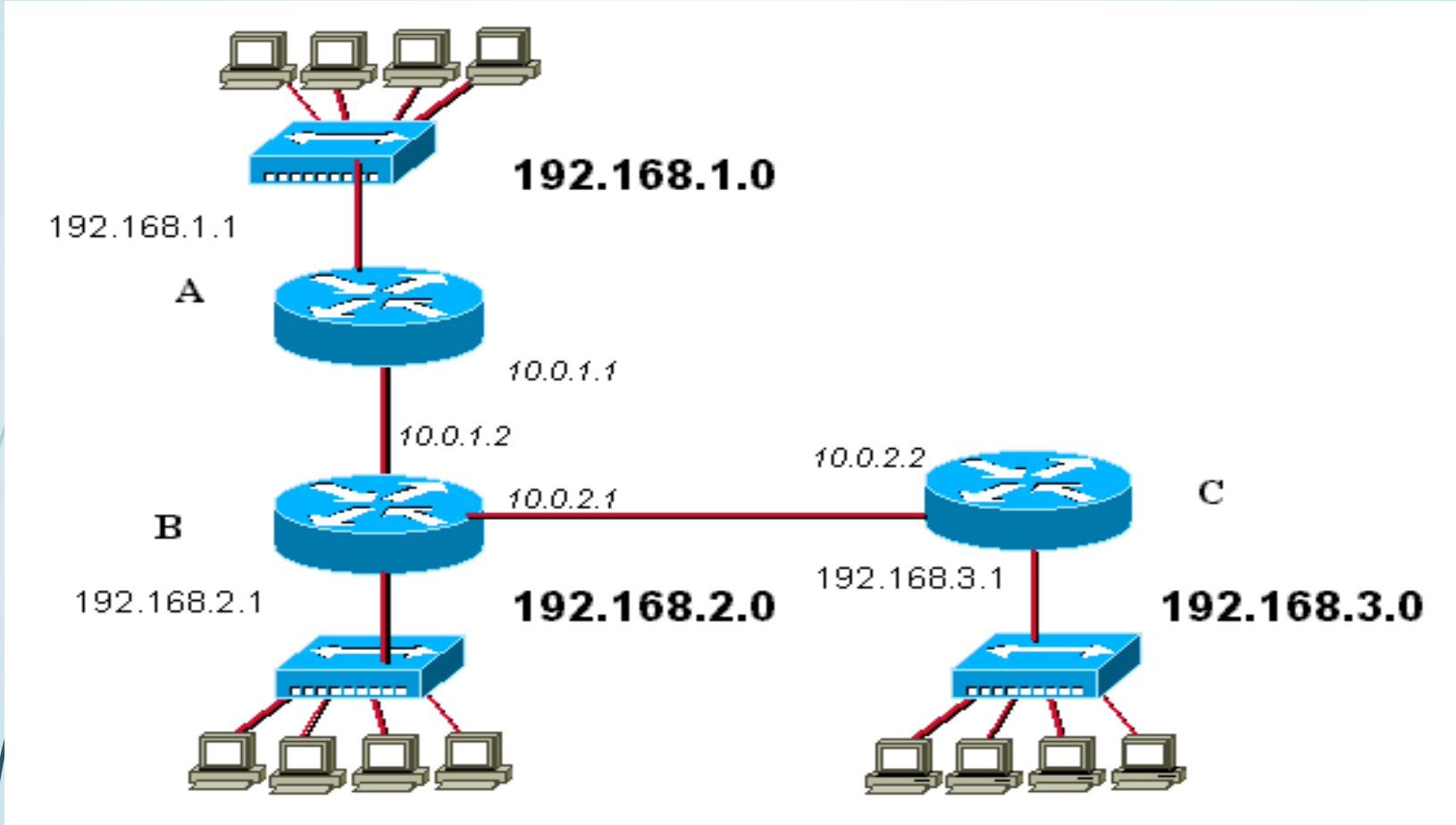
ping


Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>ping www.pusula.com
Pinging www.pusula.com [209.35.214.101] with 32 bytes of data:
Reply from 209.35.214.101: bytes=32 time=771ms TTL=112
Reply from 209.35.214.101: bytes=32 time=731ms TTL=112
Reply from 209.35.214.101: bytes=32 time=811ms TTL=112
Reply from 209.35.214.101: bytes=32 time=731ms TTL=112
Ping statistics for 209.35.214.101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 731ms, Maximum = 811ms, Average = 761ms
C:\>

tracert


What address do you want to trace the route to :
www.pusula.com
...
Trace Route
Stop
Help
Do not resolve hosts
Trace Route results :
Tracing route to 209.35.214.101, 30 hops max, 38 byte packets
1 170ms 171ms 150ms 212.156.38.33
2 240ms 190ms 190ms 10.23.5.254
3 200ms 190ms 170ms 212.156.7.193
4 * 340ms * if-10-1-0.bbl.Miami.Teleglobe.net (207.45.198.129)
5 330ms 360ms 330ms if-8-0.core1.Miami.Teleglobe.net (207.45.210.6)
6 350ms 340ms 361ms if-4-0.core2.Atlanta.Teleglobe.net (64.86.83.185)
7 371ms 381ms 380ms if-6-0.core2.Washington.Teleglobe.net (64.86.83.182)
8 590ms 621ms 621ms ATM2-0.BR2.DCA6.ALTER.NET (137.39.52.165)
9 610ms 601ms 601ms 0.so-4-0-0.XL1.DCA6.ALTER.NET (152.63.38.134)
10 611ms 601ms 621ms 0.so-7-0-0.XR1.DCA6.ALTER.NET (152.63.38.86)
11 631ms 611ms * 0.so-3-0-0.TR1.DCA6.ALTER.NET (152.63.11.97)
12 620ms 591ms 601ms 121.at-5-0-0.TR1.ATL5.ALTER.NET (152.63.0.101)
13 630ms 611ms 641ms 0.so-7-0-0.XR1.ATL5.ALTER.NET (152.63.9.230)
14 601ms 631ms 641ms 193.ATM6-0.GW5.ATL5.ALTER.NET (152.63.82.9)
15 611ms 611ms 620ms interland1-gw.customer.alter.net (157.130.255.134)
16 631ms 611ms 621ms 64.224.0.68
17 731ms 621ms 611ms pusula.com (209.35.214.101)
Trace finished. Destination is 17 away.

örnek


192.168.1.0
192.168.1.1
A
10.0.1.1
10.0.1.2
10.0.2.2
10.0.2.1
B
C
192.168.3.1
192.168.2.1
192.168.2.0
192.168.3.0

Ağ Geçidi (GATEWAY)

- Geçit, iki farklı protokol arasındaki dönüşümleri sağlar.
- Bu cihaz bir Köprü, Switch veya Yönlendirici olabilir.
- Genellikle Yönlendirici (Router) bu görevi üstlendiğinden varsayılan ağ geçidi (default gateway) olarak o tanımlıdır.

Modem

Modemler bilgisayardaki verileri yani digital sinyali, analog sinyale çevirerek kablo üzerinden iletilmesini sağlayan cihazlardır. Bağlantı için ya bütün bilgisayarlar arasına kablo çekilecek ya da mevcut telefon hatları kullanılacaktır. Kablo çekmek çok pahalı olduğundan, telefon hatlarını kullanmak çok daha mantıklıdır. Bilgi transferinin bir zorunluluk haline gelmesi ile birlikte mevcut telefon hatları üzerinden birbirine çok uzak bilgisayarların modemler aracılığı ile bağlantı kurmaları da kaçınılmaz olmuştur.

Modem

Standart telefon hatları sadece ses transferi yapabilir. İşte bu noktada modem devreye girer. Modem bilgisayardaki dijital bilgiyi analog bilgiye çevirir buna modülasyon (modulation), karşı taraftaki modemle hattan aldığı analog bilgiyi dijitale yani bilgisayarın anlayacağı dile çevirmesine de demodülasyon (demodulation) denir. Modem bu kelimelerin birleştirilmesi ile oluşmuş bir kelimedir.

Modem

Dial Up

Bu modemler internet servis sağlayıcılarının (ISS) belirledikleri telefon numaralarını çevirerek bağlantılarını sağlarlar. Bu bağlantıya çevirmeli ağ da denir. Geliştirilen protokoller ile önce karşıdaki modem ile tanışır daha sonra oturumu açarlar. Dial Up modemlerin en büyük mahzurlarından birisi bağlantı halindeyken telefon hattını meşgul etmeleridir.

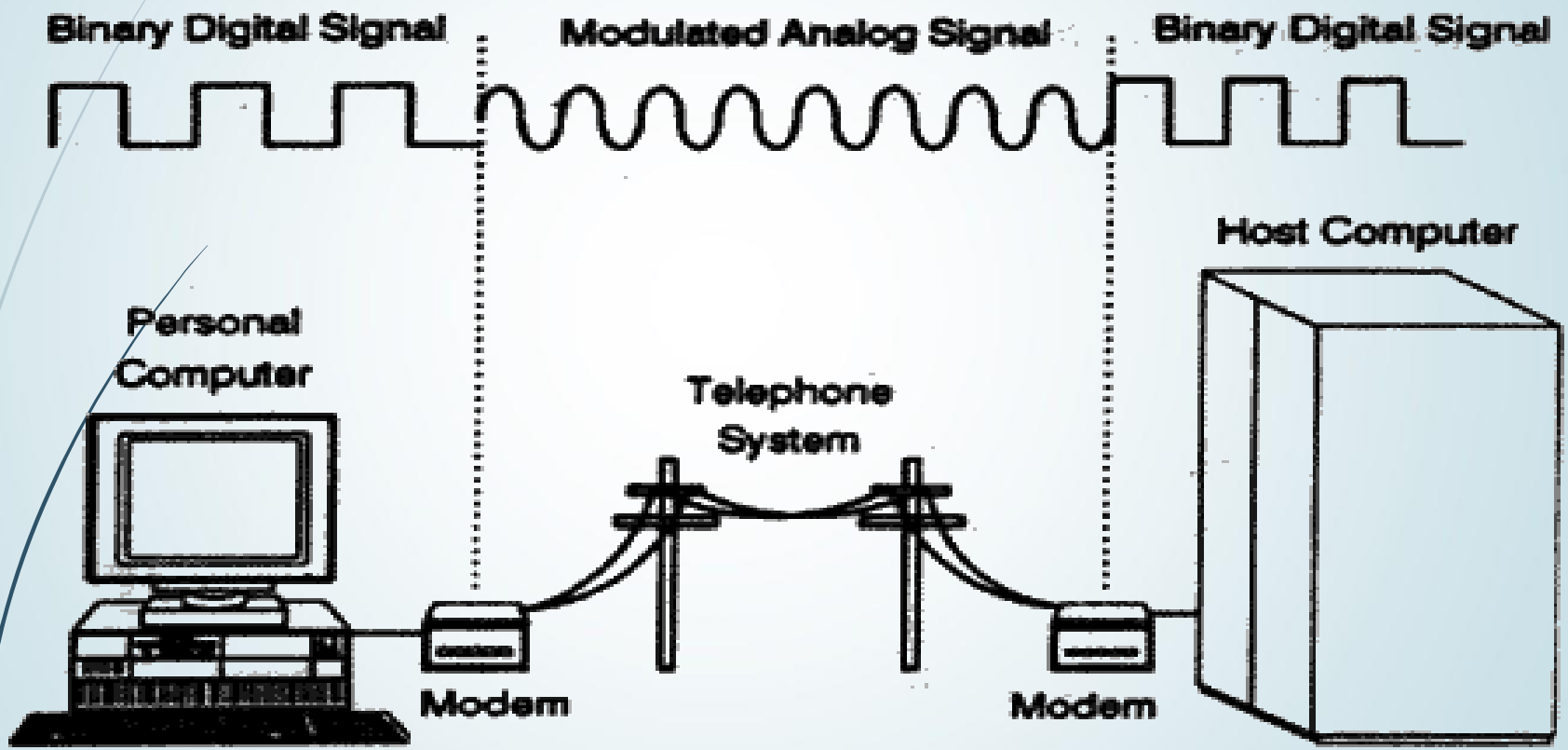
Dial Up (Çevirmeli) modemler 2400, 9600, 14400, 28800, 33600 ve 56000 bps hızlara ulaşabilirler. Şu anda piyasada satılan Dial Up modemler 56 Kbps hızındadır.

Modem

ADSL (Asymetric Digital Subscriber Line–Asimetrik Sayısal Abone Hattı)

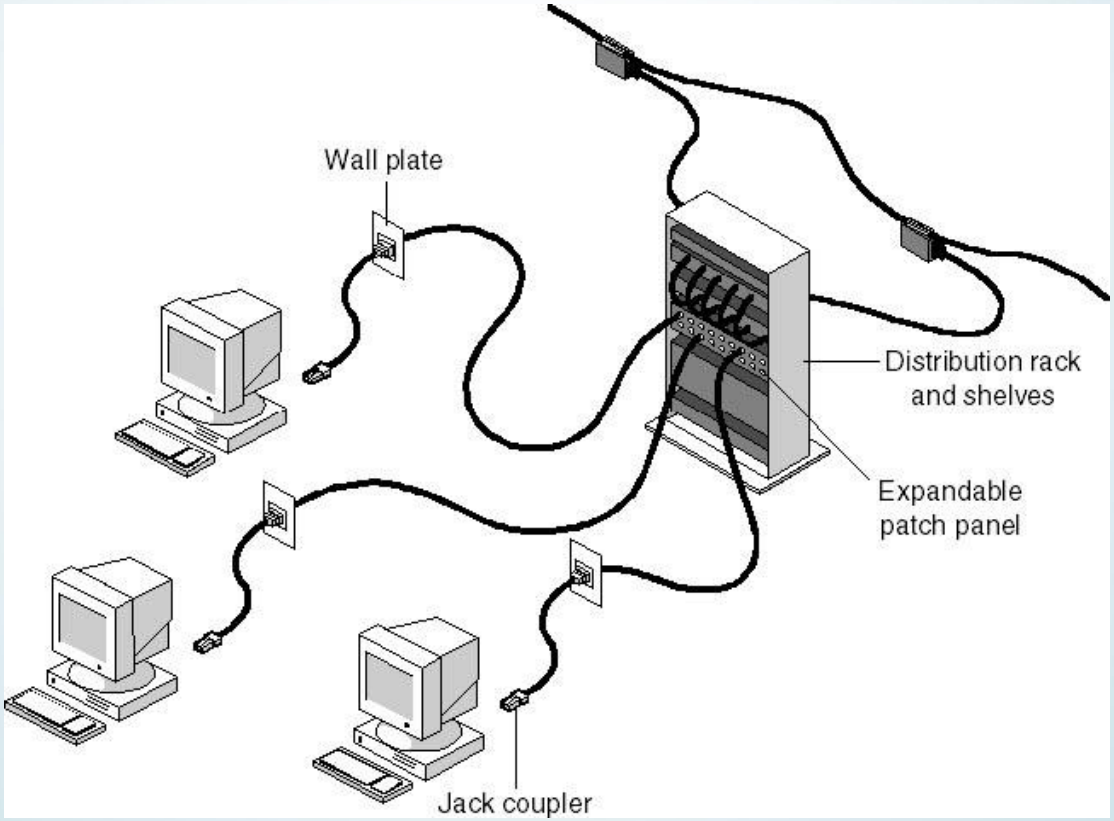
Günümüzde internet bağlantısı için en çok kullanılan bağlantı tekniğidir. Asimetrik kelimesi, veri transfer hızının, gönderim ve alım için eşit olmadığını belirtir. Kullanıcının veri alım hızı, gönderim hızından yüksek olur.
ADSL modemler digital kodlama tekniği ile telefon hatlarını % 99 verimle kullanırlar. Bağlantı sağlandığında ayırıcı splitter adlı cihaz sayesinde telefon hattını meşgul etmez.

Modem


Binary Digital Signal
Modulated Analog Signal
Binary Digital Signal
Host Computer
Personal Computer
Telephone System
Modem
Modem

Patch Panel

Bağlantı panosu



OSI ve cihazlar

OSI Katmanı	**Cihaz**
Uygulama	Ağ geçidi (Gateway)
Sunum	Ağ geçidi (Gateway)
Oturum	Ağ geçidi (Gateway)
Taşıma	Ağ geçidi (Gateway)
Ağ	Yönlendirici (Router) Katman 3 Switch
Veri İletim	Köprü (Bridge) Katman 2 Switch
Fiziksel	NIC, Yineleyici (Repeater) Hub, MAU Kablo, Alıcı ve verici, patch panel

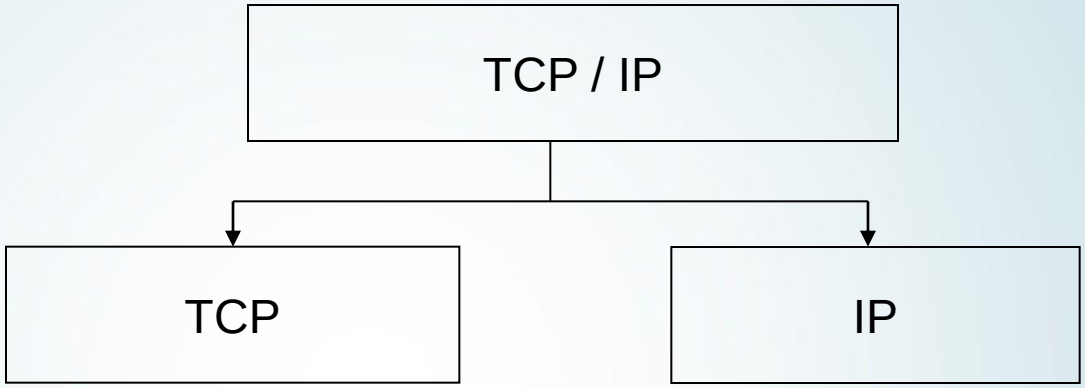
AĞ TEMELLERİ

Taşıma Katmanı veTCP/IP Protokolü

TCP/IP

- TCP/IP'nin tarihi ARPANET ile başlayan Internetin tarihidir.
- Adreslerin dağıtımı NIC (Network Information Center) tarafından yapılır.
- Türkiye'de ise bunu ODTÜ-TUBİTAK yapmaktadır.
- RFC (Request for Comments): TCP/IP standartlarını anlatan dokümanların genel adı.
- Çeşitli gönüllü kuruluşlar : ISOC (İnternetSociety : İnternet Derneği), IAB (İnternet Architecture Board : İnternet Mimarisi Kurulu)

TCP/IP

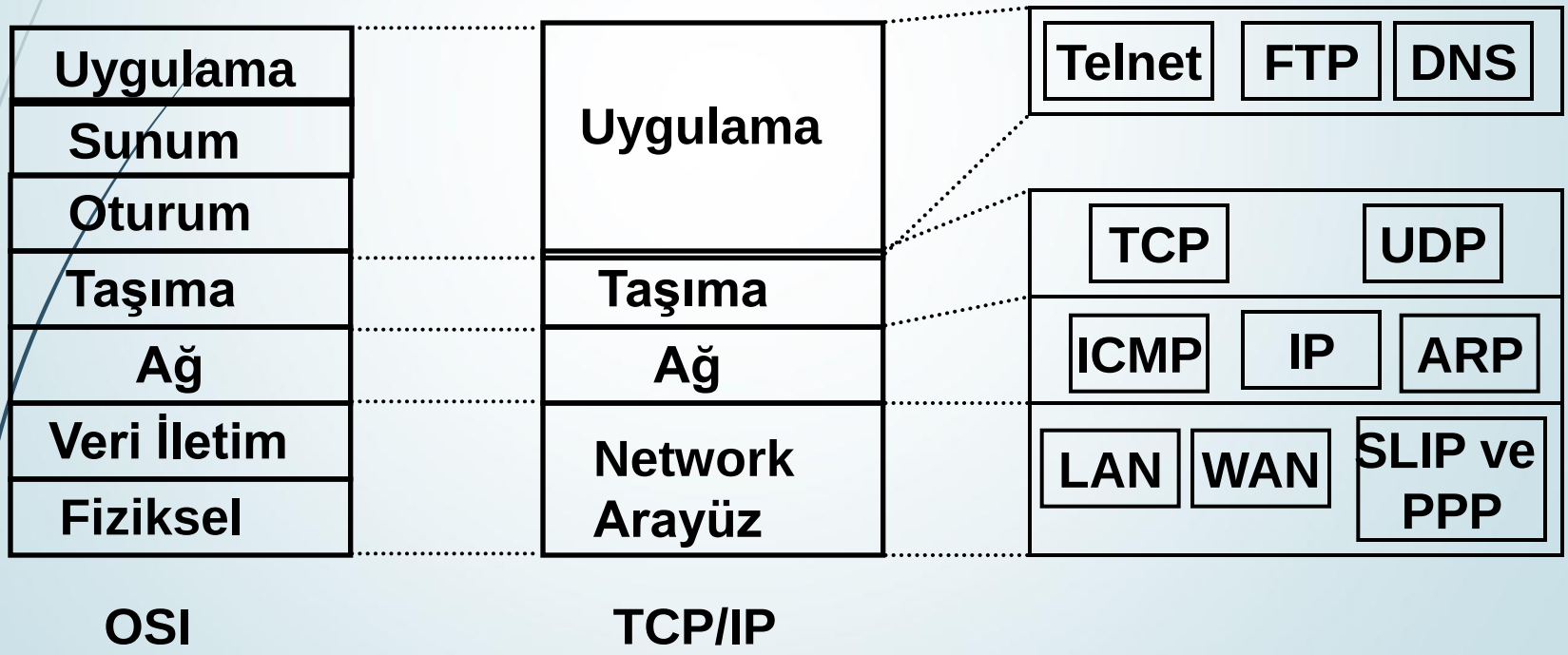


- TCP (Transmission Control Protocol)
- Paketlerin iletimi

- IP (Internet Protocol)
- Paketlerin yönlendirmesi

OSI vs. TCP/IP

1. Uygulama Katmanı (Application Layer)
2. Taşıma Katmanı (Transport Layer)
3. Ağ Katmanı (Network Layer/Internet Layer/Internetwork Layer)
4. Fiziksel Katman (Network Access Layer/Link and Physical Layer)



TCP/IP Veri Aktarımı

Terminal A

İşlem Gönderimi

Veri

Terminal B

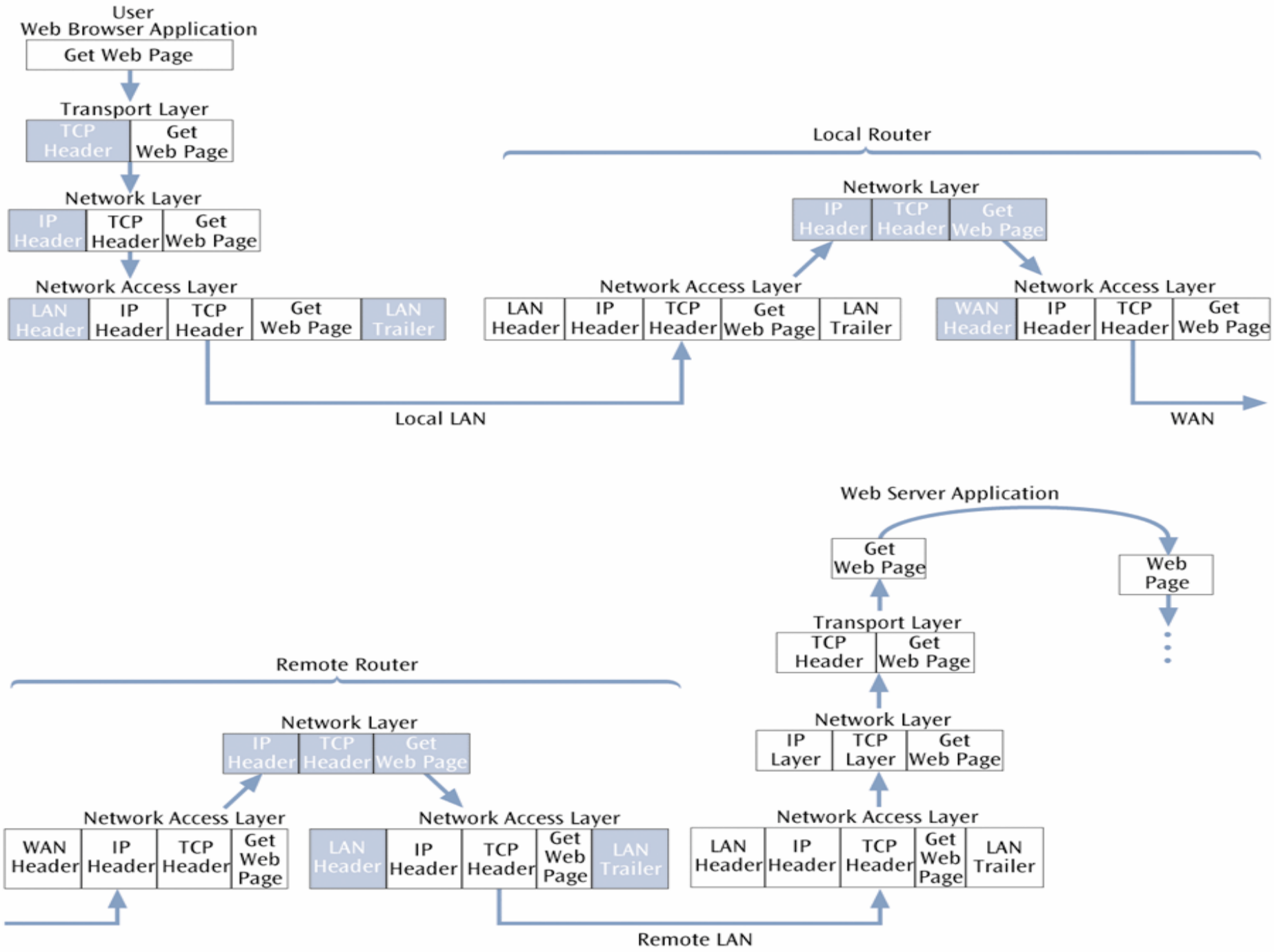
İşlem Alımı

4	**Uygulama**	Veri				**Uygulama** 4
3	**Taşıma**	Veri	TCP B.			**Taşıma** 3
2	**Ağ**	Veri	TCP B.	IP B.		**Ağ** 2
1	**Network Arayüz**	CRC	Veri	TCP B.	IP B.	MAC B. **Network Arayüz** 1

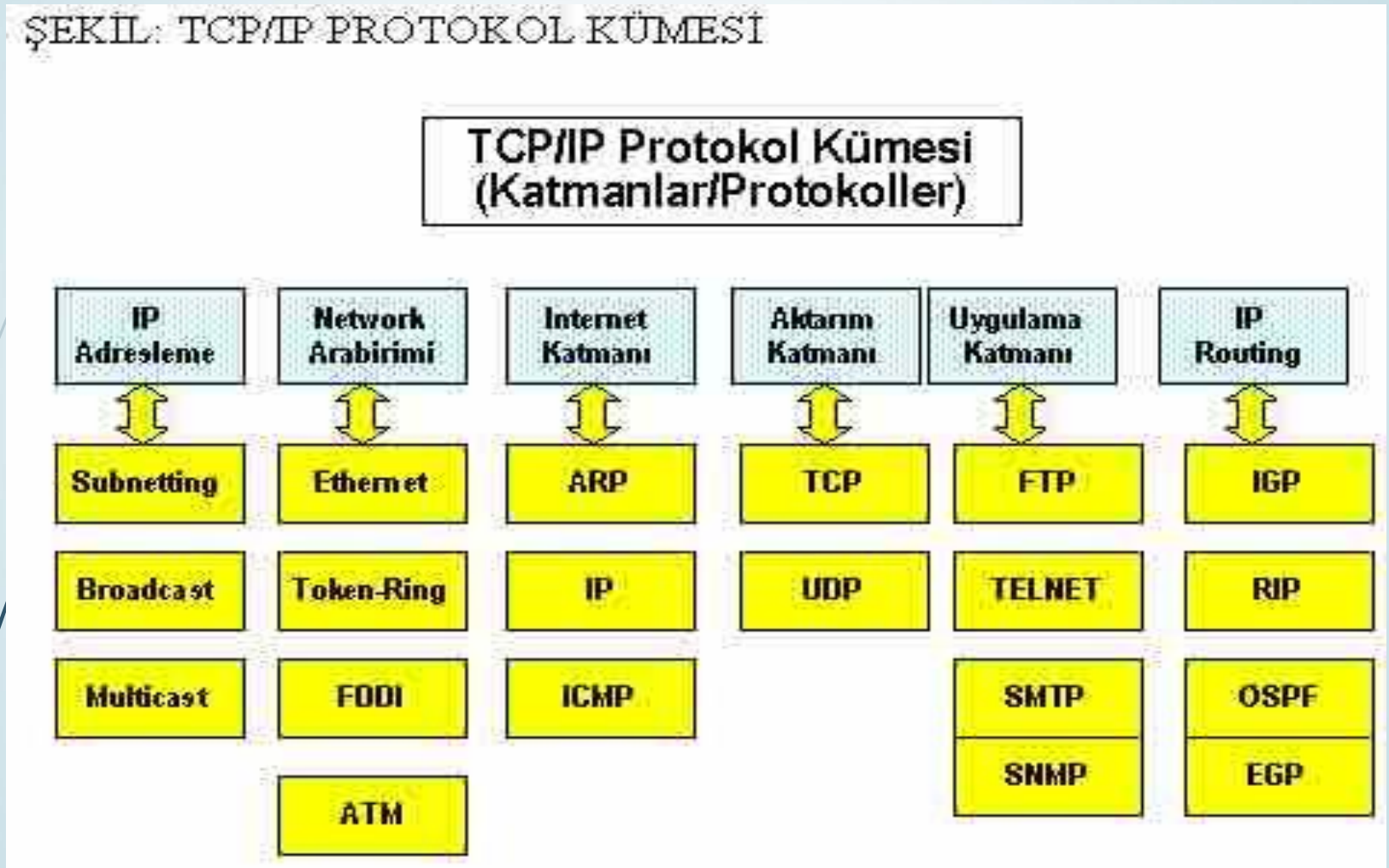
01110011110111100111001110111101

Fiziksel veri aktarımı; Kablolar vb…

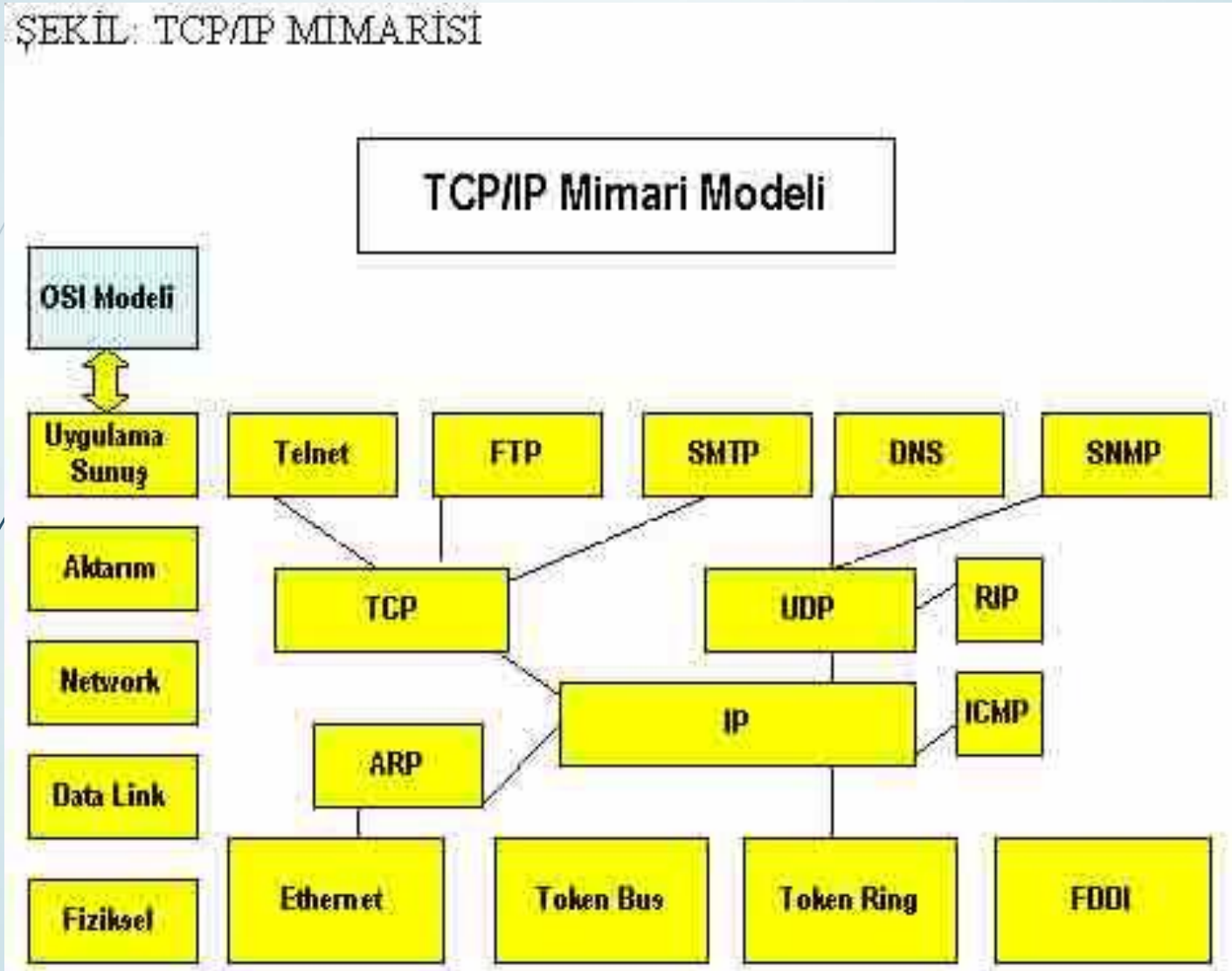
CRC: Hata kontrol kodu


User
Web Browser Application
Get Web Page
Transport Layer
TCP Header
Get Web Page
Network Layer
IP Header
TCP Header
Get Web Page
Network Access Layer
LAN Header
IP Header
TCP Header
Get Web Page
LAN Trailer
Local Router
Network Layer
IP Header
TCP Header
Get Web Page
Network Access Layer
LAN Header
IP Header
TCP Header
Get Web Page
LAN Trailer
Network Access Layer
WAN Header
IP Header
TCP Header
Get Web Page
Local LAN
WAN
Web Server Application
Get Web Page
Web Page
Transport Layer
TCP Header
Get Web Page
Remote Router
Network Layer
IP Header
TCP Header
Get Web Page
Network Layer
IP Layer
TCP Layer
Get Web Page
Network Access Layer
WAN Header
IP Header
TCP Header
Get Web Page
Network Access Layer
LAN Header
IP Header
TCP Header
Get Web Page
LAN Trailer
Network Access Layer
LAN Header
IP Header
TCP Header
Get Web Page
LAN Trailer
Remote LAN

ŞEKİL: TCP/IP PROTOKOL KÜMESİ



ŞEKİL: TCP/IP MİMARİSİ



Uygulama Katmanı Protokolleri

- DNS (*Domain Name System-Alan Adı Sistemi*)
  - Alan adı verilen isimler (www.gazi.edu.tr) ile IP adreslerini (194.27.16.10) birbirine bağlayan sistemdir.
  - Paylaştırılmış bir veritabanı olarak çalışır.
- HTTP (*HyperText Transfer Protocol-Hiper Metin Gönderme Protokolü*)
  - HTML sayfaları göndermek vb…
- HTTPS (*Secure HTTP-Güvenli HTTP*)
  - HTTP'nin RSA (İki anahtarlı şifreleme veya asimetrik anahtarlı şifreleme) şifrelemesi ile güçlendirilmiş halidir. Örneğin bankaların internet siteleri.

Uygulama Katmanı Protokolleri

- FTP (*File Transfer Protocol)* sunucu-istemci arasında dosya transfer etmek için kullanılan protokoldür. Dosya transferi için TCP, protokolü kullanılır. Binary veya ascii formatta veriler çift yönlü transfer edilebilir. Güvenilir ve connection-oriented bir servistir. ftp uygulamaları esnasında iki adet bağlantı gerçekleştirilir. Birincisi kullanıcı ve sunucu arasında bağlantı sağlarken (yetkilendirme ve güvenlik amacıyla) ikincisi veri transferi esnasında oluşturulur. Veri transferi tamamlandığında ikinci bağlantı otomatik olarak sonlandırılırken birinci bağlantı ise kullanıcı tarafından sonlandırılabilir.
- SFTP veya FTPS (*Secure FTP*),
  - FTP'nin şifreleme ile güçlendirilmiş halidir.

Uygulama Katmanı Protokolleri

- SNMP (Simple Network Managment Protocol- Basit Ağ Yönetimi Protokolü)
  - Ağlar büyüdükçe bu ağlar üzerindeki birimleri denetlemek amacıyla tasarlanmıştır.
  - PC'ye bağlı kullanıcılar, internet bağlantı hızı, sistem çalışma süresi vb. bilgiler tutulur.

Uygulama Katmanı Protokolleri

- DHCP (Dynamic Host Configuration Protocol)
  - Terminallere otomatik ip adresi dağıtır.
- NFS (Network File System-Ağ Dosya Sistemi)
  - Ağdaki paylaştırılmış dosyalara ulaşmayı sağlar
- LPD (Line Printer Daemon)
  - Ağdaki yazıcının kullanılmasını sağlar.

Uygulama Katmanı Protokolleri

- SMTP (Simple Mail Transfer Protocol, - Basit Posta Gönderme Protokolü)
  - E-posta göndermek için kullanılır.
- POP3 (Post Office Protocol 3)
  - E-posta almak için kullanılır.
- Telnet (Telecommunication Network)
  - Çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için kullanılır.

Fiziksel Katman Protokolleri

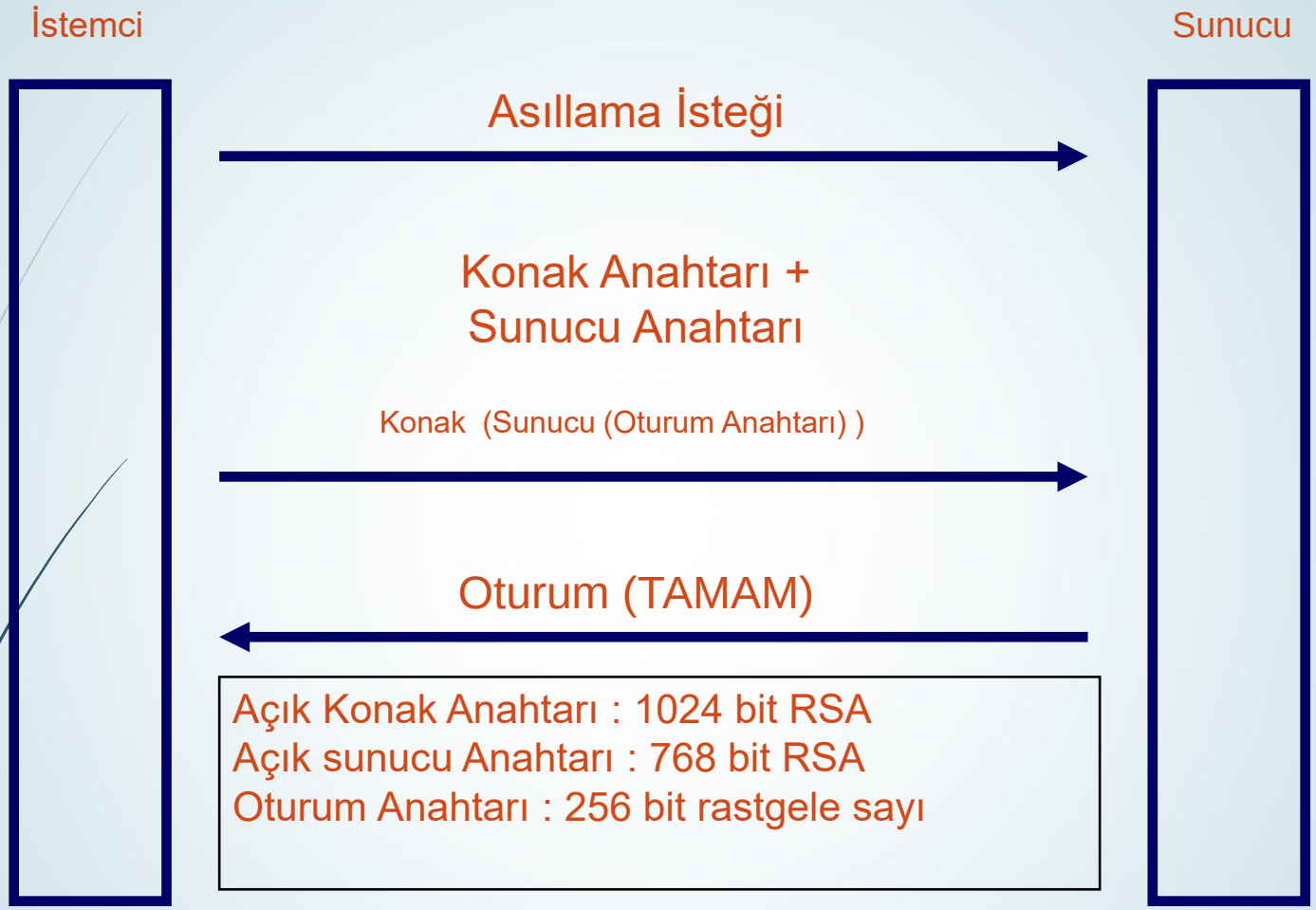
- SLIP (Serial Line Internet Protocol)
  - IP verilerinin, seri iletişim teknikleri ile iletimini sağlayan protokoldür. Dial-up veya kiralık hat bağlantılarında kullanılır. Veriler seri iletişim teknikleri kullanılarak iletilir.
- PPP (Point-to-Point Protocol)
  - SLIP'e benzer, yine dial-up bağlantıda kullanılır. Ancak PPP;
    - Verileri sıkıştırır
    - Bir çok donanım çoğunlukla destekler
    - Hata düzeltme ve belirleme algoritmaları kullanır.

Taşıma Katmanı Protokolleri

- TCP (Transmission Control Protocol-Transfer Kontrol Protokolü)
  - Veri aktarımı yapılacak iki bilgisayar arasındaki bağlantıyı kurar
  - Hata denetimi yapar. Paketler gitmediyse bir daha gönderir.
- UDP (User Datagram Protocol)
  - TCP gibi ağ üzerinden paketi gönderir ama bu protokol paketin gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağını garantilemez. Daha çok küçük paketlerin tüm PC'lere gönderilmesinde kullanılır.

Taşıma Katmanı Protokolleri

- SSH (Secure Shell, Güvenli kabuk) bir bilgisayara uzaktan girmenizi ve orada komutlar çalıştırmanızı sağlayan oldukça basit yapılı bir uygulamadır. SSH güçlü bir asıllama ve güvenli iletişim gereklerini karşılar. SSH ile bir bilgisayara bağlanabilmek için kullanıcı, öncelikle kimliğini ispatlayabilmelidir .

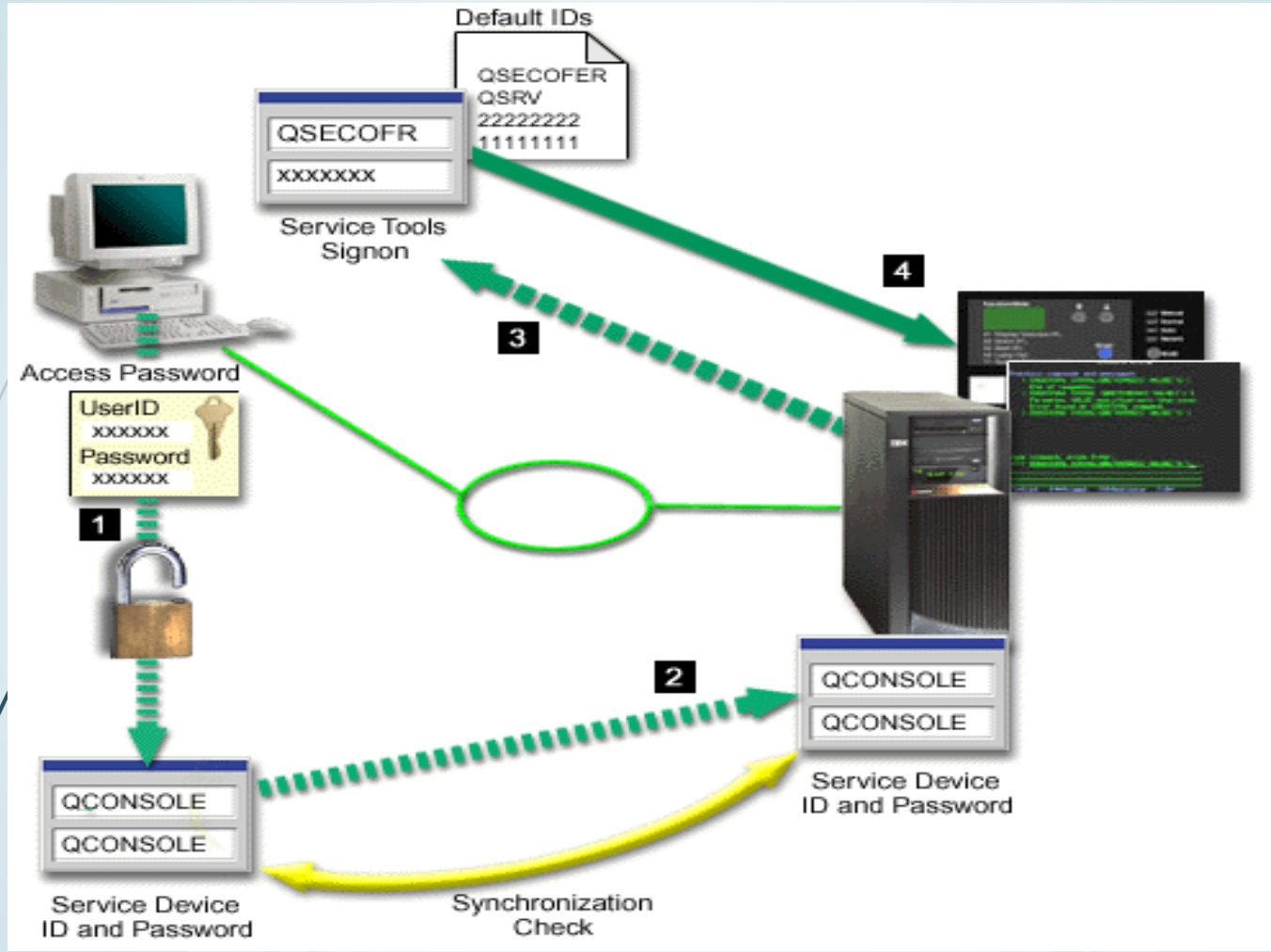

İstemci
Sunucu
Asıllama İsteği
Konak Anahtarı +
Sunucu Anahtarı
Konak (Sunucu (Oturum Anahtarı))
Oturum (TAMAM)
Açık Konak Anahtarı : 1024 bit RSA
Açık sunucu Anahtarı : 768 bit RSA
Oturum Anahtarı : 256 bit rastgele sayı

Taşıma Katmanı Protokolleri

- SSL network üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla Netscape tarafından geliştirilmiş bir güvenlik protokolüdür.
- SSL gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini sağlar. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Her iki tarafta da doğrulama yapılarak işlemin ve bilginin gizliliği ve bütünlüğü korunur .

Taşıma Katmanı Protokolleri

- Veri akışında kullanılan şifreleme yönteminin gücü kullanılan anahtar uzunluğuna bağlıdır. Anahtar uzunluğu bilginin korunması için çok önemlidir.
- Örneğin; 8 bit üzerinden bir iletimin çözülmesi son derece kolaydır. Bit, ikilik sayma düzeninde bir rakamı ifade eder. Bir bit, 0 veya 1 olmak üzere 2 farklı değer alabilir. Bir bilgisayar bu 256 (2^8=256) farklı olasılığı sıra ile inceleyerek bir sonuca ulaşabilir.
- SSL protokolünde 40 bit ve 128 bit şifreleme kullanılmaktadır. 128 bit şifrelemede 2^128 değişik anahtar vardır ve bu şifrenin çözülebilmesi çok büyük bir maliyet ve zaman gerektirir. Kötü niyetli bir kişinin 128 bitlik şifreyi çözebilmesi için 1 milyon dolarlık yatırım yaptıktan sonra 67 yıl gibi bir zaman harcaması gerekir. Bu örnekten anlaşıldığı gibi SSL güvenlik sistemi tam ve kesin bir koruma sağlar .


Default IDs
QSECOFER
QSRV
22222222
11111111
QSECOFR
xxxxxxx
Service Tools
Signon
4
3
Access Password
UserID
xxxxxx
Password
xxxxxx
1
2
QCONSOLE
QCONSOLE
Service Device
ID and Password
QCONSOLE
QCONSOLE
Service Device
ID and Password
Synchronization
Check

Taşıma Katmanı Protokolleri

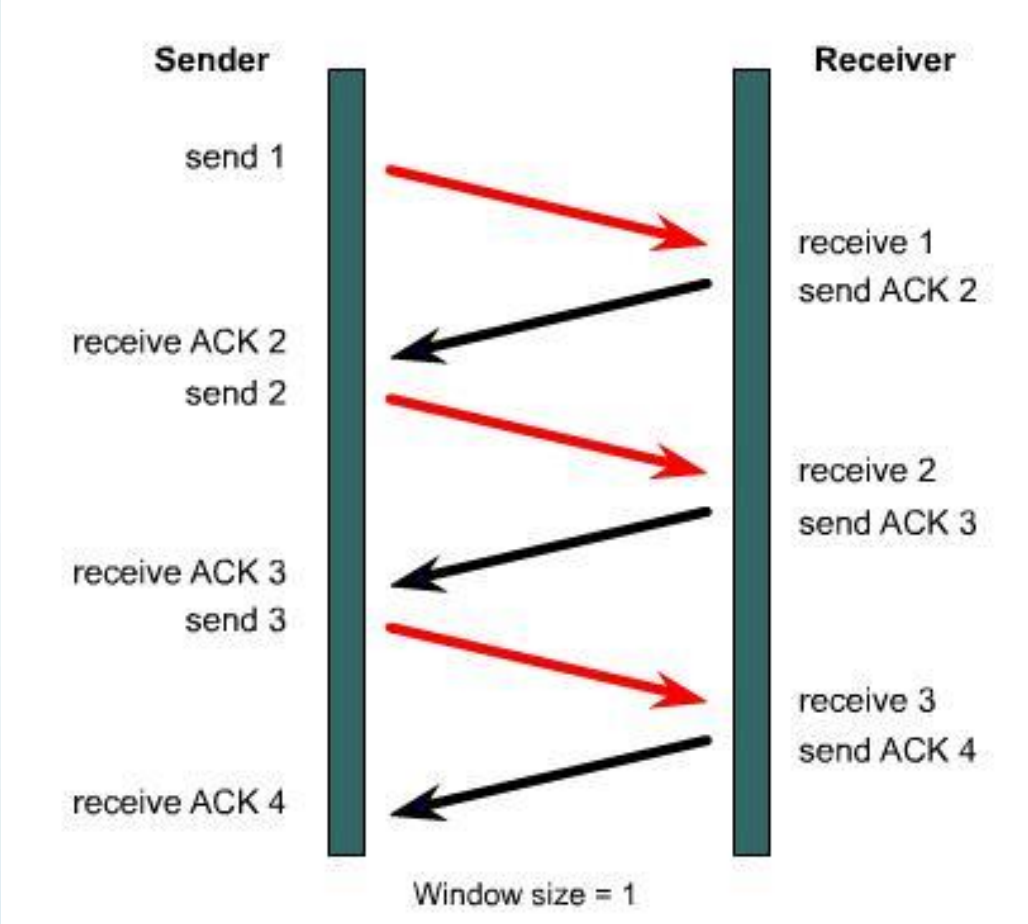
- **PCT (Private Communication Technology)** Microsoft tarafından 1995 yılında Netscape'e karşılık vermek amacıyla çıkarılmış, temelinde SSL 2.0'dan farkı olmayan bir iletişim kuralıdır .
- **TLS (Transport Layer Security)** IETF tarafından SSL 2.0, SSL 3.0, SSH 2.0 ve PCT 1.0 temel alınarak geliştirilmiştir.
- TLS kayıt ve tokalaşma iletişim kuralları ayrılarak geliştirilmiş ve belgeleri hazırlanmıştır. Tüm bunların yanında geriye uyumu sağlamak amacıyla TLS 1.0 SSL 3.0 ile çalışabilecek şekilde tasarlanmıştır .

TCP Görevleri

1. Bir üst katmandan gelen verinin uygun uzunlukta parçalara bölünmesi,
2. Her bir parçaya alıcı kısımda aynı biçimde sıraya koyabilmesi amacıyla sıra numarası verilmesi,
3. Kaybolan veya bozuk gelen parçaların tekrarlanması imkânı verilebilir.

TCP Özellikleri

1. Bir bağlantının (connection) kurulması ve sonlandırılması.
2. Güvenilir (reliable) paket dağılımının sağlanması.
3. Akış kontrolü (flow kontrol) ile hostlarda veri taşmasının (overflow) önlenmesi.
4. Bozulmuş verilerin düzeltilmesi. (Error recovery)
5. Alıcı host içerisinden birçok uygulama arasından çoğaltma yapılması.


Sender
Receiver
send 1
receive 1
send ACK 2
receive ACK 2
send 2
receive 2
send ACK 3
receive ACK 3
send 3
receive 3
send ACK 4
receive ACK 4
Window size = 1

TCP (Transmission Control Protocol)

Bağlantı kurulumu;

A bilgisayarı B bilgisayarına TCP yoluyla bağlanmak istediğinde şu yol izlenir.

- A bilgisayarı B bilgisayarına TCP bağlantı isteği yollar.
- B bilgisayarı A bilgisayarının isteğini aldığına dair bir TCP ACK mesajı yollar.
- A bilgisayarı B bilgisayarına TCP ACK mesajını aldığını teyit eder.

Bağlantı Three Way Handshake sonucunda gerçekleşir.

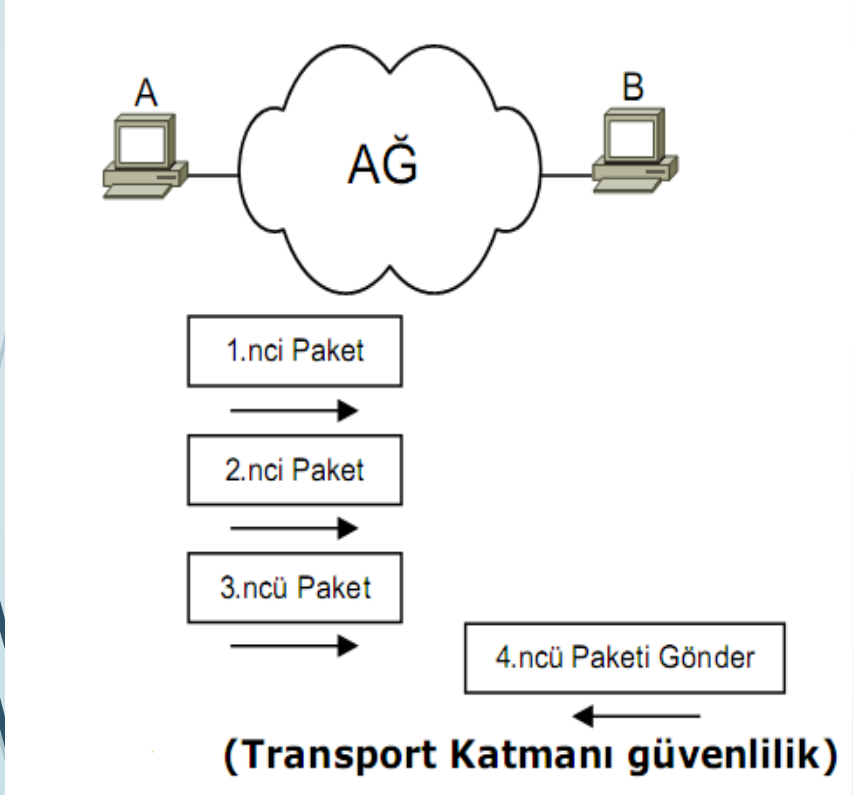
TCP Fonksiyonları

Nakil katmanı, datayı kaynak bilgisayardan hedef bilgisayara güvenli bir şekilde taşıyan ve data akışını düzenleyen katmandır. Bu işlem sırasında yapılan 2 önemli fonksiyon vardır.

- Güvenlilik (Reliability)
- Akış Kontrolü (Flow Kontrol)

Güvenlilik (Reliability)

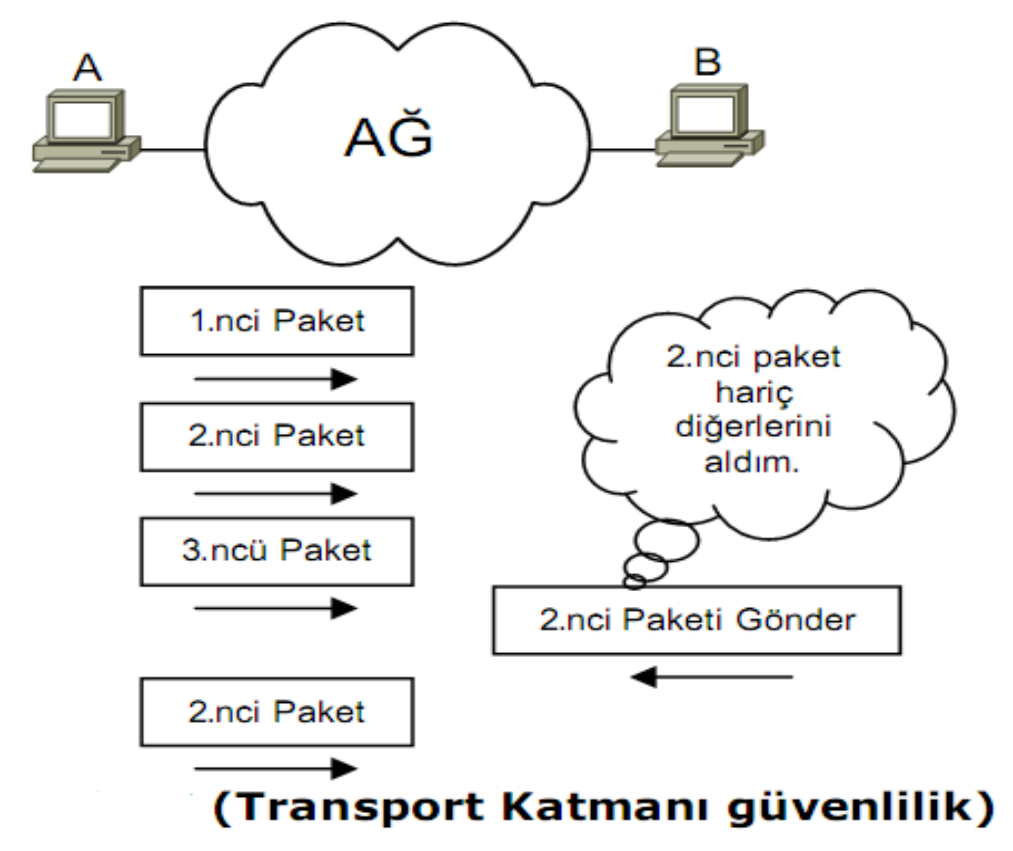
İki bilgisayar arasında gerçekleştirilen data iletişiminde gönderilen datanın sağlıklı bir şekilde alınıp alınmadığını yöneten, alınmadığı takdirde tekrar gönderilmesini sağlayan bir fonksiyondur.



A bilgisayarı B bilgisayarına 3 data paketi göndermiş ve bu dataların alındığını onaylamak istemektedir. Gönderilen her bir data transport katmanı protokolü tarafından numaralandırılmaktadır. B bilgisayarı da gönderilen dataları aldığını ve bir sonraki data paketlerini beklediğini belirten bir onay mesajı gönderir. Bu mesaja gönderim onayı (forward acknowledgment) denir.

Güvenlilik (Reliability)

Eğer A bilgisayarının gönderdiği data paketlerinden ikinci paket B bilgisayarı tarafından alınmamışsa bu A bilgisayarına bildirilir. A bilgisayarı da ya sadece 2 nolu paketi ya da 2'den sonraki bütün paketleri tekrar gönderir.



Akış Kontrolü (Flow Control)

İletişim halindeki bilgisayarlardan gönderen bilgisayar, data paketlerini alan bilgisayarın alabileceği kapasiteden daha fazla olabilmektedir. Dolayısıyla datayı alan bilgisayar, data paketlerini yok edebilmektedir. Ayrıca gönderen bilgisayar,ağda bulunan anahtar ve yönlendirici gibi ağ cihazlarının kapasitesini zorlayabilmektedir. Aynı şekilde bu cihazlar da data paketlerini yok edeceklerdir. Bazen datayı alan bilgisayarın arabelleği (buffer) yeteri kadar büyük olmayabilir veya işlemcisi çok miktarda datayı işliyor olabilir. Bütün bu sebeplerden dolayı tıkanma (congestion) olmaktadır. Bu tıkanıklığı giderebilmek için data gönderim miktarını kontrol etmek üzere akış kontrol sistemi kullanılmaktadır. Bu sistemde 3 metot kullanılmaktadır. Bunlar;

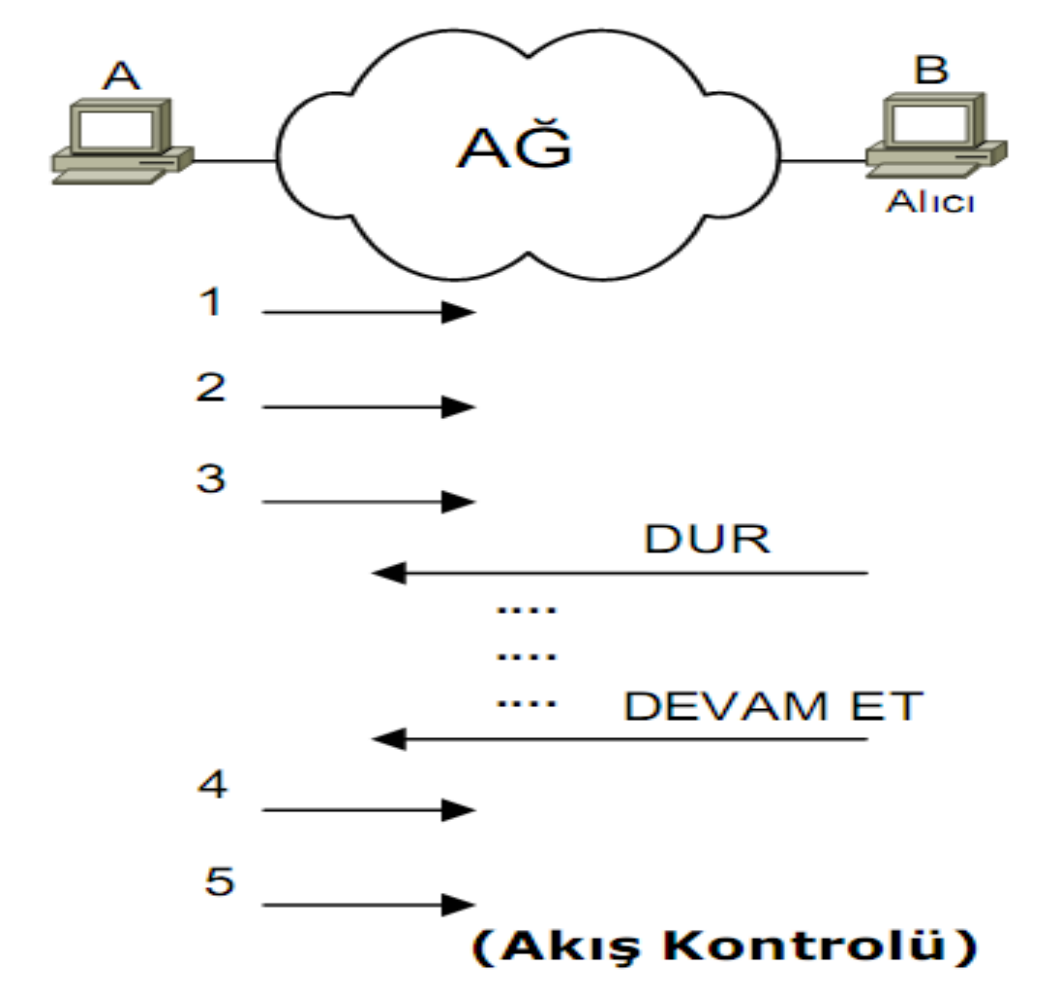
- Ara Bellekleme (Buffering)
- Tıkanıklıktan Kaçınma (Congestion Avoidance)
- Pencereleme (Windowing)

➢ Ara Bellekleme (Buffering)

Data akış hızına müdahale etmeden alınan data, bilgisayarın kapasitesini aştığı durumlarda bilgisayarın ara belleğinde yer açma işlemidir. Böylece belli bir süre arabellekte tutulan data, bilgisayarın yükü azaldığı zaman hemen işleme sokulmaktadır.

➢ Tıkanıklıktan Kaçınma (Congestion Avoidance)

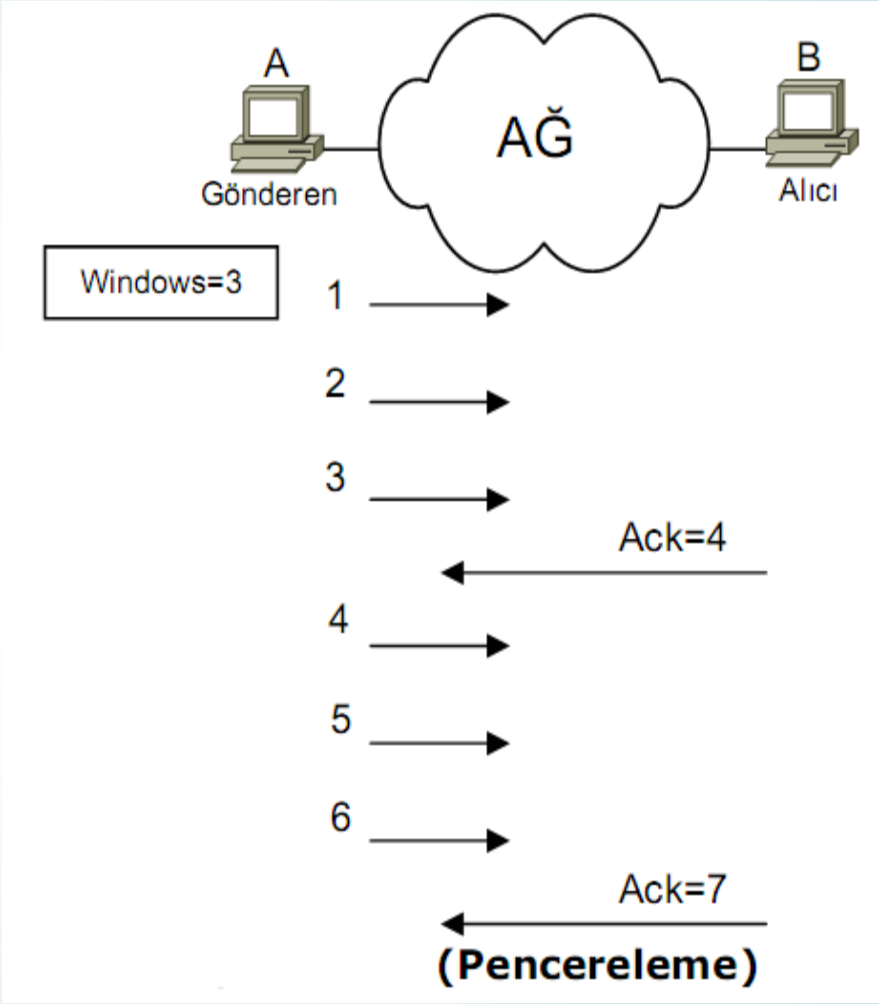
Data paketlerini alan bilgisayarın arabelleği dolduğu durumlarda data paketlerini gönderen bilgisayara ya gönderme işlemini durdur ya da yavaşlat şeklinde mesajlar göndermektedir. Böylece alınmış olan data paketlerini işlemek üzere belli bir süre kazanmaktadır. TCP/IP iletişimde ICMP mesajları içerisinde “Source Quench” adlı mesaj data paketlerini gönderen bilgisayara hızını yavaşlatmasını ifade etmektedir.


A
AĞ
B
Alıcı
1
2
3
DUR
....
....
....
DEVAM ET
4
5
(Akış Kontrolü)

➢ Pencereleme (Windowing)

Data iletişimi sırasında gönderilen datanın güvenli bir şekilde gidip gitmediğinin öğrenilmesi ve oluşacak data kayıplarının telafi edilmesi çok önemlidir. Bu takibin daha etkili bir şekilde yapılması için gönderen bilgisayarın onay almadan gönderebileceği maksimum miktarda data paketi belirlenir. Bu işleme pencereleme (windowing) denir.

Şekilde görüldüğü gibi pencere sayısı 3 olan bir iletişimde ilk üç data paketi gönderilir ve sonrasında bu paketlerin güvenli bir şekilde gidip gitmediğine dair onay beklenir. Eğer bozulmuş paket varsa bu paket tekrar gönderilir ve tekrar başka bir 3 data paketi gönderilir. Bu şekilde sistem çalışmaya devam eder.



ACK(Acknowledge-aldığını bildirmek)

TCP Segment Yapısı

TCP'nin (Transmission Control Protocol-İletişim Kontrol Protokolü) temel işlevi, üst katmandan (uygulama katmanı) gelen bilginin segmentler haline dönüştürülmesi, iletişim ortamında kaybolan bilginin tekrar yollanması ve ayrı sıralar halinde gelebilen bilginin doğru sırada sıralanmasıdır. Peki bu segmentlere ayrılma işi nasıl gerçekleşmekte ?

Şekil 1.8: TCP segment formatı

TCP kendisine atanmış olan bu görevleri yapabilmek amacıyla, ulaşım katmanında veri parçalarının önüne başlık bilgisi ekler. Başlık bilgisi veri parçası, ikisi birlikte TCP segmenti olarak anılır. TCP segmenti bir alt katmana (IP katmanına) gönderilir, oradan da bu segmente IP başlığı eklenerek alıcıya yönlendirilir.

TCP Segment Yapısı

Şekil 1.8: TCP segment formatı

TCP Segment Yapısı

- Gönderici Port: Gönderen bilgisayarın çalıştırdığı uygulamanın portu.(2 byte)
- Alıcı Port: Alan bilgisayarın çalıştıracağı uygulamanın portu.(2 byte)
- Sıra No: Gönderilen paketin sıra numarasını gösterir.(4 byte)
- Onay No: Gelecek TCP oktetinin ilk bitinin sıra numarasıdır. (4 byte)
- Başlık Uzunluğu: TCP başlığında var olan 32 bit uzunluğundaki sözcüklerin sayısını gösterir. (4 bit)
- Saklı Tutulmuş (Reserved): Sıfır olarak ayarlanmıştır.(6 bit)

TCP Segment Yapısı

- Kod Bit: Oturumun oluşturulması ve kesilmesi gibi kontrol fonksiyonlarıdır. (6bit)
- Pencere: Gönderilecek maksimum data miktarını belirler.(2 byte)
- Hata sınama bitleri (Checksum): Data ve başlık alanlarını kullanarak yapılan bir hesap.(2 byte)
- Acil işaretcisi (Urgent): Acil datanın sona erdiğini belirtir. (2 byte)
- Seçenekler: Sadece bir tane tanımlanmıştır. Maksimum TCP segment büyüklüğü ya da 32 bittir.
- Kullanıcı Verisi: Üst katmandan gelen datadır.

Transport Katmanı Port Numaraları

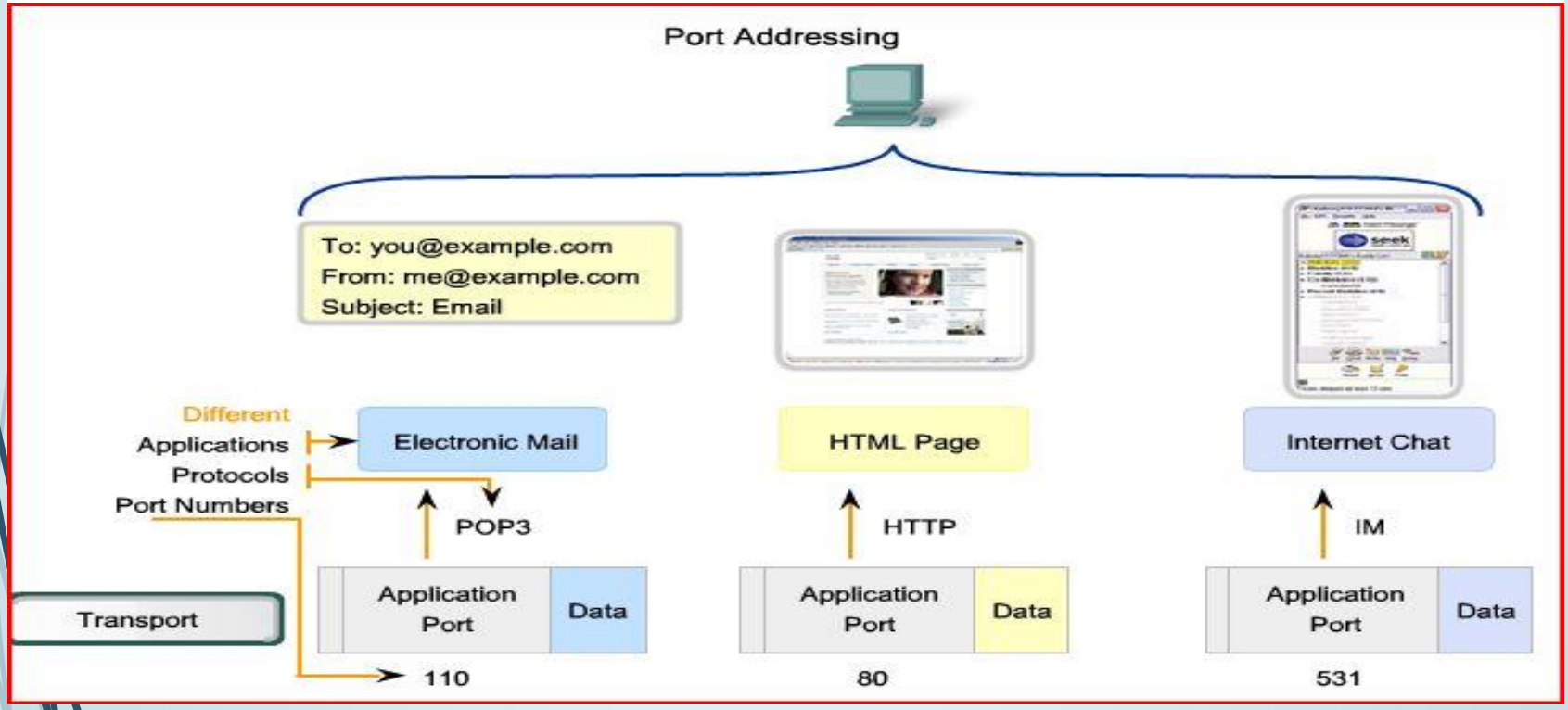
TCP/IP ortamında programların çalıştırılması ve servisler genellikle istemci-sunucu tabanlıdır. Sunucu ve istemci arasında bir haberleşme gerçekleşir. Bu işlemi gerçekleştirmek için her servise bir numara verilmiştir. İşte istemciler bu numaraları kullanarak hangi uygulamayla konuşacağını belirtir. Bu numaralar port numaraları olarak adlandırılır. İnternet sunusunda binlerce port vardır. Ancak etkin bir kullanım için iyi bilinen ve her zaman kullanılan servislere standart port numarası verilmiştir.

Bazı servislerin standart port numaraları

Transport Katmanı Port Numaraları

Uygulama Katmanı	FTP	TELNET	DNS	SMTP	SNMP	TFTP
Port No	21	23	53	25	161	69
Transport Katmanı	TCP				UDP	

(Port Numaraları)



Transport Katmanı Port Numaraları

Ağ Servisi	Port No
FTP veri transferi	TCP Port 20
FTP kontrol	TCP Port 21
Telnet	TCP Port 23
SMTP	TCP Port 25
DNS	UDP port 53
HTTP	TCP/UDP Port 80
POP3	TCP Port 110
SHTTP	TCP/UDP Port 443

Ağ Katmanı Protokolleri

- IP (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)

Ağ Katmanı

- OSI ağ katmanı, ağlar arasında iletilmek üzere oluşturulan Ağ katmanı paketini, en uygun yolu belirleyerek iletmekten sorumludur.

- Ağ katmanı veriyi belirli bir ağa yönlendirir ve ilgili olmayan ağlara veri göndermez .

Ağ Katmanı

- Ağ katmanı veri paketinin farklı bir ağa gönderilmesi durumunda yönlendiricilerin kullanacağı bilginin eklendiği katmandır.

- Örneğin; IP protokolü bu katmanda görev yapar.

IP

- IP (Internet Protocol)
- IP adresi bir ağa bağlı bilgisayarların ağ üzerinden birbirlerine veri yollamak için kullandıkları adrestir.
- IP adresleri şu anda yaygın kullanımda olan IPv4 için 32 bit boyunda olup, noktalarla ayrılmış 4 adet 8 bitlik sayıyla gösterilirler. Örneğin: 192.167.10.5
- IP adresi sayısal bir değer olup IP ağlardaki her bir cihazın sahip olması gerekir. IP adresleri MAC adreslerinin tersine donanımsal bir adres değil sadece yazılımsal bir değerdir.

Adres Çözümleme Protokolü (ARP)

- Adres Çözümlemesi'nden kasıt, karşı bilgisayarın IP adresini sisteme vermemize karşılık veri hattı katmanından karşı makinenin LAN adaptörüne ait olan MAC adresini elde etmektir.
- ARP, IP adresinden MAC adresi elde eden bir protokoldür.

Niçin MAC adresi alınır?

- Ağ katmanı protokollerinin (TCP/IP, Netbios gibi) adresleri herhangi bir veriden farksız işlem görür. LAN'da yapılacak her türlü iletişim için LAN adaptör kartının donanımsal adresini bilmemiz gerekiyor. Çünkü fiziksel katmanda asıl iletişimi bu alt seviye katmanları yapacaktır.

Çalışma Sistemi;

- Genelde ARP, ARP belleği olarak bilinen haritalama tabloları ile çalışır. Tablo, bir IP adres ile bir fiziksel adres (MAC adresi) arasında haritalama yapılmasını sağlar.
- ARP hedef IP adresini alır ve haritalama tablosundan bunun karşıladığı hedef fiziksel adresi arar. Eğer ARP adresi bulursa, bulduğu fiziksel adresi , isteği yapan cihaza yollar.

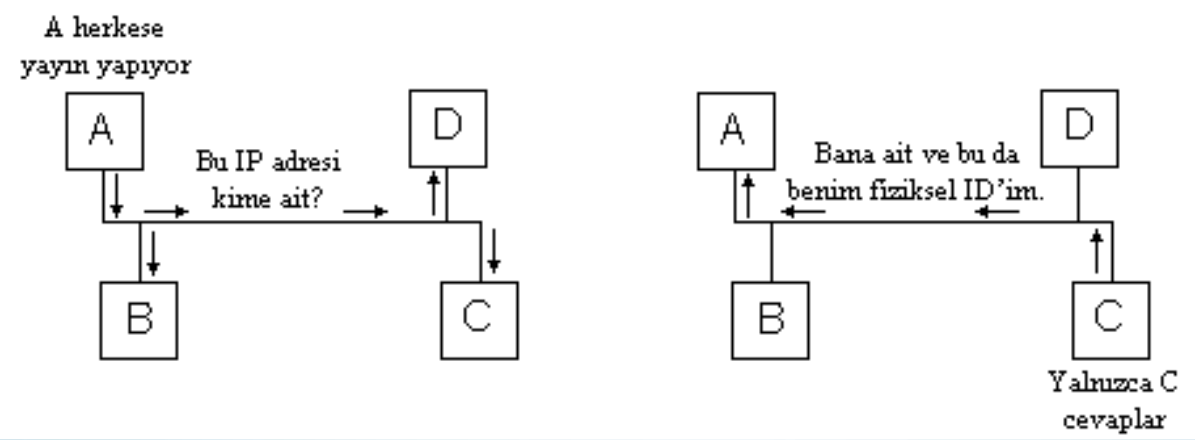
Çalışma Sistemi;

- Gerekli adres ARP belleğinden bulunamazsa, ARP modülü ağa bir yayın yapar. Yayına ARP isteği (ARP request) denir. Bu yayın bir IP hedef adresi içerir.

- ARP isteğindeki IP adresine sahip olan host, isteği yapan host'a kendi MAC adresini içeren ARP cevap (ARP reply) gönderir.

Örnek 1:

ARP isteği ve cevabı kavramları Şekil 1'de gösterilmiştir. A host'u C'nin fiziksel adresini bulmak istemektedir. A bu yüzden B, C, D'ye datagram (ip paket birimi) yayınlar. Bu yayına yalnızca C cevap verir çünkü gelen ARP istek datagramında kendi IP adresinin olduğunu görür. C host'u kendi MAC adresini ARP cevabı formunda bir IP datagramına yerleştirir.



Şekil 1: ARP İsteği ve Cevabı

Adres Çözümleme Protokolü (ARP)

ARP istek ve cevap paketlerine ait alanlar:

- **Fiziksel katman başlığı:** Fiziksel katman paketinin başlığıdır.
- **Donanım:** Donanım arabirim tipini belirtir (Ethernet, paket radyo vs.).
- **Protokol:** Göndericinin kullandığı protokol tipini tanımlar; tipik olarak EtherType'dır.
- **Donanım adres uzunluğu:** Paketteki donanım adreslerinin bayt olarak uzunluğunu belirtir.
- **Protokol adres uzunluğu:** Paketteki protokol adreslerinin bayt olarak uzunluğunu belirtir (Ör, IP adresleri).
- **Opcode:** Paketin bir ARP request (1) veya bir ARP reply (0) olduğunu belirtir.
- **Gönderici donanım adresi:** Göndericinin donanım adresini içerir.
- **Gönderici protokol adresi:** Göndericinin IP adresini içerir.
- **Hedef donanım adresi:** Sorgulanan host'un donanım adresini içerir.
- **Hedef protokol adresi:** Sorgulanan host'un IP adresini içerir.

Not: Request (İstek) paketinde hedef donanım adresi alanı dışındaki tüm alanlar kullanılır. Reply (Cevap) paketinde ise tüm alanlar kullanılır.

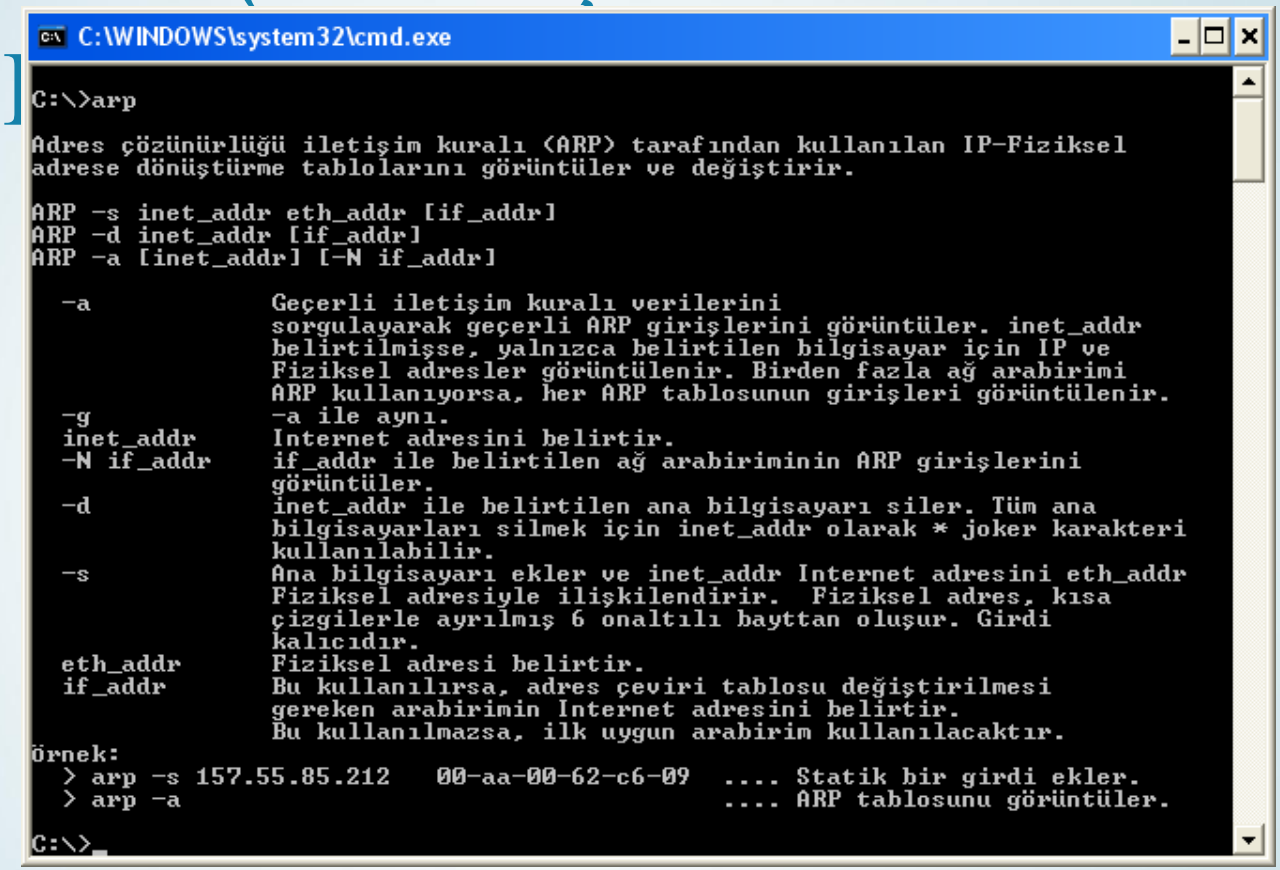
ARP Önbelleği:

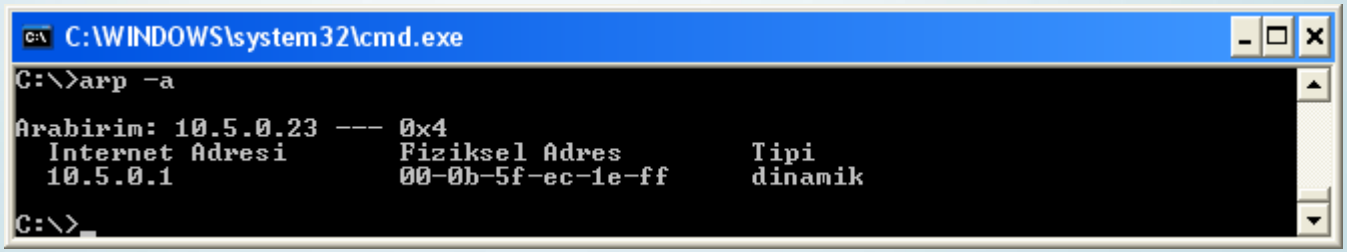
ARP yayın sayısını en alt düzeye düşürmek için, haritalama yaptığı IP adresleri ile MAC adreslerini ön belleğinde tutar. ARP önbelleğinde dinamik ve statik girdiler olabilir.

Her dinamik ARP önbelleği girdisi potansiyel olarak 10 dakikalık bir ömre sahiptir. Önbelleğe eklenen yeni girdilere zaman bilgisi girilir. Bir girdi eklendikten sonra 2 dakika içinde yeniden kullanılmazsa zaman aşımına uğrar ve ARP önbelleğinden silinir.

Not: Her ağ bağdaştırıcısı için ayrı bir ARP önbelleği vardır.

ARP (Adres Çözümleme
]





Ters Adres Çözümleme Protokolü (RARP)

- RARP (**R**everse **ARP**) ARP'ın yaptığının tersini yapar, yani hangi MAC adresinin hangi IP adresine tekabül ettiğini bulur.
- RARP'de ise host kendi IP adresini bilmez. Yayın yaparak ağdaki cihaza donanım adresini yollar ve ağın RARP sunucusu bu host'a IP adresini bildirir.

AĞ TEMELLERİ

Fiziksel Katman

Fiziksel Katman Nedir?

- Fiziksel katman; verinin bit dizisi halinde iletim ortamı üzerinden aktarılması için gerekli işlevleri kapsar.
- Fiziksel katman, verinin doğrudan iletim ortamına aktarılması için gerekli tanımlamaları ve arayüz standartlarını içerir.
- Taşıyıcı işaretin şekli, bağlantılarda kullanılacak konnektör şekli, kablo türü, kablosuz iletim, verici ve alıcı konumundaki uç noktaların elektriksel ve mekaniksel özellikleri fiziksel katman içinde tanımlanır.

Fiziksel Katman Nedir?

- Fiziksel katman verinin gönderilmesini ve alınmasını tanımlayan katmandır.
- Fiziksel katman verilerin bit olarak (elektronik olarak) iletimiyle ilgilenir. Veri paketleriyle, framelerle, adreslerle ya da verinin ulaşacağı hedef ile ilgilenmez.
- Verinin iletileceği medya ile ilgilidir.

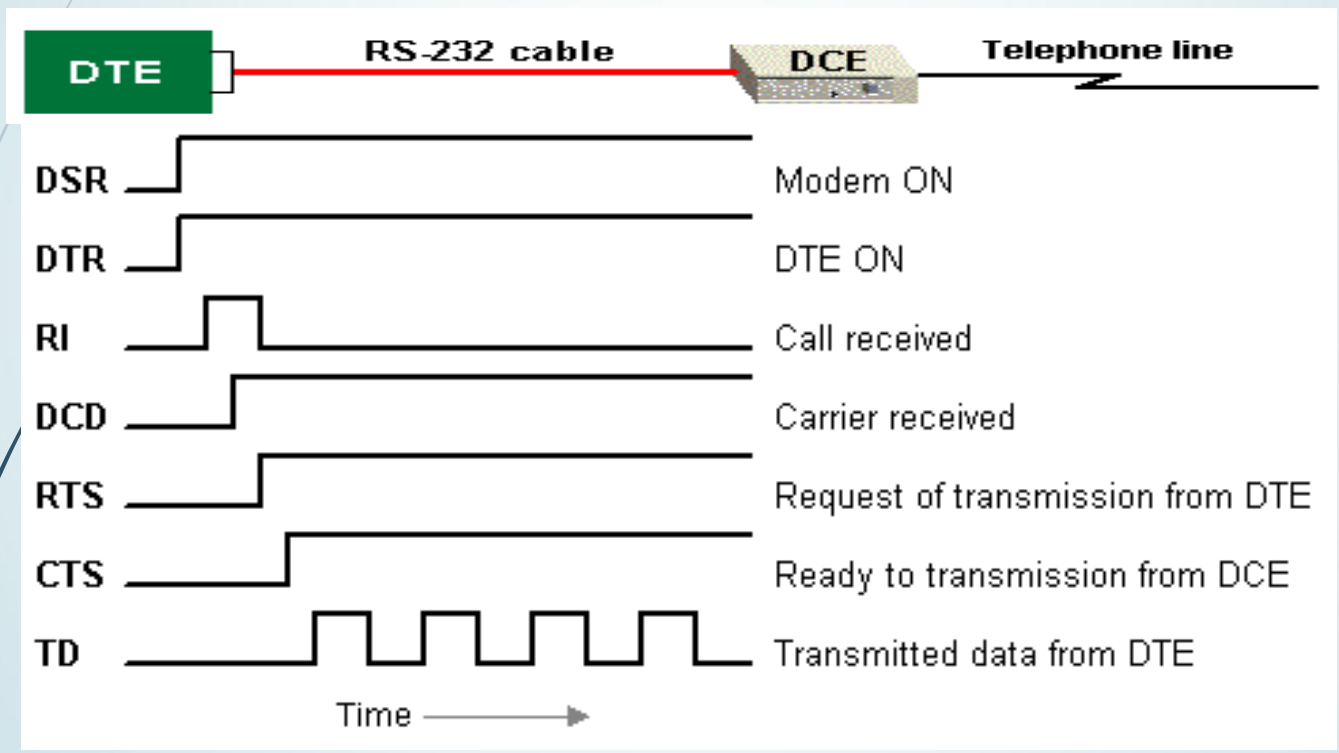
DTE- DCE NEDİR?

- DTE (Data Terminal Equipment): Veriyi iletişim kanalında taşınacak biçime sokan veya iletişim ortamından gelen bilgiyi terminallerin kullanacağı hale getiren düzeneklerdir.

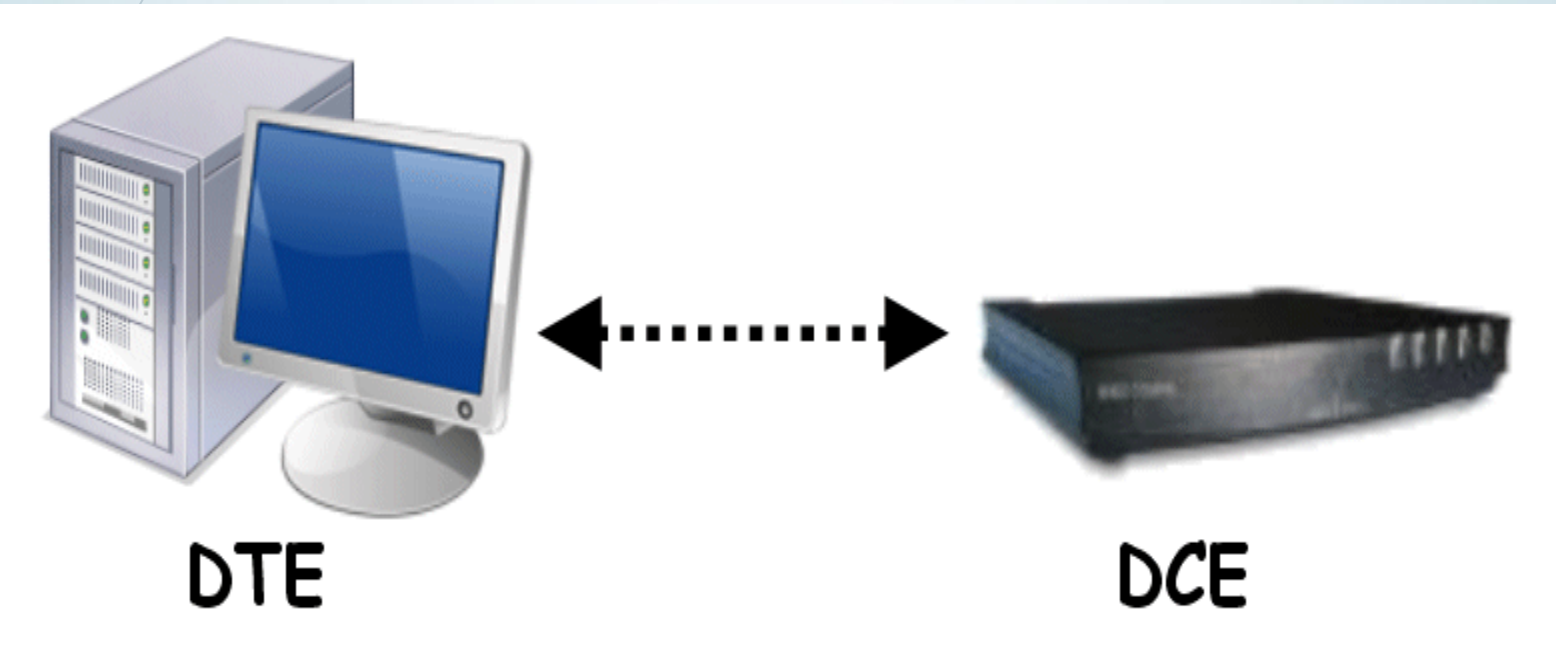
  Örnek: PC, Yönlendirici, Yazıcı

- DCE (Data Communication Equipment) : “Veri devresi sonlandırma düzeneği”. İletme ve almayı fiziksel olarak gerçekleştiren aygıtlardır.
- Veri iletişim araçları olarak da bilinirler.
- Örnek olarak modem verilebilir.

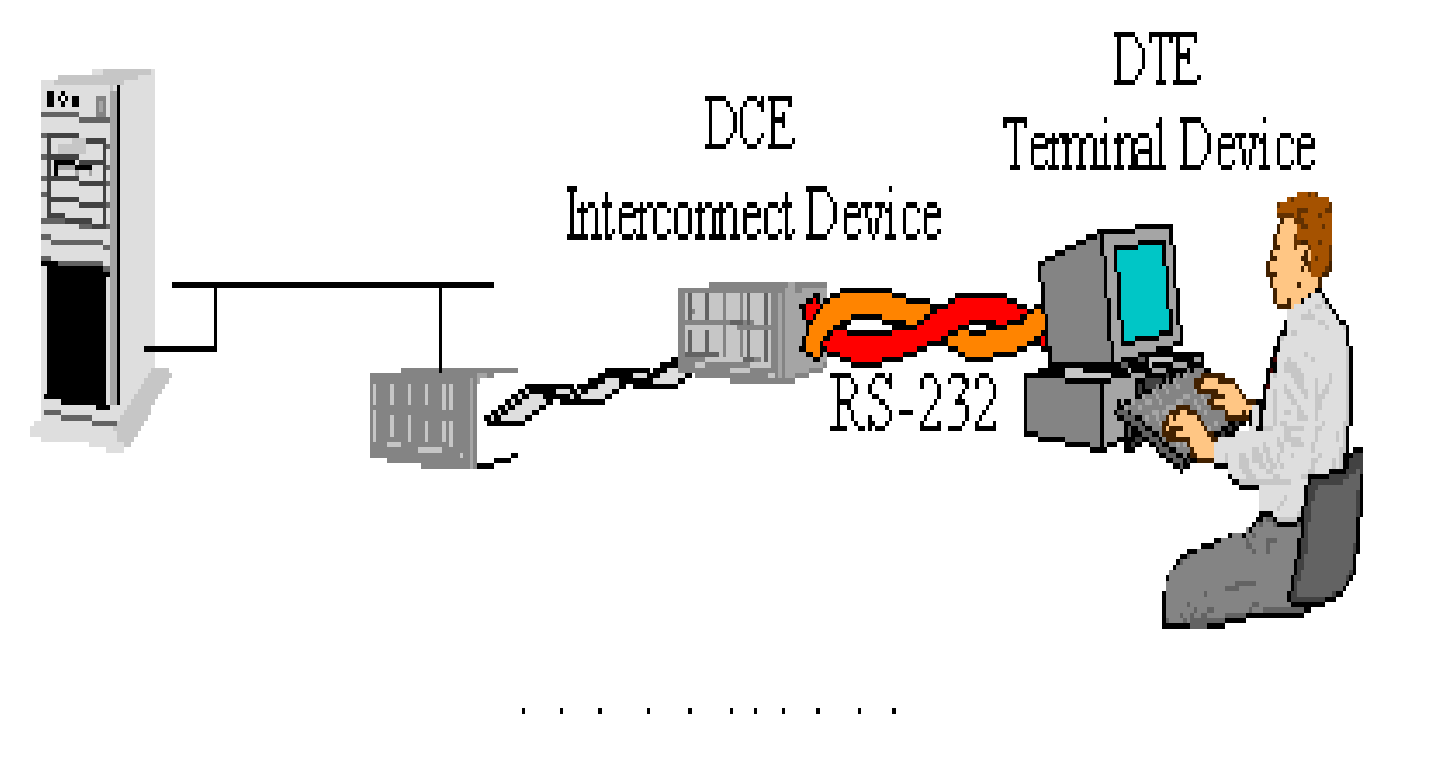
DTE-DCE Arasında Veri İletimi



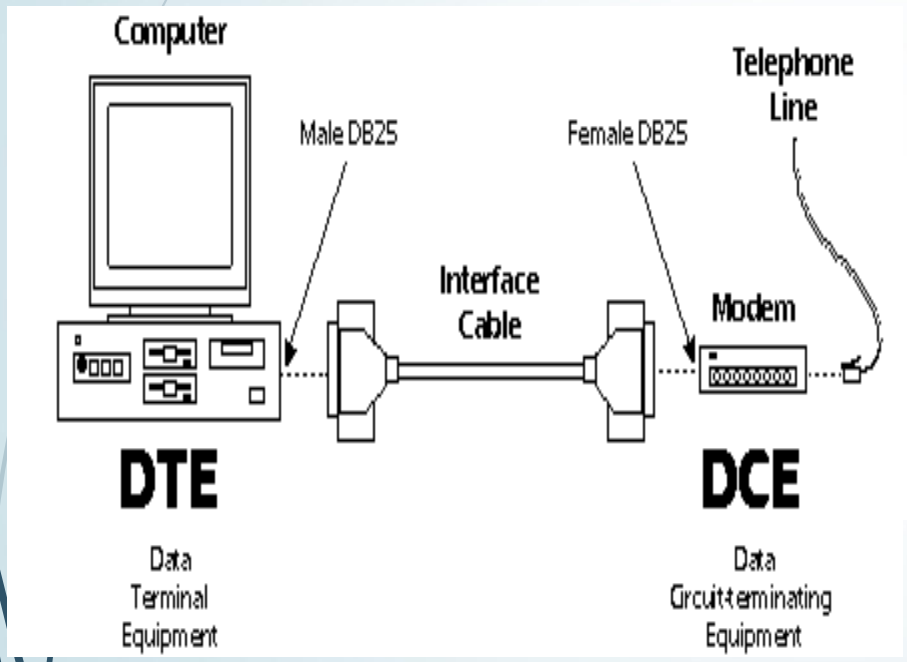
DTE-DCE Bağlantı Örnekleri

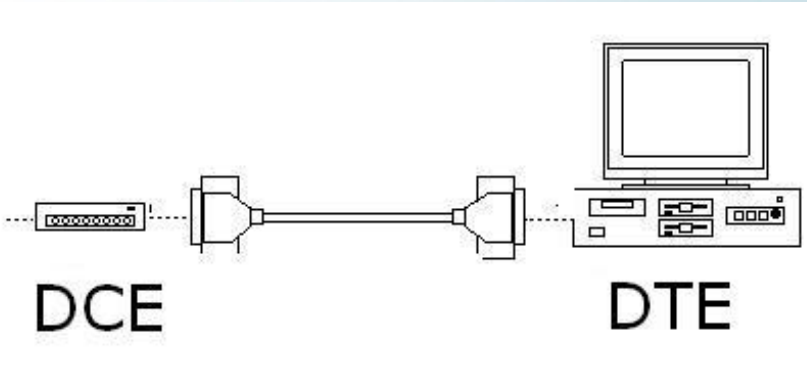


DTE-DCE Bağlantı Örnekleri



DTE-DCE Bağlantı Örnekleri



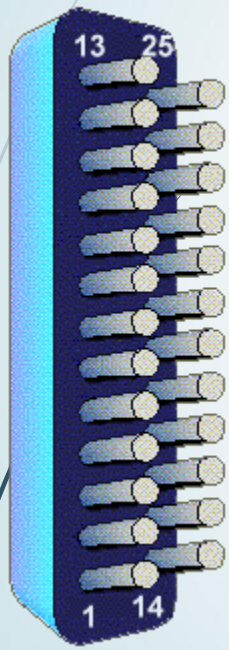


DTE-DCE Standartları

- RS-232/V.24 Standardı
- RS-422A,RS-423A Standardı
- RS-449/V.35 Standardı

RS-232 Standardı

RS232 Pinout on DB25



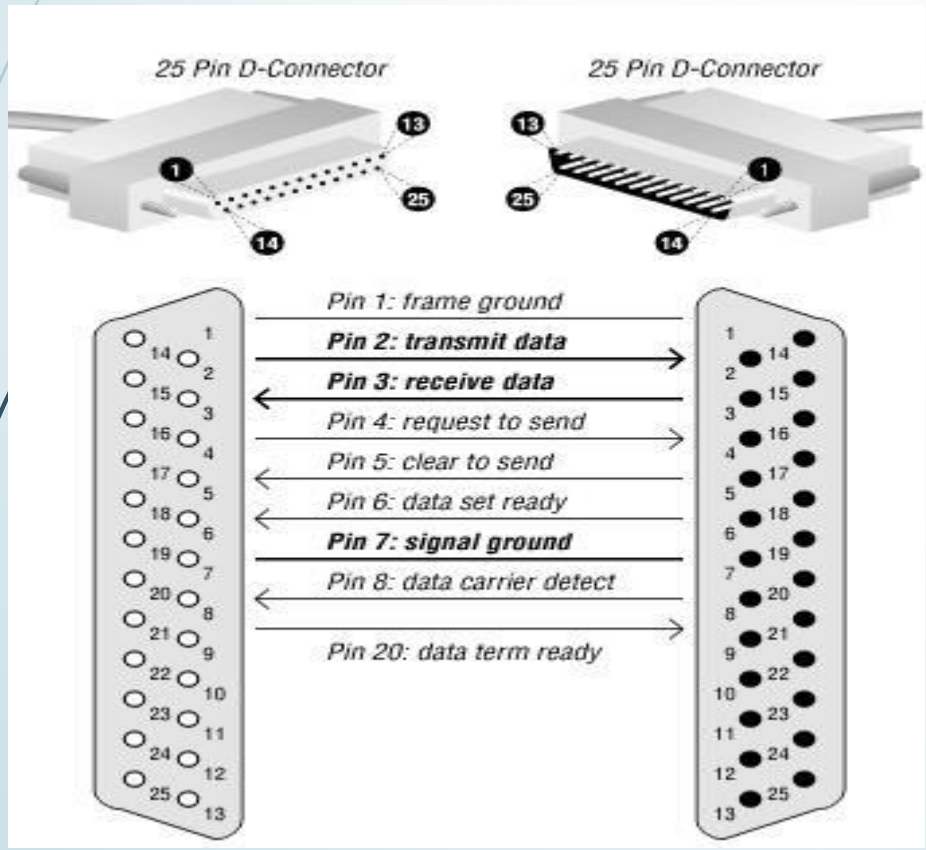
2 Transmit Data (TxD)
3 Receive Data (RxD)
4 Request to Send (RTS)
5 Clear to Send (CTS)
6 Dataset ready (DSR)
7 Signal Ground
8 Data Carrier Detect (DCD)
15 Transmit Clock
17 Receive Clock
20 Data Terminal Ready (DTR)
24 Auxiliary Clock

RS-232 Standardı

- EIA' nın bilgisayar,terminal ve modem ara bağlaşımı için önerdiği bir standarttır.
- Bu standart tanımlaması hem senkron hem de asenkron veri iletişimini kapsar.
- Analog telefon sistemine, ITU' nun V.24/V.28, ISO' nun 2110 standartlarına uyumludur.

RS-232 Standardı

- RS-232, seri arabirim standartlarının en eskisi ve en yaygın olarak kullanılanıdır.



Şekilde 2 nolu uç seri çıkış, 3 nolu uç seri giriş uçlarıdır. Yanda görülen 25 uçlu konektörde 7, 9 uçlu konektörde ise 5 nolu uç işaret referans toprağıdır.

RS-232 Sinyal Kodlaması

- RS–232 C hatları TTL sinyal seviyelerini (+5V, OV) taşımaz.
- Tipik olarak gerilim seviyeleri +12 V ve -12V'dur.
- Fakat RS–232 hatları, +25V DC‘ ye kadar yüksek olan sinyal seviyeleri ile -25 V DC‘ ye kadar düşük olan sinyalleri taşıyabilir.
- Bilindiği üzere bilgisayardaki veri iletimi ikilik sistemde olmaktadır.

RS-422A RS-423A Standardı

- RS-232 göre daha kaliteli bir elektriksel ara bağlaşım gereksinimini EIA RS-449,RS-422A ve RS-423A standartları karşılamaktadır.
- RS- 422A' da dengeli iletimle verinin daha güvenli ve daha hızlı iletimi sağlanmıştır.

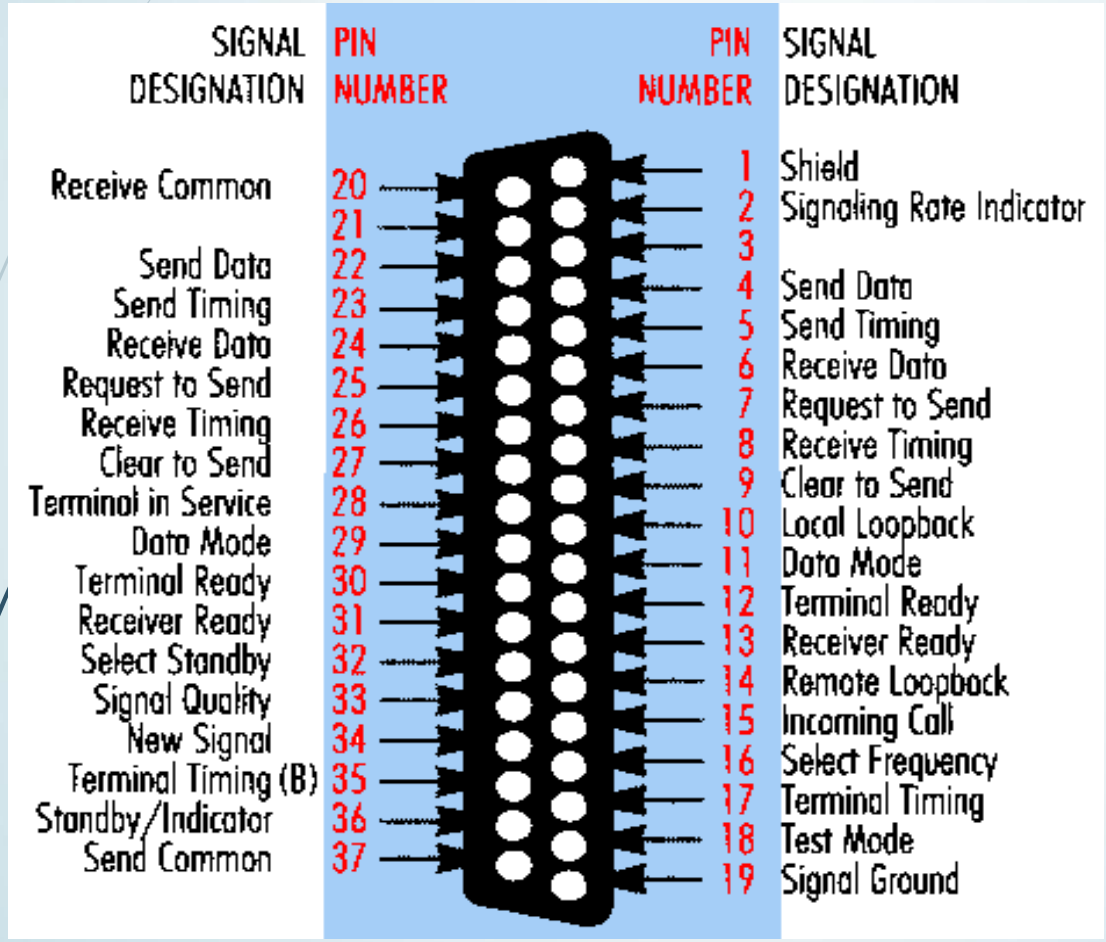
RS-422A RS-423A Standardı

- Dengeli iletim sayesinde hız ve verinin ulaştırılabileceği uzaklık artmıştır.
- RS-423A'da ise RS-232' ler gibi devreler kullanılır.
- Önemli bir fark üretilen ve alınan işaretlerin ayrı ayrı toprakları referans almalarıdır.

RS-422A RS-423A Standardı

- RS-423A kullanıldığında 10 m DTE DCE uzaklığı en çok 300 kbps, 1000 m uzaklıkta ise 3 kbps hızına çıkabilir.

RS-449/V.35


SIGNAL DESIGNATION
PIN NUMBER
PIN NUMBER
SIGNAL DESIGNATION
Receive Common 20
21
Send Data 22
Send Timing 23
Receive Data 24
Request to Send 25
Receive Timing 26
Clear to Send 27
Terminal in Service 28
Data Mode 29
Terminal Ready 30
Receiver Ready 31
Select Standby 32
Signal Quality 33
New Signal 34
Terminal Timing (B) 35
Standby/Indicator 36
Send Common 37
1 Shield
2 Signaling Rate Indicator
3
4 Send Data
5 Send Timing
6 Receive Data
7 Request to Send
8 Receive Timing
9 Clear to Send
10 Local Loopback
11 Data Mode
12 Terminal Ready
13 Receiver Ready
14 Remote Loopback
15 Incoming Call
16 Select Frequency
17 Terminal Timing
18 Test Mode
19 Signal Ground

RS-449/V.35

- Bu standart RS-422A, RS-423A elektriksel standartlarını karşılayan bir standarttır.
- Biri 37 uçlu, diğeri 9 uçlu olmak üzere 2 konnektör kullanılmasını öngörüyor.
- Uygulamalarda hemen her zaman 37 uçlu olanı tek başına kullanılmaktadır.

RS-449/V.35

- RS-232’ de elektriksel işaretlerin dengesiz devreler üzerinde akmasına karşılık, RS-449 dengesiz ya da dengeli devrelerin ikisi de kullanılır.
- RS-449 (V.35)’ un dengeli devre kullanan elektriksel standardı, RS-422 (V.11) olarak yayımlanmıştır. Diğerlerine göre elektriksel hızı daha fazladır.

KABLOSUZ İLETİMDE FİZİKSEL KATMAN

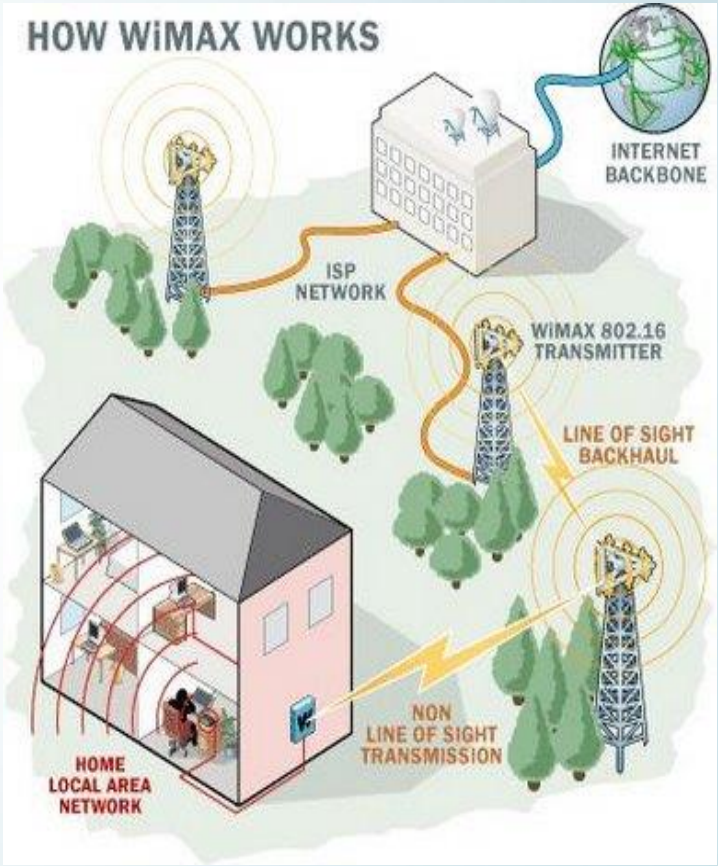
KABLOSUZ İLETİMDE FİZİKSEL KATMAN

- Kablosuz yerel ağ, kablolu iletişime alternatif olarak uygulanabilecek esnek bir iletişim sistemidir. Radyo frekans (RF) teknolojisini kullanarak havadan bilgi alışverişi yapar böylece kablolu bağlantı miktarını azaltır.

Kablosuz Yerel Ağların Çalışması

Kablosuz yerel ağlar havadan yayılan elektromanyetik dalgalarla bir noktadan başka bir noktaya fiziksel bağlantı olmaksızın bilgi iletişimini sağlar.

Tipik bir kablosuz yerel ağ uygulamasında, erişim noktası denilen hem alıcı hem verici konumundaki cihaz standart kablolamayla, kablolu ağa bağlanır. Erişim noktası kablolu ağ omurgası ve kablosuz ağ arasında veri alışverişini üstlenir.



Kablosuz Yerel Ağların Çalışması

Erişim noktası genelde yüksek bir noktaya konur fakat istenilen kapsama alanı sağlandıkça her noktaya konulabilir. Uç noktalar ise kablosuz ağa, kablosuz ağ adaptörleriyle , dizüstü bilgisayarda PCMCIA kartlarla, masaüstü bilgisayarlarda ise ISA kartlarla erişirler. Kablosuz ağ adaptörleri sunucudaki ağ işletim sistemi ile manyetik dalgalar arasında bir anten yardımıyla köprü oluştururlar.

PCMCIA

ISA

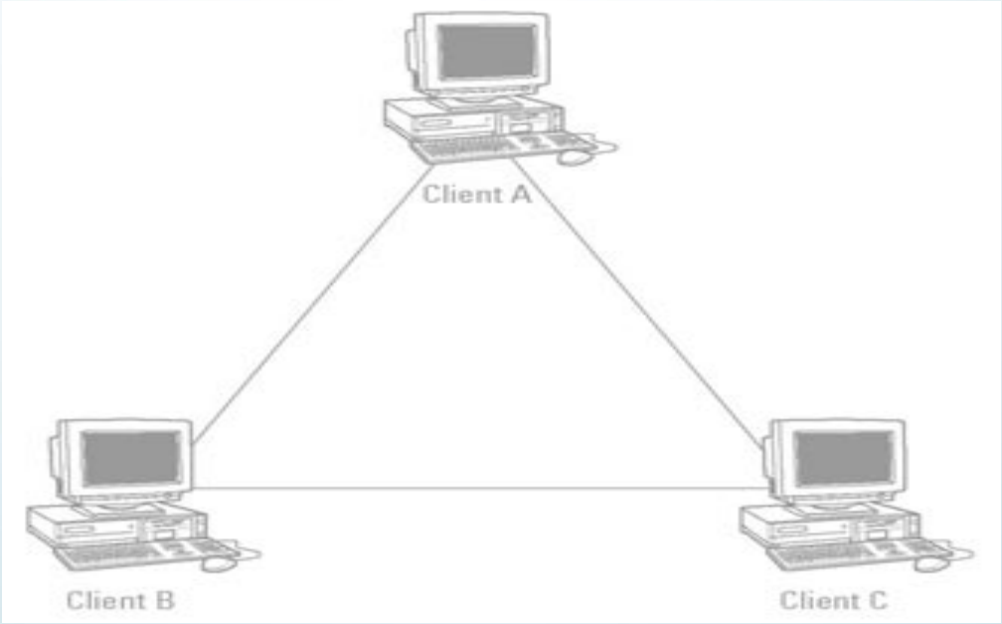
KABLOSUZ AĞ ADAPTÖRÜ

Kablosuz Yerel Ağların Çalışması

Standart kablosuz ağlar şu 2 moddan biri ile çalışırlar.

- Peer-to-peer (makinadan makinaya) modeli:

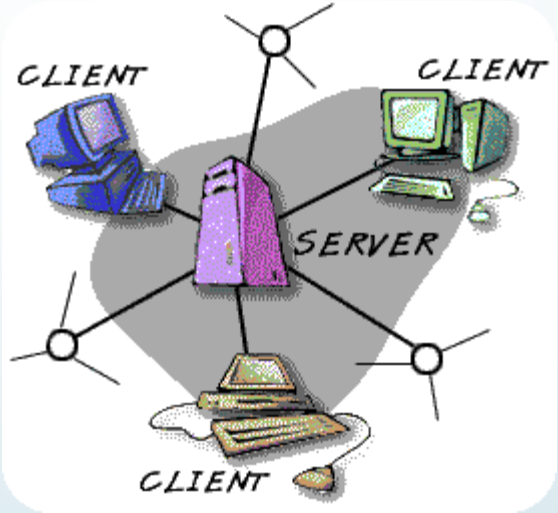
Bu modda her kullanıcı ağdaki bir diğeri ile direkt iletişim kurar. Bu mod, birbirleri ile iletişim mesafesinde olan kullanıcılar için tasarlanmıştır.



Kablosuz Yerel Ağların Çalışması

- Client/Server (İstemci/Sunucu) modeli :

Diğer bir adı da altyapı modeli olan bu model ise tüm bilgisayarlar erişim noktası (acces point) adlı ürünle mevcut olan kablolu ağa bağlanmıştır. Acces Point adlı cihazlar ile kablosuz ağ ortamı kablolu ağ ortamıyla bağlantısı yapılırken veri iletişimi daha geniş alanlara aktarılır.



Kablosuz Yerel Ağların Çalışması

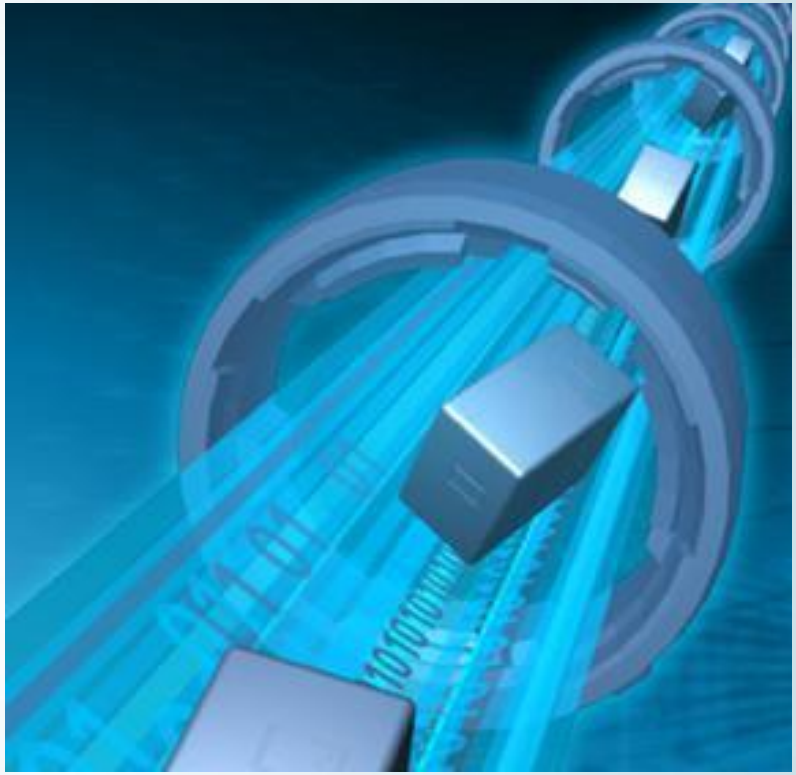
Kablosuz ağ kurmak için şu anda kullanılan ana standart IEEE (The Institute of Electrical and Electronics Engineers) 802.11'dir. IEEE 802.11 ilk olarak 1999 da yayınlanmıştır ve 2.4 Ghz de 2Mbps (DSL bağlantı gibi) hızında veri iletişimi için tasarlanmıştır

- 802.1 - Güvenlik ve diğer konular
- 802.2 - Mantıksal Bağlantı Kontrolleri (LLC - Logical Link Control)
- 802.11 - WLAN'lar için standartlar üretmek (Kablosuz lokal ağlar)
- 802.15 - WPAN'lar için standartlar üretmek (Kablosuz kişisel ağlar)

Kablosuz Ağ Türleri

Günümüzde kullandığımız 4 tip kablosuz ağ vardır. Bunlar ucuz ve yavaş olandan, pahalı ve hızlı olana doğru sıralanırsa :

- BlueTooth
- IrDA
- HomeRF
- WECA (Wi-Fi)



Niçin Kablosuz ?

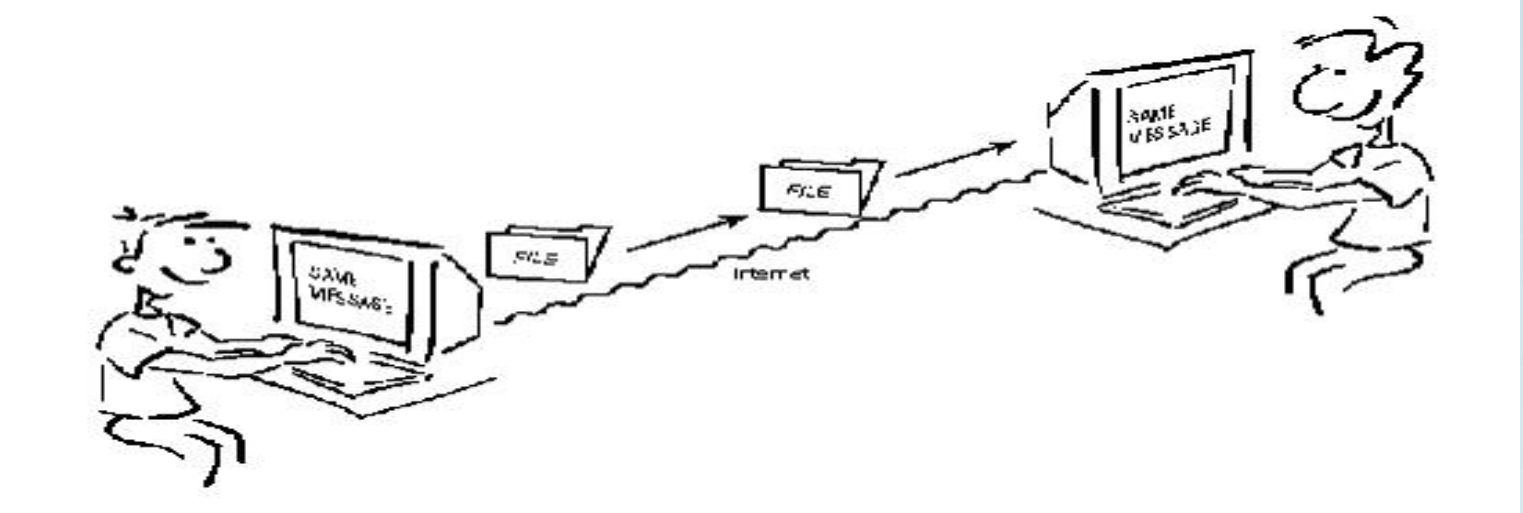
- Mobilite
- Kurulum Hızı ve Basitliği
- Kurulum Esnekliği
- İleriye Yönelik Maliyet Kazancı
- Genişletilebilirlik

Kablosuz Yerel Ağların Yaygın Kullanım Alanları

- Hastanelerde
- Kampüs
- Büyük işletmelerde
- Üretim kuruluşları ve fabrikalar
- Danışmanlık ve muhasebe

İŞARETLERİN KODLANMASI

- Analog İşaretlerin Kodlanması
- Sayısal İşaretlerin Kodlanması



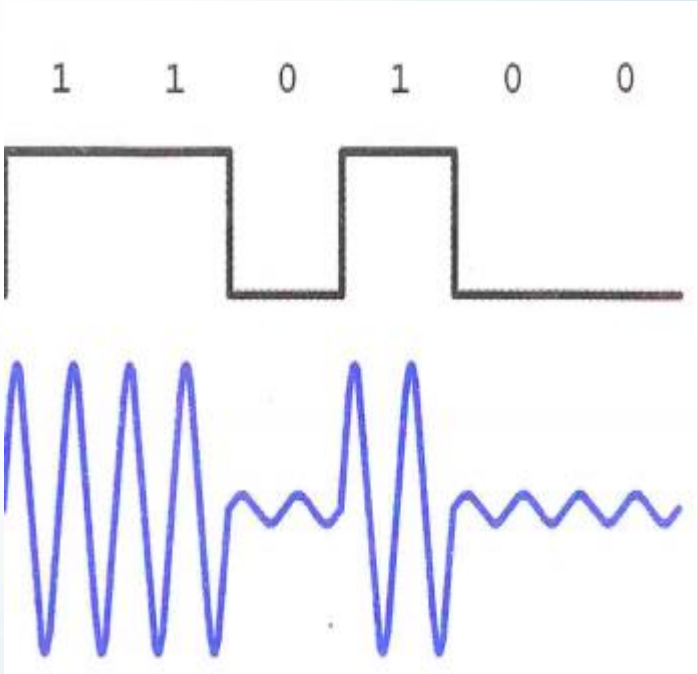
İkili düzende sıralanmış bir veriyi kablolu bir iletişim ortamından aktarabilmek için ikili veriyi oluşturan her öğenin (ikilin) elektrik işaretine dönüştürülmesi gerekir. Çünkü, telefon hattı aracılığıyla gönderilen elektrik işaretleri analog işarettir. Elektrik işaretine dönüştürülen veriler bir telefon hattı aracılığıyla alıcı bilgisayara iletilir ve tekrar elektrik işaretinden ikili veriye dönüştürülür.

Analog İşaret Kodlanması

Analog bir işaret üzerinden sayısal bir veriyi göndermek (kodlamak) için, işaretin temel bileşenlerinden (genlik, sıklık ve evre) bir veya birkaçını değiştirme yöntemi kullanılır.

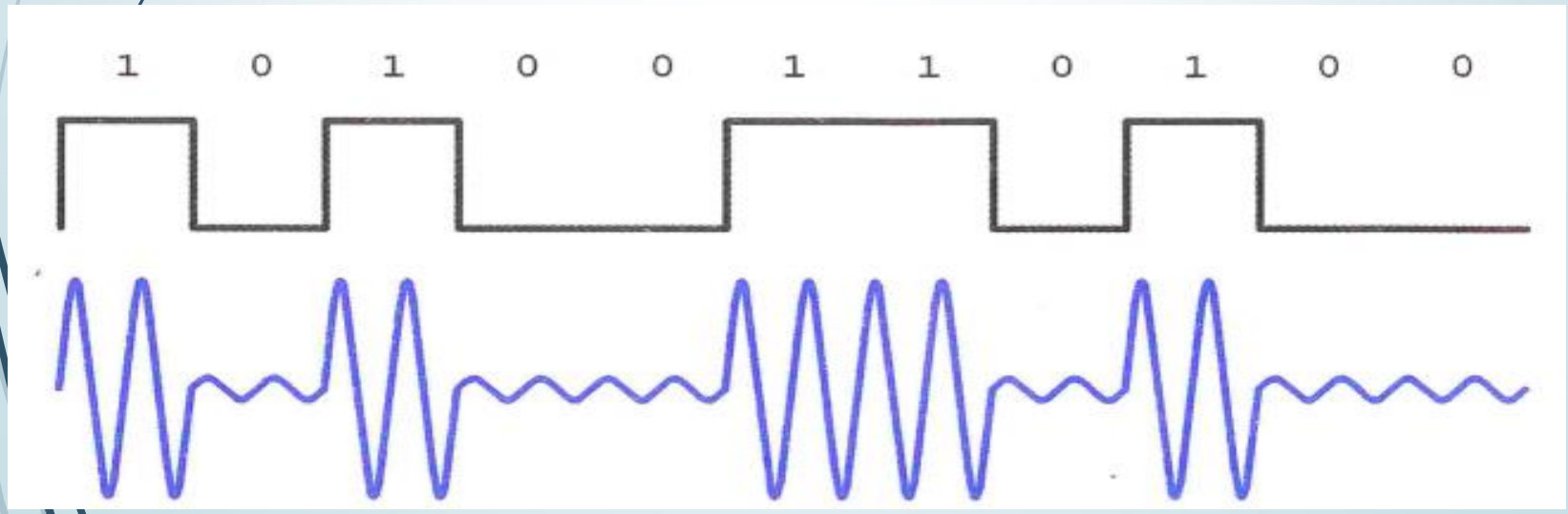
Bu yöntemler;

- Sayısal genlik kiplenimi, ASK (Amplitude-shift keying),
- Sayısal sıklık kiplenimi, FSK (Frequency-shift keying),
- Evre kaydırmalı kiplenim, PSK (Phase-shift keying)



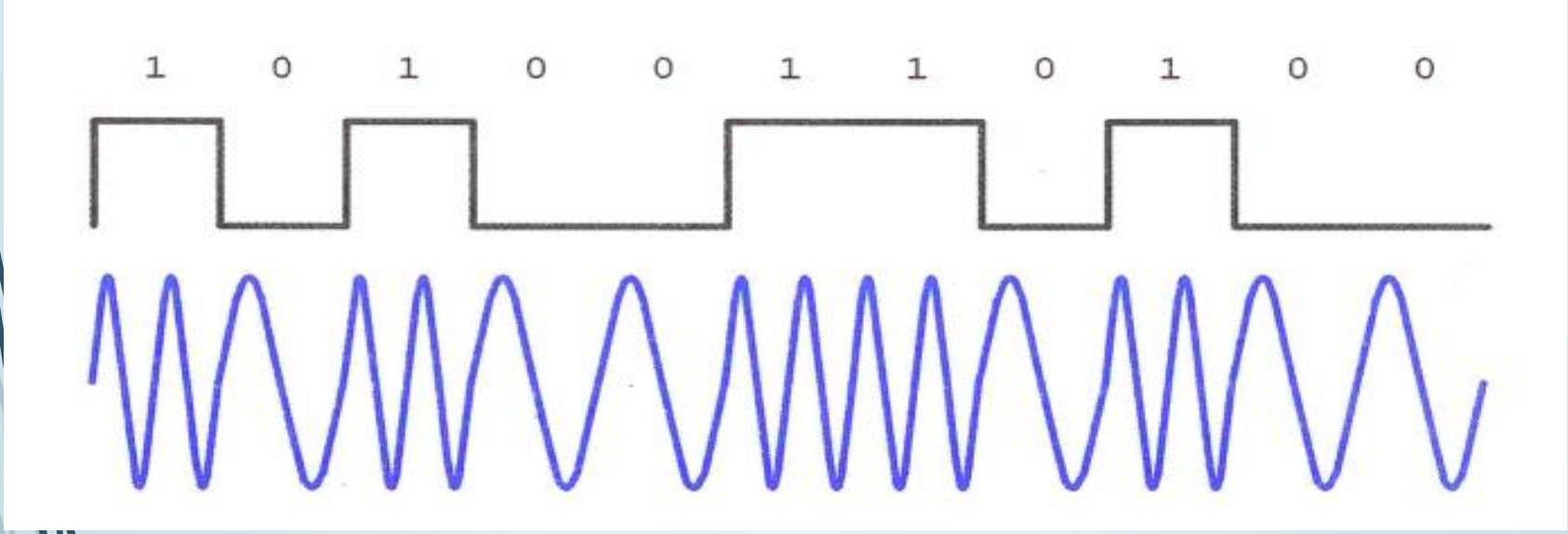
Sayısal Genlik Kiplenimi (ASK)

ASK, sayısal yerinin işaret genliğini iki ya da daha çok düzey arasında değiştirerek gösterir. Örneğin Şekilde 1011001 ikillerinin genlik kiplemesi kullanılarak gönderilmesi örneklenmektedir. Bu örnekte işaretin sıklık ve evre bileşenleri sabit tutulurken, 1 ikili 1 voltluk genlik düzeyi ile, 0 ikili ise 0-0.05 genlik düzeyi arasında değiştirilerek kodlanmıştır.



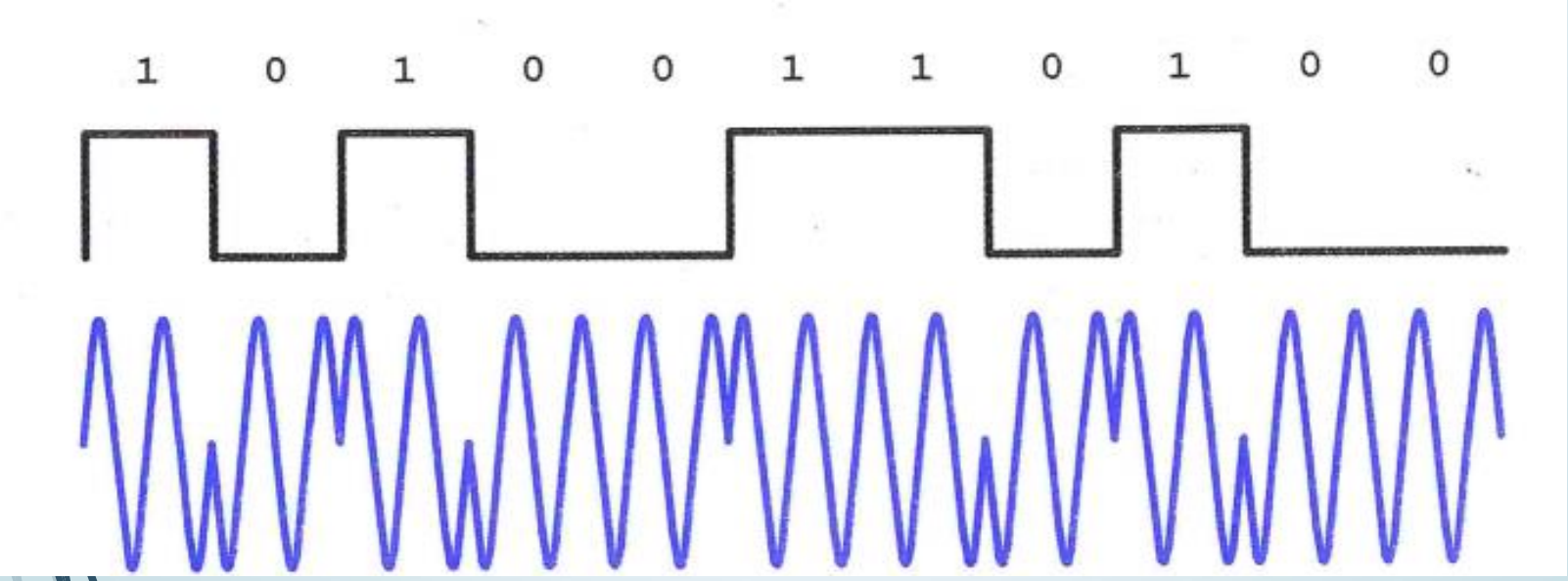
Sayısal Sıklık Kiplenimi (FSK)

FSK, sayısal işaretleri farklı sıklıklarda kodlayarak gönderir. Şekilde, 10100110100 ikillerinin farklı sıklıklar kullanılarak gönderilmesi örneklenmektedir.



Evre Kaydırmalı Kiplenim (PSK)

PSK ise, işarette bir evreden diğerine geçişi sağlayarak ikili 0 ve 1'i kipler. Örneğin, evre açısındaki 180 derecelik bir kayma sayısal işaretin değiştiğini gösterir, ikili bit eğer 1 ise 0'a veya 0 ise 1'e geçildiğini gösterir.



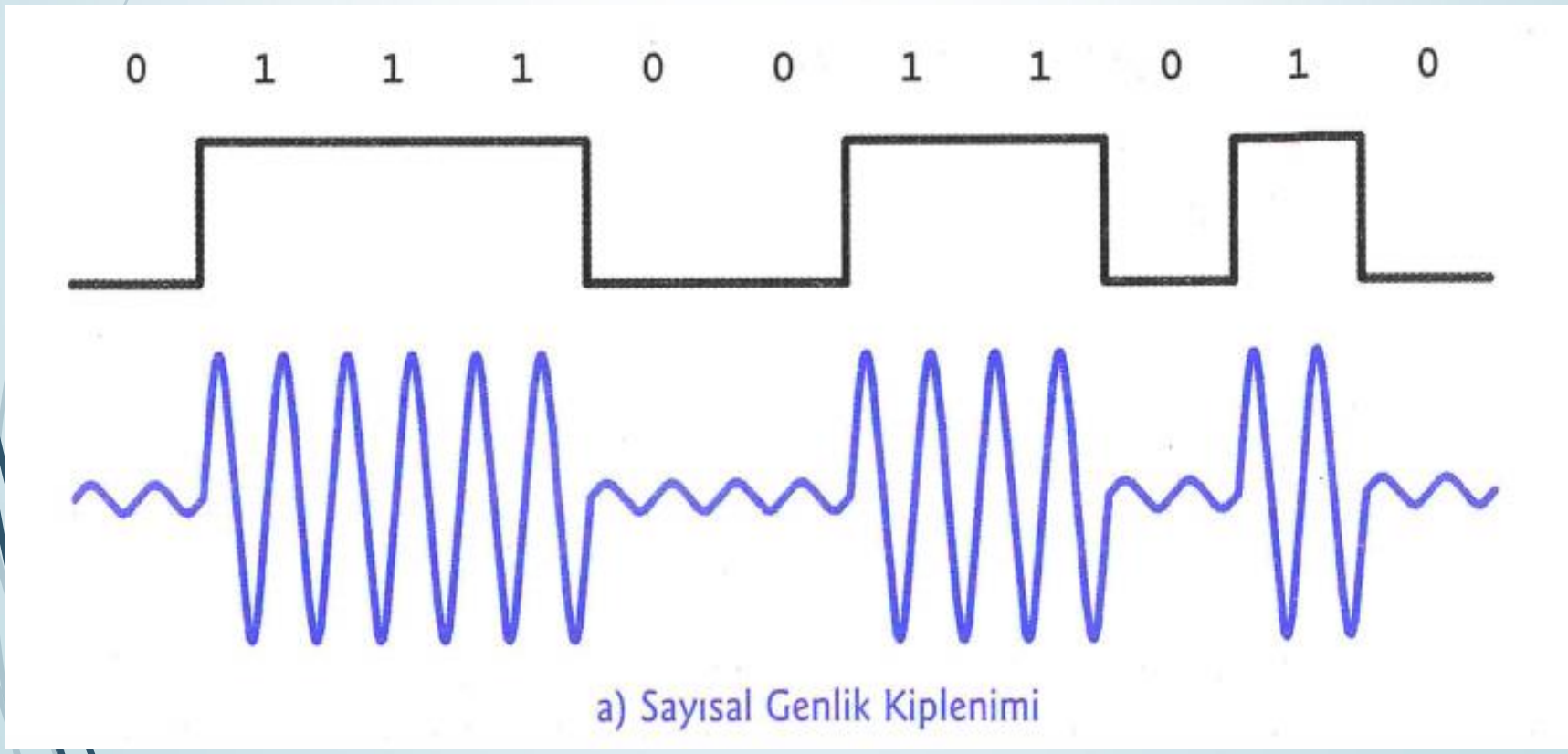
Örnek 1:

Sayısal Genlik Kiplenimi (ASK), Sayısal Sıklık Kiplenimi (FSK) ve Evre Kaydırmalı Kiplenim (PSK) tekniklerini kullanarak aşağıdaki ikili veriyi kodlayınız.

Veri: 01110011010

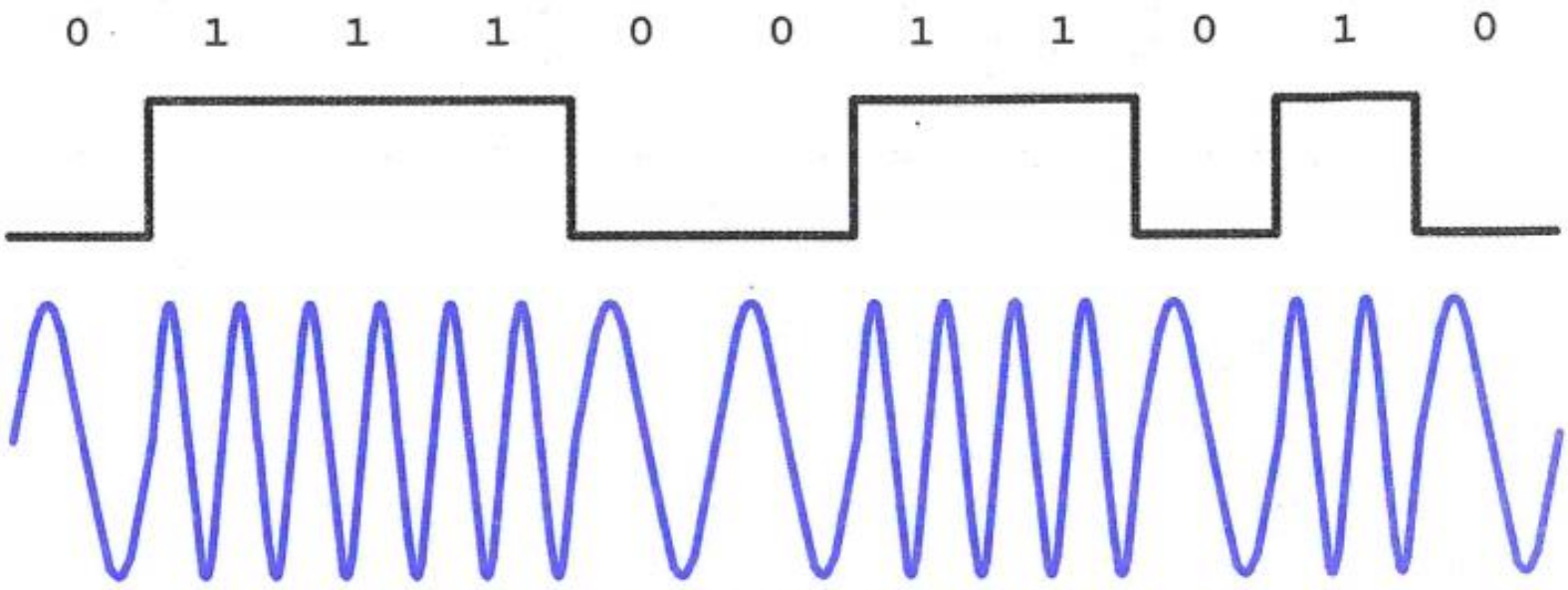
Çözüm:
a) Sayısal Genlik Kiplenimi

- Veri: 01110011010



Çözüm:
b) Sayısal Sıklık Kiplenimi

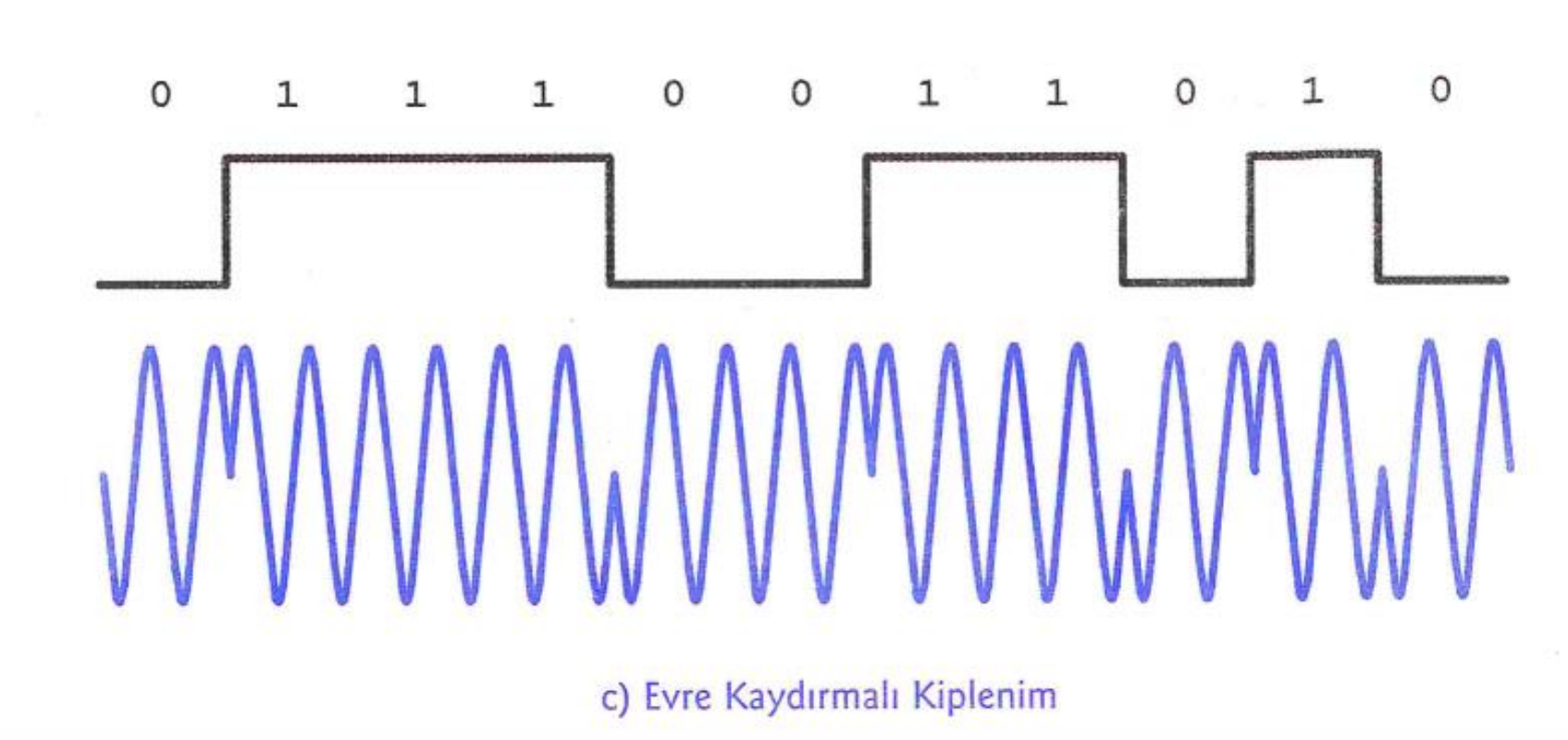
- Veri: 01110011010



b) Sayısal Sıklık Kiplenimi

Çözüm:
c) Evre Kaydırmalı Kiplenim

- Veri: 01110011010



Sayısal İşaretin Kodlanması

Sayısal işaret, ikili bir verinin voltaj değişimleri kullanılarak kodlanmasıdır.

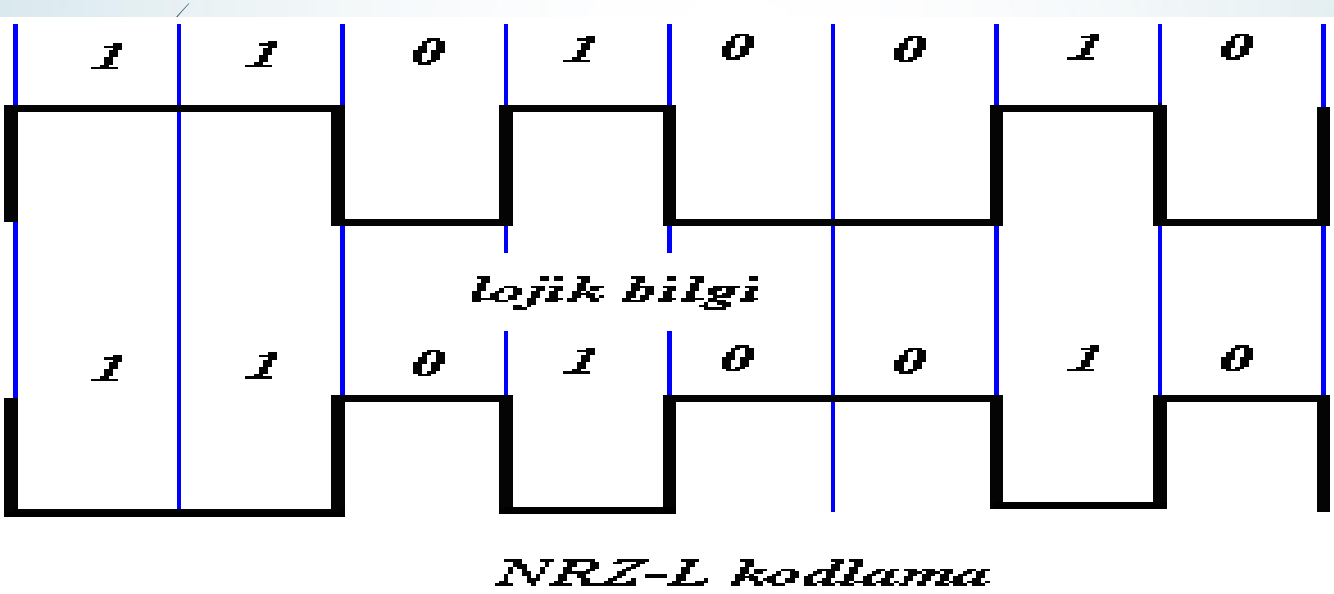
Sayısal işaret iletim ortamına kodlanarak çıkartılır; alıcı taraf bu kodlamaya dayanarak kendisine gelen veriyi algılar. Kodlama yöntemi olarak temelde iki farklı yöntem kullanılır. Birinde, lojik değerlerin gösterilmesi için sabit gerilim düzeyleri kullanılırken (NRZ-L, NRZ-I), diğer yöntemde her bir bitin ortasında 0'dan 1'e veya tersi şeklinde geçiş yapılır (Manchester, Farksal Manchester).

Sayısal İşaretlerin Kodlanmasında Kullanılan Teknikler

- Sıfıra dönüşsüz kodlama (non return zero - NRZ),
- Ters sıfıra dönüşsüz kodlama (non return zero-invertive NRZ-I).
- Manchester kodlama (manchester encoding)
- Fark Manchester kodlama (differential machester encoding)

Sıfıra Dönüşsüz Kodlama(NRZ)

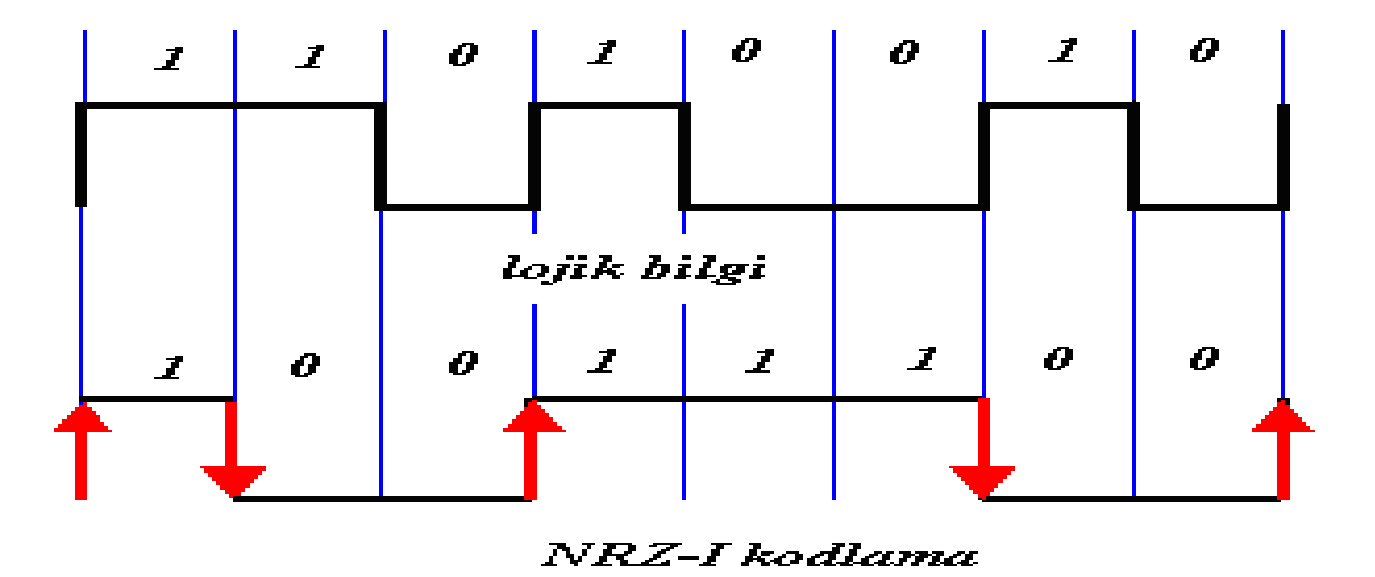
Sıfıra dönüşsüz kodlamanın NRZ-L ve NRZ-I olmak üzere iki çeşidi vardır. Bunlardan NRZ-L kodlamada 0 biti pozitif gerilim ile 1 biti negatif gerilim ile temsil edilir. Genellikle seri haberleşmede kullanılır.



NRZ-L kodlama

Ters Sıfıra Dönüşsüz Kodlama(NRZ-I)

NRZ-I kodlamada ise 1 biti önceki bitin tersi, 0 biti önceki bitin aynı olarak kodlanır. Diğer bir deyişle 0 biti kodlanırken gönderilen sinyalde hiçbir değişme olmaz aynen devam eder, 1 biti yollanırken gönderilen sinyal önceki bitin tersine çevrilir.

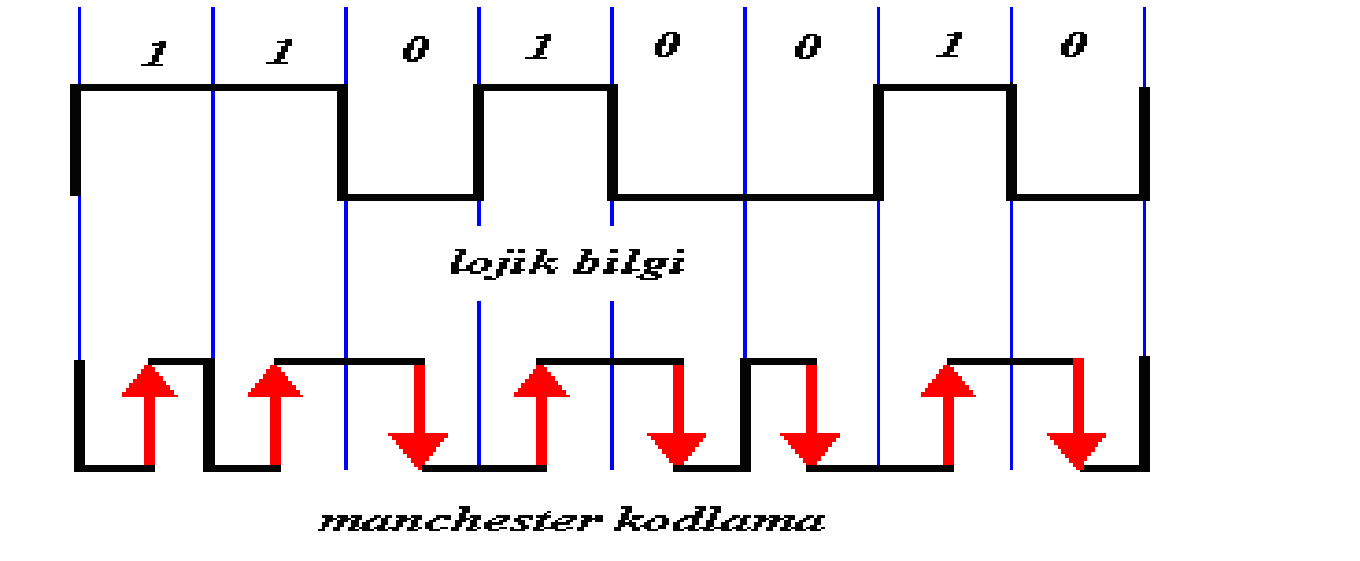


NRZ-I kodlama

Manchester Kodlama

Manchester kodlamada, bitlerin tam orta yerlerinde, 1 biti 0 dan 1 e geçiş ile 0 biti 1 den 0 a geçiş ile ifade edilir. Böylece gerçek bilgi değiştirilmeden bilginin kodlanması değiştirilmiş olur.

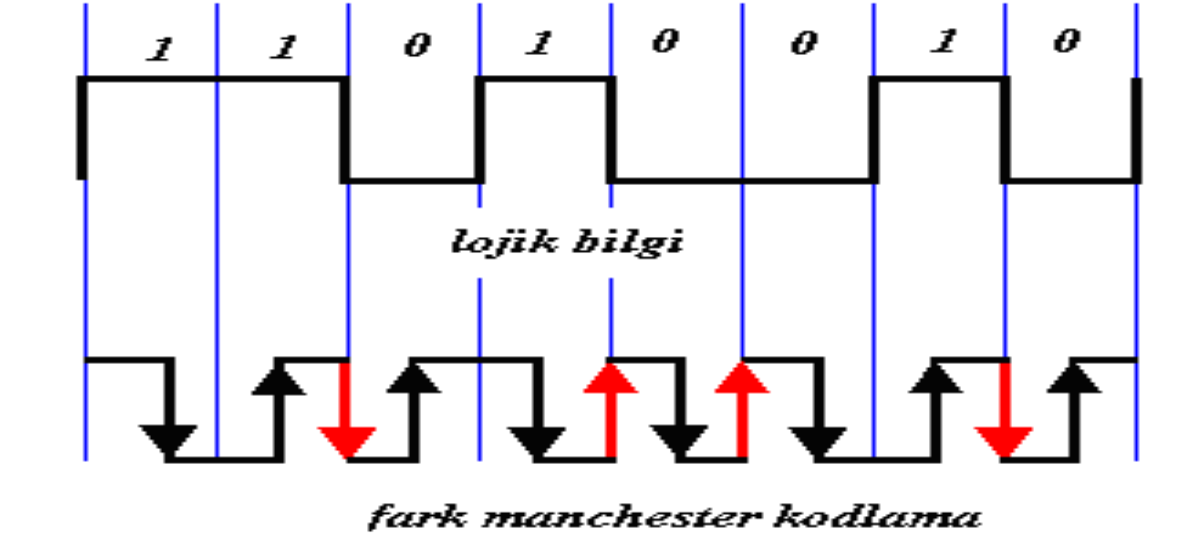
Gerçek Bilgi	*Gönderilen Bilgi*
Lojik 1	0 dan 1 e geçiş
Lojik 0	1 den 0 a geçiş



Fark Manchester Kodlama

Fark Manchester Kodlamada bitlerin orta noktalarında yine 0 dan 1 e ve 1 den 0 a geçişler olur. Fakat burada geçiş yönlerinin bir önemi yoktur yani 0 için 0 dan 1 e, 1 için 1 den 0 a geçişler olabilir. Bu kodlamada önemli olan bit başlangıç anlarında geçiş olup olmadığıdır. 0 biti için başlangıç anında geçiş vardır, (şekilde kırmızı oklar) 1 biti için başlangıç anında geçiş yoktur. Diğer bir deyimle sinyal, 1 biti için önceki konumu aynen devam ettirirken 0 biti önceki konumun tersine çevrilir.

Gerçek Bilgi	*Gönderilen Bilgi*
Lojik 1	1 den 0 a geçiş
Lojik 0	0 dan 1 e geçiş



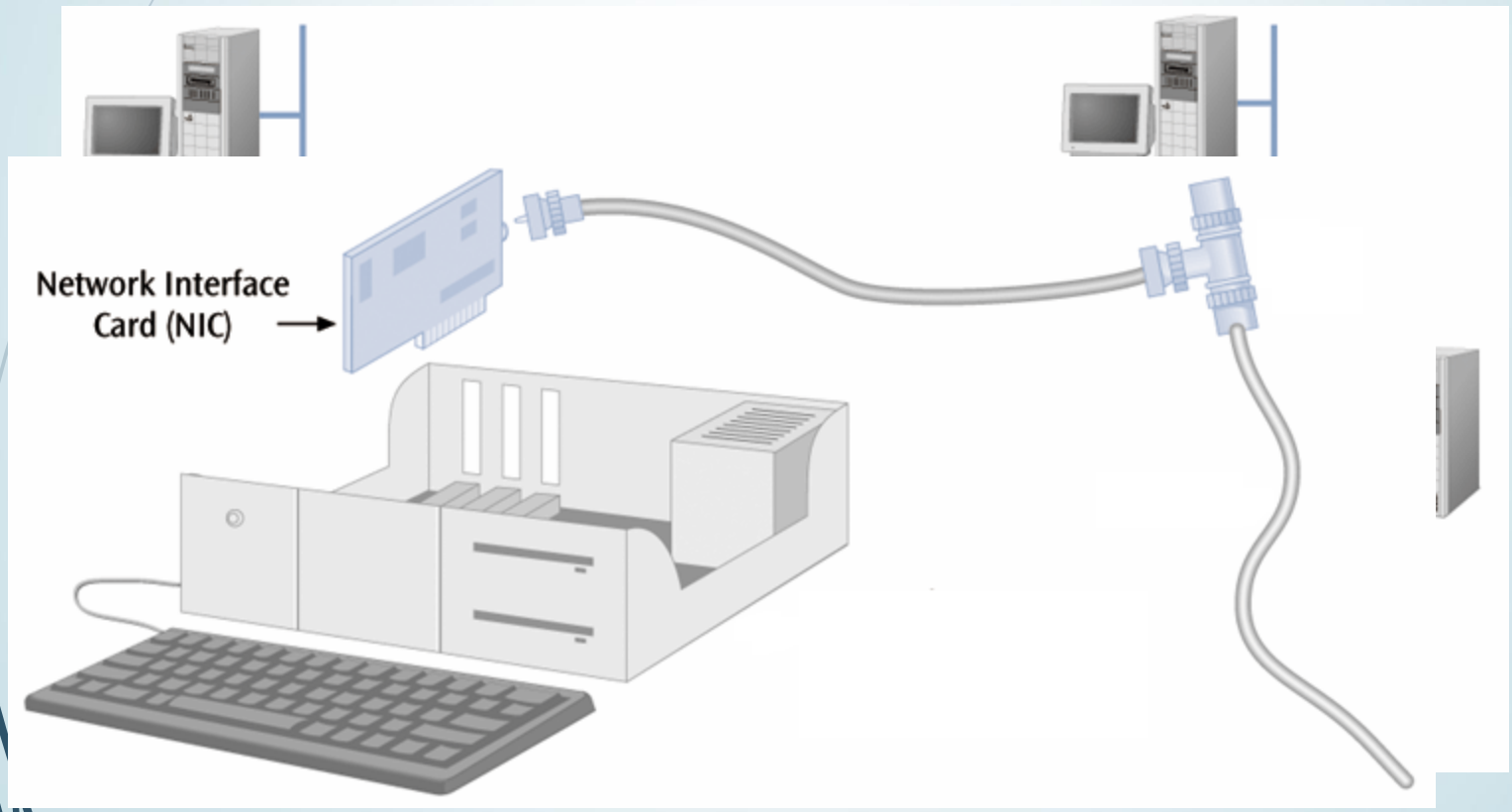
Kablo Tipleri

Bilgisayar ağlarında kullanı **LAN** kablo tipleri şunlardır:

- Koaksiyel Kablo (Coaxial Cable)
  - RG-8
  - RG-6 (Ağlarda kullanılmasa da bilmemiz gerekiyor.)
  - RG-58
- Dolanmış Çift Kablo (Twisted Pair Cable)
  - Kaplamalı Dolanmış Çift (Shielded Twisted Pair-STP)
  - Kaplamasız Dolanmış Çift (Unshielded Twisted Pair-UTP)
- Fiber Optik Kablo (Fiber Optic Cable)

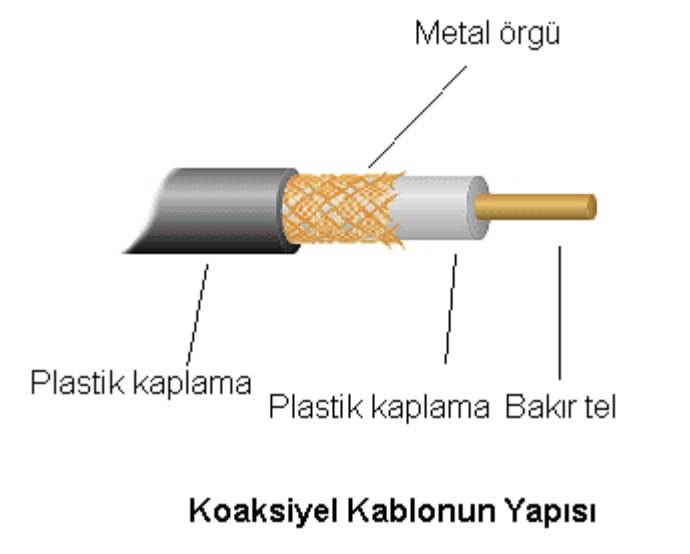
Doğrusal Topoloji

- Koaksiyel kablo, BNC konnektör, BNC T konnektör



Koaksiyel Kablo (Coaxial Cable)

Koaksiyel(veya kısaca "koaks") kablo, merkezde iletken kablo, kablonun dışında yalıtkan bir tabaka, onun üstünde tel zırh ve en dışta yalıtkan dış yüzeyden oluşur.



Koaksiyel Kablonun Yapısı

Koaksiyel Kablo (Coaxial Cable)

Koaksiyel kablo elektromanyetik kirliliğin yoğun olduğu ortamlarda düşük güçte sinyalleri iletmek için geliştirilmiş bir kablodur. Koaksiyel kablo çok geniş bir kullanım alanına sahiptir. Ses ve video iletiminde kullanılır. Çok değişik tiplerde karşımıza çıkabilir. Ancak bilgisayar ağlarında şimdiye kadar kullanım alanı bulmuş yalnızca iki tip koaksiyel kablo vardır: RG-8 ve RG-58.

Koaksiyel kablo tipleri kendi RG kodlarına sahiptir. Koaksiyel kabloda bizim için önemli olan ve değişkenlik arzeden değer kablonun empedansı veya omajıdır. Bu değer kablonun belirli bir uzunlukta elektrik akımına karşı gösterdiği dirençtir. Koaksiyel kablolar dıştan bakıldığında birbirlerine çok benzerler, ancak kabloya daha yakından bakınca üzerinde RG kodunu ve empedansını görebilirsiniz. Empedans değeri "50 Ω " veya "75 Ω " şeklinde omega karakteriyle yazılır.

Koaksiyel Kablo (Coaxial Cable)

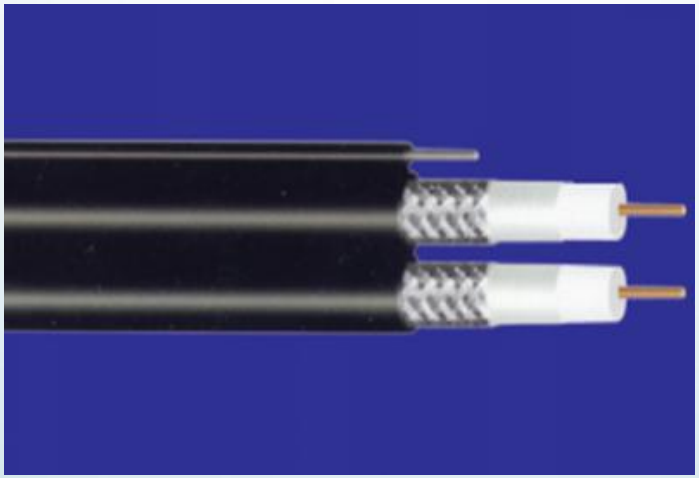
RG-8

RG-8 veya genellikle söylendiği gibi Thicknet(kalın net) kablo ethernetin ilk kullandığı kablo tipidir. Günümüzde bu kabloyu kullanan bir ağ bulmak gerçekten zordur. Sonradan kullanılan kablolarda bir renk sınırlaması yokken bu kablolar genellikle sarı/portakal veya kahverengi renkte ve 2.5 metrede bir siyah bir bantla işaretlenmiş olarak üretilmişlerdi. 50 Ω olan bu kablo adına yakışır şekilde kalın ve mukavemetli bir kabloydu.

Koaksiyel Kablo (Coaxial Cable)

RG-6

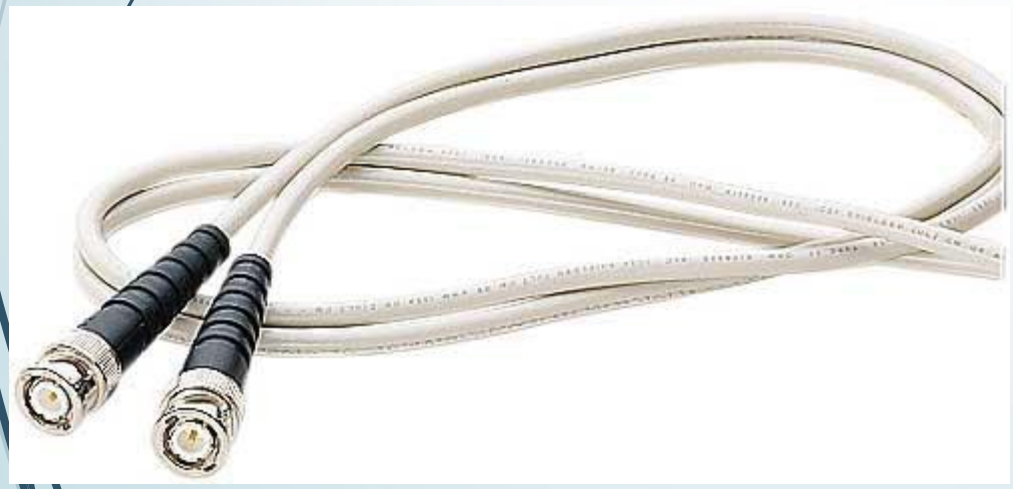
RG-6 75Ω değerindedir ve bilgisayar ağlarında hiçbir zaman kullanılmamıştır. Ancak günlük hayatta çok sık karşımıza çıkar. Televizyonlara giren anten kablosu RG-6'dır. Görünüş olarak RG-58 ile aynıdır. Ancak kablo üzerindeki empedans değeri 75 Ω olarak okunduğunda ne olduğu anlaşılabilir.

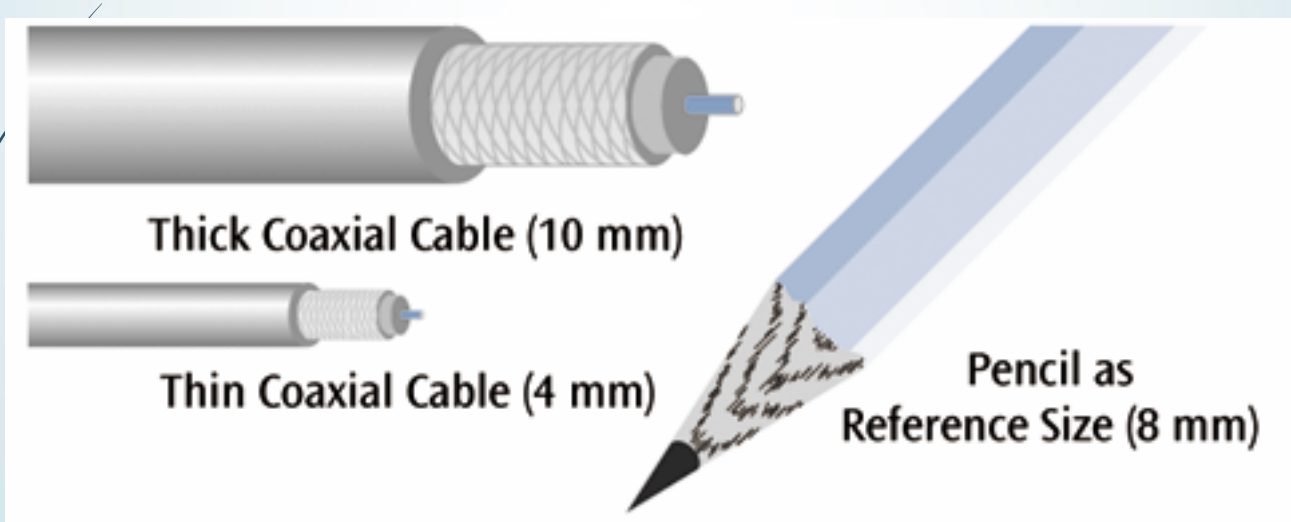


Koaksiyel Kablo (Coaxial Cable)

RG-58

Günümüzde karşılaşabileceğiniz tek koaksiyel ağ kablosu RG-58'dir. Diğer isimleri Thinnet(ince net) ve Cheapernet(ucuz net)'dir. Aynı RG-8 gibi 50 Ω olan bu kablo RG-8'e göre ucuz, uygulaması kolay bir kablodur. UTP yaygınlaşıncaya kadar yerel ağlarda geniş uygulama alanı bulmuştur.



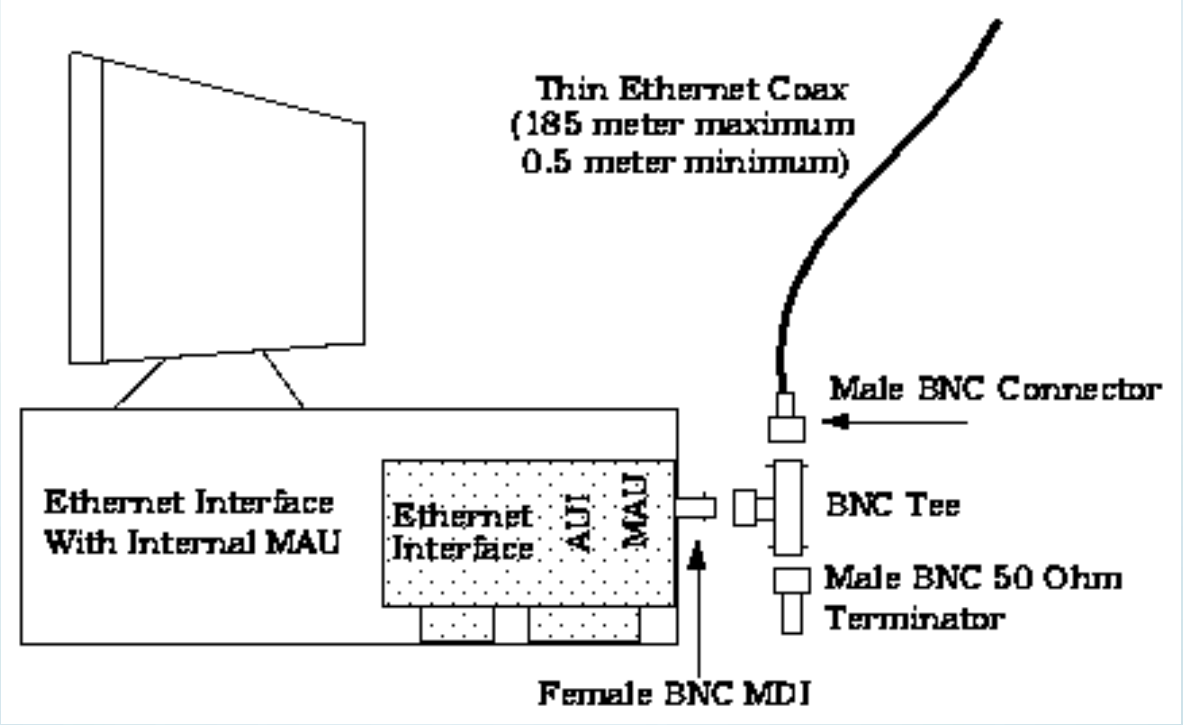

Thick Coaxial Cable (10 mm)
Thin Coaxial Cable (4 mm)
Pencil as
Reference Size (8 mm)

Eş eksenli (Koaksiyel) Kablo Tipleri

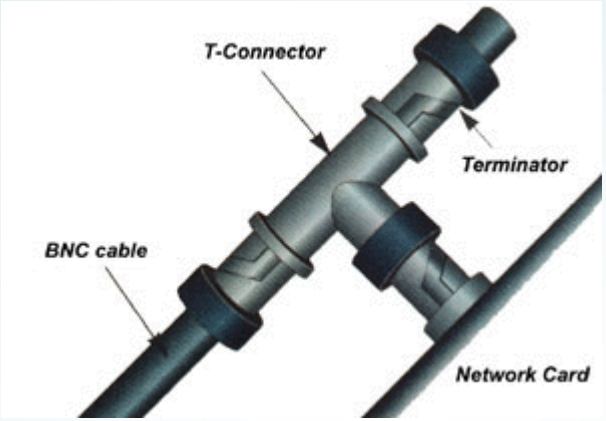
TİP	EMPEDANS	KULLANIM
RG-8	**50 Ohm**	10BASE-5 (Kalın-Thicknet) - 500 m
RG-58	**50 Ohm**	10BASE-2* (İnce-Thinnet) - 185 m
RG-59	**75 Ohm**	Kablo TV
RG-6	**75 Ohm**	Anten kablosu

* Yerel ağlarda en çok kullanılan standart. Bunlarda kablo mesafesi IEEE standartlarına göre 185 m'dir.

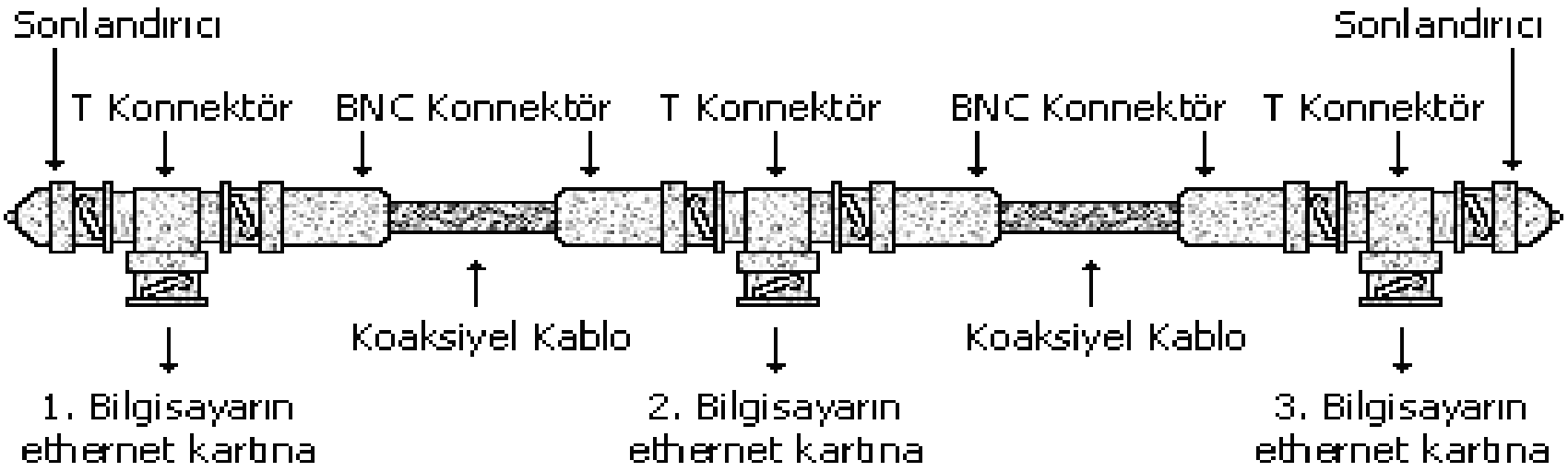
Koaksiyel Kablo Konnektörleri



Koaksiyel Kablo Konnektörleri



- Eşeksenli kablolar BNC konnektörleri ile sonlandırılır ve bilgisayar arkasındaki aktarım aygıta takılacak T-şeklindeki bağlayıcılara takılırlar.
- Kablo sonunda 10Base5 ise 75, 10Base2 ise 50 Ohm'luk sonlandırıcı (Terminator) takılır.


Sonlandırıcı
T Konnektör
BNC Konnektör
T Konnektör
BNC Konnektör
T Konnektör
Sonlandırıcı
Koaksiyel Kablo
Koaksiyel Kablo
1. Bilgisayarın ethernet kartına
2. Bilgisayarın ethernet kartına
3. Bilgisayarın ethernet kartına

BNC

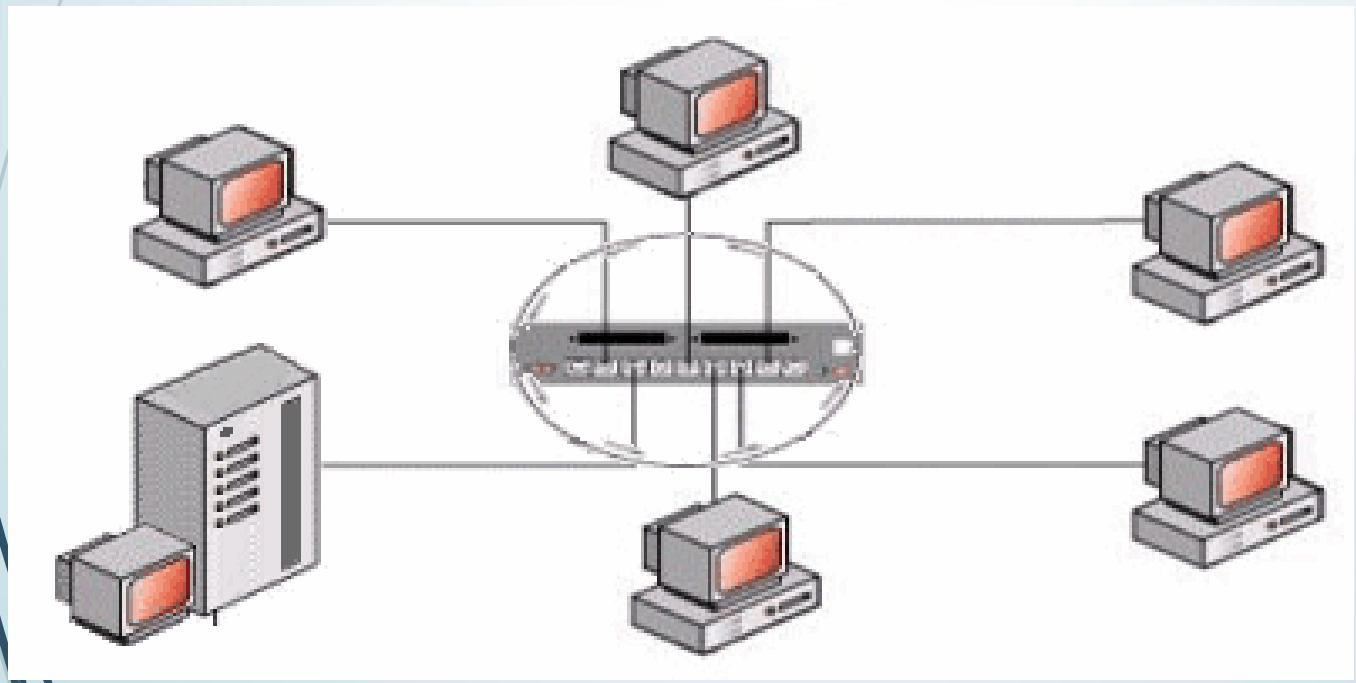
- **BNC ‘NİN AVANTAJLARI**
- Tek bir kablo kullanıldığı için malzeme sarfiyatı minimum noktadadır.
- Ayrıca altyapının sağlamlığını test etmek zahmet gerektirmez. Kopuk nokta hemen tespit edilir.

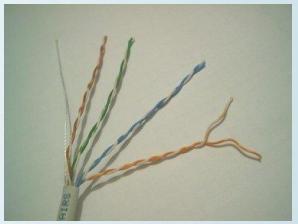
BNC’ NİN DEZAVANTAJLARI

- Hız oldukça düşüktür.
- Ayrıca eğer kabloda kopma olursa bütün ağ kilitlenir.

Yıldız Topoloji

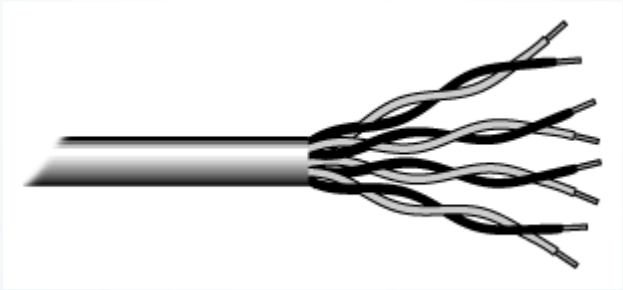
- UTP, STP kablo, RJ-45 konnektör





Dolanmış Çift Kablo (Twisted Pair Cable)

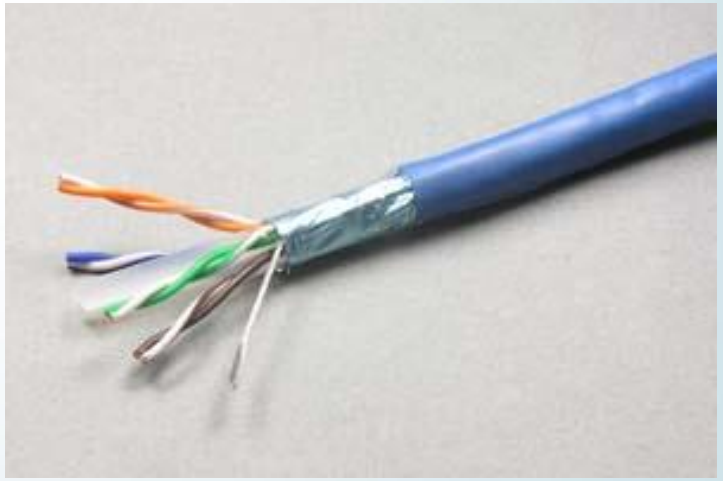
Günümüzde en yaygın kullanılan ağ kablosu tipi birbirine dolanmış çiftler halinde, telefon kablosuna benzer yapıdaki kablodur.



1- Kaplamalı Dolanmış Çift (Shielded Twisted Pair-STP)
2- Kaplamasız Dolanmış Çift (Unshielded Twisted Pair-UTP)

1- Kaplamalı Dolanmış Çift (Shielded Twisted Pair-STP)

Bu tip kabloda dolanmış tel çiftleri koaksiyel kabloda olduğu gibi metal bir zırh ile kaplıdır.



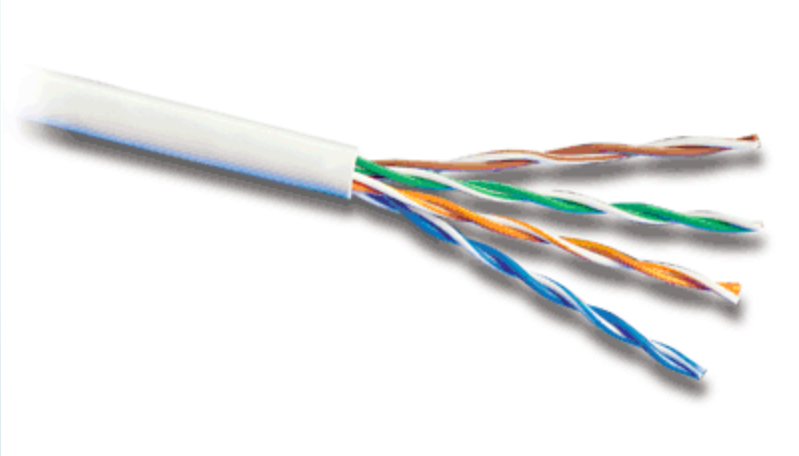
1- Kaplamalı Dolanmış Çift (Shielded Twisted Pair-STP)

STP kablolar ilk kullanılmaya başlandığı dönemlerde (belkide koaksiyelden geçiş aşamasında?) STP kablo UTP'ye göre daha güvenli kabul edilmiştir. En dıştaki metal zırh'ın elektromanyetik alanlardan geçerken kablo içindeki sinyalin bozulmasına mani olması beklenir. Ancak STP ilk dönemde pahalı olmasıyla yaygınlaşamamıştır. Eski kaynaklarda STP'nin UTP'ye göre daha güvenli olduğu ama pahalı bir çözüm olduğu ileri sürülür. Oysa günümüzde bir çok kaynakta STP'nin kurulumunun zor olduğundan ve söylendiği kadar da yüksek koruma sağlamadığından söz ediliyor. Hatta düzgün uygulanmadığında daha kötü sonuçlara yol açabileceğinden bahsediliyor. STP kullanılırken dikkat edilmesi gereken en önemli nokta, dıştaki metal zırh'ın düzgün bir şekilde topraklanmasıdır. Aksi halde zırh elektromanyetik dalgaları toplayan bir anten vazifesi görür. Ayrıca zırh'ın kablonun hiçbir noktasında zedelenmemiş olması da çok önemlidir. En dıştaki zırh ile sağlanan topraklama verinin geçtiği tüm noktalarda (ağ kartından duvar prizlerine ve hub'a kadar) devamlı olmasıda çok önemlidir.

2- Kaplamasız Dolanmış Çift (**U**nshielded **T**wisted **P**air)

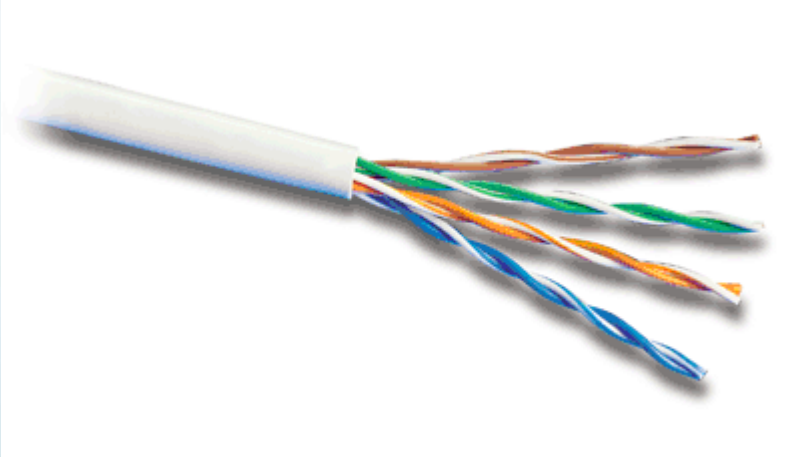
UTP birbirine dolanmış çiftler halinde ve en dışta da plastik bir koruma olmak üzere üretilir. Kablonun içinde kablonun dayanıklılığını arttırmak ve gerektiğinde(ne için gerekir diye sormayın..) dıştaki plastik kılıfı kolayca sıyırmak için naylon bir ip bulunur.

Tel çiftlerinin birbirine dolanmış olmaları hem kendi aralarında hem de dış ortamdan oluşabilecek sinyal bozulmalarının tedbirdir.



2- Kaplamasız Dolanmış Çift (**U**nshielded **T**wisted **P**air)

Kablo içindeki teller çiftler halinde birbirine dolanmıştır. Her çiftin bir ana rengi bir de "beyazlı" olanı vardır. Yukarıdaki resimde de görüldüğü gibi ana renkler turuncu, mavi, yeşil ve kahverengidir. Bunlara sarılı olan beyaz teller ise, diğerleriyle karışmasın diye, sarılı olduğu renkle aynı bir çizgiye sahiptir. Böylece 8 telin de turuncu, turuncu-beyaz, mavi, mavi-beyaz, yeşil, yeşil-beyaz, kahverengi, kahverengi-beyaz olmak üzere 8 farklı renkte ama 4 grupta toplanmış olduğunu görüyoruz.



2- Kaplamasız Dolanmış Çift (**U**nshielded **T**wisted **P**air)

UTP kablolar dış görünüş olarak birbirine çok benzer. Ancak her kablonun üzerinde kategorisi yazmaktadır.

2- Kaplamasız Dolanmış Çift (Unshielded Twisted Pair)

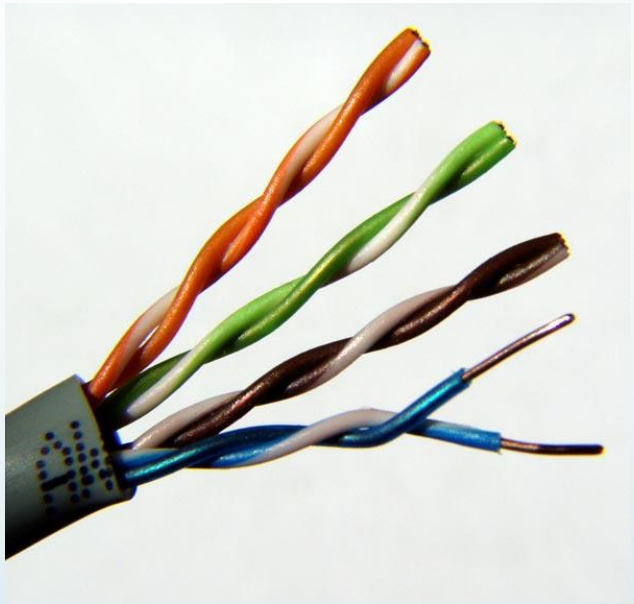
Kablonun kategorisi üretim kalitesiyle ilgilidir. Yapılan çeşitli testler ile kablonun belirtilen hızlarda elektrik sinyalini ne kadar sağlıklı ve az kayıpla iletebildiği, manyetik alan etkisine karşı sinyali ne kadar koruyabildiği ölçülür. Testler ile ortaya konan değerler kategorinin kriteridir. Bu kriterleri tutturabilen kablo bu kategoriyi almaya hak kazanır.

CAT5 ile 100 Mbit hızında veri aktarımı yapılabilir. Bir sonraki standart CAT5e (Enhanced CAT5, gelişmiş CAT5) standardıdır. Bu CAT5 ile aynı yapıda olup, daha üst seviye değerlere erişebilen bir kablodur. CAT5e ile gigabit hızına ulaşılabilir. Gigabit ethernet'te CAT5 kullanılabilmekle beraber CAT5e tavsiye edilir.

CAT6'da da aynı durum söz konusu CAT5e'den de daha yüksek değerlere erişebilir. CAT6 şu anda 568A standardına eklenmiş yani resmen kullanıma sunulmuştur. 1000Mhz hızı için, yani Gigabit ethernet için en uygun kablodur. Görüntüde bir fark yoktur.

2- Kaplamasız Dolanmış Çift (**U**nshielded **T**wisted **P**air)

UTP kablo ile ilgili bir diğer bir konu ise "stranded" ve "solid" kablo ayrımıdır. Yani çok damarlı veya tek damarlı kablo. Eğer mavi veya mavi-beyaz dediğimiz tel (veya diğerleri) tek parça bakır ise bu tek damarlıdır. Eğer ince-ince birden fazla telden oluşmuşsa buna da çok damarlı diyoruz.



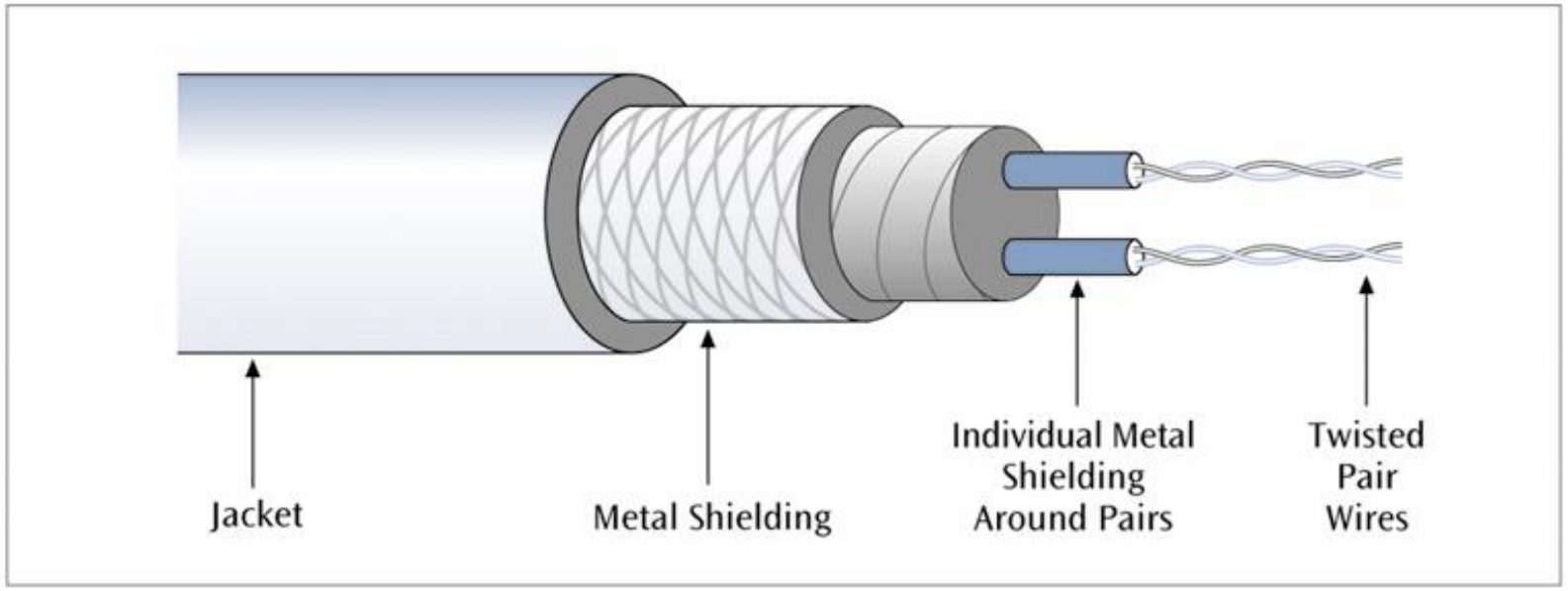
2- Kaplamasız Dolanmış Çift (Unshielded Twisted Pair)

Kablo seçimi yaparken dikkat edilmesi gereken nasıl bir ortamda kullanılacağıdır.

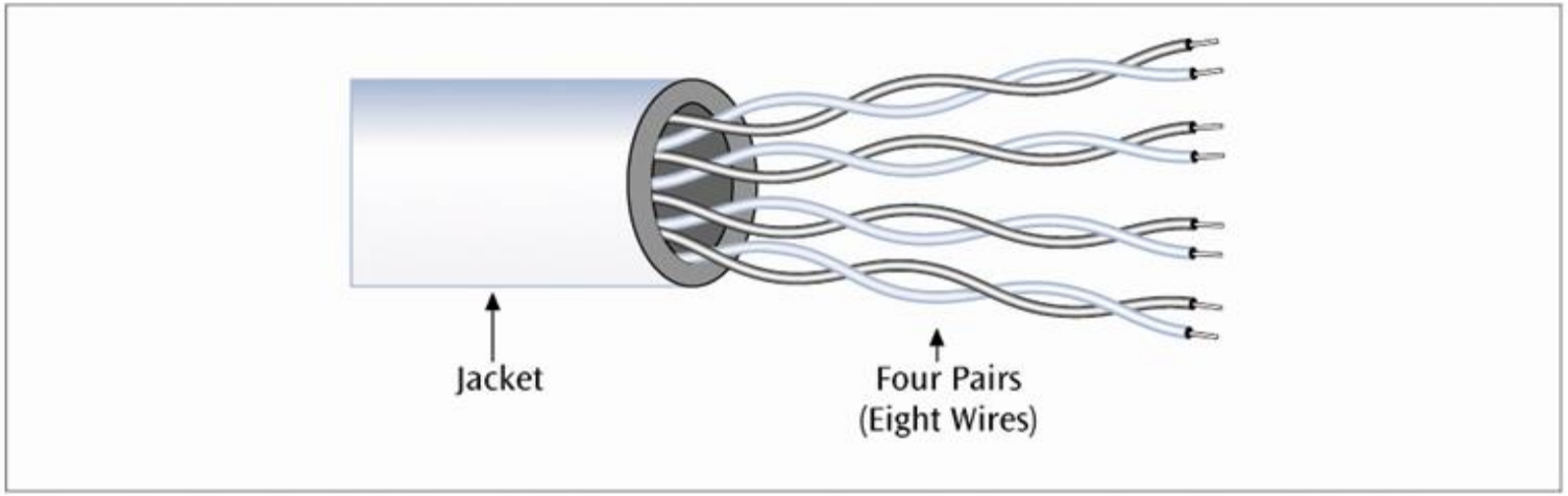
Duvar içlerinden giden, patch panellere gelen ve bir kere kurulduktan sonra bir daha hareket ettirilmeyecek kabloları tek damarlı, bilgisayar ile duvar prizi arasındaki kabloyu ise çok damarlı yapın. Çünkü tek damarlı daha mukavemetli bir kablodur ama fazla kıvırıp bükerseniz içindeki tek damar tellerden birisi kırılabilir. Oysa çok damarlıda, her bir tel bir çok ince telden oluştuğu için kırılma tehlikesi yoktur. Bu nedenle ayak altında olacak yerlerde bunu kullanın.

Bir diğer nokta çok damarlı bir kabloda renk kodları bazen farklı olabiliyor. En önemlisi ise, çok damarlı kablo ile kullanacağınız RJ-45 jakın mutlaka çok damarlıya göre dizayn edilmiş olması gerekiyor. Piyasa bulacağınız jaklar genelde tek damarlıya uygundur ve sıktığınızda damarın içine gömülen pinleri vardır. Böyle bir jak çok telli kabloda problem yaratabilir.

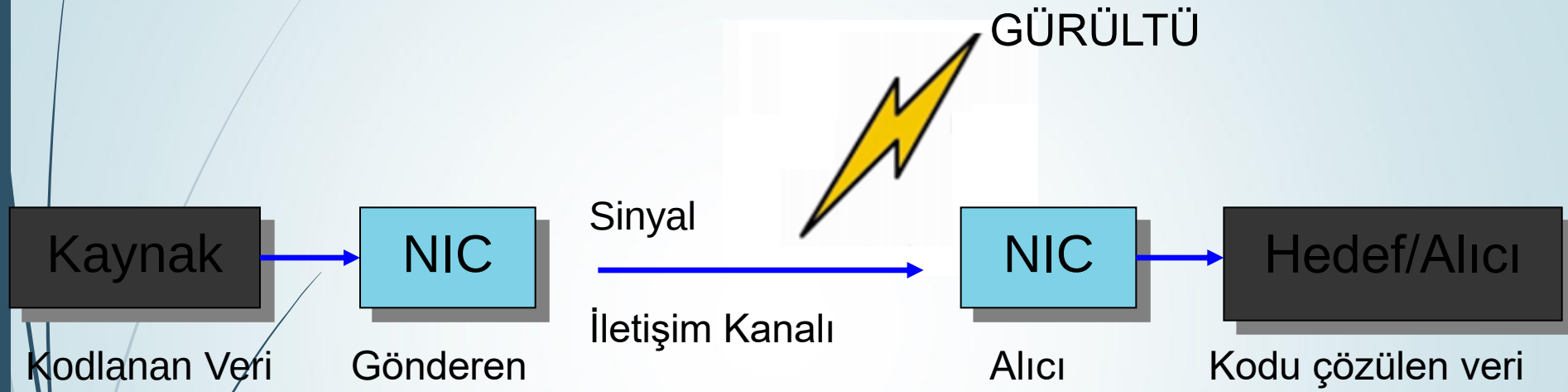
STP


Jacket
Metal Shielding
Individual Metal Shielding Around Pairs
Twisted Pair Wires

UTP

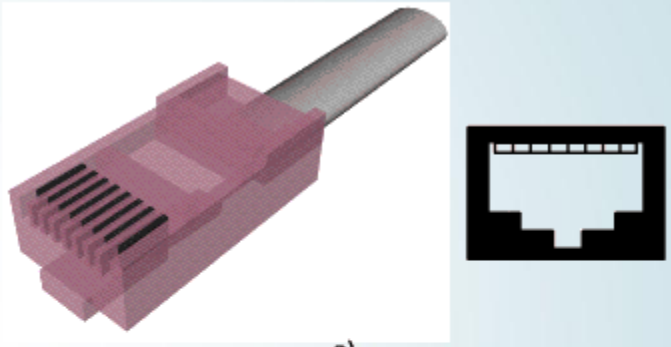

Jacket
Four Pairs (Eight Wires)

Gürültü


GÜRÜLTÜ
Kaynak
NIC
Sinyal
İletişim Kanalı
NIC
Hedef/Alıcı
Kodlanan Veri
Gönderen
Alıcı
Kodu çözülen veri

Çift Burgulu Kablo Konnektörü

- Bu tür kablolar RJ-45 konnektörü ile bilgisayar bağlanır. RJ-45'in en çok kullanılan standardı 10BASE-T'dir
- 10/100 Mbps hızındadırlar.
- Halka ve yıldız tipi topolojilerde kullanılır.

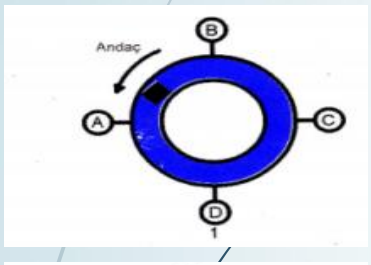


a)

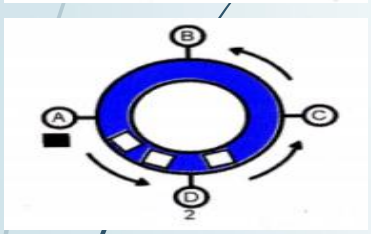
b)

TOKEN RING

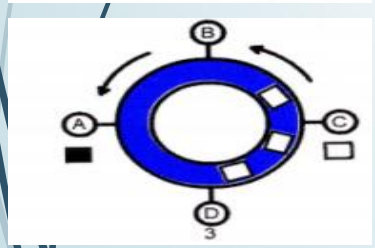
A bilgisayarının C bilgisayarına bir çerçeve göndermek istediğini varsayalım.



A bilgisayarı kontrol andacının üstteki komşusundan kendisine gelmesini bekler.

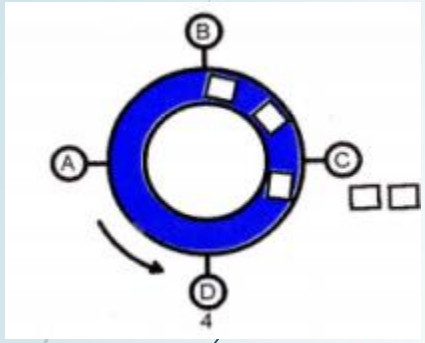


A bilgisayarı çerçeveyi halka üzerinden göndermeyi başlatır.

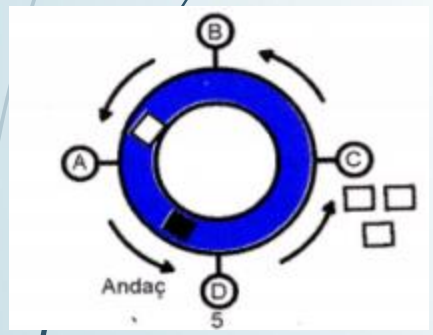


C bilgisayarı kendisine gönderilen çerçeveyi kopyalar. Çerçeve halka etrafında dolaşmaya devam eder.

TOKEN RING

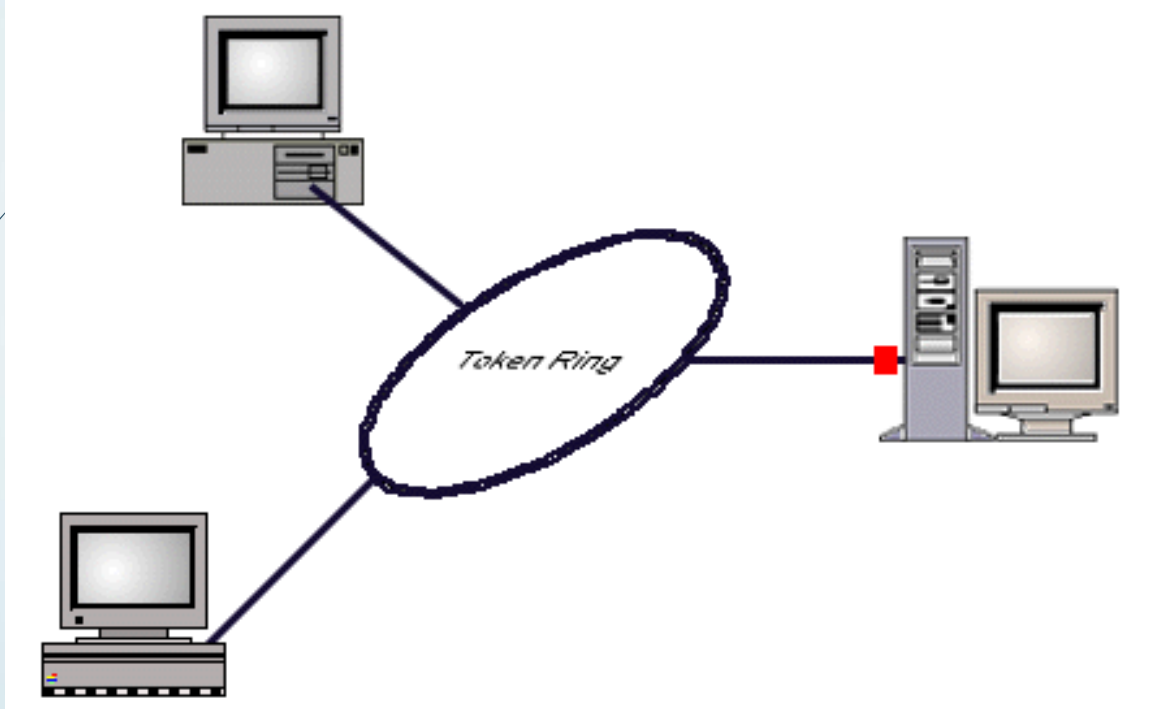


A bilgisayarı çerçeve başının alınmasını ve kendisine yeniden dönmesini bekler ve çerçeveyi siler.



A bilgisayarından çerçevenin son ikili gönderildiğinde, andaç A tarafından serbest bırakılır. (erken andaç bırakması)

TOKEN RING



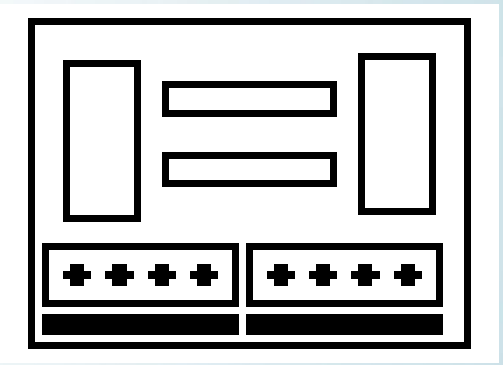
TOKEN RING

- **Konnektör ve yapısı**

- Bu ağlarda kullanılan kablonun fiber veya bakır olmasına göre konnektör türleri farklıdır.
  - Bakır ise RJ45
  - Fiber ise ST,SC

- Jetonlu halka da farksal manchester kodlaması ve buna ek olarak çerçeve ayracı anlamında her çerçeve arasında boş bir bit kullanır.
- TR konnektörünün bağlandığı noktaya "MAU"(MEDİA ADAPTOR UNİT) denir.

Tr konnektörü



Fiber Optik Kablo

Fiber Optik Kablo
1950'li yıllarda görünebilir imajların optik fiber kanallardan geçirilmesiyle ilgili yapılan çalışmalar tıp dünyasında kullanım alanı buldu. 1966 yılında Charles Kao ve George Hockham cam fiber üzerinden veri aktarımı da yapılabileceği fikrini ortaya attılar. Sonraki dönemlerde fiber üzerindeki kayıp oranları o kadar az seviyelere indirildi ki, fiber veri aktarımı için bakır'a göre çok daha avantajlı bir konuma geldi.

Fiber Optik Kablo

Düşük sinyal kayıpları nedeniyle fiber ile bakır kablolara göre daha yüksek hızlarda ve çok daha uzun mesafelerde veri aktarımı mümkündür. Bu mesafe repeater kullanılmadan 2 Km'ye kadar çıkabilir. Bakır UTP kablolarda bu mesafe 100m ile sınırlıdır.

Fiber'in hafif ve ince yapısı bakır kablo kullanmanın zor olduğu ortamlarda kullanılabilmesini sağlar.

Bütün bunlar fiber'in önemli özellikleri olmakla beraber, fiber'in en önemli özelliği elektomanyetik alanlardan hiç etkilenmemesidir. Çünkü fiber kablodan elektrik değil ışık aktarılır.

Fiber Optik Kablo

Fiber iletken olmadığı için elektriksel yalıtımın zorunlu olduğu yerlerde kullanılabilir. Binalar arasında toprak hattındaki fark problemi fiber için sorun değildir. Fiber kimyasal fabrikalar, askeri üsler gibi küçük bir elektrik akımının patlamaya neden olabileceği ortamlar için de idealdir.

Son olarak UTP veya diğer kabloların aksine, fiber bir kablodan bilgi çalmak çok daha zordur.

Fiber'in en büyük dezavantajı fiyatı ve kurulumunun zor oluşudur.

Fiber Optik Kablo

Tüm fiber teknolojileri veri alımı ve gönderimi için fiber'i çiftler halinde kullanır. Üreticilerde fiber kabloları bu şekilde üretmektedir.

Fiber Optik Kablo

Fiber kabloda normal ışık veya lazer kullanılabilir. Bu iki tip fiber tamamen farklı donanım kullanır.

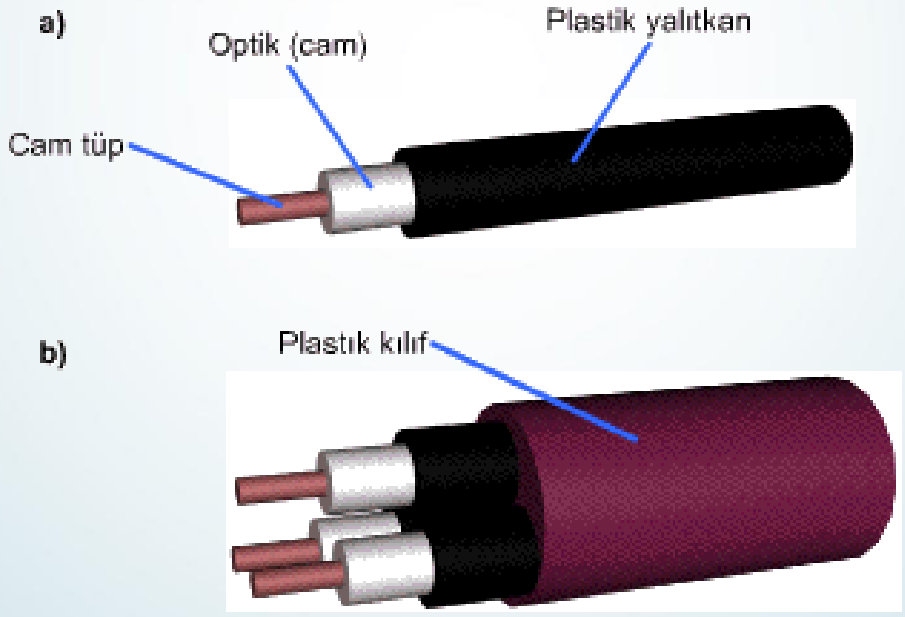
Işık sinyalleri yollamak için LED (Ligth Emitting Diot) kullanan fiber tipi multi-mode olarak adlandırılır ve en yaygın tiptir.

Fiber Optik Kablo

Lazer ışığı kullanan single-mode fiber çok yüksek veri aktarım değerlerine ulaşabilmesine rağmen pahalı ekipmanı nedeniyle yaygın değildir.

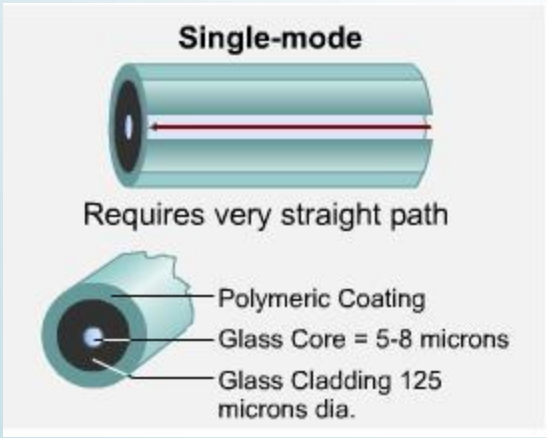
Fiber Optik Kablolar

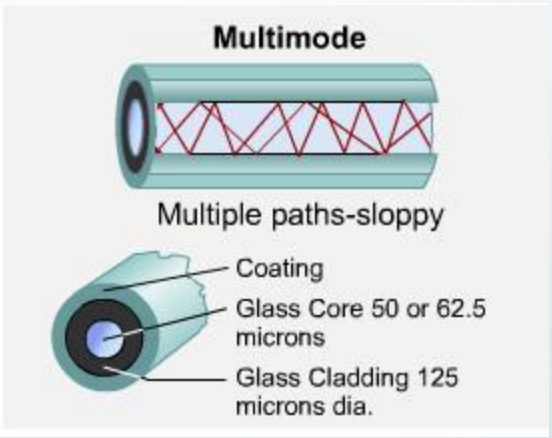
- 2 Km’ye kadar uzayabilen geniş alanlarda, elektriksel sinyallerden etkilenmeden yüksek kapasiteli iletişim ortamı sağlamada kullanılır.



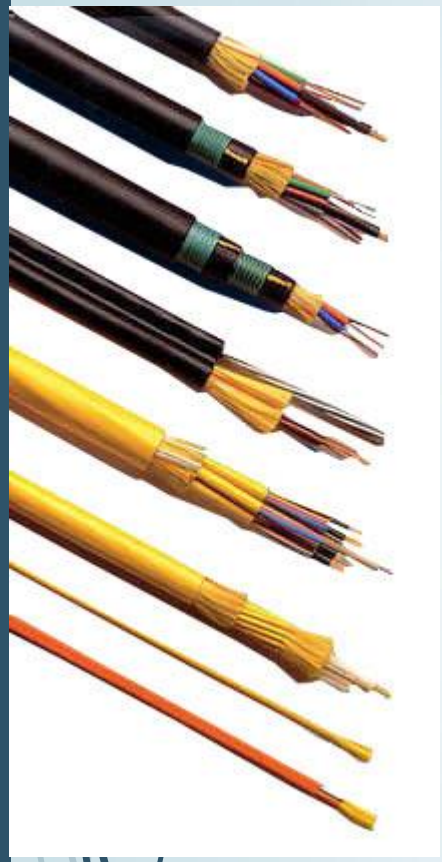
Fiber Optik Kablo Çeşitleri

- Tek, Çok modlu ve çok modlu kademeli olmak üzere 3 çeşidi vardır.
  - Tek Mod Fiberler (Single Mode Fiber- SMF) :
    - Işığın tek bir modda ya da tek bir yolda ilerlemesine olanak tanırlar
    - Düşük sinyal kayıplarının olduğu ve yüksek veri iletişim hızının gerektirdiği durumlarda kullanılırlar.
  - Çoklu Mod Fiberler (Multi Mode Fiber- MMF) :
    - Işığın birden fazla modunu ileten fiberlerdir.
    - Işın çarpışmaları meydana gelebileceğinden kısa mesafeler için kullanılır.

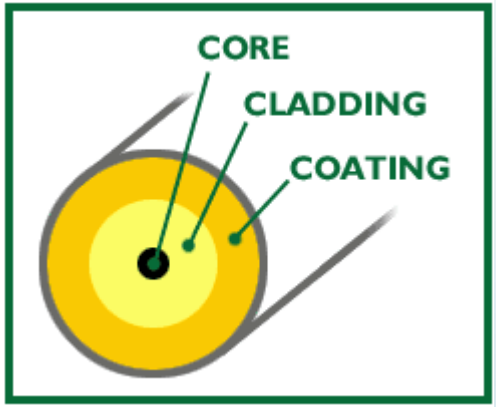




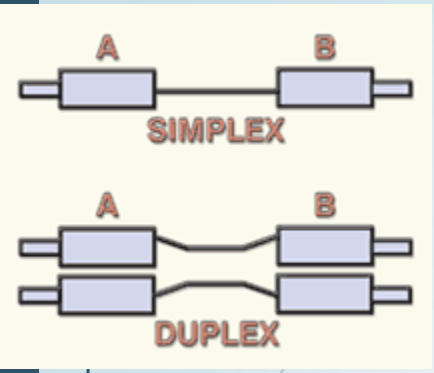
Fiber Optik Kablo Çeşitleri



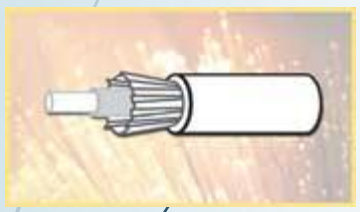
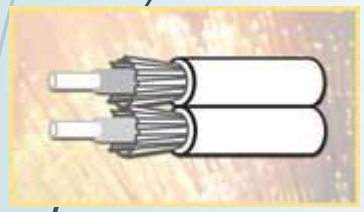
- Tek Mod Fiberler
  - 8.3/125 micron SMF
- Çoklu Mod Fiberler
  - * 62.5/125 micron MMF
  - 50/125 micron MMF
  - 100/140 micron MMF



Fiber Optik Kablolar



- Her bir fiberden tek yönlü haberleşme sağlanır. İki yönlü bir haberleşme için en az iki fiber gereklidir. Veya bir fiberde hem veri gönderimi hem de verinin alımını sağlayan iki ayrı yol olmalıdır.

	Simplex: İçerisinde sadece bir optik kablo var
	Duplex: İçerisinde 2 optik kablo var. LAN omurga kablosu olarak çok tercih edilmektedir.
	Multifiber: İçerisinde 2'den fazla optik kablo var.

Kablolar - Özet

Ethernet Adı	Kablo Tipi	Max. Veri Transfer Hızı	Max. Veri Transfer Uzaklığı	Açıklama
10Base5	Kalın Koaksiyel	10 Mbps	500 metre	BNC, T
10Base2	İnce Koaksiyel	10 Mbps	185 metre	BNC, T
10BaseT	UTP	10 Mbps	100 metre	RJ-45
100BaseT	UTP	100 Mbps	100 metre	RJ-45
1000BaseT	UTP	1000 Mbps	100 metre	RJ-45, CAT5 ve üstü
1000BaseTX (Gigabit Ethernet)	UTP	1000 Mbps	100 metre	RJ-45, CAT5 ve üstü
10BaseFL	Fiber (multimode)	10 Mbps	2000 metre	Ağlar arası, Fiber optik hub ve NIC arası bağlantı
100BaseFX	Fiber (multimode)	100 Mbps	2000 metre	100 Mbps Ethernet ağlarda
1000BaseSX	Fiber (multimode)	1000 Mbps	260 metre	SC, PC ve hub arası bağlantı için tasarlanmıştır.
1000BaseLX	Fiber (singlemode)	1000 Mbps	550 metre	1000BaseSX'in daha uzun mesafeler arası kullanması için, genellikle omurga olarak kullanılır.

Kablolar - Özet

Kategori	Desteklediği maksimum veri aktarım miktarı
Kategori 1	Telefon hatları-veri aktarımında kullanılmaz
Kategori 2	4 Mbit/Saniye
Kategori 3	16 Mbit/Saniye
Kategori 4	20 Mbit/Saniye
Kategori 5/5e	100 Mbit/Saniye
Kategori 6	1000 Mbit/Saniye

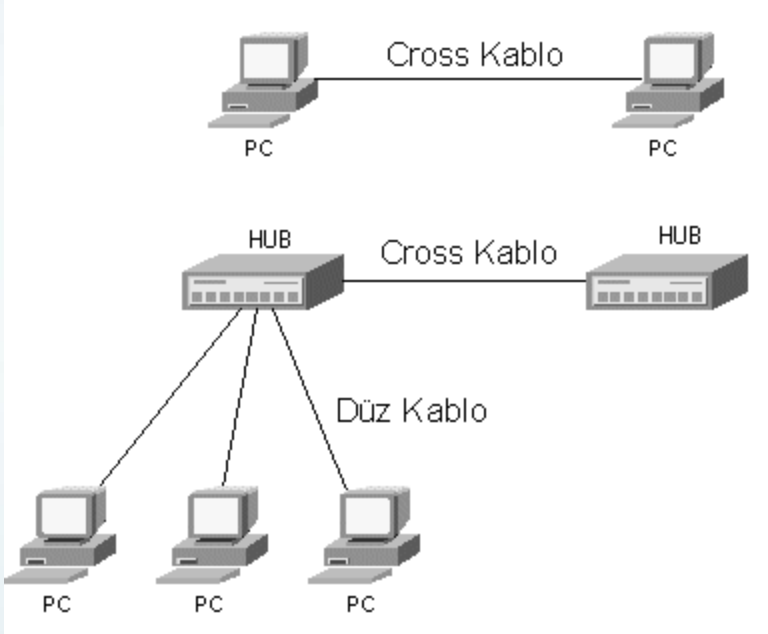
UTP KABLO YAPIMI

UTP KABLO YAPIMI

UTP kablo yapımında kullanım yerine göre 2 çeşit bağlantı türü vardır.

- Düz Kablo
- Çapraz Kablo (Cross)

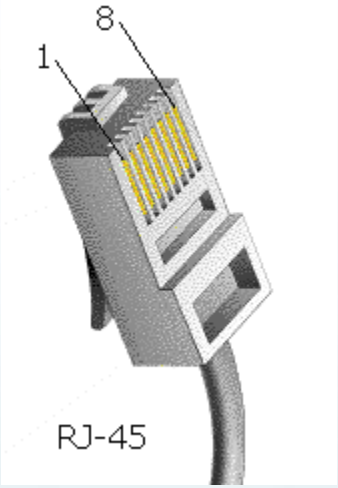
UTP KABLO YAPIMI



Gördüğünüz gibi aynı cihazlar arasında(PC-PC veya Hub-Hub) cross kablo kullanılır. PC'den hub'a gidecek kablo ise düz kablo kullanılmalıdır.

UTP KABLO YAPIMI

UTP kablonun ucuna taktığımız RJ-45 jak üzerindeki pinler jakın pinleri size bakacak şekilde tutulduğunda soldan sağa 1'den 8'e kadar sıralı kabul edilir.



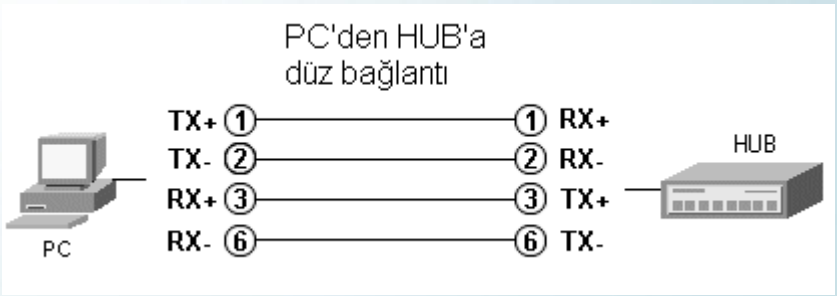
UTP KABLO YAPIMI

Network için kablo yaparken öncelikle bakmanız gereken şey kablonuzun standardıdır.

CAT5 kablolar için genel olarak kullanılan iki standart var 586-A ve 586-B. Bu standartlar kablonuzun üzerinde yazar. Kablonuzu renklerine göre bağlayacağınız standartlarda bunlardan ibarettir.

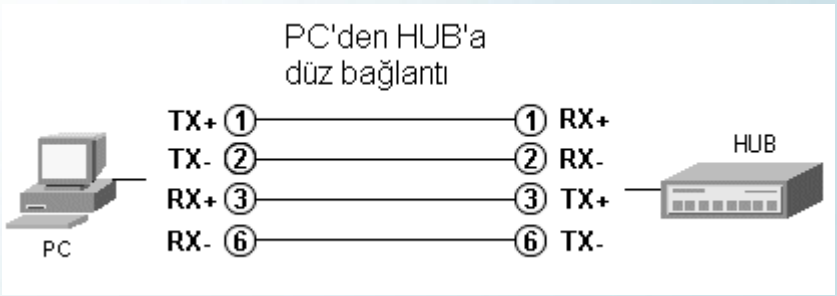
586-A Düz Bağlantı

Bilgisayar		Hub	
1	Yeşil-Beyaz	**1**	Yeşil-Beyaz
2	Yeşil	**2**	Yeşil
3	Turuncu-Beyaz	**3**	Turuncu-Beyaz
4	Mavi	**4**	Mavi
5	Mavi-Beyaz	**5**	Mavi-Beyaz
6	Turuncu	**6**	Turuncu
7	Kahverengi-Bayaz	**7**	Kahverengi-Bayaz
8	Kahverengi	**8**	Kahverengi



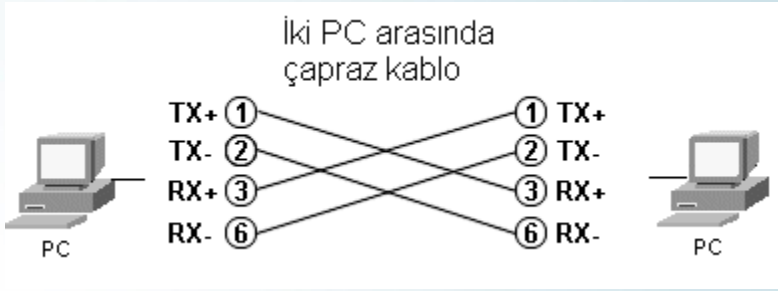
586-B Düz Bağlantı

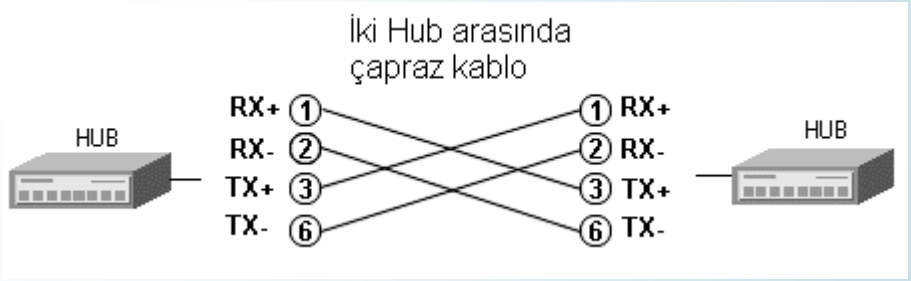
Bilgisayar		Hub	
1	Turuncu-Beyaz	**1**	Turuncu-Beyaz
2	Turuncu	**2**	Turuncu
3	Yeşil-Beyaz	**3**	Yeşil-Beyaz
4	Mavi	**4**	Mavi
5	Mavi-Beyaz	**5**	Mavi-Beyaz
6	Yeşil	**6**	Yeşil
7	Kahverengi-Bayaz	**7**	Kahverengi-Bayaz
8	Kahverengi	**8**	Kahverengi



Çapraz Bağlantı

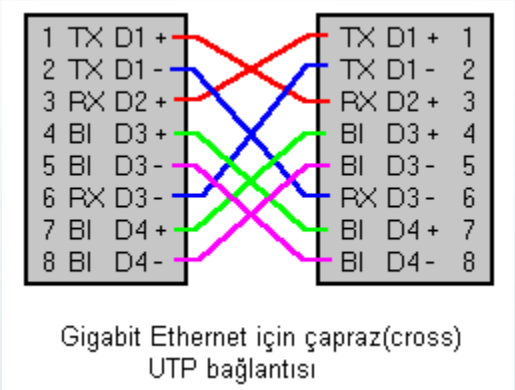
Bilgisayar/HUB 586-B		Bilgisayar/HUB 586-A	
1	Turuncu-Beyaz	**1**	Yeşil-Beyaz
2	Turuncu	**2**	Yeşil
3	Yeşil-Beyaz	**3**	Turuncu-Beyaz
4	Mavi	**4**	Mavi
5	Mavi-Beyaz	**5**	Mavi-Beyaz
6	Yeşil	**6**	Turuncu
7	Kahverengi-Bayaz	**7**	Kahverengi-Bayaz
8	Kahverengi	**8**	Kahverengi





Gigabit Ethernet

Yukarıdaki kablo bağlantıları 10BaseT ve 100BaseTX için yani 10Mbit ve 100Mbit ethernet için geçerlidir. 1000BaseT yani UTP kablo üzerinden gigabit ethernet kullanacaksanız düz bağlantıda bir farklılık yoktur. Çapraz kabloda ise alttaki şemayı kullanılmalıdır.

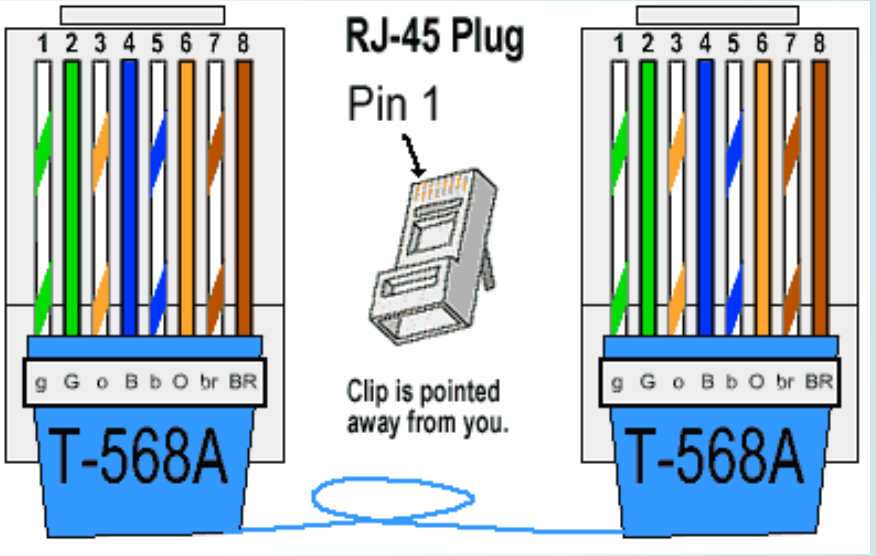


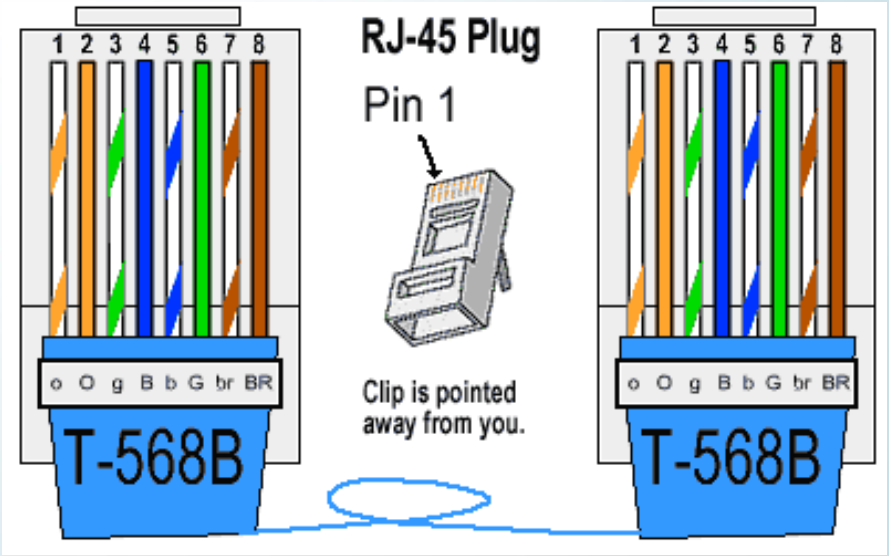
Gigabit Ethernet için çapraz(cross) UTP bağlantısı

Düz kablo (Straight-Through Ethernet Cable) 568A<->568A veya 568B<->568B olmalıdır.

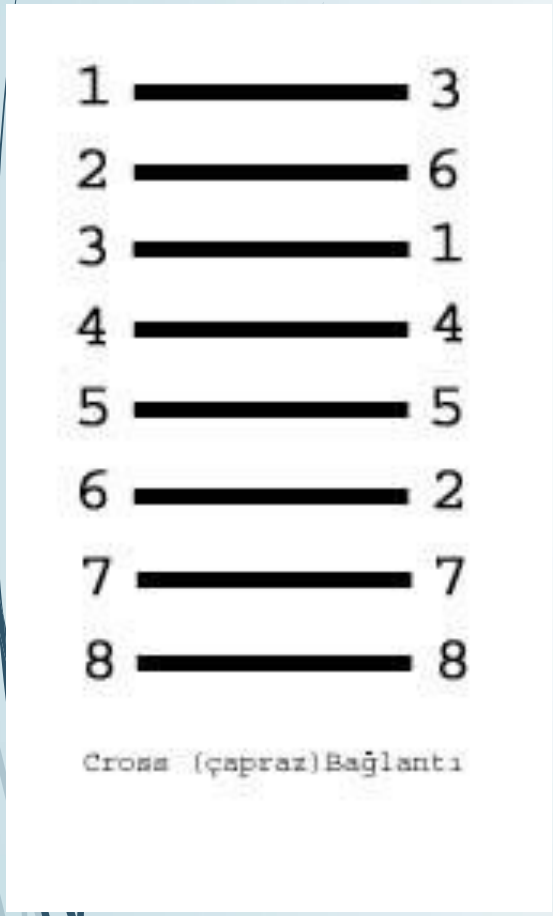
Turuncu Beyaz	▬▬	Turuncu Beyaz
Turuncu	▬▬	Turuncu
Yeşil Beyaz	▬▬	Yeşil Beyaz
Mavi	▬▬	Mavi
Mavi Beyaz	▬▬	Mavi Beyaz
Yeşil	▬▬	Yeşil
Kahve Beyaz	▬▬	Kahve Beyaz
Kahve	▬▬	Kahve

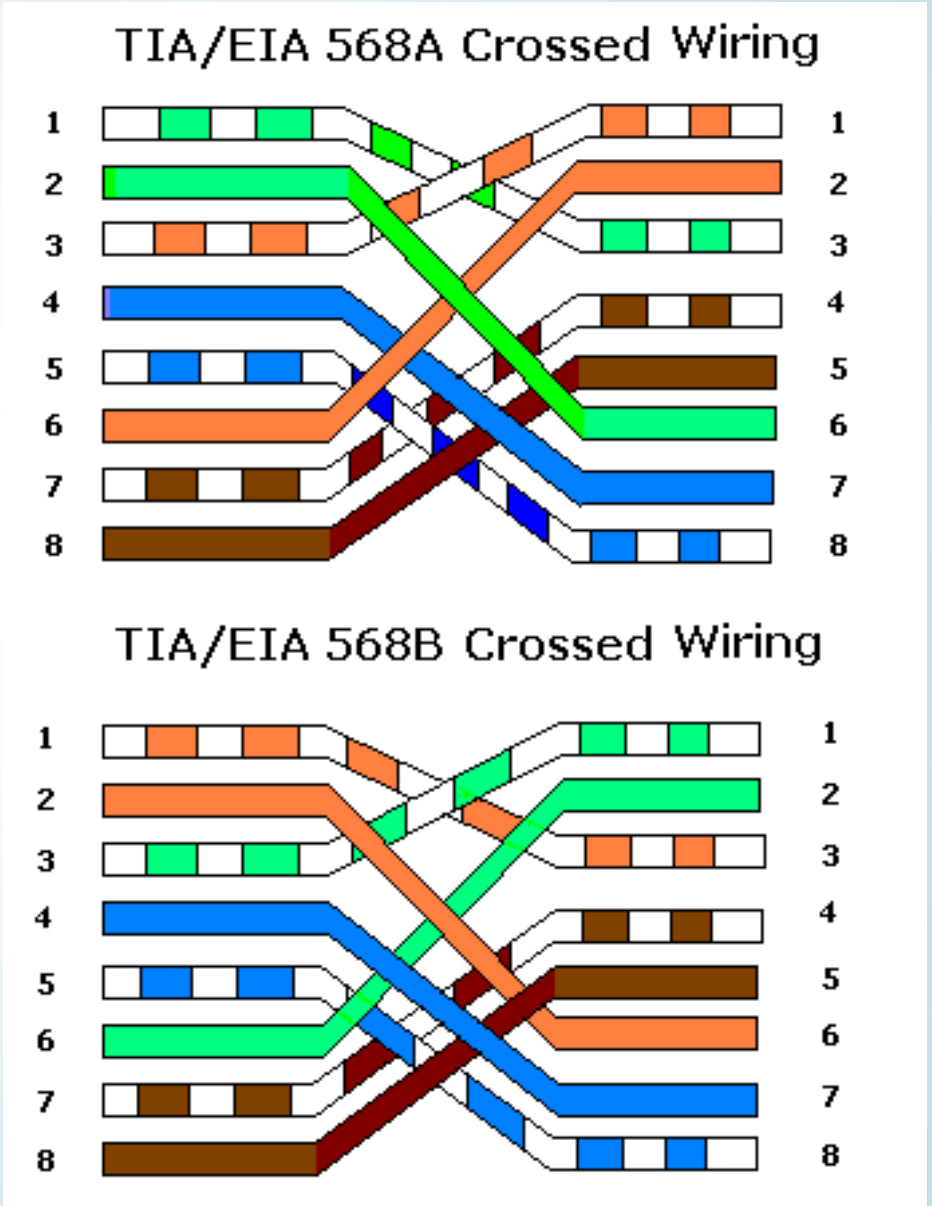
1:1 Bağlı 100 MBit Şeması





Çapraz Kablo (Crossover Ethernet Cable) 568A<->568B olmalıdır.





UTP KABLO YAPIMI

Birden çok bilgisayarı bir birine bağlamak istiyorsanız, Hub ya da Swich yardımıyla bu işi rahatlıkla yapabilirsiniz. Kablonun renklerine göre bağlama yöntemi ise yine kablonuzun üzerinde yazan standart'a göre yapmanız tavsiye edilir. Standartlara uyulmadan farklı renklerde bağlanan da bir network ağı çalışır. Ama en iyi performans alacağınız biçim kablonun üzerinde yazan standart'a göre kablo'nun uçlarını bağlamaktır.

Bilgisayarları Hub yada Swich ile birbirine bağlıyorsanız, kabloyu düz bağlanmalıdır. Kablonun her iki ucu da, kablonun üzerindeki standart'a göre ya 586-A yada 586-B'ye göre bağlayınız.

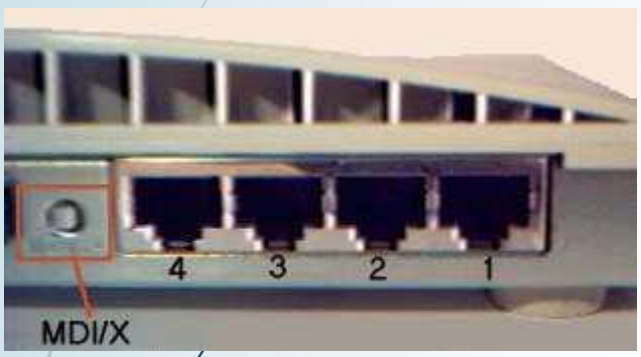
UTP KABLO YAPIMI

İki bilgisayarı birbirine bağlamak için cross(çapraz bağlantılı) kablo yapmak gerekir. Bunun için de kablonun bir ucunu 586-A'ya göre bir ucunu da 586-B'ye göre yapmanız yeterli olacaktır.

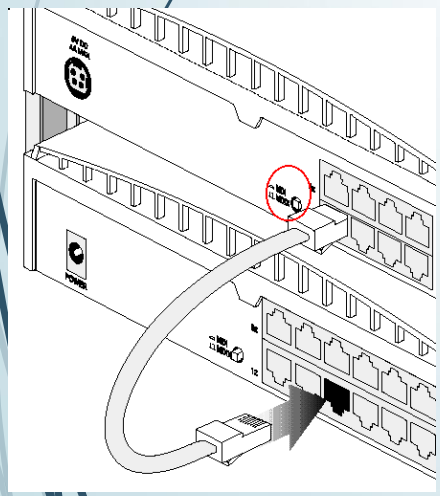
Hubların bir çoğunda portlardan en büyük numaraya sahip olanın yanında crossover, uplink, out, MDI/X gibi ibareler bulunur. Bu şu anlama gelir:

"Eğer bu hub ile başka bir hub'ı bağlayacaksan, düz kablo kullanabilirsin. Düz kablonun bir ucunu bu porta tak ve portun yanında bir düğme varsa ona bas, kablonun diğer ucunu ise, diğer hub'ın normal bir portuna tak."

UTP KABLO YAPIMI



4. numaralı portun yanındaki düğmeye dikkat.



İki hub'ı düz kablo ile bağlarken, kablonun bir ucu 1. hub'un uplink portuna, diğer ucu ise diğer hub'ın normal bir portuna takılır.

Üçüncü bir hub daha bağlanırken bu sefer 2. hub'ın uplink portu kullanılacaktır.

UTP KABLO YAPIMI

Eğer iki hub'da da BNC çıkışı varsa koaksiyel kablo ile de hub'ları bağlayabilirsiniz. Tabii ki iki uçta sonlandırıcı olması gerekiyor.

UTP KABLO YAPIMI

Jak'ı takma

Jak takmaya geçmeden kullanacağımız aletleri tanıyalım.

Basit bir RJ-45 sıkma aleti

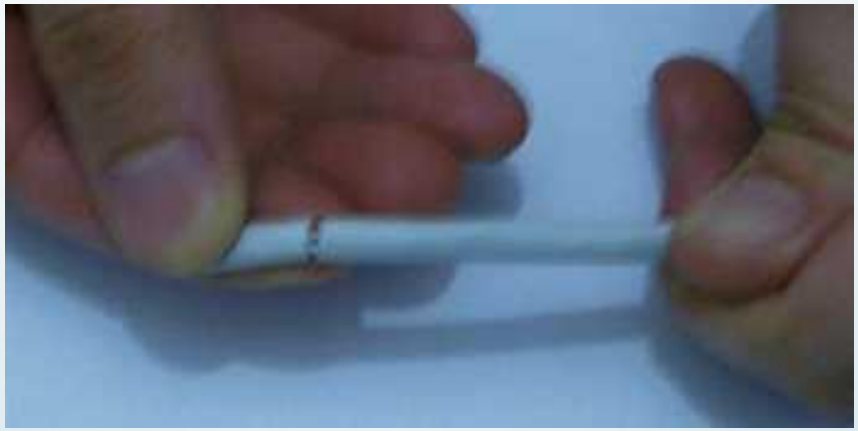
Kablo Soyma Aleti

UTP KABLO YAPIMI

1- Biz elimizdeki sıkma aletini kullanarak kablonun ucunu açalım. Yapmamız gereken kablonun ucunu 2cm kadar aletin iki tarafında da bıçak olan bölümüne sokmak, sadece en dıştaki plastiği kesecek kadar aleti sıkıp, sol elimizle kabloyu tutarken, sağ elimizle aleti çevirmek.

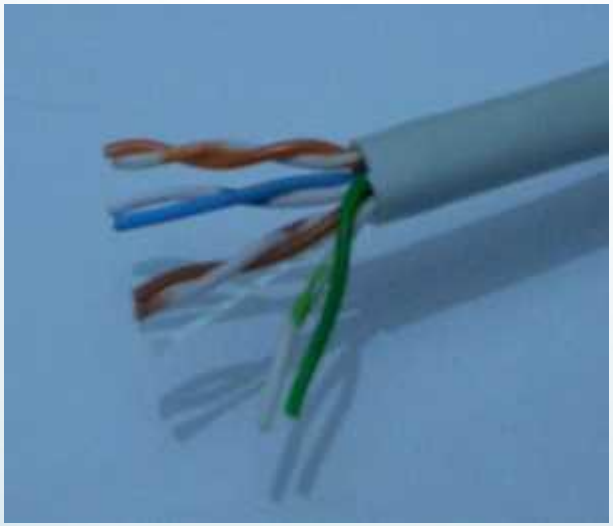
UTP KABLO YAPIMI

2- Bu hareketi yapınca kablonun dışındaki plastik kesilmiş olacak ve elimizle hafifçe bükünce bunu iyice görebileceğiz. Bu parçayı elimizle sıyıralım. İçerdeki tellerin kesinlikle yaralanmamış olması gerekiyor.



UTP KABLO YAPIMI

3- Şimdi telleri görebiliyoruz. Sıra geldi telleri kullanacağımız şablona göre sıraya dizmeye. Elimizle, telleri soldan sağa, sağdan sola "çekiştirerek" istediğimiz sıraya getiriyoruz.



UTP KABLO YAPIMI

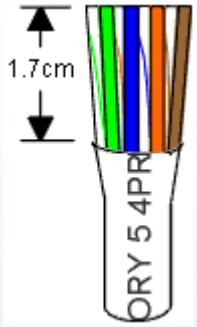
4- Şimdi de teller düz sırada iken telleri baş ve işaret parmağımız arasında "yoğurarak" düzeltiyoruz.

UTP KABLO YAPIMI

5- Düz hale de getirdikten sonra aletin bir bıçaklı olan ağzına yerleştirip tüm uçlar düz olacak şekilde uçları kırpıyoruz.

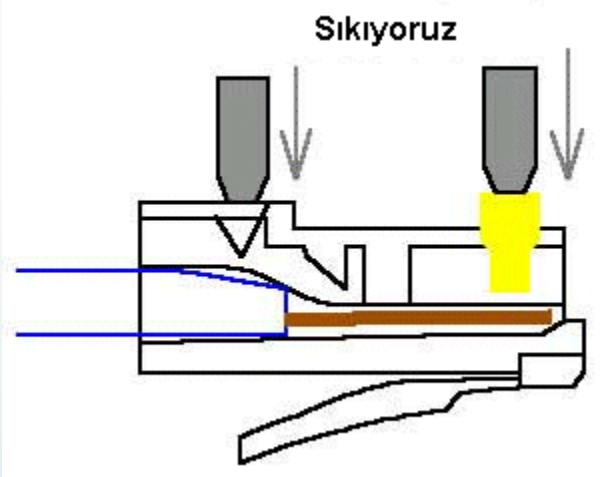
UTP KABLO YAPIMI

6- Gördüğünüz gibi teller düzgün sırada ve uçları da dümdüz. Bu noktada açıkta olan tellerin boyu 1.7cm den daha uzun olmamalı. Aksi halde teller arasında sinyal bozulması olabilir.



UTP KABLO YAPIMI

7- Kabloyu jakın içine sokuyoruz. Bu noktada iki şey önemli. Birincisi tüm uçlar jakın içteki en son noktasına değmeli yani yandaki resme göre jakın sağından bakıldığında, tüm teller sonuna kadar girmiş olmalı.

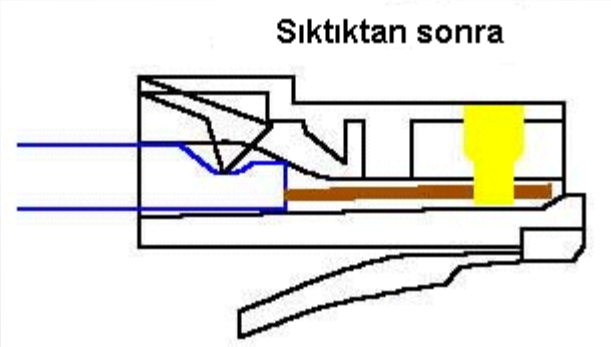


UTP KABLO YAPIMI

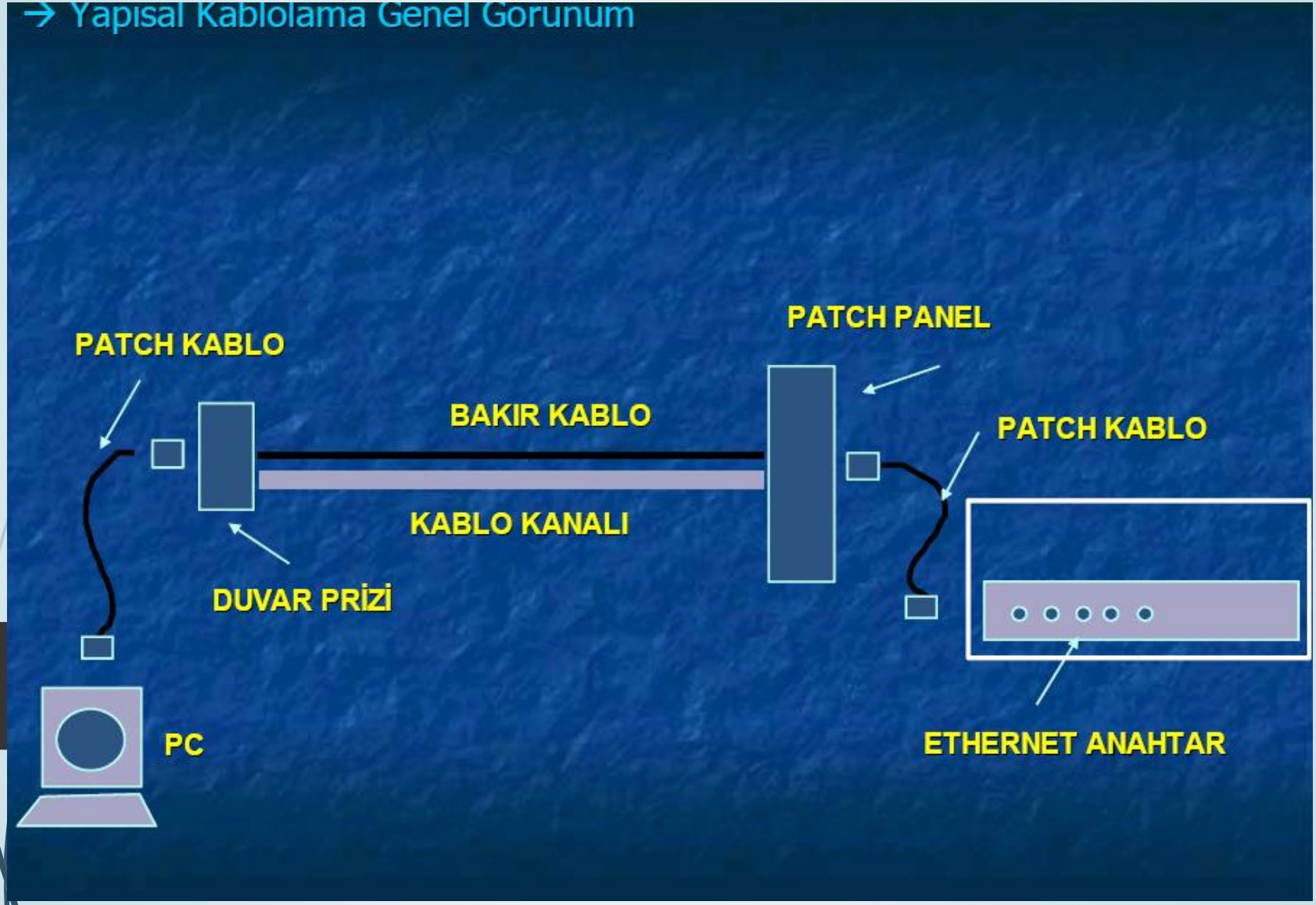
8- Jakı alete takıyoruz ve tek harekette fazla abanmadan sıkıyoruz.

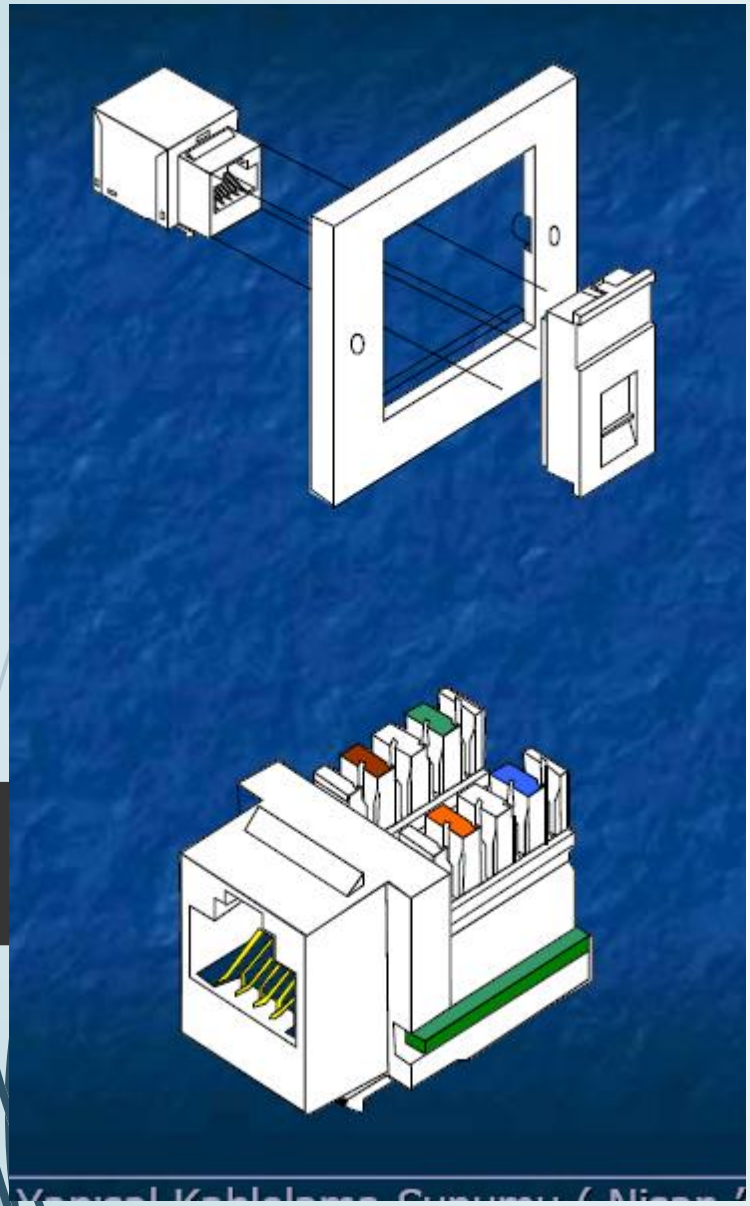
UTP KABLO YAPIMI

9- Sıktıktan sonra yandan bakıldığında pinlerin kablolara gömüldüğünü ve jakın arkasındaki plastiğin de kablonun en dış plastiğini(yanda mavi olarak çizilmiş) ezdiğini görebiliriz/görmeliyiz.



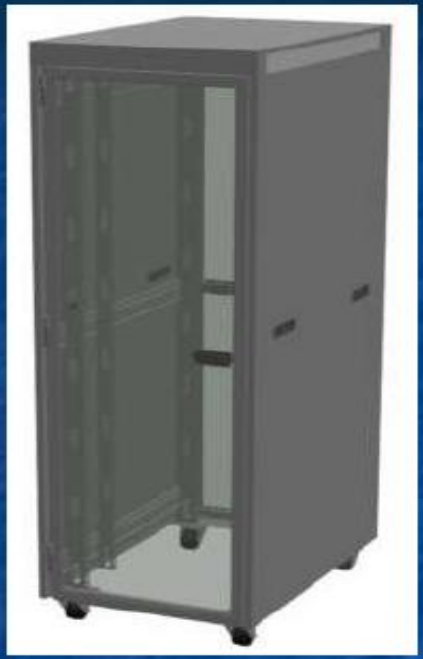
→ Yapısal Kablolama Genel Görünüm

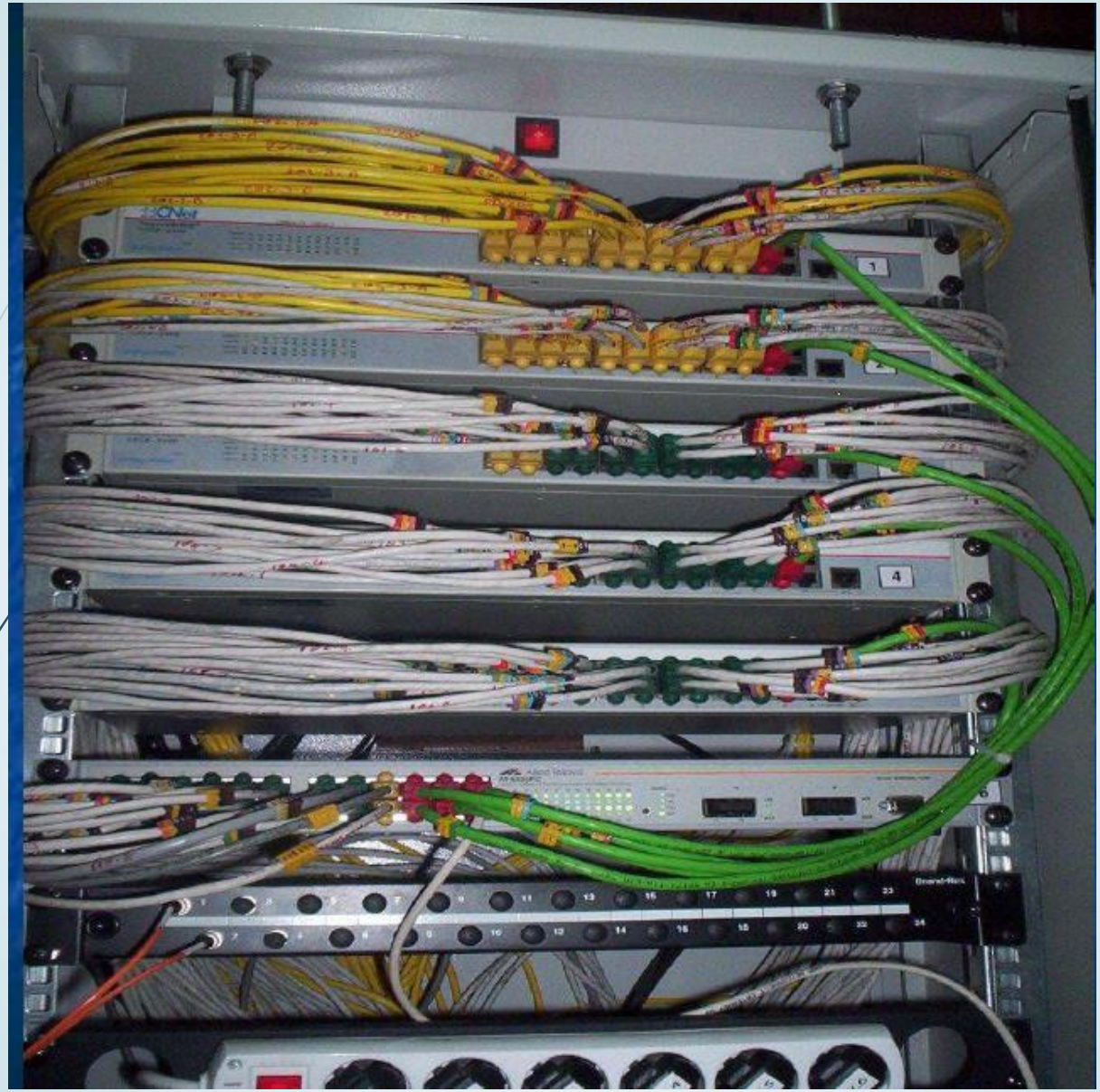




→ Kabinetler

1) Ölçüler, 19" , U , (450,600,800)
2) Yer ve Duvar Tipi
3) Kilit, Ön ve Yan Kapaklar
4) Rack Demirleri Hareket
5) Termostat, Fan ve Sessizliği
6) Kabinet İçi Elektrik Düzeni
7) Kablo Organizasyonu
8) Kablolara Toplu Pay

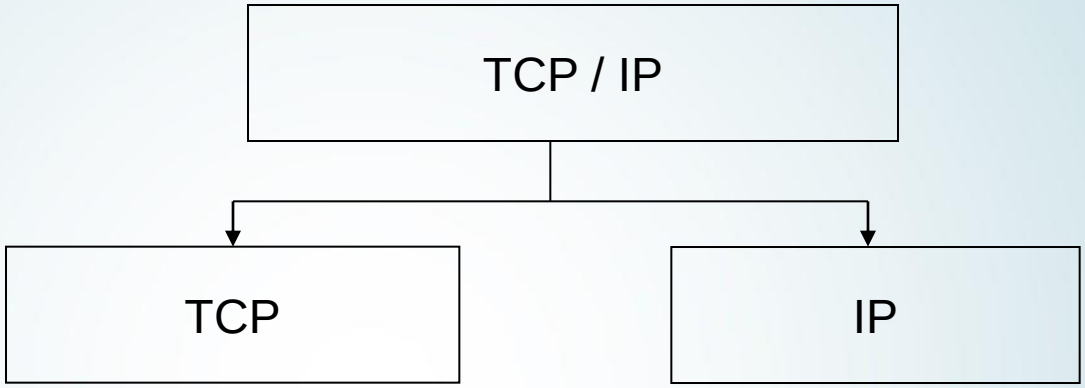




AĞ TEMELLERİ

Ağ Katmanı ve Protokolleri

TCP/IP

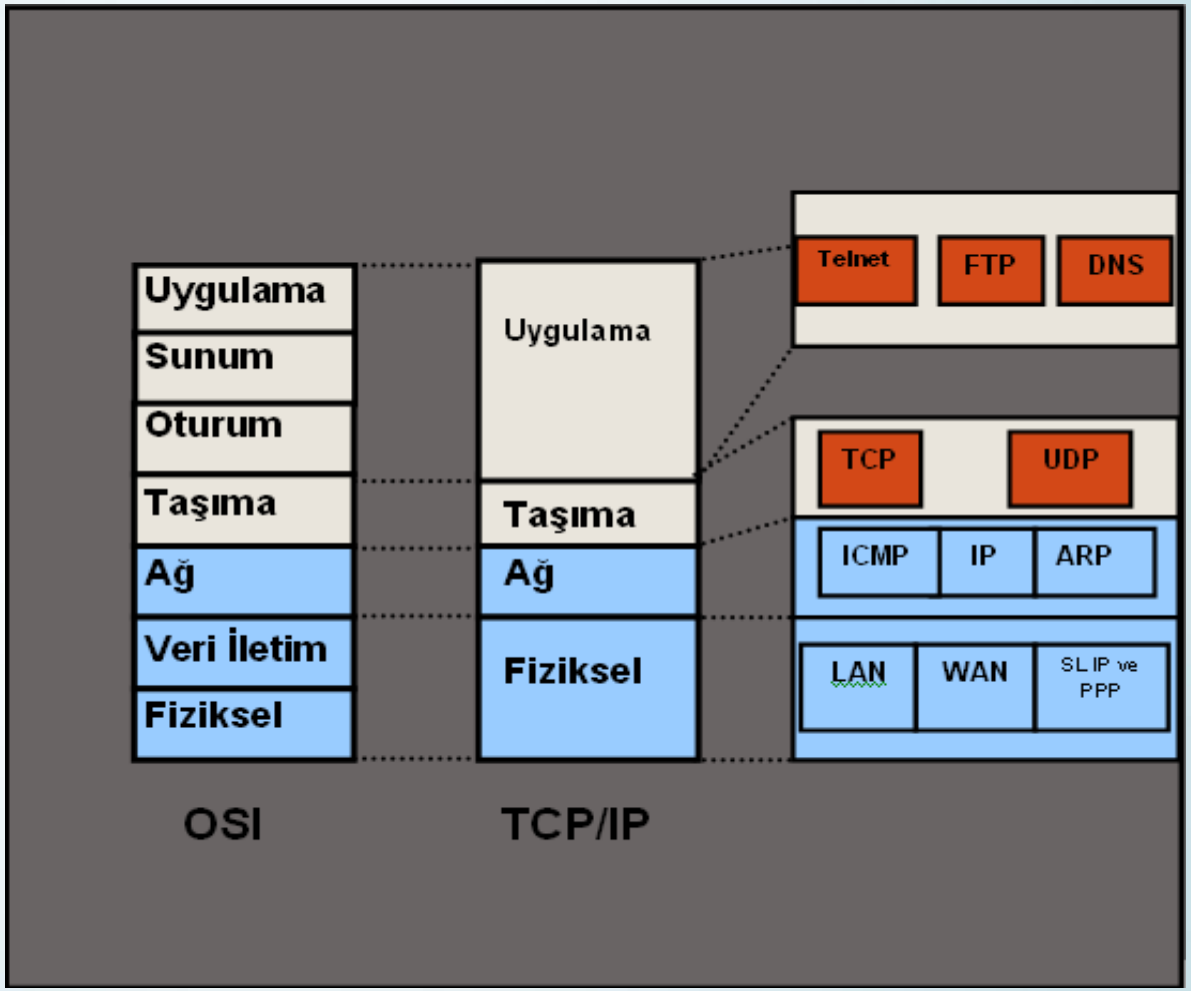


- TCP (Transmission Control Protocol)
- Paketlerin iletimi

- IP (Internet Protocol)
- Paketlerin yönlendirmesi

OSI ve TCP/IP

- Uygulama Katmanı (Application Layer)
- Taşıma Katmanı (Transport Layer)
- Ağ Katmanı (Network Layer/Internet Layer/Internetwork Layer)
- Fiziksel Katman (Network Access Layer/Link and Physical Layer)



Ağ Katmanı

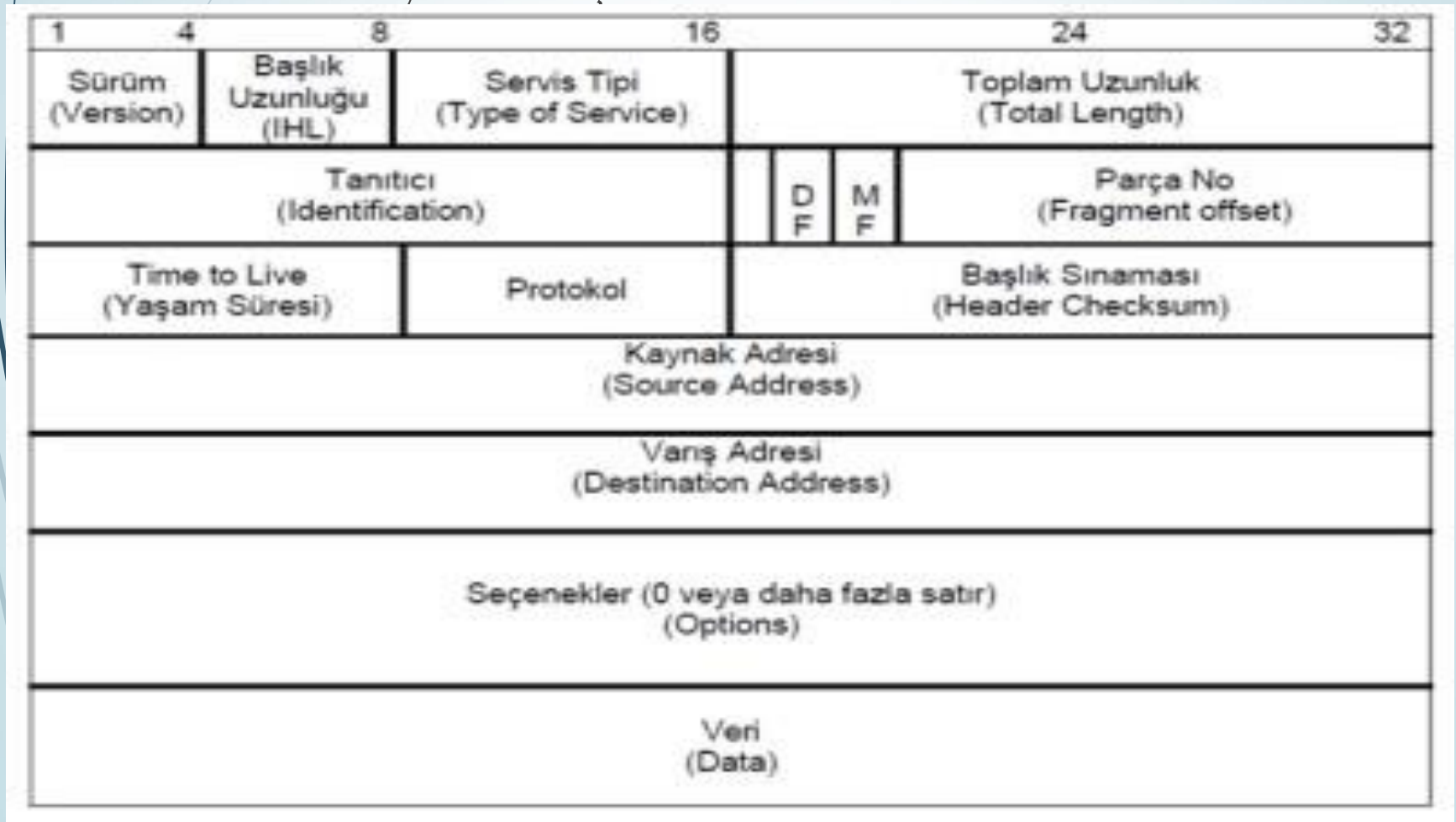
- OSI ağ katmanı, ağlar arasında iletilmek üzere oluşturulan Ağ katmanı paketini, en uygun yolu belirleyerek iletmekten sorumludur.
- Ağ katmanı veriyi belirli bir ağa yönlendirir ve ilgili olmayan ağlara veri göndermez .
- Ağ katmanı veri paketinin farklı bir ağa gönderilmesi durumunda yönlendiricilerin kullanacağı bilginin eklendiği katmandır.
- Örneğin; IP protokolü bu katmanda görev yapar.

Ağ Katmanı Protokolleri

- IP (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)
- BGP (Border Gateway Protocol)
- IPsec (IP Security)
- RIP(Routing Information Protocol)
- OSPF(Open Shortest Path First)

IP (Internet Protocol)

- IP (Internet Protocol)
  - IP adresi bir ağa bağlı bilgisayarların ağ üzerinden birbirlerine veri yollamak için kullandıkları adrestir.



IP Paket yapısı

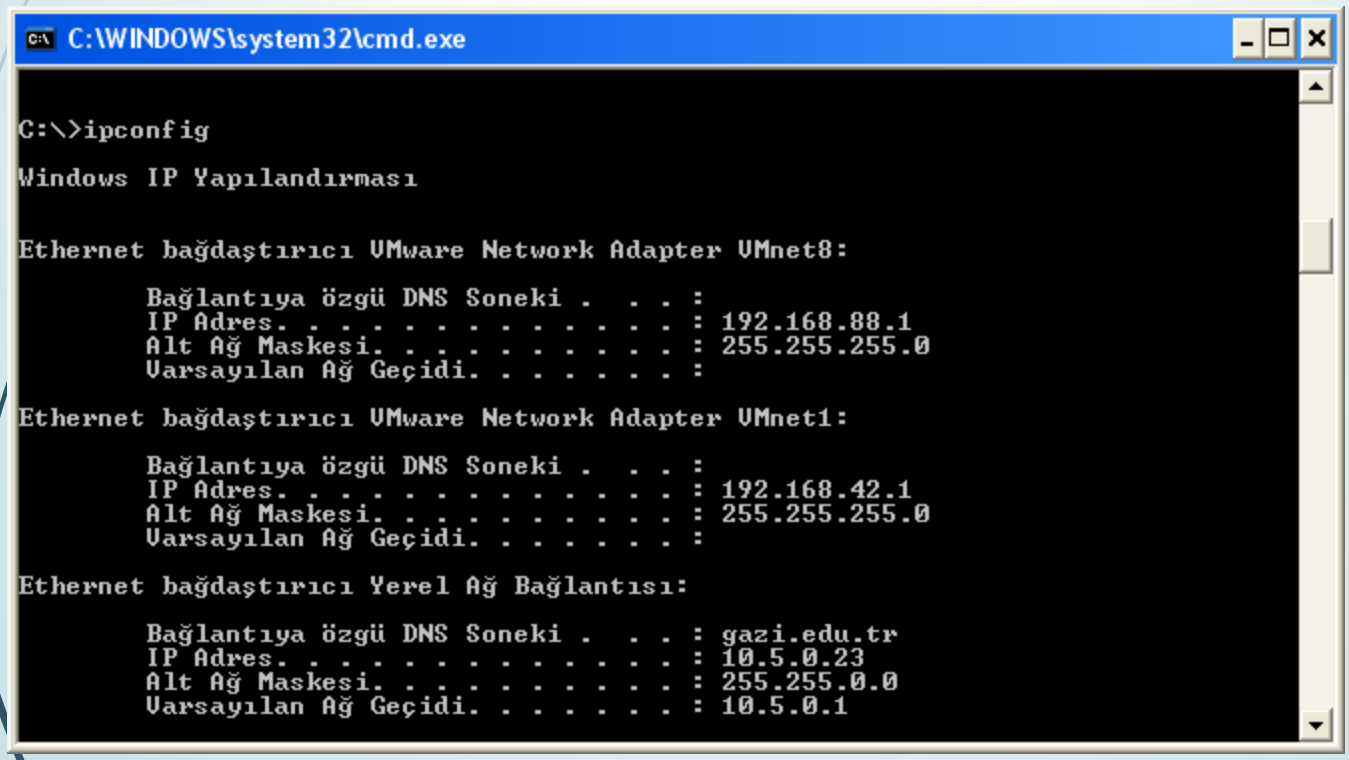
- Hizmet türü: Host'un ne tür bir hizmet istediği: Hızlı (örneğin ses), hatasız (örneğin dosya) veya güvenli iletim gibi.
- Kimlik: Paket bölümünün bağlı olduğu bölümün kimliği, o pakete ait olan bölümlerin hepsinde aynı tanım yazar.
- TTL (Time to Live): Paketin ömrü.
- Başlık kontrol toplamı: Sadece paketin kontrolünü sağlar.

IP (Internet Protocol)

- Yaygın olarak IPv4 adresler kullanılıyor.
- Toplam 32 bit ve noktalarla ayrılmış 4 adet 8 bitlik sayı.
- Örnek bir IP adresi:
  - 10000000 10011100 00001110 00000111
  - w.x.y.z
  - 128.156.14.7
- Ip adresleri dünyada $2^{32} = 4$ milyardır.
- Dinamik ip adresleri : Evden modem ile bağlanma
- Statik ip adresleri: IIS

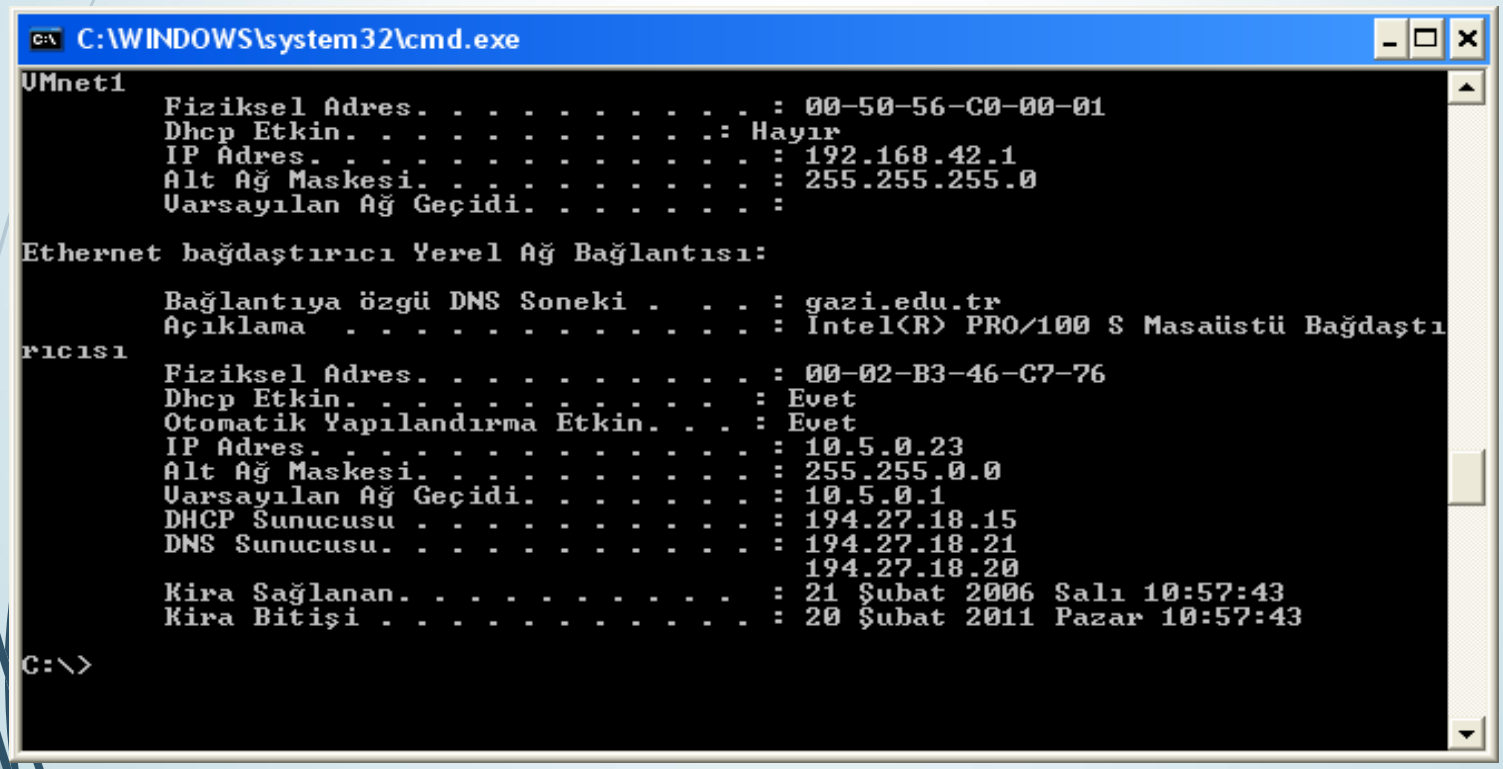
IPConfig Komutu

- Tüm ip ile konfigürasyonu (MAC adres vb.) görmek için kullanılır.



IPConfig Komutu

- Ipconfig /?
- ipconfig /all ile tüm seçenekler görülebilir.



AĞ KATMANI -ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

- İki ya da daha fazla bilgisayar arasında veri transferi sırasında meydana gelebilecek hataları ve kontrol mesajlarını idare eder. Bu nedenle ICMP ağ problemlerini tespit etmek için çok önemli bir protokoldür.
- ICMP protokolü kullanılarak tespit edebileceğimiz bazı sorunlar şu şekildedir:
- Lokal makinede TCP/IP'nin düzgün yapılandırılmış olduğunu kontrol etmek
- Bir bilgisayarın ayakta olup olmadığını,
- Ağ geçitlerinin tıkanık olup olmadığını,
- Bir mesajın kaybolup kaybolmadığını
- kontrol etmek .

ICMP

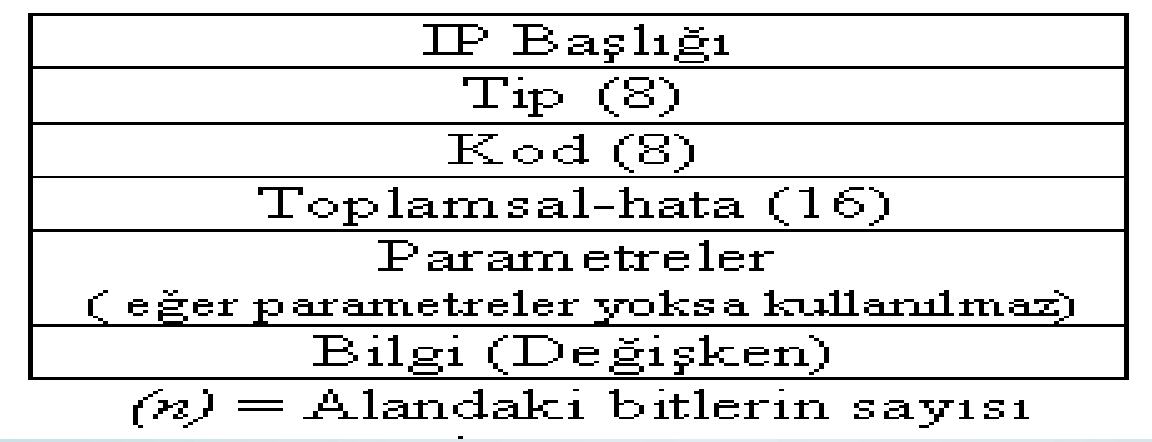
- Internet protokolü (IP) hata-raporlama veya hata-düzeltme mekanizmalarına sahip değildir; bu işler ICMP denilen bir modüle kalır. ICMP bir host bilgisayarında IP'nin yanında yer alır.

- ICMP paketleri ortamda bir geri besleme sağlarlar. Bu yolla ciddi sorunları, haberleşen birimlere bildirerek bir hata bildirim mekanizması oluştururlar. Ancak buradan ICMP'nin IP'yi güvenilir bir protokol haline dönüştürme amacı ile geliştirildiği yargısı çıkarılmamalıdır.

- ICMP mesajı, IP paketinin veri bölümünde taşınır. Bu yüzden ICMP paketlerinin dağıtım güvenilirliği, IP paketlerinin dağıtım güvenilirliği ile sınırlı kalmaktadır. Buradan ICMP paketlerinin güvenilir iletilemeyeceği ve hedefe vardığının garanti edilemeyeceği sonuçları çıkarılabilir .

ICMP Mesaj Formatı

- ICMP mesajları IP datagramının kullanıcı verisi alanında taşınır. IP başlığındaki protokol alanı 1'e set edilerek ICMP'nin kullanıldığı gösterilir. Tüm ICMP mesajları üç alandan oluşur:
- Tip alanı: mesajın tipini tanımlar
- Kod alanı: hata veya durum bilgisi tipini tanımlar.
- Toplamsal-hata (checksum) alanı: ICMP mesajının 16-bitlik 1'e tümleyenini hesaplar.



ICMP Mesaj Formatı

- ICMP hata raporlama mesajları aynı zamanda internet başlığı ve kullanıcı veri alanının ilk 64 bitini taşırlar.
- Bu bitler problem giderme ve problem analizi için faydalıdır .

İletişim Bağlantısını Sorgulama (PING)

- Ping komutu internet veya intranet de tcp/ip kullanan 2 aygıt arasındaki bağlantıyı test eder.

  Ping 131.140.1.1
  PİNG Aygit_ismi

  Şeklinde kullanılır.

- Bir makineye genelde 32 baytlık bir ICMP (Internet Control Message Protocol, yani Internet Yönetim Mesajlaşması Protokolü) paketi gönderir ve aynı paketin geri gelmesini bekler. Bu basit program, birçok işe yarayabilmektedir.

- Ping (echo) pakedi gönderilen makinenin o anda çalışmakta olduğunu teyid eder.
- Ağın o anki paket kayıp oranı hakkında bir bilgi verebilir.
- Kaynak makine ile karşı makine arasındaki iletişimin süresini gösterebilir .

İletişim Bağlantısını Sorgulama (PING)

- Ping uygulamasının kullandığı iki tür ICMP paketi vardır. Bunlar,
- 1. ICMP echo request paketi (istemciden giden paket)
- 2. ICMP echo reply paketidir. (istemciye gelen paket)
- Not: Kendi bilgisayarınızda 127.0.0.1 adresine ping edildiğinizde, ping yanıt vermezse pc de tcp/ip çalışmıyordur.
- Not: ICMP paketleri çoğu Firewall tarafından bloke edilirler.
- Örnek:
- ping google.com cevap verirken
- ping microsoft.com Request timed out (istek zama aşımına uğradı) mesajı verir, nedeni ise microsoft' un internet sunucuları hiçbir ping'e cevap vermezler.

İletişim Bağlantısını Sorgulama (PING)

- Örnek ping uygulaması:
- ping http://www.google.com/

32 bayt veri ile google.com [66.249.93.99] 'ping' ediliyor:

66.249.93.99 cevabı: bayt=32 süre=271ms TTL=47
66.249.93.99 cevabı: bayt=32 süre=269ms TTL=47
66.249.93.99 cevabı: bayt=32 süre=270ms TTL=47
66.249.93.99 cevabı: bayt=32 süre=268ms TTL=47

66.249.93.99 için Ping istatistiği:
Paket: Giden = 4, Gelen = 4, Kaybolan = 0 (0% kayıp),
Mili saniye türünden yaklaşık tur süreleri:
En Az = 268ms, En Çok = 271ms, Ortalama = 269ms .

İletişim Bağlantısını Sorgulama (PING)

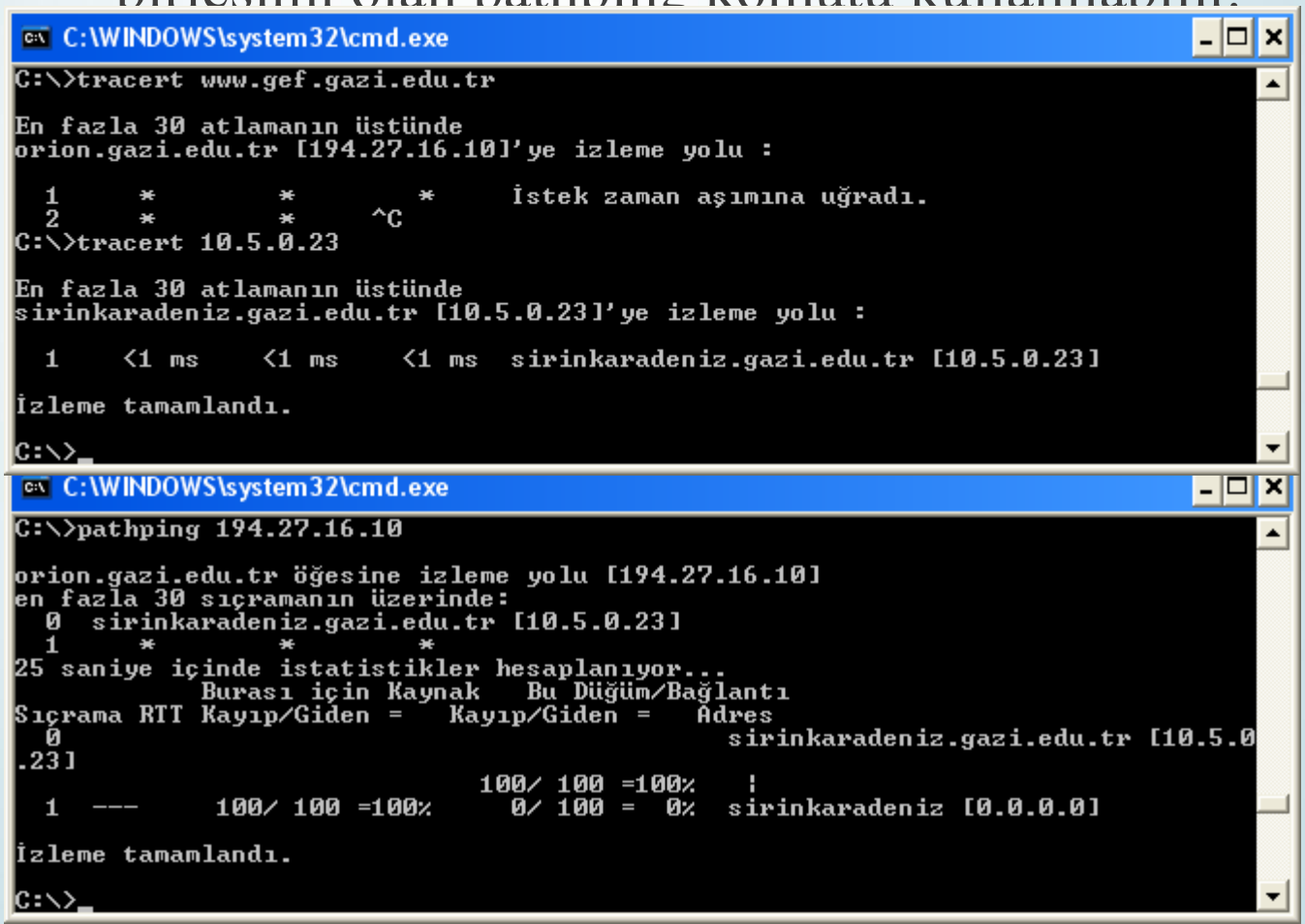
- Örnek ping uygulaması:

- Burada TTL (time to live – Paketin yaşam süresi) degeri 255'den başlar ve hedef makinaya ulaşıncaya kadar kaç tane yönlerdiriciden geçerse TTL degeri bir azalır, eger TTL 0 olusursa (destination unreachable) hedef ulaşılamaz mesajını alırız .

  66.249.93.99 adresi google.com' un reeel ip adresin vermektedir.
  bayt=32; gönderilen icmp paketi
  süre=52ms; 51ms degeri ise hedef aygıta ulaşıncaya kadar geçen süre. Bir başka deyişle iki aygıt arasındaki bağlantının kalitesini belirtir .

Tracert Komutu

- Bir adrese giden yolu gösterir.
- Microsoft'ta tracert ve ping komutlarının birleşimi olan pathping komutu kullanılabilir.



Adres Çözümleme Protokolü (ARP)

- Adres Çözümlemesi'nden kasıt, karşı bilgisayarın IP adresini sisteme vermemize karşılık veri hattı katmanından karşı makinenin LAN adaptörüne ait olan MAC adresini elde etmektir.
- ARP, IP adresinden MAC adresi elde eden bir protokoldür.

Niçin MAC adresi alınır?

- Ağ katmanı protokollerinin (TCP/IP, Netbios gibi) adresleri herhangi bir veriden farksız işlem görür. LAN'da yapılacak her türlü iletişim için LAN adaptör kartının donanımsal adresini bilmemiz gerekiyor. Çünkü fiziksel katmanda asıl iletişimi bu alt seviye katmanları yapacaktır.

Çalışma Sistemi;

- Genelde ARP, ARP belleği olarak bilinen haritalama tabloları ile çalışır. Tablo, bir IP adres ile bir fiziksel adres (MAC adresi) arasında haritalama yapılmasını sağlar.
- ARP hedef IP adresini alır ve haritalama tablosundan bunun karşıladığı hedef fiziksel adresi arar. Eğer ARP adresi bulursa, bulduğu fiziksel adresi , isteği yapan cihaza yollar.

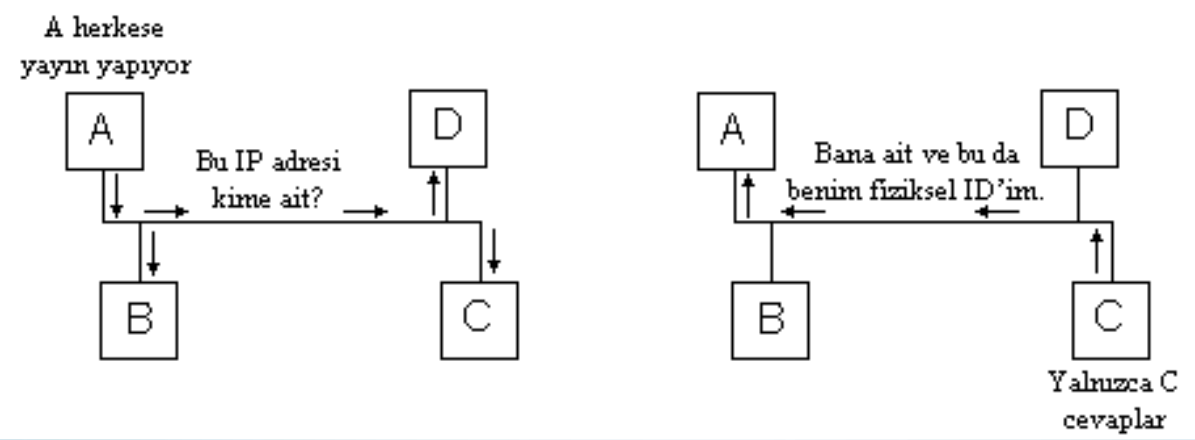
Çalışma Sistemi;

- Gerekli adres ARP belleğinden bulunamazsa, ARP modülü ağa bir yayın yapar. Yayına ARP isteği (ARP request) denir. Bu yayın bir IP hedef adresi içerir.

- ARP isteğindeki IP adresine sahip olan host, isteği yapan host'a kendi MAC adresini içeren ARP cevap (ARP reply) gönderir.

Örnek 1:

ARP isteği ve cevabı kavramları Şekil 1'de gösterilmiştir. A host'u C'nin fiziksel adresini bulmak istemektedir. A bu yüzden B, C, D'ye datagram (ip paket birimi) yayınlar. Bu yayına yalnızca C cevap verir çünkü gelen ARP istek datagramında kendi IP adresinin olduğunu görür. C host'u kendi MAC adresini ARP cevabı formunda bir IP datagramına yerleştirir.



Şekil 1: ARP İsteği ve Cevabı

Adres Çözümleme Protokolü (ARP)

ARP istek ve cevap paketlerine ait alanlar:

- **Fiziksel katman başlığı:** Fiziksel katman paketinin başlığıdır.
- **Donanım:** Donanım arabirim tipini belirtir (Ethernet, paket radyo vs.).
- **Protokol:** Göndericinin kullandığı protokol tipini tanımlar; tipik olarak EtherType'dır.
- **Donanım adres uzunluğu:** Paketteki donanım adreslerinin bayt olarak uzunluğunu belirtir.
- **Protokol adres uzunluğu:** Paketteki protokol adreslerinin bayt olarak uzunluğunu belirtir (Ör, IP adresleri).
- **Opcode:** Paketin bir ARP request (1) veya bir ARP reply (0) olduğunu belirtir.
- **Gönderici donanım adresi:** Göndericinin donanım adresini içerir.
- **Gönderici protokol adresi:** Göndericinin IP adresini içerir.
- **Hedef donanım adresi:** Sorgulanan host'un donanım adresini içerir.
- **Hedef protokol adresi:** Sorgulanan host'un IP adresini içerir.

Not: Request (İstek) paketinde hedef donanım adresi alanı dışındaki tüm alanlar kullanılır. Reply (Cevap) paketinde ise tüm alanlar kullanılır.

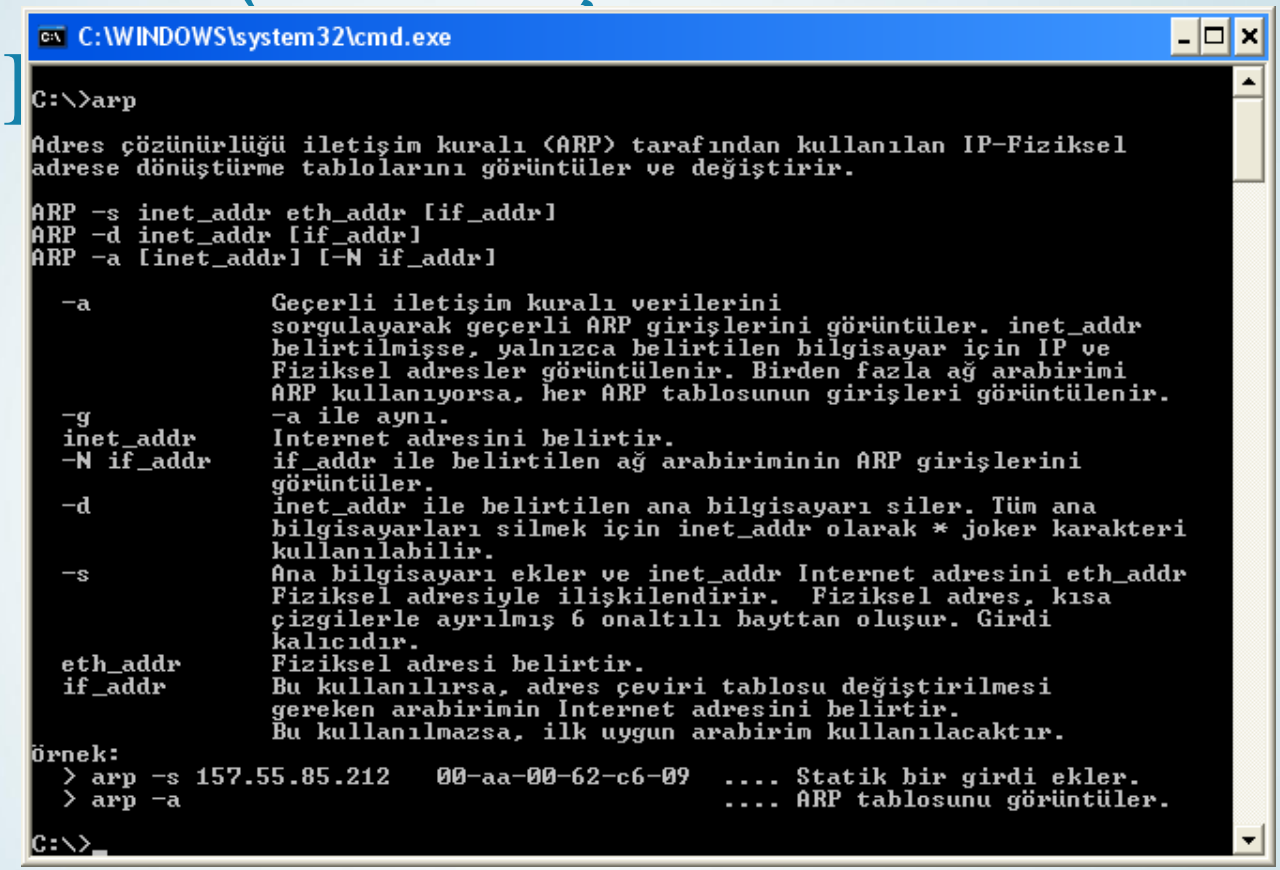
ARP Önbelleği:

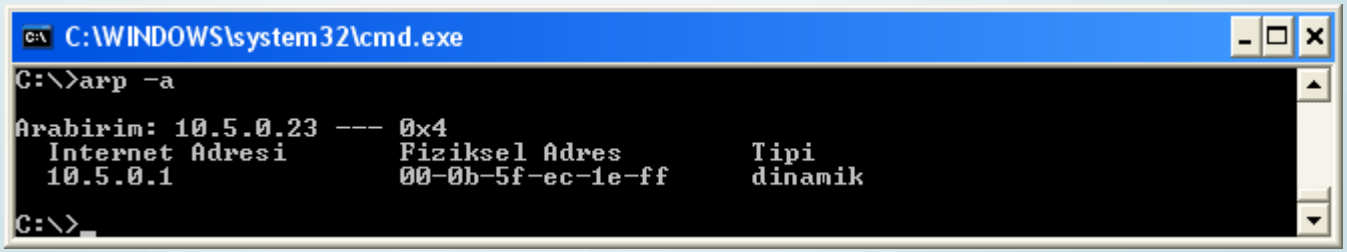
ARP yayın sayısını en alt düzeye düşürmek için, haritalama yaptığı IP adresleri ile MAC adreslerini ön belleğinde tutar. ARP önbelleğinde dinamik ve statik girdiler olabilir.

Her dinamik ARP önbelleği girdisi potansiyel olarak 10 dakikalık bir ömre sahiptir. Önbelleğe eklenen yeni girdilere zaman bilgisi girilir. Bir girdi eklendikten sonra 2 dakika içinde yeniden kullanılmazsa zaman aşımına uğrar ve ARP önbelleğinden silinir.

Not: Her ağ bağdaştırıcısı için ayrı bir ARP önbelleği vardır.

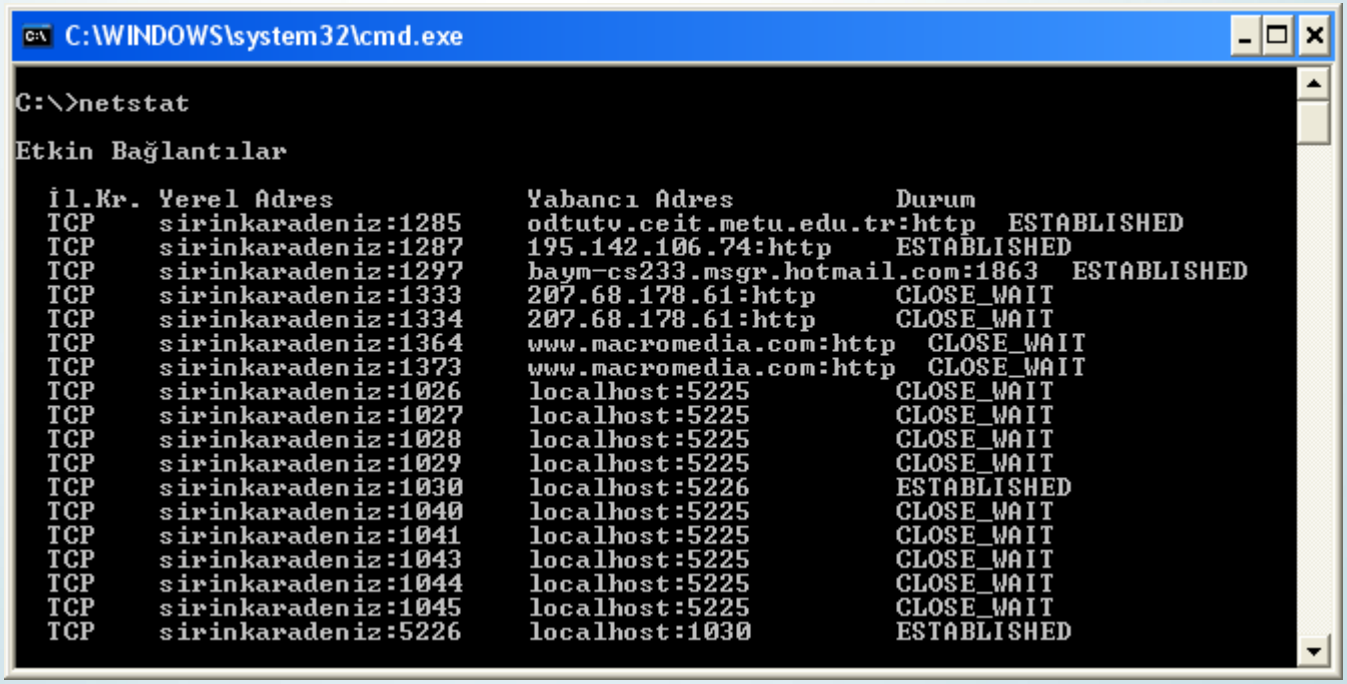
ARP (Adres Çözümleme
]





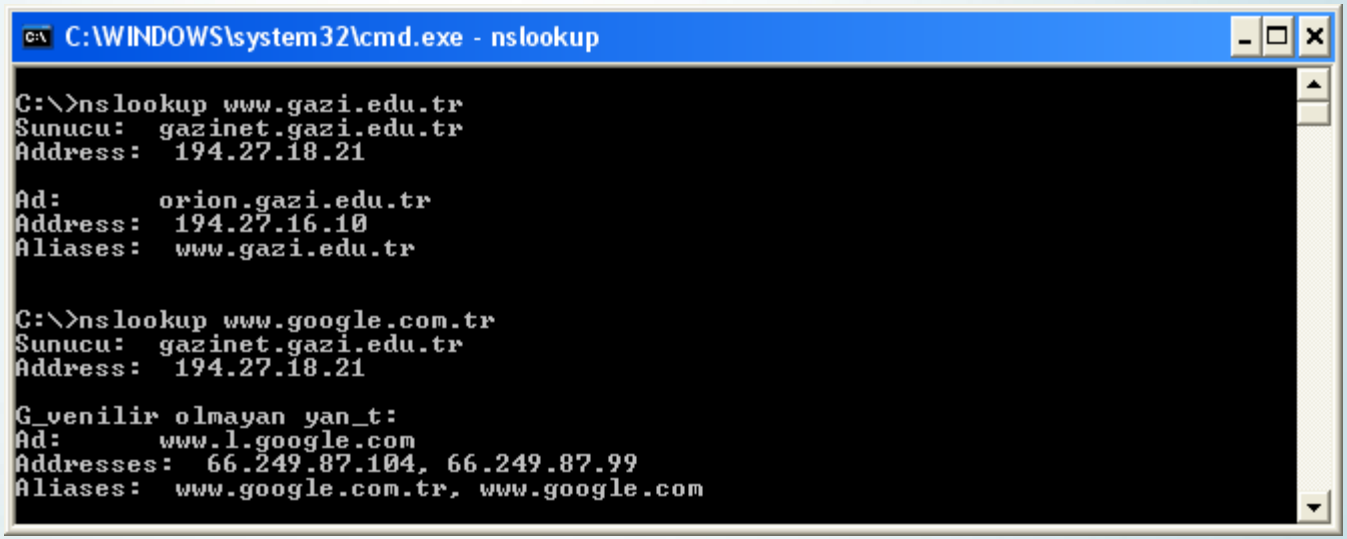
Netstat Komutu

- TCP/IP bağlantılarını, gönderilen ve alınan paketlerin detaylarını görmek için kullanılır.

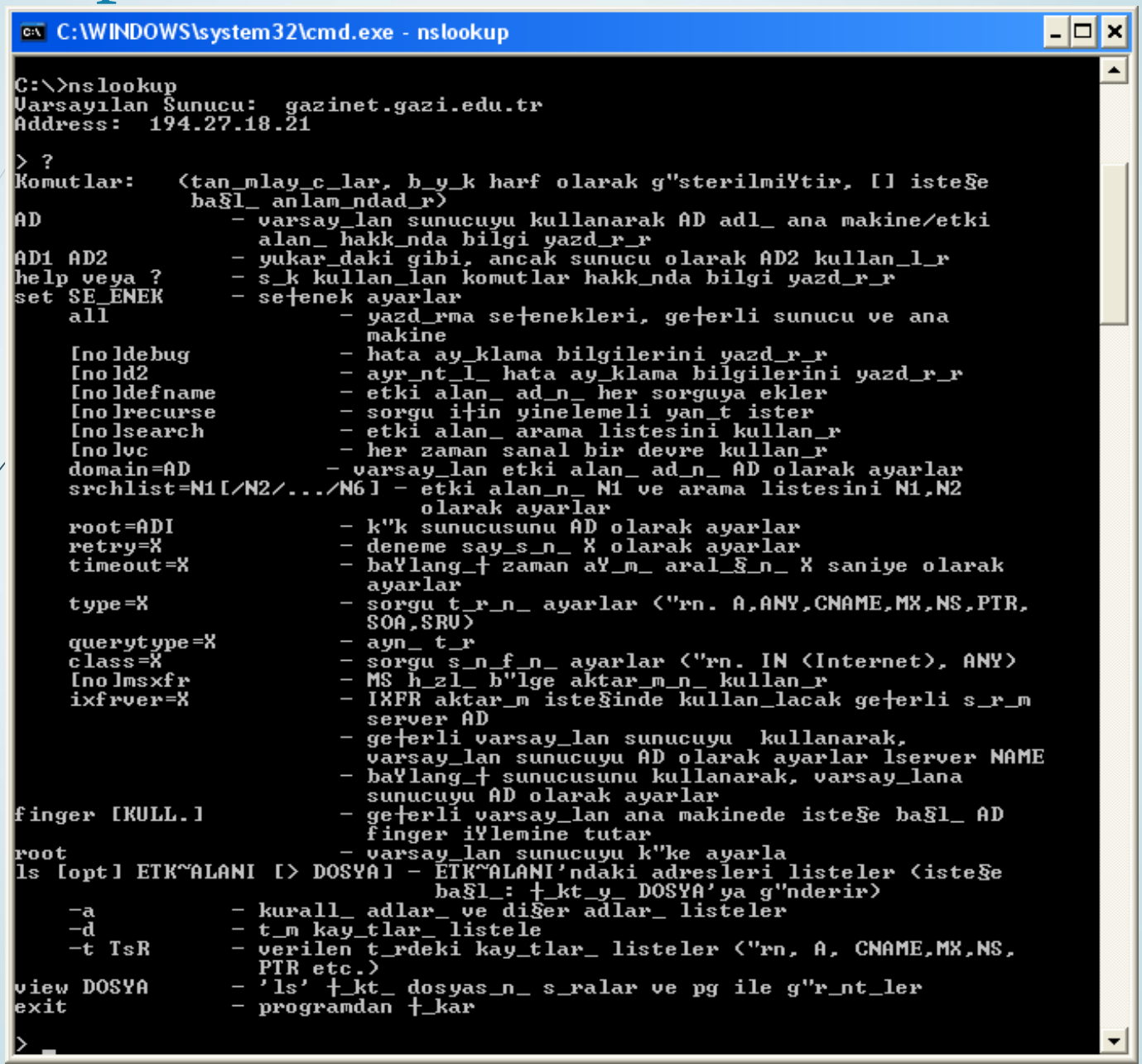


Nslookup Komutu

- Bir adresin TCP/IP numarasını bulunmasını sağlar.



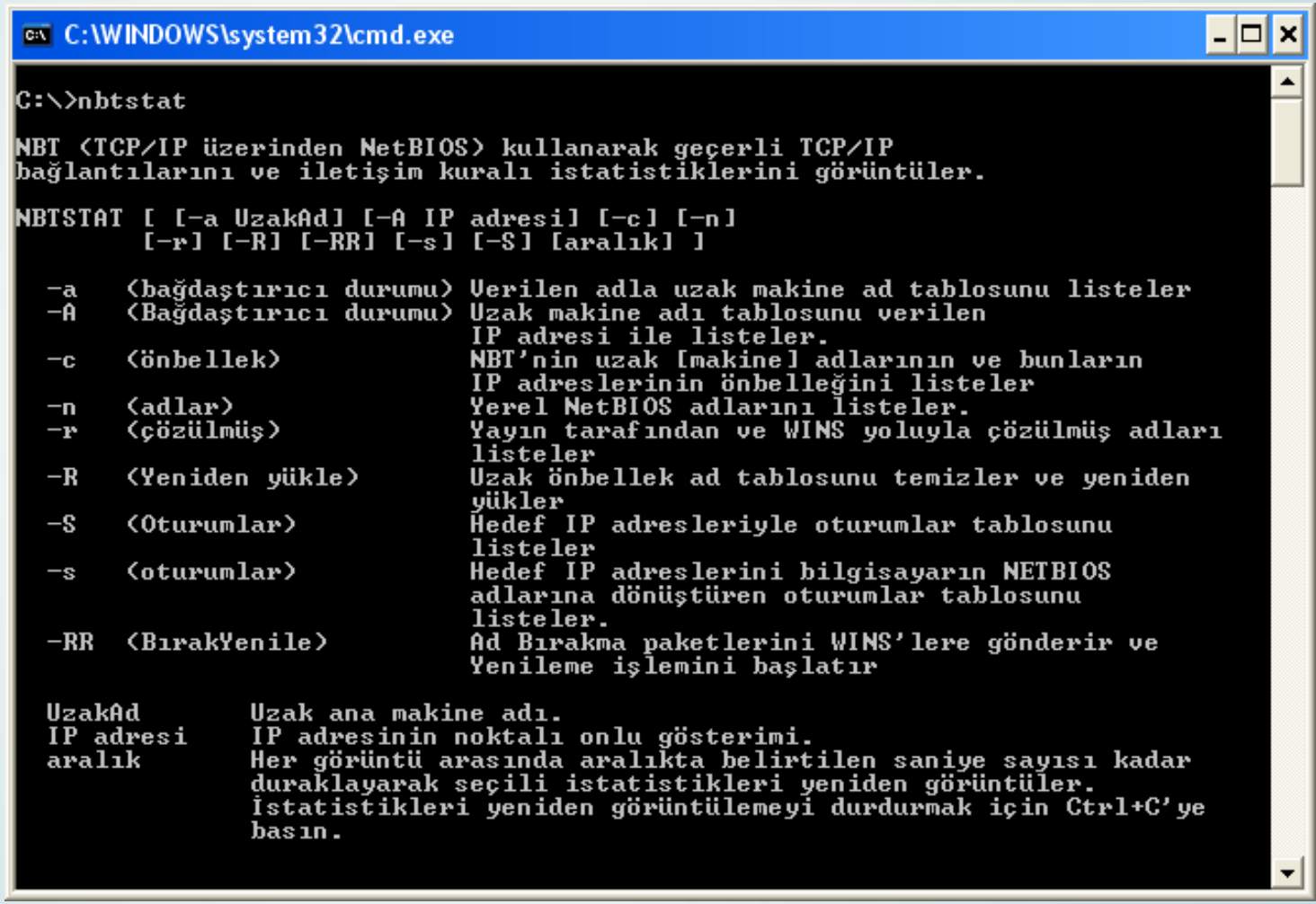
Nslookup Komutu



Nbstat Komutu

- TCP/IP üzerinden NETBIOS bağlantılarının detaylarını görmeyi sağlar.
- NETBIOS (Network Basic Input/Output System) **:** Farklı bilgisayarlardaki uygulamaların bir yerel alan ağı ile iletişim kurabilmelerini sağlayan program.

Nbstat Komutu



Ters Adres Çözümleme Protokolü (RARP)

- RARP (**R**everse **ARP**) ARP'ın yaptığının tersini yapar, yani hangi MAC adresinin hangi IP adresine tekabül ettiğini bulur.
- RARP'de ise host kendi IP adresini bilmez. Yayın yaparak ağdaki cihaza donanım adresini yollar ve ağın RARP sunucusu bu host'a IP adresini bildirir.

IPv4 Adresleme

Sınıf	IP adres	Ağ No	Host No	Ağ bit	Host bit	Ağdaki PC Sayısı
A	1-126	0+7 bit	b.c.d	8	24	$2^{24} = 16,777,214$
B	128-191	10+14 bit	c.d	16	16	$\mathbf{2^{16} = 65534}$
C	192-223	110+21 bit	d	24	8	$\mathbf{2^{8} = 254}$
D	224-239	1110				
E	240-247	1111				

a.b.c.d

Ayrılmış IP Adresler

- **Bazı IP adresleri bazı kullanımlar için ayrılmıştır. Yerel ağlar için ayrılmış adresler:**
  - **127.0.0.0 loopback**
  - **10.0.0.0 - 10.255.255.255**
  - **172.16.0.0 - 172.31.255.255**
  - **192.168.0.0 - 192.168.255.255**
  - **169.254.0.0 - 169.254.255.255**
- 0 → bir ağı göstermektedir
- 255 → broadcast adres; bir ağ içerisindeki tüm PC'ler

Ağ ve Broadcast Numaraları

- C sınıfı 129.23.123.2 adres için;
  - Ağ numarası: 129.23.123.0
  - Bu ağdaki tüm PC'lere mesaj göndermek isteyen bir cihaz şu adrese mesajı atacaktır;
    - 129.23.123.255
- B sınıfı 124.50.120.2 adres için;
  - Ağ numarası: 124.50.0.0
  - Bu ağdaki tüm PC'lere mesaj göndermek isteyen bir cihaz şu adrese mesajı atacaktır;
    - 124.50.255.255

Alt Ağ Maskesi (Subnet Mask)

- **Ağdaki iki bilgisayarın veya cihazın aynı ağda olduklarını anlamalarını sağlar.**

Sınıf	IP adres	Ağ No	Host No	Ağ bit sayısı	Host bit sayısı	Ağ Maskesi
A	1-126	a	b.c.d	8	24	**255.0.0.0**
B	128-191	a.b	c.d	16	16	**255.255.0.0**
C	192-223	a.b.c	d	24	8	**255.255.255.0**

255.0.0.0 ➔ (11111111.00000000.00000000.00000000

255.255.0.0 ➔ (11111111. 11111111.00000000.00000000

255.255.255.0 ➔ (11111111. 11111111. 11111111.00000000

Alt Ağ Maskesi (Subnet Mask)

Bilgisayarlar ağ tanımlayıcılarını bulmak için IP adreslerini, subnet maskeleri ile mantıksal bir "AND" işleminden geçirirler.

Örnek: İlk bilgisayarın adresi 194.134.60.2, ikinci bilgisayarın IP'si ise 194.134.60.110 olsun. Bu iki bilgisayar aynı ağda mıdır?

Çözüm:

194.134.60.2 AND 255.255.255.0 = 194.134.60.0

194.134.60.110 AND 255.255.255.0= 194.134.60.0

Ağ adresleri aynıdır. Bu iki bilgisayar aynı ağdadır.

Alt Ağ Maskesi (Subnet Mask)

1.bilgisayar 195.60.24.35		2.bilgisayar 195.60.24.36
3.bilgisayar 195.60.42.100		4.bilgisayar 195.60.42.101

Örnek: Yukarıdaki bilgisayarlar aynı ağda mıdır?

Çözüm:

Alt Ağ Maskesi (Subnet Mask)

Network Address		Subnet Mask	Broadcast Address
172.0.0.0		255.0.0.0	172.255.255.255
172.0.0.1	ve	172.255.255.254	
172.16.0.0		255.255.0.0	172.16.255.255
172.16.0.1	ve	172.16.255.254	
192.168.1.0		255.255.255.0	192.168.1.255
192.168.1.1	ve	192.168.1.254	
192.168.0.0		255.255.0.0	192.168.255.255
192.168.0.1	ve	192.168.255.254	
192.168.0.0		255.255.255.0	192.168.0.255
192.168.0.1	ve	192.168.0.254	

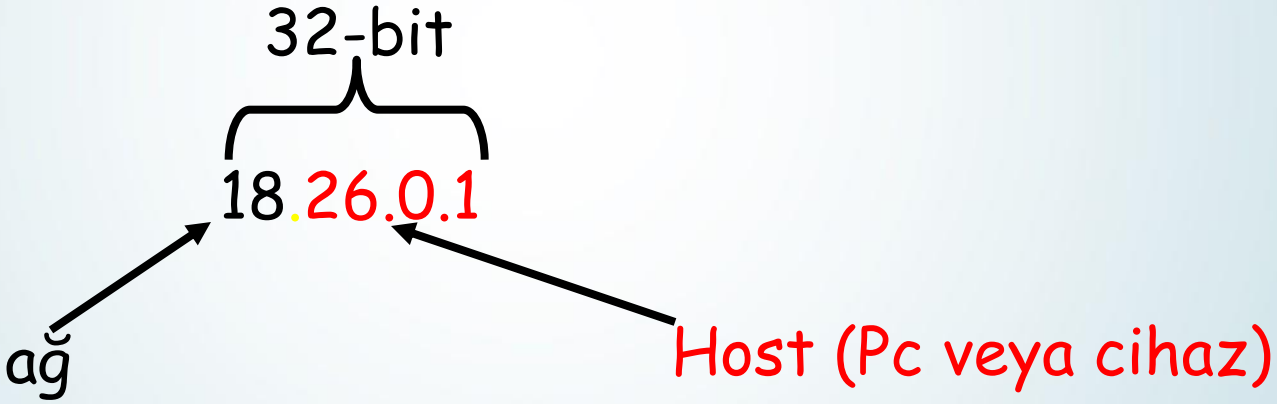
A Sınıfı (1-126)

IP adres: 18.26.0.1

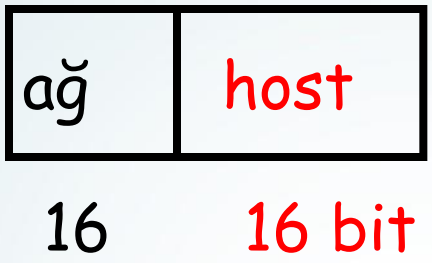
Ağ adresi: 18.0.0.0

Alt Ağ maskesi: 255.0.0.0

Broadcast adres: 18.255.255.255



B Sınıfı (128-191)

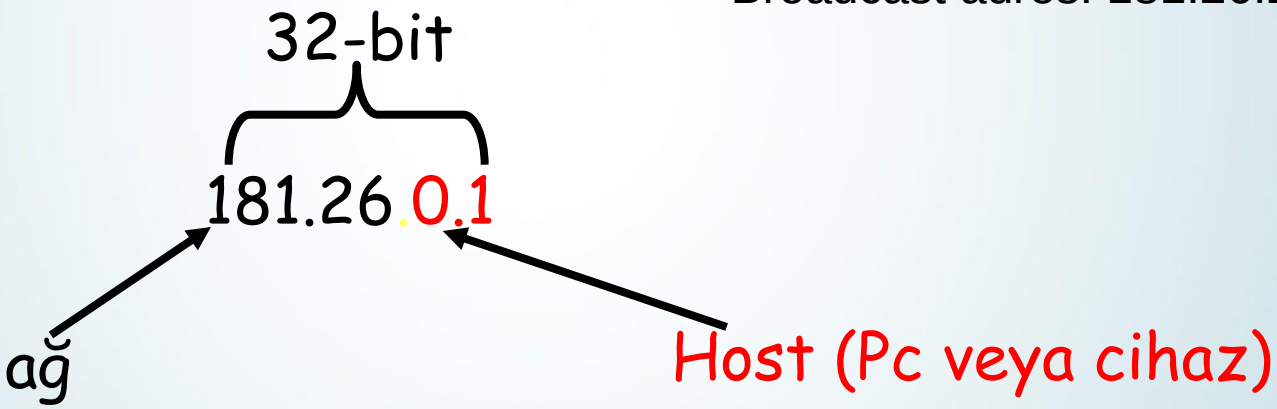


IP adres: 181.26.0.1

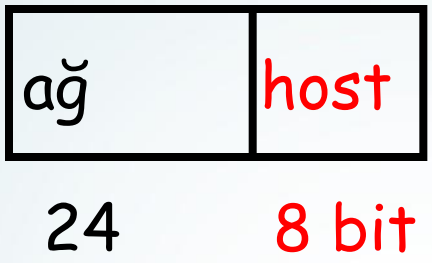
Ağ adresi: 181.26.0.0

Alt Ağ maskesi: 255.255.0.0

Broadcast adres: 181.26.255.255



C Sınıfı (192-223)

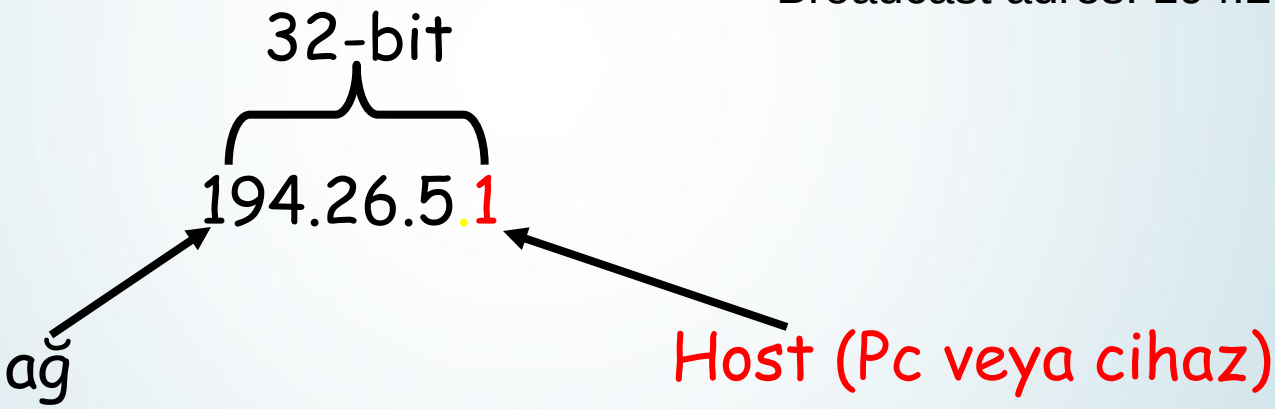


IP adres: 194.26.5.1

Ağ adresi: 194.26.5.0

Alt Ağ maskesi: 255.255.255.0

Broadcast adres: 194.26.5.255



Alıştırma

a) 131.107.20.4

b) 208.234.23.4

c) 108.15.45.4

- Yukarıdaki adreslerin
  - IP sınıfını
  - Alt ağ maske numarasını
  - Bağlı olduğu ağ numarasını
  - Broadcast adreslerini yazınız.

Alt ağlarda TCP/IP

- Bir kurum içerisinde alt bölümler için alt ağlar (subnet) oluşturulabilir.
- Örneğin Gazi Üniversitesi Ağında, GEF bir alt ağ, GEF BÖTE onun da altında bir alt ağdır.
- Bu durumda sanal IP adresleri ile bu alt ağlara IP numarası verilir.

Alt ağlara ayırma

- Elimizdeki bir ağı alt ağlara bölmek için host adresi için ayrılmış olan bitlerden yeterli kısmını ağ adresine katmak gerekir.

Örnek: Elimde ise 195.143.90.0 olan tek bir ağ tanımlayıcım var. 5 alt ağ oluşturmak istiyorum. 5 den büyük ya da eşit bir değer elde etmeliyim.

$2^n-2 >= 5$

$2^3-2=6$

$n=3$

3 tane bitin host adresinden alınıp ağa katılması gerekir.

Alt ağlara ayırma

3 tane bitin host adresinden alınıp ağa katılması gerekir.

8 bitin 3 ünü kullandık, geriye 5 bit kaldı, bu durumda;

$2^5 - 2 = 30$ olur. Bu da her bir ağda 30 adet bilgisayar tanımlayabileceğimizi gösterir.

Üç bitin 8 kombinezonu var.

0 0 0
0 0 1
0 1 0
0 1 1
1 0 0
1 0 1
1 1 0
1 1 1

Bunlardan ikisi, (hepsi 0 ve hepsi 1 olanlar) işimizde kullanılamaz. Geriye kalanları kullanarak ağları ve ağlarda yer alacak bilgisayarları tek tek ayarlayalım.

Alt ağlara ayırma

Üç bitin 8 kombinezonu var.

Ağ	İlk host	Son host	Broadcast
195.143.90.001 00000 (195.143.90.32)	195.143.90.001 00001 (195.143.90.33)	195.143.90.001 11110 (195.143.90.62)	195.143.90.001 11111 (195.143.90.63)
195.143.90.010 00000 (195.143.90.64)	195.143.90.010 00001 (195.143.90.65)	195.143.90.010 11110 (195.143.90.94)	195.143.90.010 11111 (195.143.90.95)
195.143.90.011 00000 (195.143.90.96)	195.143.90.011 00001 (195.143.90.97)	195.143.90.011 11110 (195.143.90.126)	195.143.90.011 11111 (195.143.90.127)
195.143.90.100 00000 (195.143.90.128)	195.143.90.100 00001 (195.143.90.129)	195.143.90.100 11110 (195.143.90.158)	195.143.90.100 11111 (195.143.90.159)
195.143.90.101 00000 (195.143.90.160)	195.143.90.101 00001 (195.143.90.161)	195.143.90.101 11110 (195.143.90.190)	195.143.90.101 11111 (195.143.90.191)
195.143.90.110 00000 (195.143.90.192)	195.143.90.110 00001 (195.143.90.193)	195.143.90.110 11110 (195.143.90.222)	195.143.90.110 11111 (195.143.90.223)

Alt ağlara ayırma sorular

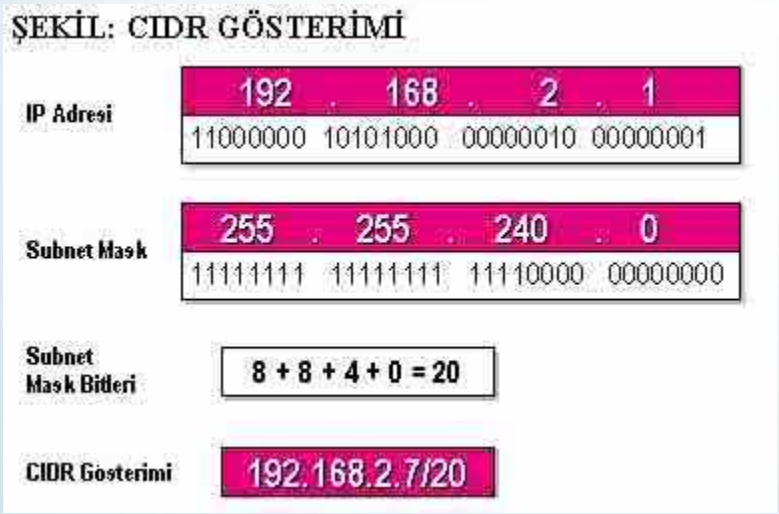
- B sınıfı 164.55.0.0 ağını 254 alt ağa bölmek için gerekli subnet mask, alt ağ, ilk-son host ve broadcast adreslerini bulunuz.
- C sınıfı 194.240.120.0 ağını 12 alt ağa bölmek için gerekli subnet mask, alt ağ, ilk-son host ve broadcast adreslerini bulunuz.
- C sınıfı bir ağda maksimum sayıda host tanımlamak için subnet mask kaç olmalıdır? Kaç tane alt ağ, her bir alt ağda kaç tane host tanımlanabilir?

C sınıfı subnet masking

Subnet sayısı	Bit sayısı	Subnet Mask	host/subnet
0	1	Yok	Yok
1-2	2	255. 255. 255.192	62
3-6	3	255. 255. 255.224	30
7-14	4	255. 255. 255.240	14
15-30	5	255. 255. 255.248	6
31-62	6	255. 255. 255.252	2
Yok	7	Yok	Yok
Yok	8	Yok	Yok

CIDR (CLASSLESS INTER-DOMAİN ROUTİNG) (“/” ile) Gösterim

CIDR gösterimi subnet maskı oluşturan 1'ler sayısıdır. Örneğin 192.168.2.1/20 IP adresinin subnet mask bilgisinde 20 tane 1 vardır. Geriye kalan 12 bit ise 0 değerine sahiptir.



CIDR örnekler

192.168.10.5/10 Ip adresine sahip bilgisayarın Network ve Alt ağ maskesi adreslerini hesaplayınız.

Çözüm:

192.168.10.5		11000000 10101000 00001010 00000101
		AND
/10	subnet mask	11111111 11000000 00000000 00000000
	ağ adresi	11000000 10000000 00000000 00000000
		192.128.0.0

CIDR örnekler

10.2.2.5/14 Ip adresine sahip bilgisayarın Network ve Alt ağ maskesi adreslerini hesaplayınız.

Çözüm:

10.2.2.5		00001010 00000010 00000010 00000101
		AND
/14	subnet mask	11111111 11111100 00000000 00000000
	ağ adresi	00001010 00000000 00000000 00000000
		10.0.0.0

CIDR sorular

- 10.0.0.3 /24 Ip adresine sahip bilgisayarın Network ve Alt ağ maskesi adreslerini hesaplayınız.
- 10.0.0.4 /20 Ip adresine sahip bilgisayarın Network ve Alt ağ maskesi adreslerini hesaplayınız.
- 10.0.0.4 /17 ile gösterilen bilgisayar için ALT ağ maskesi nedir. Network (Ağ) adresi nedir.
- 10.0.0.4/20 ile gösterilen bir bilgisayar ile 10.0.1.4 /20 ile gösterilen bir bilgisayar birbiri ile konuşabilir mi?
- 10.0.0.4/10 ile gösterilen bir bilgisayarın alt ağ maskesi ve ağ adresi nedir. Bu ağ da kullanılabilecek ilk IP adresi ve Son Ip adresi nedir. Toplam kaç bilgisayara IP adresi verilebilir?

IPv6

- IPv4: 32 bit
- IPv4: $2^{32} = 4{,}3\ 10^{9}$
  IPv4:10'luk sayı sistemi
- IPv6:128 bit
- IPv6: $2^{128} = 3{,}4\ 10^{38}$
- IPv6:16'lık sayı sistemi

- Eski adı: IPng: IP next generation
- Bazı ülkeler (Amerika, Japonya…) kullanıyor.
- Uygulama ve fiziksel katman değişmedi.
- Daha hızlı, güvenli ve daha az başlık (header)

IPv6 adresler

8 adet 4'lü hexadecimal sayıdan oluşur.

2001:0DB8:400:965a:0000:0000:0000:0001
2001:0DB8:400:965a::1 (aynı adres)

(**::**) adreste 0 olan yerlerde kullanılarak adres kısaltılır
Örnek:

2001:0DB8:400:965a::

2001:0DB8:400:965a:0000:0000:0000:0000

2001:0DB8:400:965a:0042::1
2001:0DB8:400:965a:0042:0000:0000:0001

IPv6 adresler

IPv6 adres:

FE80:0000:0000:0000:02A0:D2FF:FEA5:E9F5 / 64

/ x → ağ numarasını gösteren bit sayısı

Örneğin; /32 ise 128 bitin ilk 32 biti ağ numarasını diğerleri host numarasını gösterir

/64 ise 128 bitin ilk 64 biti ağ numarasını diğerleri host numarasını gösterir

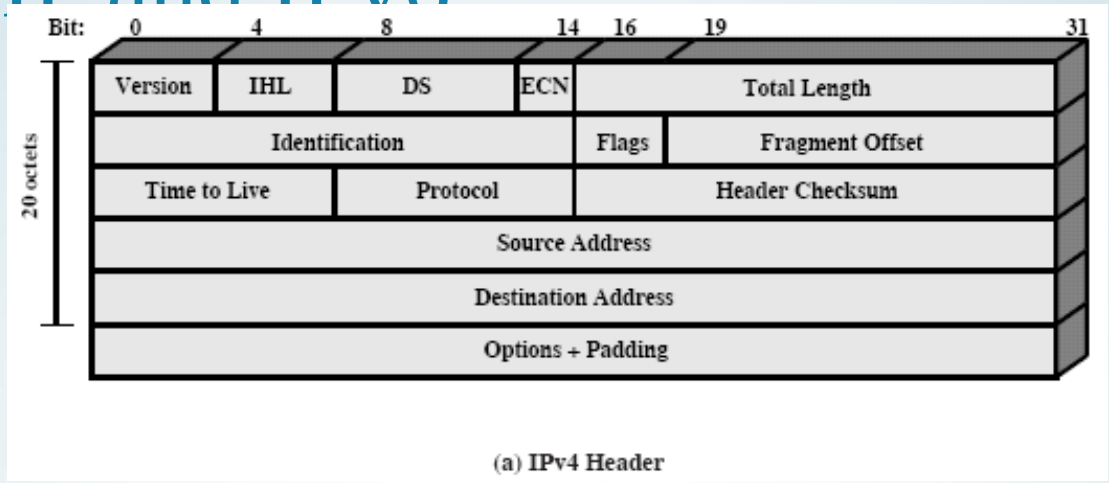
Ağ no : FE80:0000:0000:0000

Host no: 02A0:D2FF:FEA5:E9F5

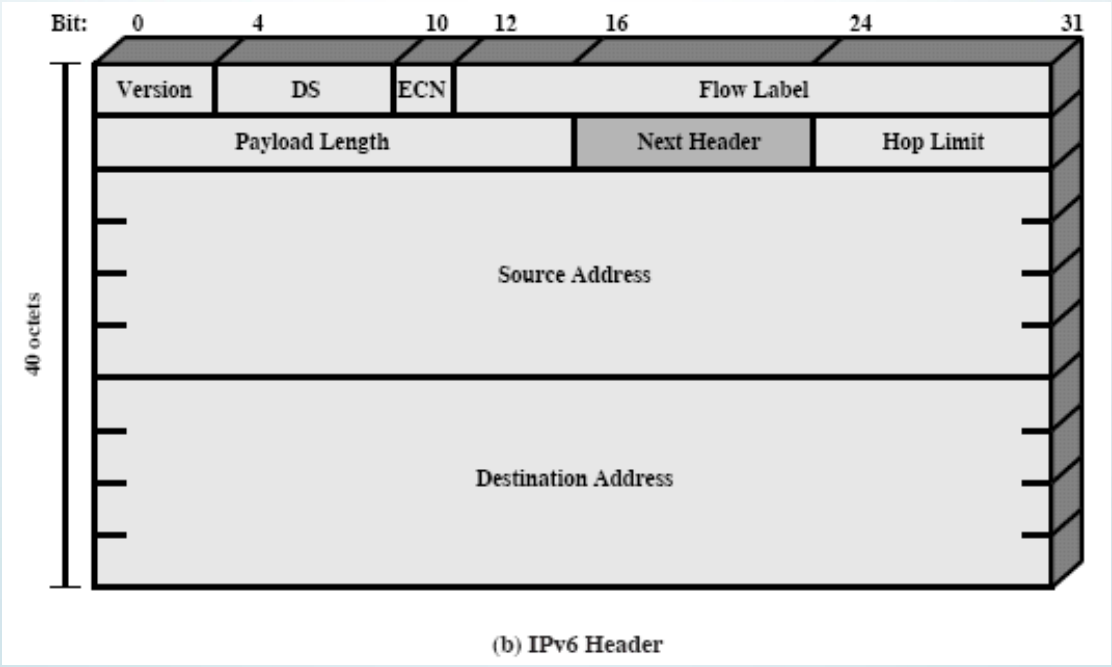
IPv6 adresler

- Ayrılmış adresler
  - 0:0:0:0:0:0:0:1 → ::1 loopback
  - 0:0:0:0:0:0:0:0 → :: belirsiz
- IPv6 ve IPv4 adreslerin kullanımı
  - 128 – 32 = 96
  - x:x:x:x:x:x:d.d.d.d
    - x: IPv6 ve d: IPv4
  - Örnek:
    - 0:0:0:0:0:0:1.2.3.4/96 → ::1.2.3.4/96

IP and IPv6



(a) IPv4 Header



(b) IPv6 Header

TCP/IP Sorun Çözme

- Ağ bağlantılarını kontrol edin
- Ping 127.0.0.1 (loopback) ile ethernet kartınızı kontrol edin
- Kendi bilgisayarınızın IP adresine ping atabilirsiniz.
- Varsayılan (Default) Router veya gateway (ağ geçidi) varsa ona ping atarak pc-alt ağ iletişimini kontrol edebilirsiniz.
- Uzaktaki bir hosta ping atabilirsiniz.

AĞ TEMELLERİ

Ağ Güvenliği

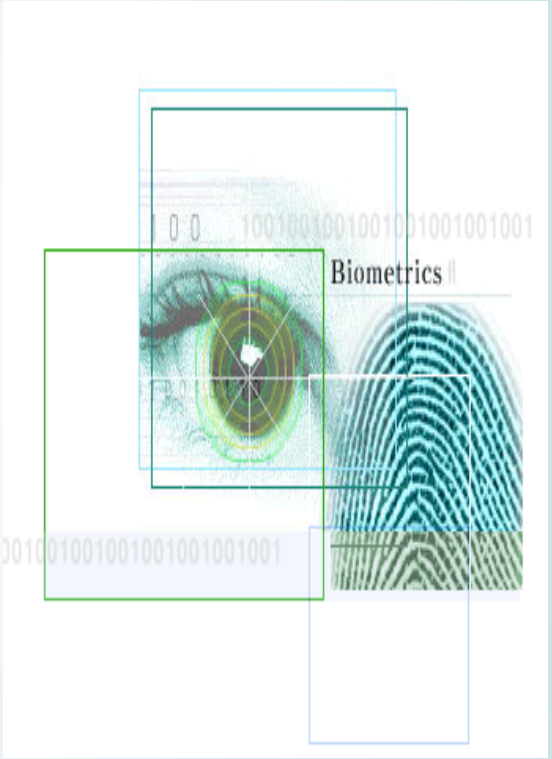
BİYOMETRİ

BİYOMETRİ (BIOMETRICS) NEDİR?

- Biyometri, biyolojik özelliklerin istatistiki analiziyle uğraşan bilim dalıdır. Elektronik ortama; güvenlik adına parmak izi, ses, retina gibi karakteristikleri kullanarak kişi tanımlamak olarak geçmiş bir kavramdır .

BİYOMETRİ (BIOMETRICS) NEDİR?

- Biyometri, bireyleri birbirinden ayıran ölçeklenebilir psikolojik yada davranışsal karakteristiklerin kimlik tespitinde kullanılan bilgisayar kontrollü sistemler olarak tanımlanabilir .



BİYOMETRİK SİSTEMLER NASIL ÇALIŞIR?

- Biyometrik sistemler kişinin sadece kendisinin sahip olduğu ve kendisini diğer kişilerden ayıran fiziksel veya davranışsal özelliklerinin tanınması prensibi ile çalışmaktadır .

- Öncelikle kayıtlar toplanır ve bu kayıtlar bir kod olarak ilgili sistemde saklanır. Talep edildiği vakit toplanmış olan bu kayıtlar ile ilgili kişi anında karşılaştırılır ve sonuca varılır .

BİYOMETRİNİN UYGULAMA ALANLARI

- İnternet bankacılığında kullanıcı tanımlama
- ATM'lerde kullanıcı tanımlama
- Çağrı merkezlerinde kimlik tespiti
- Kurumsal ağların güvenliği
- Kredi kartı uygulamaları
- Masaüstü ve dizüstü bilgisayarların güvenliği
- Elektronik imza uygulamaları
- E - ticaret işlemleri
- Kiosklarda kullanıcı tanımlama

BİYOMETRİNİN UYGULAMA ALANLARI

- Personel takibi
- SSK, vergi süreçleri gibi kamu hizmetleri
- Havaalanlarındaki giriş ve çıkış işlemleri
- Hastanelerde hasta takibi

BİYOMETRİK TEKNOLOJİLER

- Parmak İzi Tanıma Teknolojisi:

Uygulaması en basit ve ucuz biyometri teknolojisi olduğu için hızla hayatımıza giren parmak izi tanımlama sistemleri,
aslında yüzlerce yıldır insanların imzaları olarak kullandıkları
parmak izlerini dijital teknoloji ile buluşturuyor .

BİYOMETRİK TEKNOLOJİLER

- İris ve Retina Tanıma Teknolojisi:

Göz bebeğinin ön kısmında yer alan iris tabakasını veya göz merceğinin ardında görme sinirlerinin toplandığı alan olan retinayı analiz ederek kullanıcının kimliğini tespit eden sistemlerdir .

Teknolojinin bir sonraki aşamasında, banka otomatları gibi sistemlerde kişilerin hesaplarına ulaşabilmeleri, mağazalarda ödemelerini yapabilmeleri gibi senaryolar üzerine çalışılıyor .

BİYOMETRİK TEKNOLOJİLER

- Ses Tanıma Teknolojisi:

Ses tanıma teknolojisi oldukça yaygın kullanılan maliyeti
düşük ve günümüz teknolojisinde fazladan hiçbir donanım
gerektirmeyen güvenlik sistemlerinden biridir .

Ses tanıma teknolojisi genel olarak iki ana gruba ayrılır:

1. Ses Tanıma Sistemleri
2. Konuşma Tanıma Sistemleri

BİYOMETRİK TEKNOLOJİLER

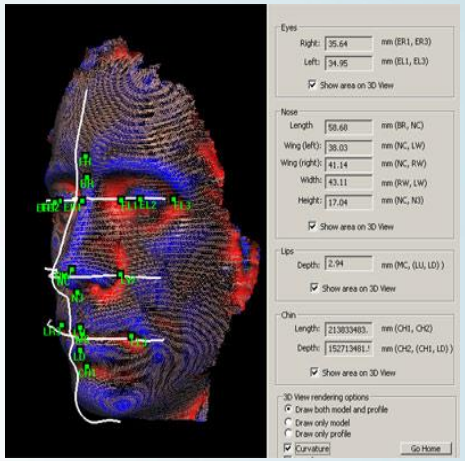
- İmza Tanıma Teknolojisi:

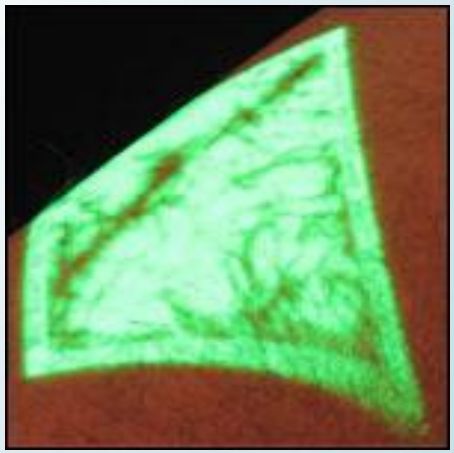
Her insanın gerçek hayatta kullandığı, el yazması metinlerde insanları ayırt edici bir özellik olan imzaları bulunmaktadır.
Eskiden beri insanlar kendilerini veya kendi ailelerini
betimleyen imza, arma, özel işaret vs. kullana gelmişlerdir .

Gerçekten dikkat edilirse imzalarımızı devamlı aynı şekilde, aynı hızda birbirleriyle oldukça benzer biçimde atarız. İmza tanıma sistemlerinin temelinde de bu mantık vardır.

BİYOMETRİK TEKNOLOJİLER

- Yüz Yapısı Tanıma Teknolojisi
- Yazma Ritmi Tanıma Teknolojisi
- Toplardamar İzi Tanıma Teknolojisi
- Avuç İçi İzi Tanıma Teknolojisi
- Kulak Şeklinden Tanıma Teknolojisi





BİYOMETRİK TEKNOLOJİLER STANDART MIDIR?

INCITS tarafından izi, iris-retina tabakası, ses tanımı gibi biyometrik tanımlama sistemlerinde kullanılacak işlemlere uluslararası bir standart getirilmektedir .

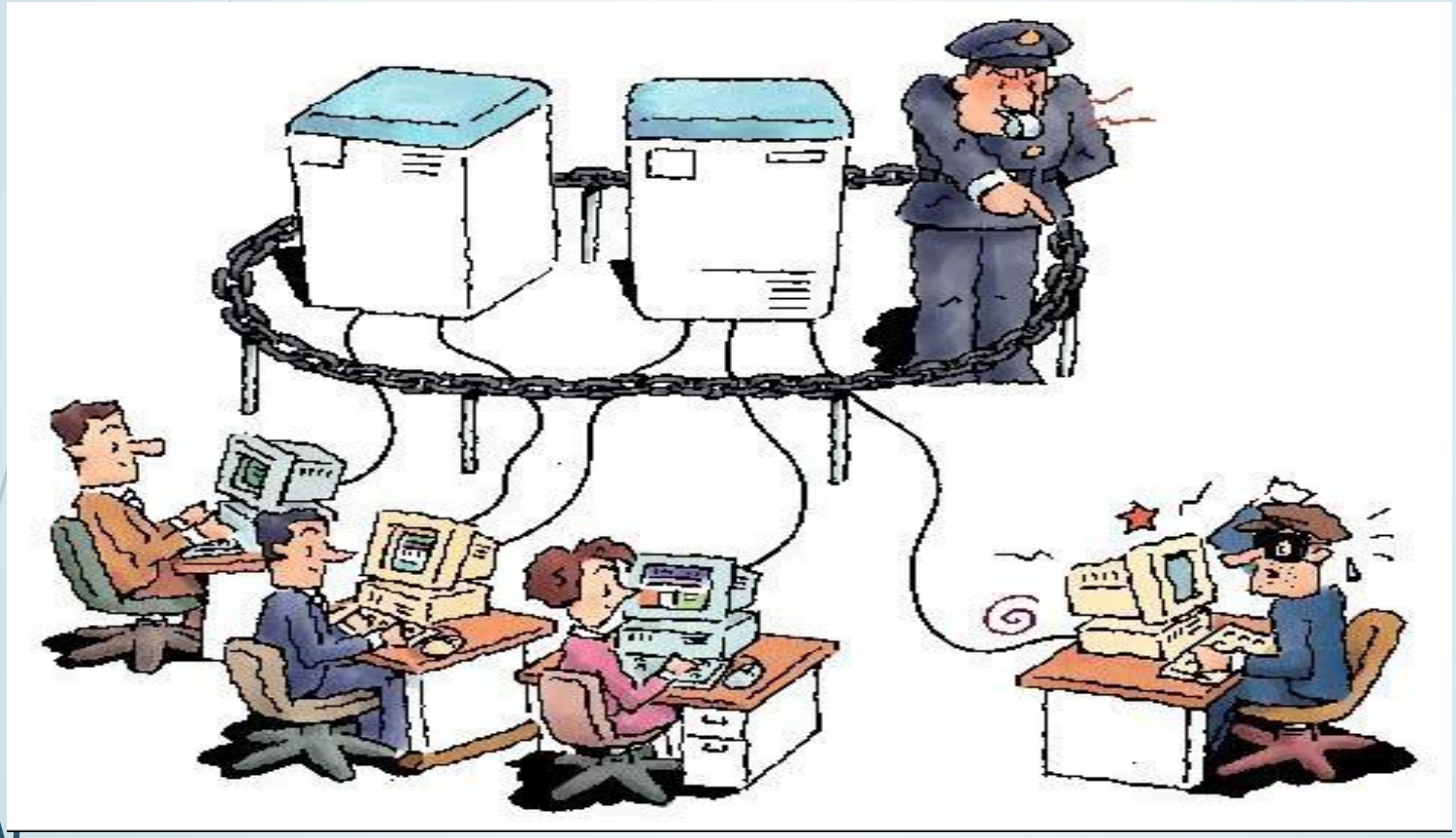
BİREY AYIRT ETME KAYNAKLARI KARŞILAŞTIRMA TABLOSU

Biyometri Kaynağı	Ayırt Edicilik	Dayanıklılık	Bulunabilirlik	Performans	Kabul Edilebilirlik	Sistemi Aldatma
Yüz	D	O	Y	D	Y	D
Parmak İzi	Y	Y	O	Y	O	Y
El Geometrisi	O	O	Y	O	O	O
Damar	O	O	O	O	O	Y
İris	Y		O	Y	D	Y
Retina	Y	O	D	Y	D	Y
İmza	D	D	Y	D	Y	D
Ses	D	D	O	D	Y	D

Y: Yüksek O: Orta D: Düşük

AĞ

- Ağ (network), paylaşım amacıyla iki ya da daha fazla cihazın bir araya getirilmesiyle oluşturulan bir yapıdır.



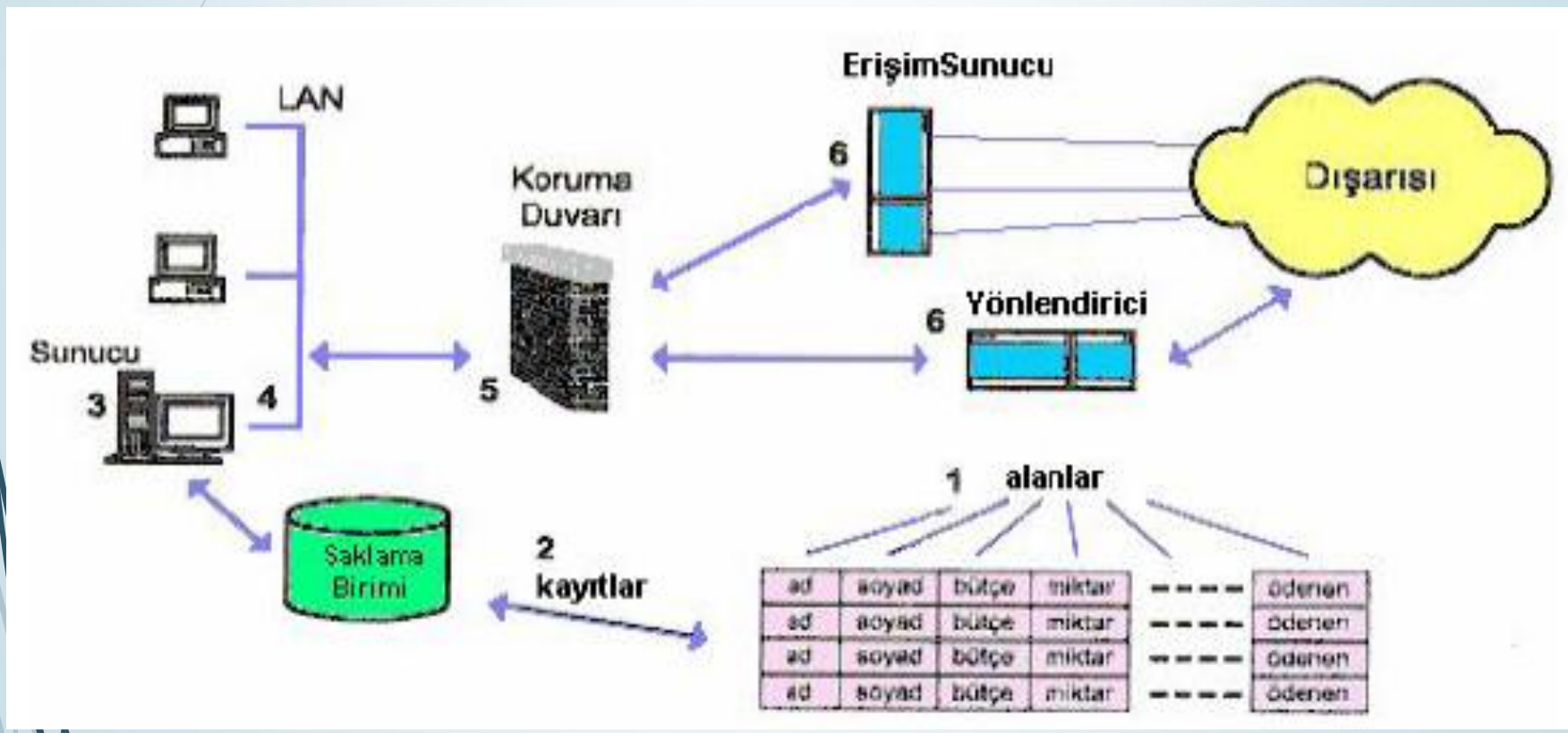
Bir zincir, ancak en zayıf halkası kadar güçlüdür.

GÜVENLİK DÜZEYLERİ

Güvenlik düzeyi, özel bir bilginin saklı olduğu yerde hangi düzeyde korunacağını gösterir. Ağ ortamındaki bilgisayarlarda bilgi çeşitli düzeylerde korunabilir.

	Güvenlik Düzeyleri	Görevi
1.	Kayıt alanı düzeyinde koruma	Bu düzeyler en sıkı korumayı sağlar. İyi bir şifreleme ve şifre anahtarı üretme algoritması kullanılmakatadır.
2.	Veri kaydı düzeyinde koruma	
3.	Uygulama programı düzeyinde sorgulama/koruma	Uygulama programına girişi sorgular.
4.	Bilgisayara bağlanmayı sorgulama	Bilgisayar sistemine girişi denetler.
5.	Ağ kaynaklarını hizmet türleri açısından koruma	Ağa dışarıdan bağlanmayı ve ağ üzerinde sunulan hizmetlere erişimi denetler. Bu güvenlik düzeyleri genel olarak koruma duvarları (firewall) tarafından sağlanır.
6.	Ağa girişi sorgulama/koruma	

GÜVENLİK DÜZEYLERİ



GÜVENLİK POLİTİKALARI

Güvenlik politikası, kurumun ağına ve ağ üzerindeki öz kaynaklara erişim kurallarını taslak olarak ortaya koyan, politikaların nasıl uygulanacağını belirten ve güvenlik ortamına ilişkin temel mimarinin bir kısmının çerçevesini çizen genel, kapsamlı bir dokümandır.

GÜVENLİK POLİTİKALARI

Güvenlik politikasının en önemli özelliği yazılı olmasıdır ve kullanıcıdan yöneticiye kurum genelinde tüm çalışanların, kurumun sahip olduğu teknoloji ve bilgi değerlerini nasıl kullanacaklarını kesin hatlarıyla anlatmasıdır.

GÜVENLİK POLİTİKALARI

Ağ güvenlik politikaları, kurumların yapılarına ve gereksinimlerine göre değiştiğinden bir şablondan söz etmek mümkün değildir. Bunun nedeni, politikaların konuya veya teknolojiye özgü olmasıdır. Ağ güvenliğinin sağlanması için gerekli olan temel politikalar aşağıda sıralanmıştır.

POLİTİKALAR

1) Kabul edilebilir kullanım politikası
2) Erişim politikası
3) Ağ güvenlik duvarı (firewall) politikası
4) İnternet politikası
5) Şifre yönetimi politikası
6) Fiziksel güvenlik politikası
7) Sosyal mühendislik politikası

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Ağ ve bilgisayar olanakların kullanımı konusunda kullanıcıların hakları ve sorumlulukları belirtilir.

- Kaynakların kullanımına kimlerin izinli olduğu,
- Kaynakların uygun kullanımının nasıl olabileceği,
- Kimin erişim hakkını vermek ve kullanımı onaylamak için yetkili olduğu,
- Kimin yönetim önceliklerine sahip olabileceği,
- Kullanıcıların hakları ve sorumluluklarının neler olduğu,
- Sistem yöneticilerin kullanıcılar üzerindeki hakları ve sorumlulukların neler olduğu.

ERİŞİM POLİTİKALARI

Erişim politikaları kullanıcıların ağa bağlanma yetkilerini belirler. Her kullanıcının ağa bağlanma yetkisi farklı olmalıdır. Erişim politikaları kullanıcılar kategorilere ayrıldıktan sonra her kategori için ayrı ayrı belirlenmelidir. Bu kategorilere sistem yöneticileri de girmektedir.

AĞ GÜVENLİK DUVARI POLİTİKASI

Ağın dışından ağın içine erişimin denetimi burada yapılır. Bu nedenle erişim politikaları ile paraleldir.

İNTERNET POLİTİKASI

Kurum bazında her kullanıcının dış kaynaklara yani internet'e erişmesine gerek yoktur. İnternet erişiminin yol açabileceği sorunlar aşağıdaki gibidir.

- Zararlı kodlar
- Etkin kodlar,
- Amaç dışı kullanım
- Zaman kaybı

ŞİFRE YÖNETİMİ POLİTİKASI

Şifreler kullanıcıların ulaşmak istedikleri bilgilere erişim izinlerinin olup olmadığını anlamamızı sağlayan bir denetim aracıdır. Şifrelerin yanlış ve kötü amaçlı kullanımları güvenlik sorunlarına yol açabileceğinden güvenlik politikalarında önemli bir yeri vardır.

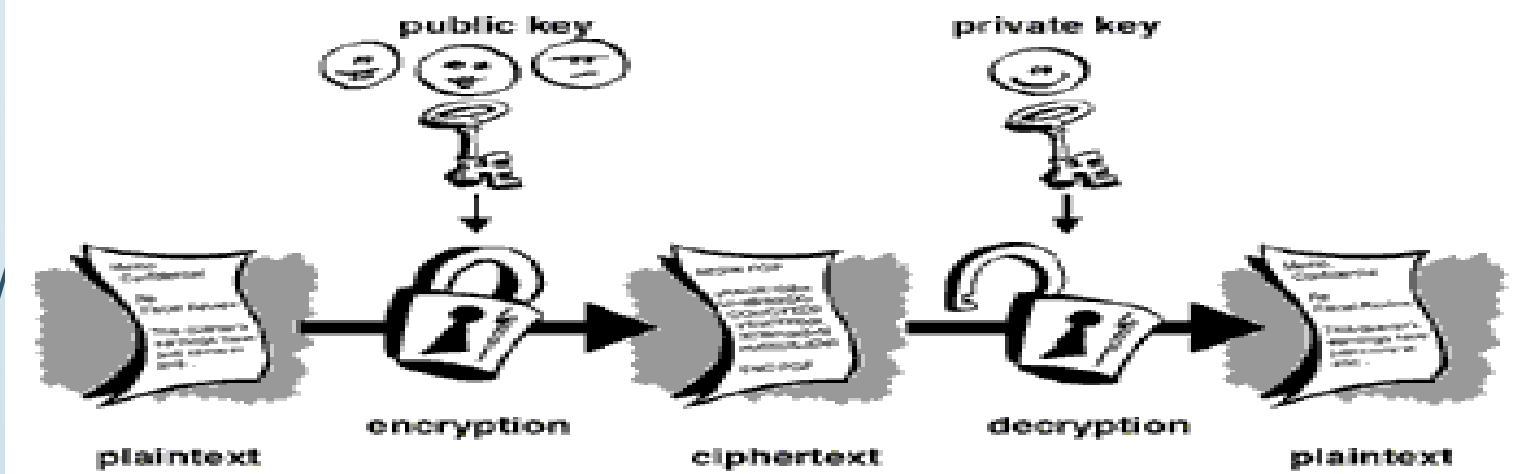


Figure 2-1. Public Key Cryptography diagram

FİZİKSEL GÜVENLİK POLİTİKASI

Bilgisayar veya aktif cihazlara fiziksel olarak erişebilen saldırganın cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal güvenlik önlemlerinin hiç bir kıymeti bulunmamaktadır.

SOSYAL MÜHENDİSLİK POLİTİKASI

Sosyal mühendislik, kişileri inandırma yoluyla istediğini yaptırma ve kullanıcıya ilişkin bilgileri elde etme eylemidir. Sistem sorumlusu olduğunu söyleyerek kullanıcının şifresini öğrenmeye çalışmak veya teknisyen kılığında kurumuna sızmak bilgi toplama gibi değişik yollarla yapılabilir.

GÜVENLİK POLİTİKASININ UYGULANMASI

Güvenlik politikaları uygulanırken 4 kısma dikkat edilmelidir.

- Politika hazırlanırken katılım sağlanmalıdır.
- Politika standartlara uygun olmalıdır.
- Yönetimin onayı alınmalı ve politika duyurulmalıdır.
- Acil durum politikası oluşturulmalıdır.

KABLOSUZ AĞLARDA GÜVENLİK

- Kablosuz Ağlarda Güvenlik Kavramı
- Kablosuz Ağlar Ne Kadar Güvenli
- Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri
  - SSID Değiştirmek
  - SSID Yayınlanmasını Durdurmak
  - Ağı Kapatmak
  - MAC Adresi Filtrelemek
  - Yayın Gücünü Azaltmak
  - Ağı Şifrelemek
    - WEP
    - WPA
    - WPA2

Kablosuz Ağlarda Güvenlik Kavramı

- Verilerimiz, sadece veriyi almasını istediğimiz kişiye gidecek; ağımızı sadece kullanmasına izin verdiğimiz kişi ya da kişiler kullanabilecek.

Kablosuz Ağlar Ne Kadar Güvenli?

- Kablosuz ağlar %100 güvenli değil. Ağda güvenliği sağlamak üzere birçok yöntem kullanılmasına rağmen %100 güvenlikten bahsedemiyoruz.

Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

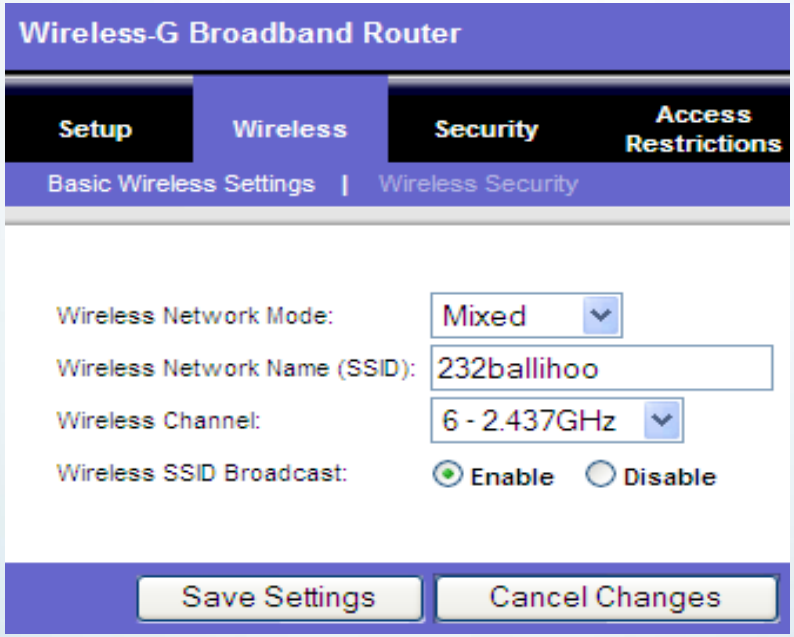
- SSID (Service Set Identifier – Servis Seti Tanımlayıcısı) Değiştirmek
- SSID Yayınlanmasını Engellemek
- Ağı Kapatmak
- MAC Adresi Filtrelemek
- Yayın Gücünü Azaltmak
- Ağı Şifrelemek
  - **WEP** (**W**ired **E**quivalent **P**rivacy - Kabloluya Eşdeğer Gizlilik)
  - **WPA** (**W**iFi **P**rotected **A**ccess - WiFi Korumalı Erişim)
  - **WPA2**

Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

- **SSID Değiştirmek:** AP'nizin SSID sini ana menüden değiştirin.

Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

- **SSID Yayınlanmasını Durdurmak:** AP'nizin SSID yayınlamasını durdurun

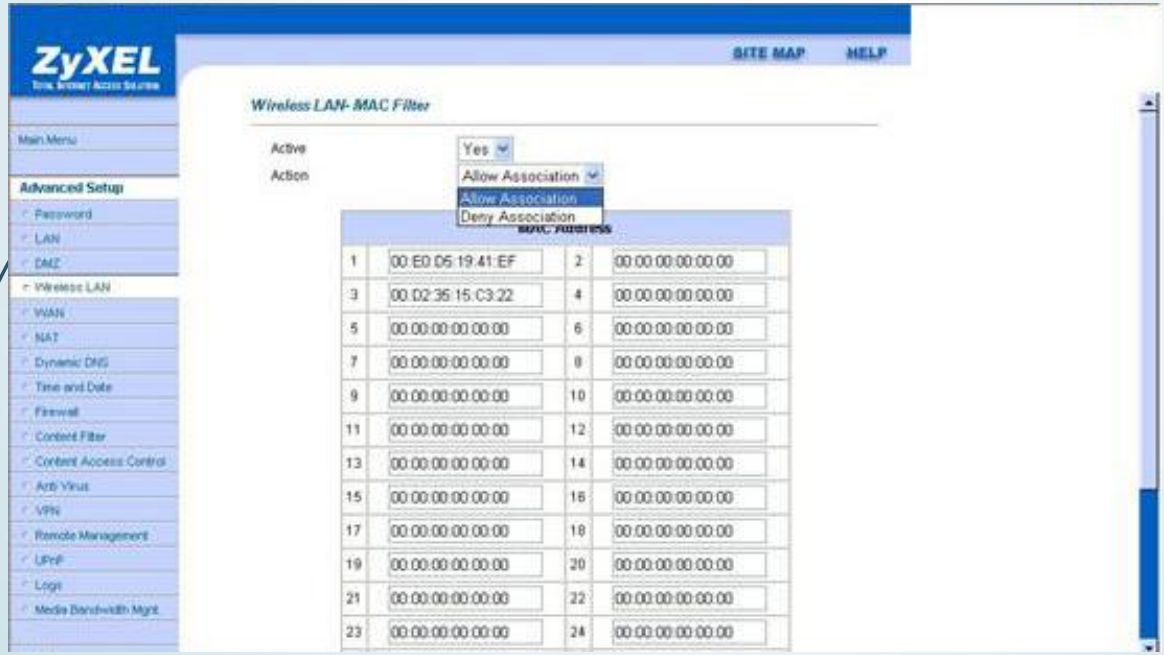


Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

- **Ağı Kapatmak:** Kablosuz modeminizi gece kullanılmadığı saatlerde kapatın.

Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

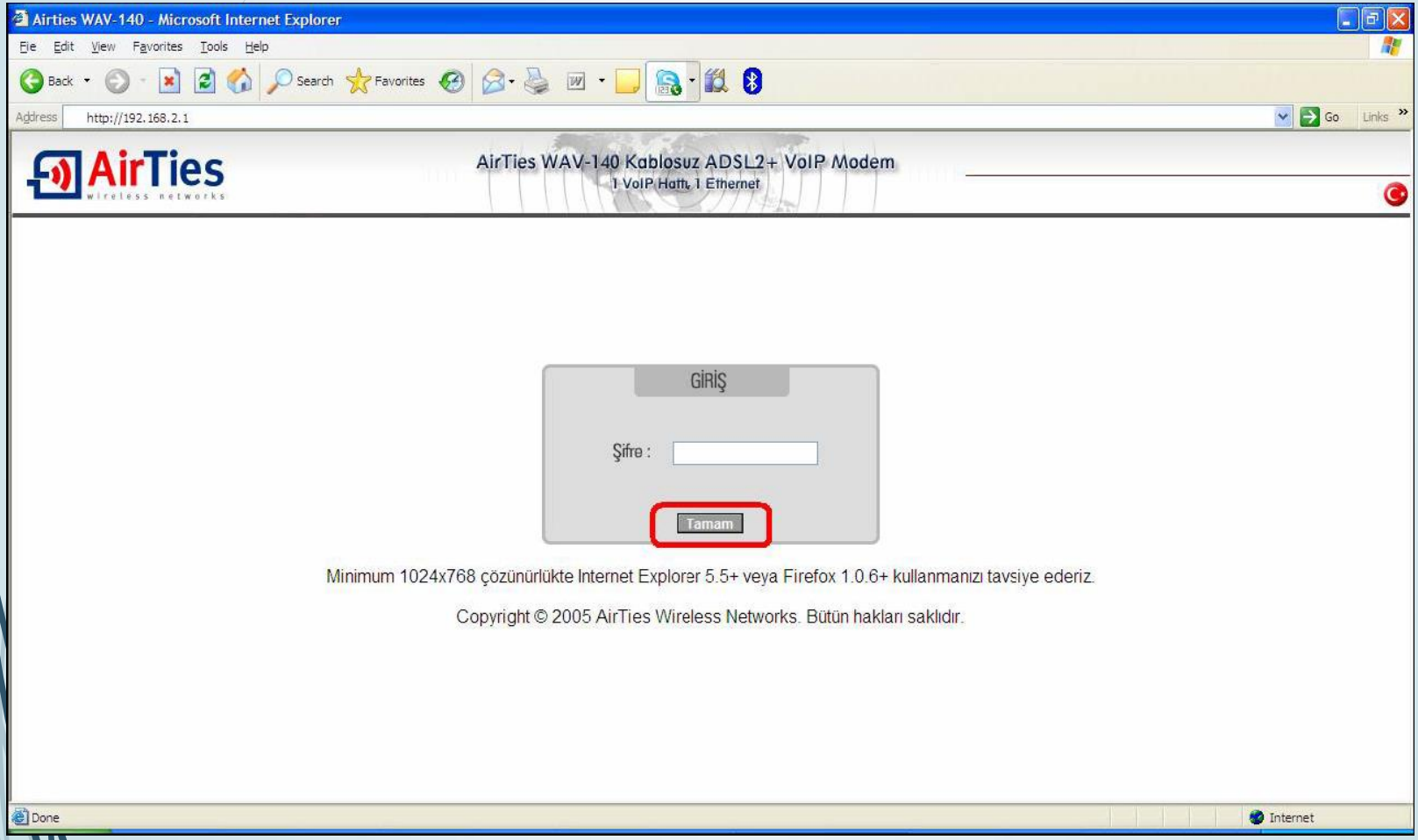
- **MAC Adresi Filtrelemek:** Mac Adresini filtrelemek, sizin mac adresini girmediğiniz cihazların access pointe bağlanmasını engeller.



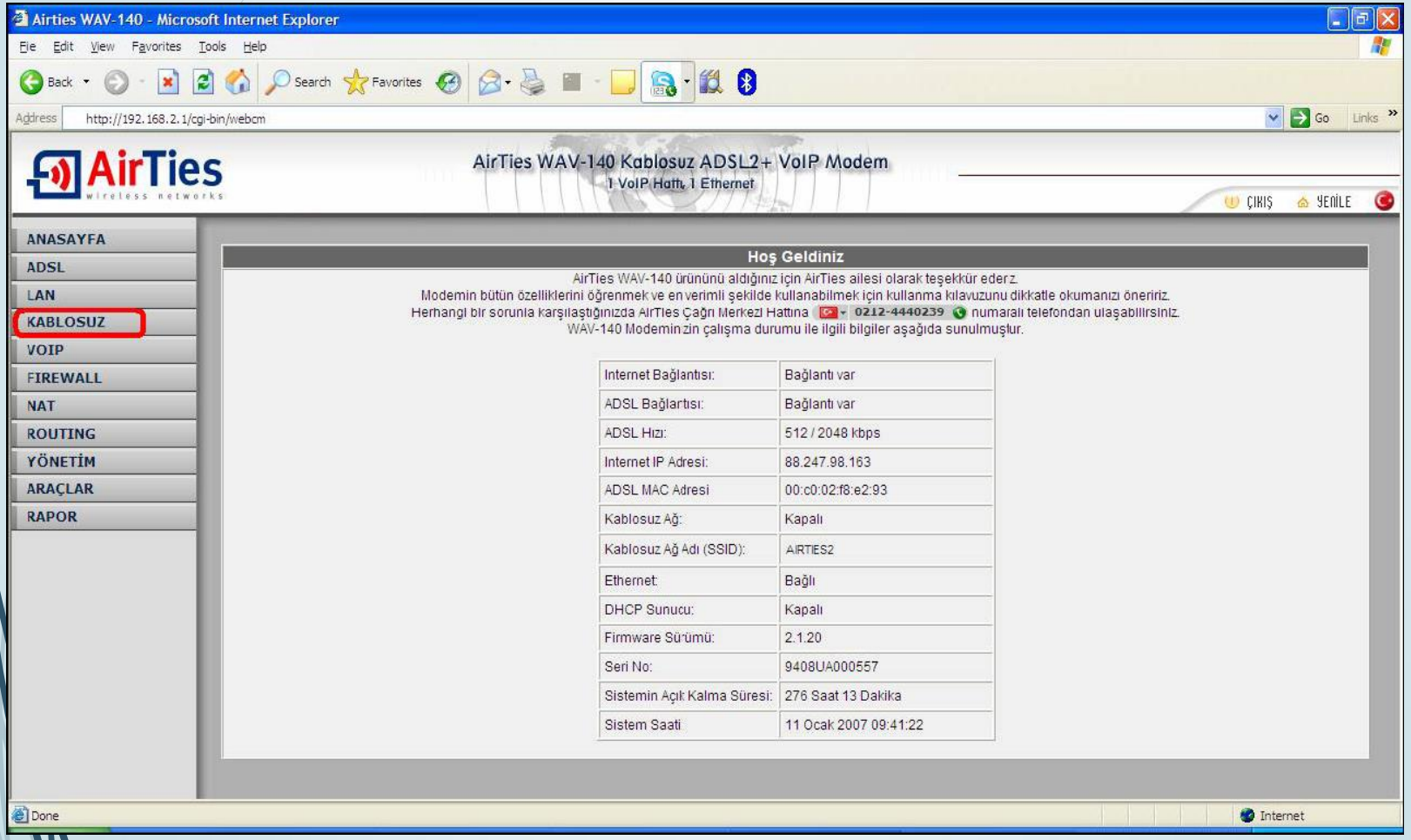
Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

- **Yayın Gücünü Azaltmak:** Bazı access pointlerde bu özellik vardır. Apartman gibi ortamlarda bu özellik işe yarayabilir. Sinyal gücünü düşürüp başkalarının modeminize erişimini engelleyebilirsiniz.

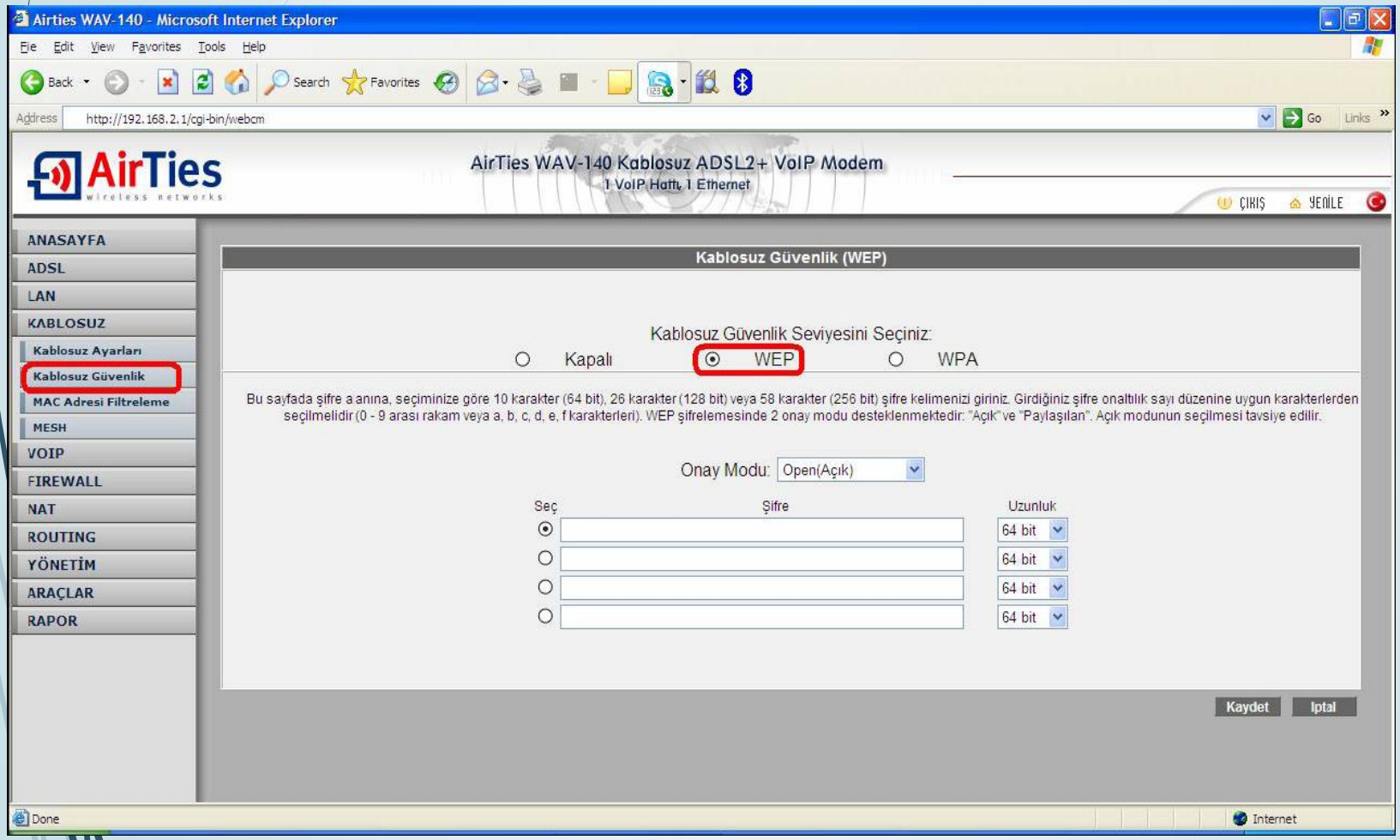
KABLOSUZ AĞLARDA GÜVENLİK



KABLOSUZ AĞLARDA GÜVENLİK

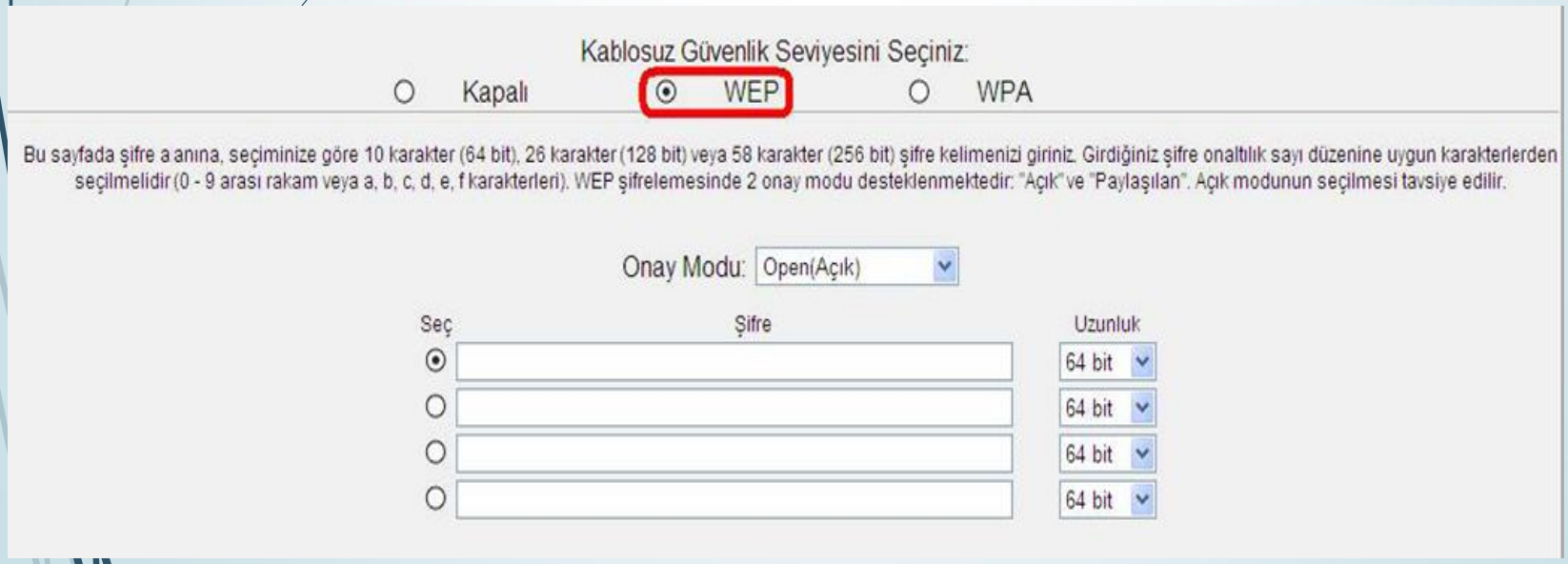


KABLOSUZ AĞLARDA GÜVENLİK



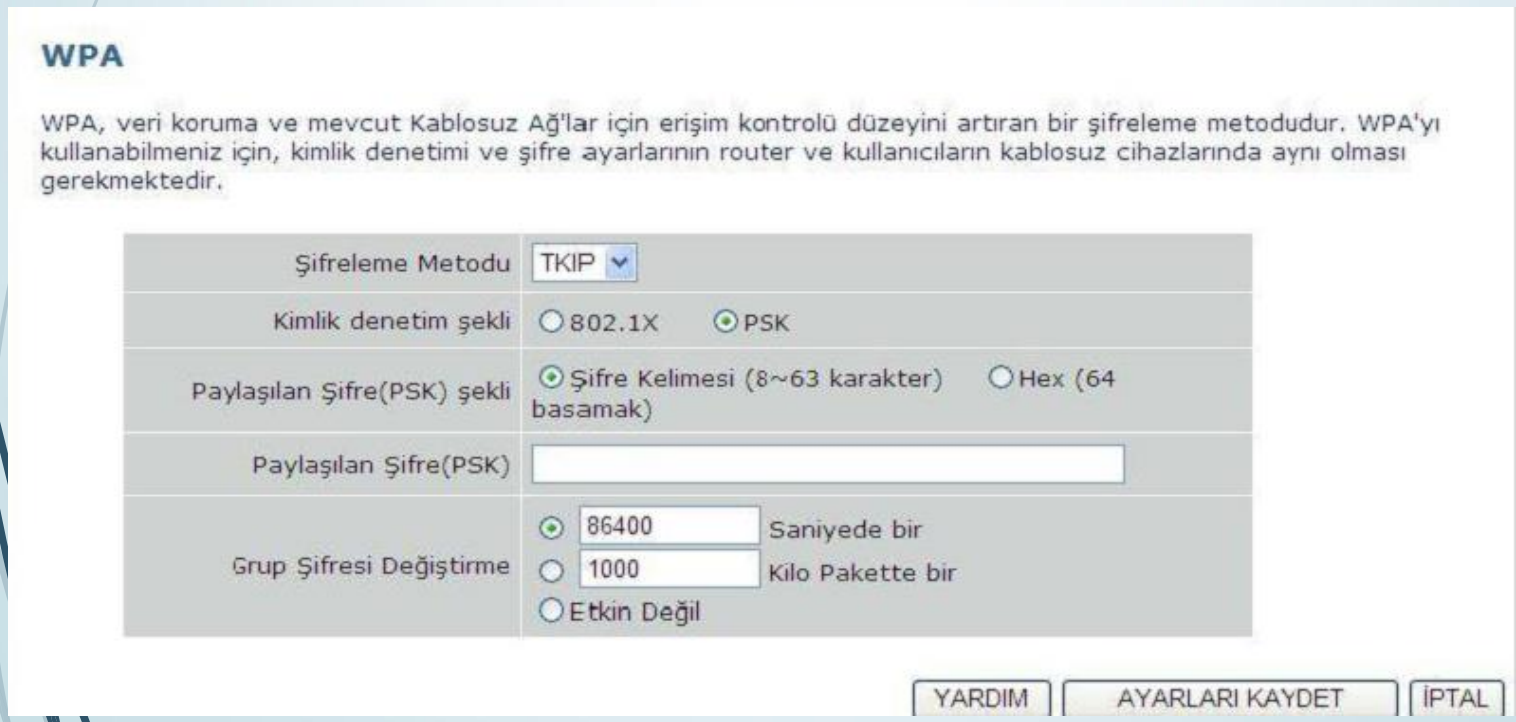
Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

- **Ağı Şifrelemek**
  - WEP (**W**ired **E**quivalent **P**rivacy)



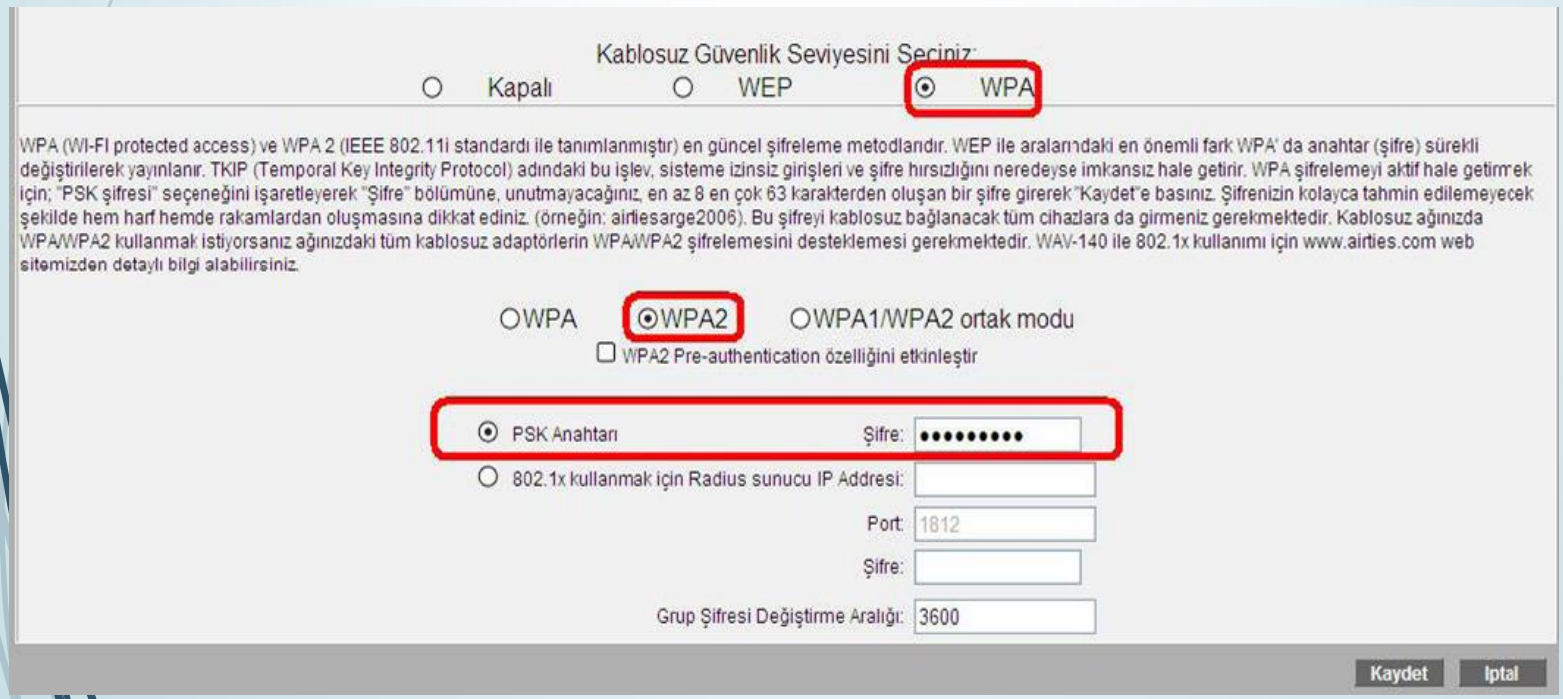
Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

- **Ağı Şifrelemek**
  - WPA (**W**iFi **P**rotected **A**ccess)



Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

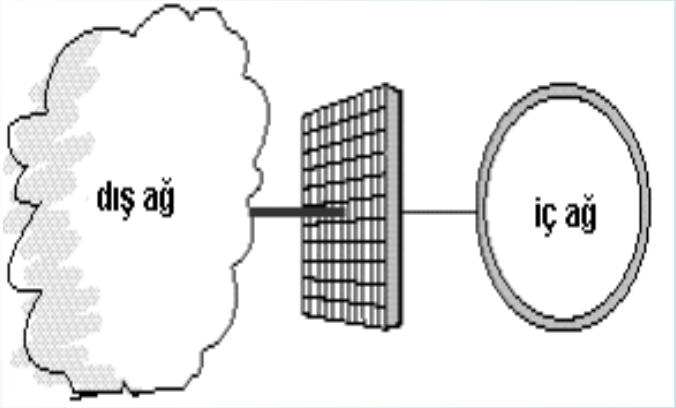
- **Ağı Şifrelemek**
  - WPA2 (**W**iFi **P**rotected **A**ccess)



Kablosuz Ağlarda Kullanılan Güvenlik Önlemleri

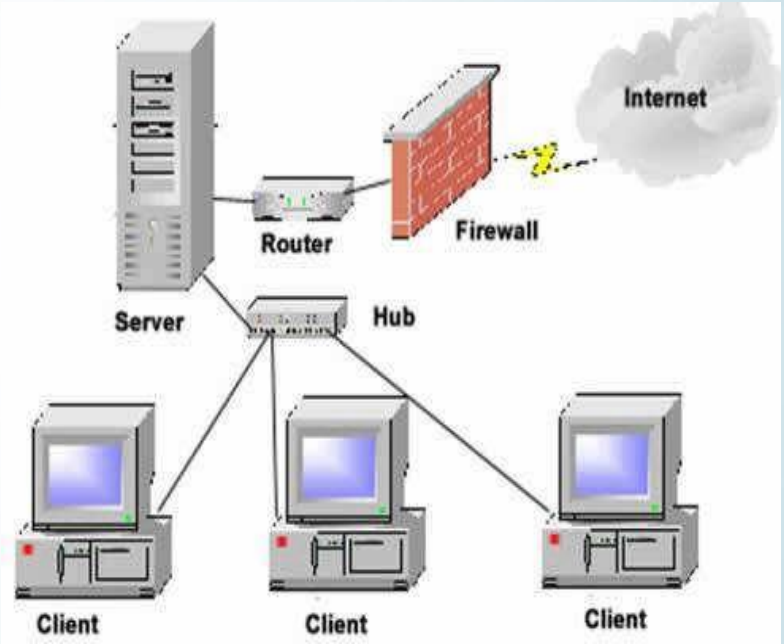
GÜVENLİK DUVARI NEDİR?

- Ateş duvarları ağın içinden veya dışından gelen yetkisiz erişimleri engelleyen, süzen ve izin denetimi sağlayan yazılımlar veya donanımlardır .



GÜVENLİK DUVARI NEDİR?

- Ağ güvenlik duvarı, içeride birbirlerine güvenen, az korumalı makinelerin olduğu bir kurum ağı ile dış ağlar (internet) arasına yerleştirilir ve aradaki fiziksel bağlantı yalnızca güvenlik duvarı tarafından sağlanır



GÜVENLİK DUVARI

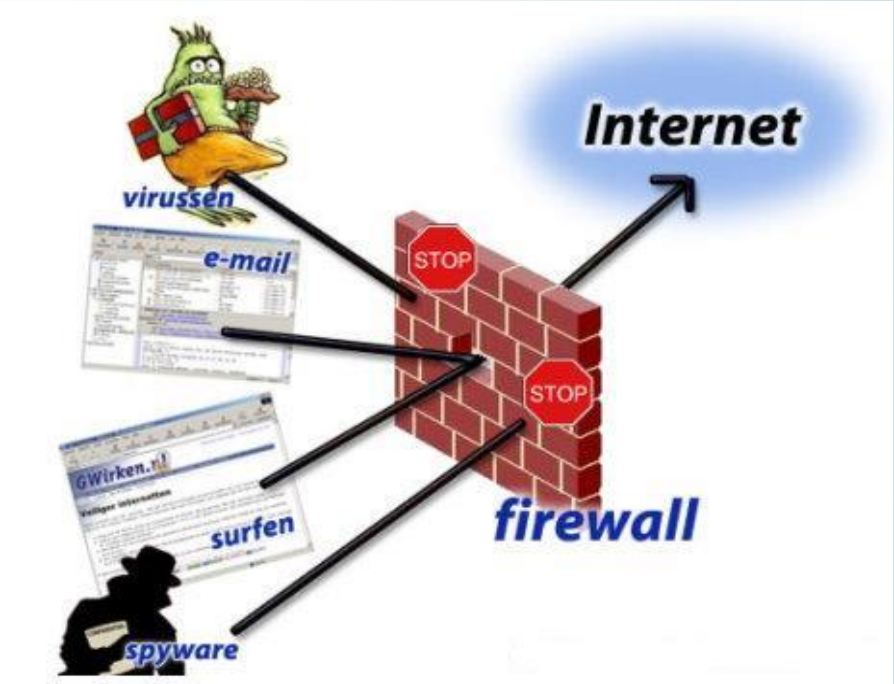
- Ağ güvenlik duvarı, yazılım veya donanımla yazılımın entegre olduğu çözümler şeklinde olabilir.

GÜVENLİK DUVARI

- İzinli girişler arasındaki bilgi alış-verişini herhangi bir gecikmeye maruz bırakmadan yapar.
- Ağa girmeye çalışan herhangi izinsiz bir materyale karşı filtre görevi yapar, ağa girişe izin vermez.
- İzinsiz ağa girmeye çalışanları, yöneticiye rapor eder.

NE TÜR GÜVENLİK DUVARI?

- Sistem kurulurken şu noktalara dikkat edilmelidir. Kurulmadan önce ne tür bilgilerin koruncağı, ne derecede bir güvenlik uygulanacağı ve kullanılacak güvenlik algoritmaları önceden belirlenmelidir



GÜVENLİK DUVARLARI NELERİ YAPAMAZ?

- Güvenlik duvarı ağınızın %100 güvenli olduğunu garanti etmez ya da edemez.
- Güvenlik duvarları içerisindeki ataklara karşı herhangi bir koruma sağlayamaz.
- Güvenlik duvarları ağın arka kapısından gelen istenmeyen veya yetkisiz erişimleri engelleyemez.
- Birçok yapılandırmada güvenlik duvarları virüslere ve zararlı kodlara karşı koruma sağlayamazlar.

GÜVENLİK DUVARLARI NELERİ YAPABİLİR?

POZİTİF ETKİLERİ

- Kullanıcı Kimlik Doğrulaması
- Denetleme ve Loglama
- Güvenlik

GÜVENLİK DUVARLARI NELERİ YAPABİLİR?

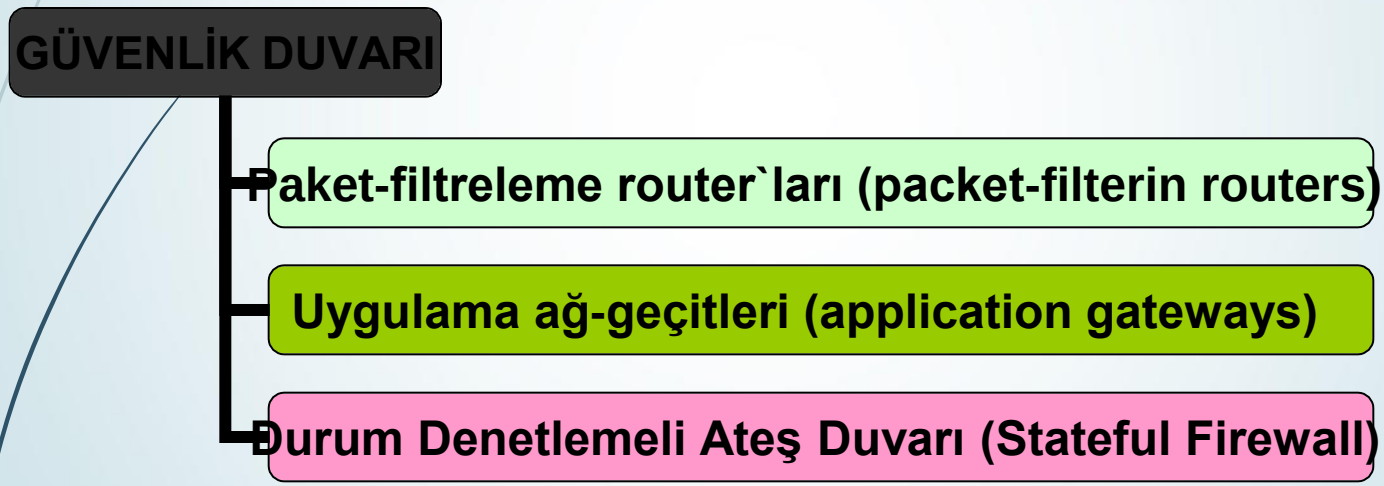
NEGATİF ETKİLERİ

- Trafik Darboğazı
- Tek Hata Noktası
- Kullanıcıyı Hayal Kırıklığına Uğratma
- Artan Yönetim Sorumluluğu

GÜVENLİK DUVARLARI NASIL ÇALIŞIR ?

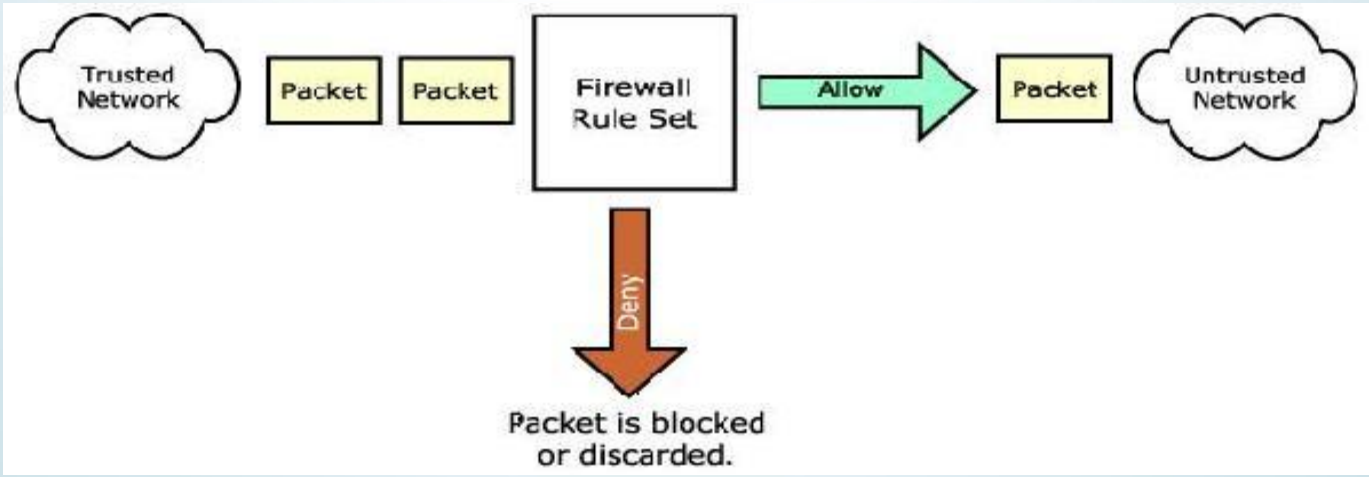
- Özel olarak izin verilmeyen her şeyi reddet.
- Özel olarak reddedilmeyen her şeyi kabul et .

GÜVENLİK DUVARI BİLEŞENLERİ



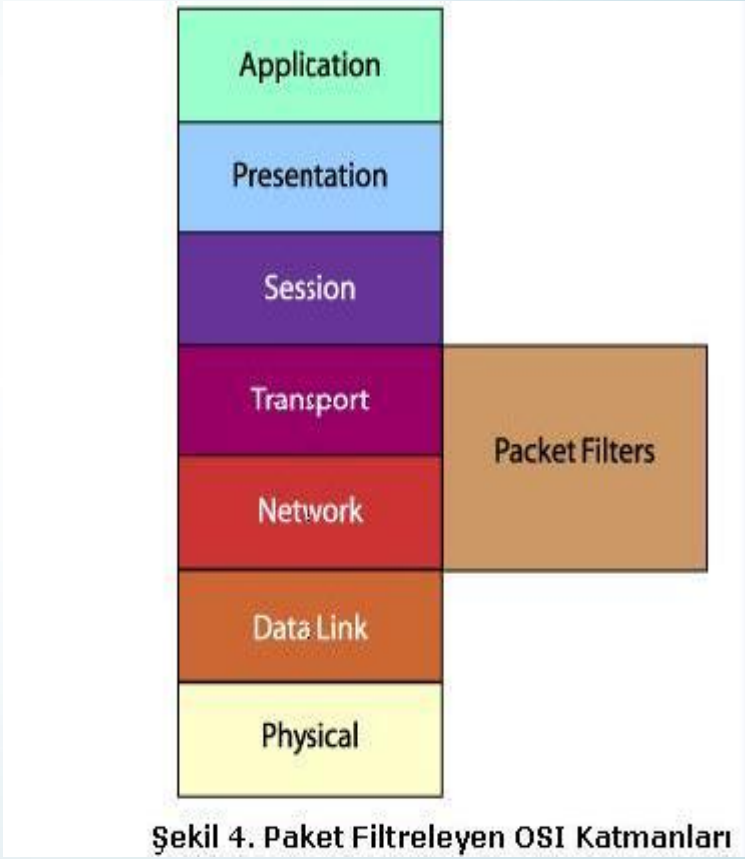
PAKET FİLTRELEME

- Her bir paket güvenlik duvarından geçtiği esnada paket başlığı bilgisi önceden tanımlı kurallar veya filtreler doğrultusunda incelenir. Kabul etme veya reddetme kararı bu karşılaştırmanın sonuçları doğrultusunda verilir.



PAKET FİLTRELEME

- Paket filtreleyen güvenlik duvarı genelde filtreleme ağ katmanında veya nakil katmanında yapıldığı için ağ katmanı güvenlik duvarı olarak da adlandırılır.



Şekil 4. Paket Filtreleyen OSI Katmanları

PAKET FİLTRELEME

Paket filtreleme kuralları veya filtreleri aşağıdaki değişkenler doğrultusunda oluşturulur:

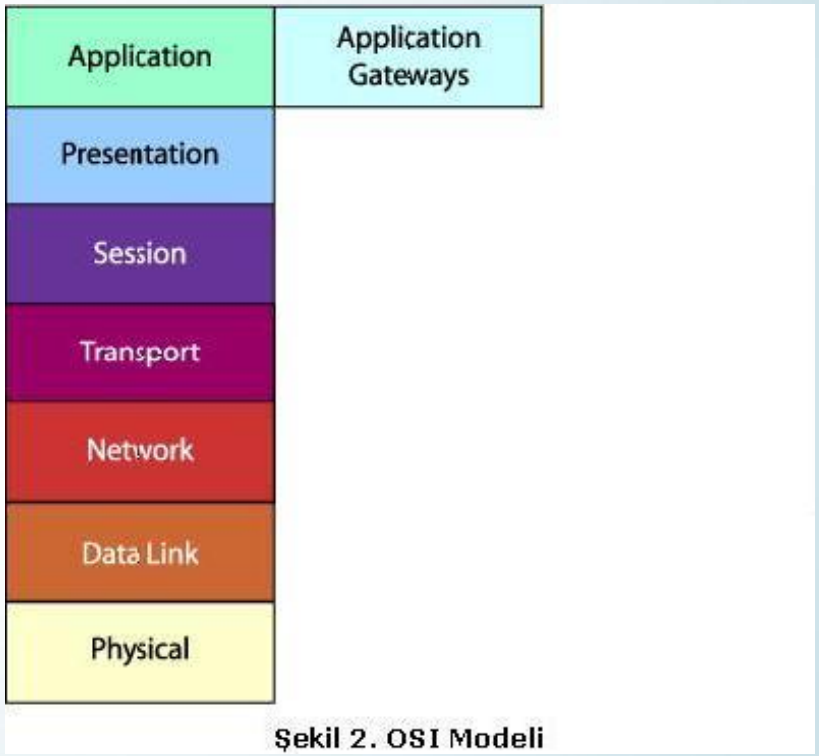
- Kaynak IP adresi
- Hedef IP adresi
- Protokol tipi (TCP/UDP)
- Kaynak port
- Hedef port

PAKET FİLTRELEME

- Paket filtreleme tipik olarak diğer paket izleme metodlarından daha hızlıdır.
- Paket filtreleyen güvenlik duvarları açık olarak konfigüre edilebilir.
- Paket filtreleyen güvenlik duvarlarında kurallar ve filtreler tanımlamak karışık bir iştir.
- Paket filtreleyen güvenlik duvarları malum ataklara karşı eğilimlidir.

UYGULAMA SEVİYELİ AĞ GEÇİDİ(VEKİL) SUNUCU

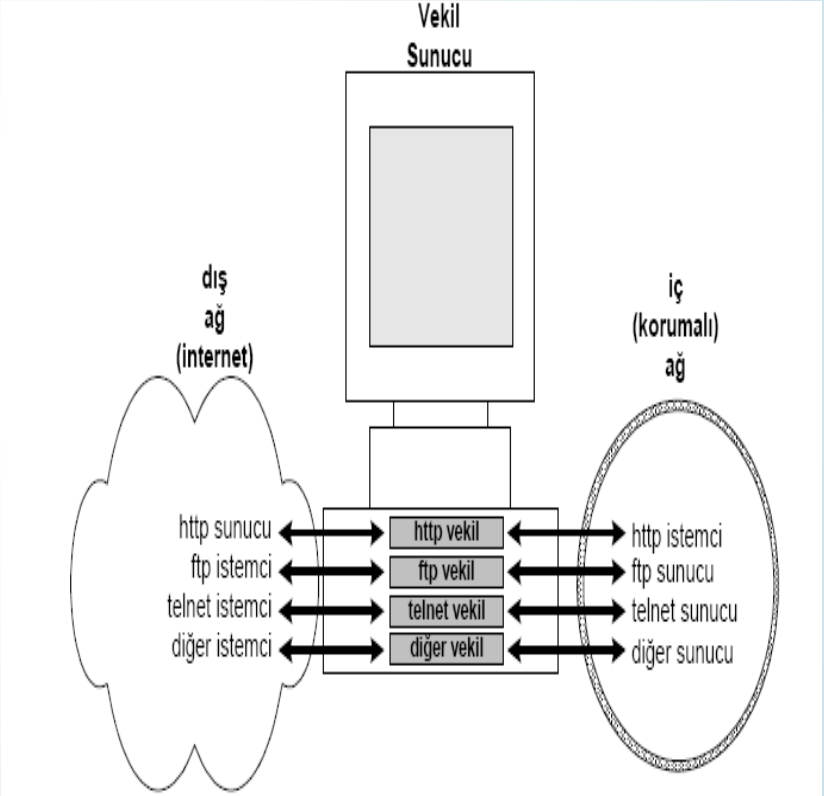
- Uygulama Seviyesindeki Güvenlik Duvarıdır. Her uygulama için özel bir vekil (proxy) aracı programı ile ağ haberleşmesi sağlanır. Bu vekil program belirlenen güvenlik politikasına göre kontrol yapar.



Şekil 2. OSI Modeli

UYGULAMA SEVİYELİ AĞ GEÇİDİ(VEKİL) SUNUCU

- Vekil sunucular genelde çift ara yüzlü konaklar üzerinde çalışırlar(dual-homed). Bu konaklar çift ağ ara yüzüne sahip olup sunucu bilgisayarlardır.



UYGULAMA SEVİYELİ AĞ GEÇİDİ(VEKİL) SUNUCU

- Bu tip güvenlik duvarları içeri veya dışarı gidecek OSI modelinde uygulama (application) katmanında çalışan belli iletişim kurallarına bakarlar .

AĞLARDA TEHDİT TÜRLERİ

1-) • Bilgisayar Ağlarında Risk ve Tehditler

2-) • Saldırı Teknikleri ve Türleri

3-) • Saldırı Yöntemleri ve Önlemler

AĞLARDA TEHDİT TÜRLERİ

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım
- Kötü Niyetli Hareketler

~ % 80

Harici Tehdit Unsurları

- Hedefe Yönelmiş Saldırılar
- Hedef Gözetmeyen Saldırılar

~ % 20

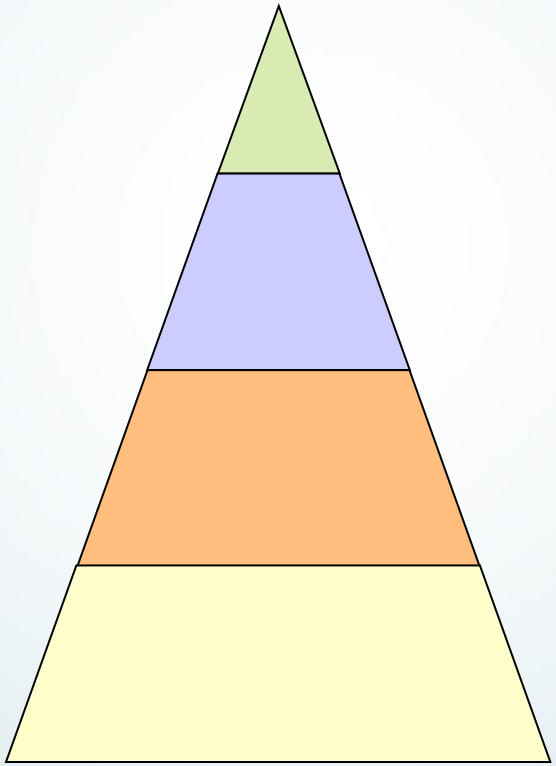
SALDIRGAN DURUMLARI VE TAHMİNİ SAYILARI

Çok Tehlikeli

Yırtıcı

Orta Seviye

Başlangıç Düzeyinde



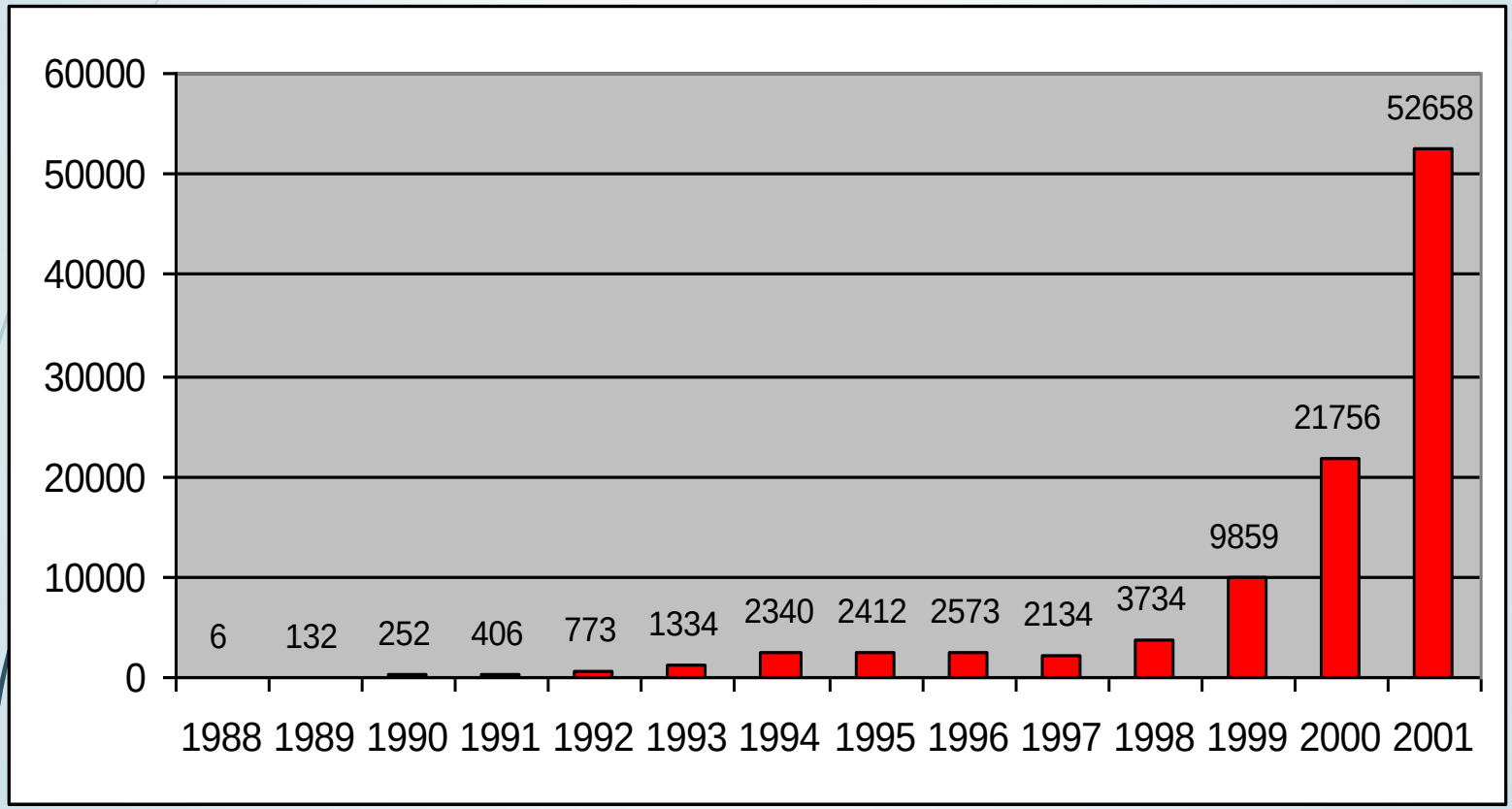
Yüzlerce

Binlerce

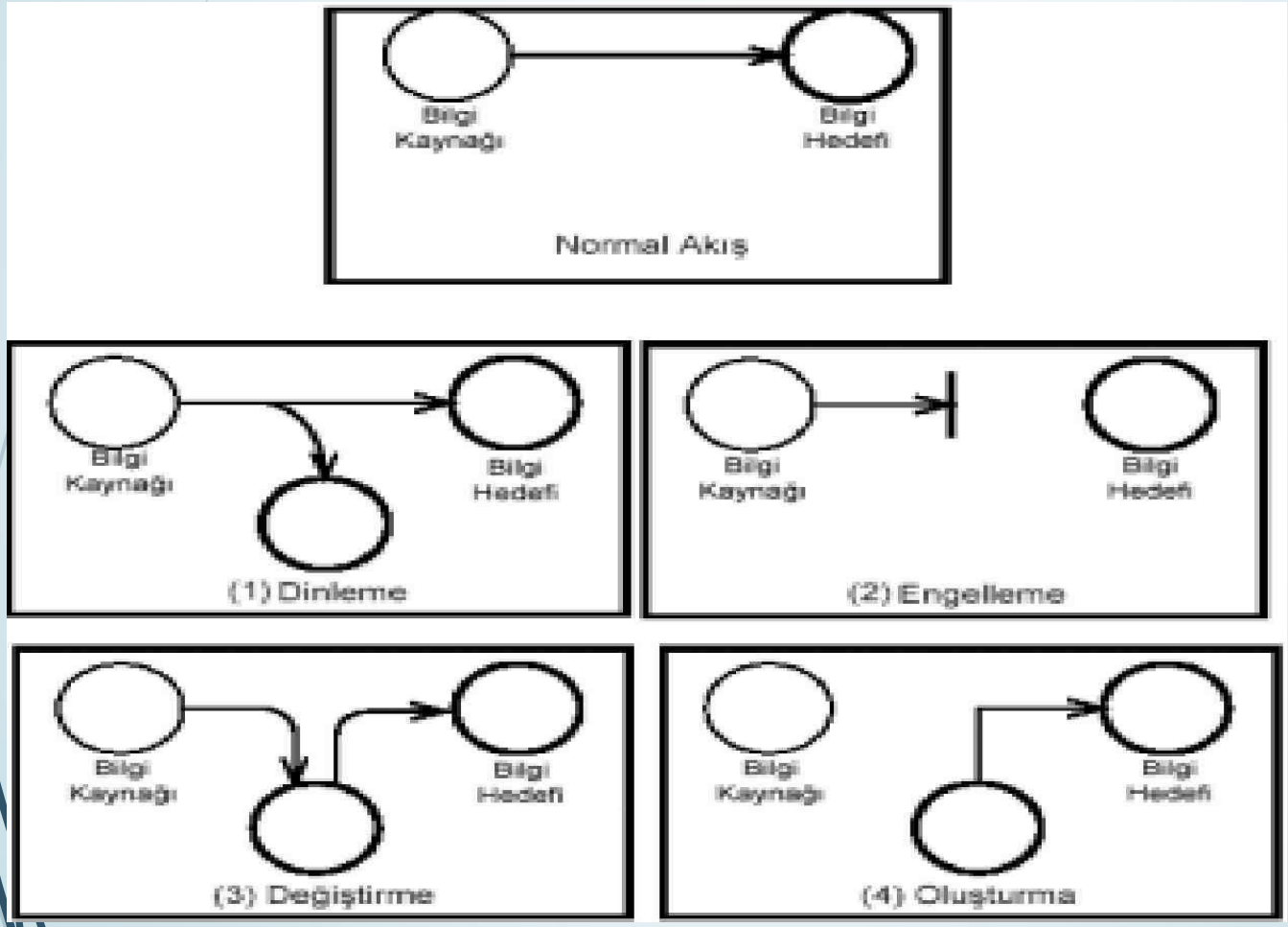
Onbinlerce

Milyonlarca

YILLARA GÖRE RAPOR EDİLEN OLAY SAYISI



SALDIRI YÖNTEMLERİ



SALDIRI TEKNİKLERİ VE TÜRLERİ

Saldırı Türleri	Dinleme	Engelleme	Oluşturma	Değiştirme
Saldırı Teknikleri	Sosyal Mühendislik	DOS	Virüs	Spoofing
	DOS Ping Tarama	Email Bombardment	Trojon	IP spoofing
	Port	IP Servis Durdurma	Worm	Email spoofing
	İşletim Sisteminin Belirlenmesi	SYN seli		
	Sniffer	NFS		
	Firewalkin			

DİNLEME

Ağdaki bileşenleri dinlemek veya ağ üzerindeki bilgiyi dinlemek olarak iki başlık altında toplanabilir. Bunlardan birincisi Tarama, “Scan” ikincisi ise Dinleme’dir “Sniffer” [1]

Scan işlemi;Aktif sistemlerin belirlenmesi, isletim sistemlerinin saptanması, ve bu bileşenlerin ağ üzerindeki konumlarının belirlenmesi gibi aşamalardan oluşur. Scan, hedef ağın yöneticisi ile aynı bilgi seviyesine ulaşana kadar bu süreç devam eder. [1]

DİNLEME

- Sniffing ağ üzerinden gidip gelen bilgilerin dinlenmesine dayanmaktadır.

- Her bilgisayar konuşacağı bilgisayarın ip numarasını öğrenir ve göndereceği paketlere o bilgisayarın ip numarasını yazarak yollar.

- Ancak ağ üzerinden gelen binlerce paket içerisinde ise sadece kendi ip numarası geçen paketleri dinler diğerlerini filtreler.

- Sniffer programlar ise bu filtreleme olayını software olarak devre dışı bırakır ve ağdaki tüm paketleri dinler.

ENGELLEME

- Tek başına bir hack snıflandırması olmasına karşın büyük ve belirli bir sistem içerisinde gerçekleştirilecek olan hack olaylarında dinlemeden sonra gerçekleştirilen ikinci adım olduğu gözlenmektedir .

DOS

- Denial-of-Service yada kısaca DoS olarak adlandınlan hack yöntemi yazılımlardaki hataları kullanarak ya da sunucu veya ağ kaynaklarını tüketme yoluyla,normal kullanıcıların erişimlerini engelleyecek şekilde,bilgisayar sistemlerini ulaşılamaz hale getirme amacıyla yapılır .

EMAIL BOMBARDMENT

Temel olarak bir DoS metodu gibi görülmekle birlikte aslında bir sistem kaynağına yok etmediği için gerçekte başka bir engelleme hacking yöntemidir. [2]

Bu metod kurbanın mail adresine normalden çok fazla ve sürekli olarak kurbanın istemediği Email mesajı yollanmasına dayanmaktadır. [2]

IP SERVİS DURDURMA

- Yanlış kaynak adresi bilgisiyle oluşturulmuş ICMP “echo request” paketleri kullanılarak gerçekleştirilir.
- Çoğu durumda hedef bilgisayarın kilitlenmesine sebep olan, ayrıca hedef olarak kullanılan ağlarda önemli derecede performans sorunları yaratabilen bir hack tekniğidir.

OLUŞTURMA

- Bu hacking türü aslında amac olarak tanımlana bilinir.
- Bu aşamadan sonra hacker sisteme sızmış ve amacına ulasmış olmaktadır.

VİRÜSLER

- TRUVA ATLARI
  - Belirli bir tarihte aktif olan virüslerdir.
  - BIOS'u siler.Harddisk'teki tüm bilgileri kullanılmaz hale getirir ve sistem göçer.

VİRÜSLER

- WORM(SOLUCAN)
  - En tehlikeli ve en hızlı yayılan virüs türüdür.
  - Genellikle E-Mail yoluyla bulaşırlar.

SPYWARE

- Casusluk yapmak için oluşturulmuş programlardır.
- İnternetten "bedava" diye reklamını görüp indirdiğiniz programlardır.
- Temel amaç: Bilgi toplamak .

VİRÜSLER

- TROJANLAR

- Belirlenmiş dosyaları silebilirler bulaşıcı ve yayılmacı özelliği yok.
- Bilgi ve dosyaları başka bir bilgisayara transfer edebilir.
- Hacker ve Cracker'lar için vazgeçilmezdir.

DEĞİŞTİRME

- İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklik yapar .

SPOOFING TEKNİKLERİ

- Spoof genel olarak IP’deki (Internet Protokolii) değerlerin olduğundan farklı olarak gösterilmesi demektir.
- DNS sunucularını ele geçirerek veya sorgulara sahte cevaplar vererek DNS spoofing yapılabilir.
- Parmak izi sistemlerinde, daha önce alınmış parmak izi örneği kullanılarak yapılabilir .

SPOOFING-ÖRNEK SPOOFING İŞLEM

Yerine Geçilecek Sistem

1

Devre Dışı Kal

2

Ben "O"yum

Saldırgan

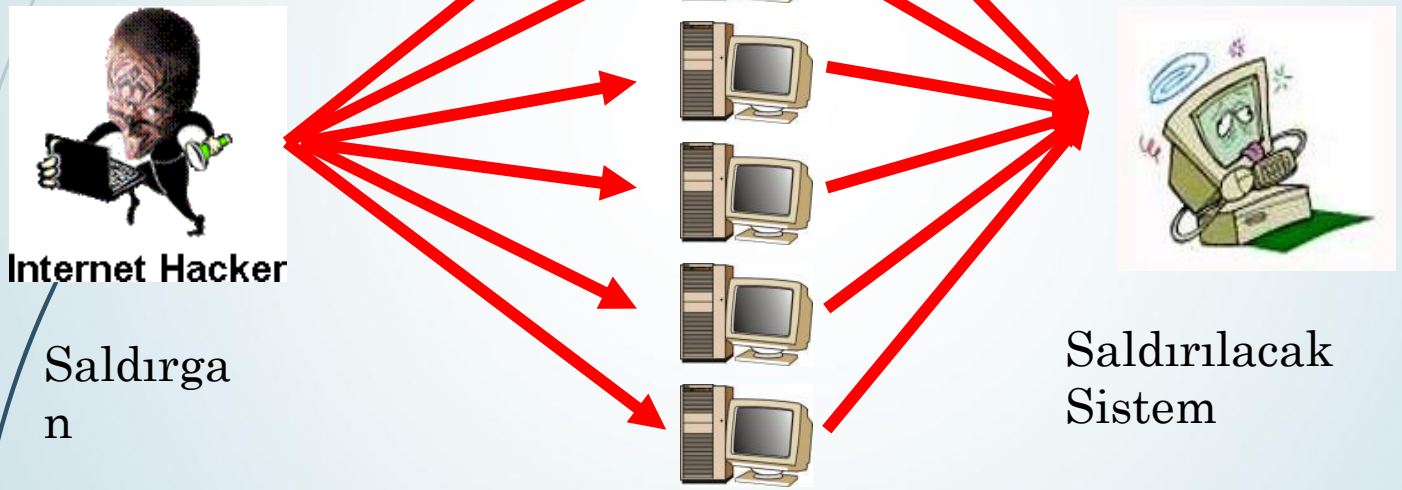
SPOOFING-ÖNLEME YÖNTEMLERİ

- Harici doğrulama sistemleri kullanmak,
- Switch'lerde her porta bir MAC adresi eşleşmesini sağlamak ve Swtich'leri tablo taşmalarından korumak,
- Doğrulama bilgilerinin (şifre, dosyalar vb.) istemci sisteminde tutulmasını engellemek

HİZMET AKSATMA SALDIRILARI

- İşletim sistemi zayıflıkların sonucunda, sunucunun servis veremez hale getirilmesidir.
- Sunucu, servis, uygulama veya ağın devre dışı bırakılması olabilir.
- Tek merkezli yada çok merkezli olarak yapılabilir.

DAĞITIK HİZMET AKSATMA SALDIRILARI



HİZMET AKSATMA SALDIRILARINI ÖNLEME YÖNTEMLERİ

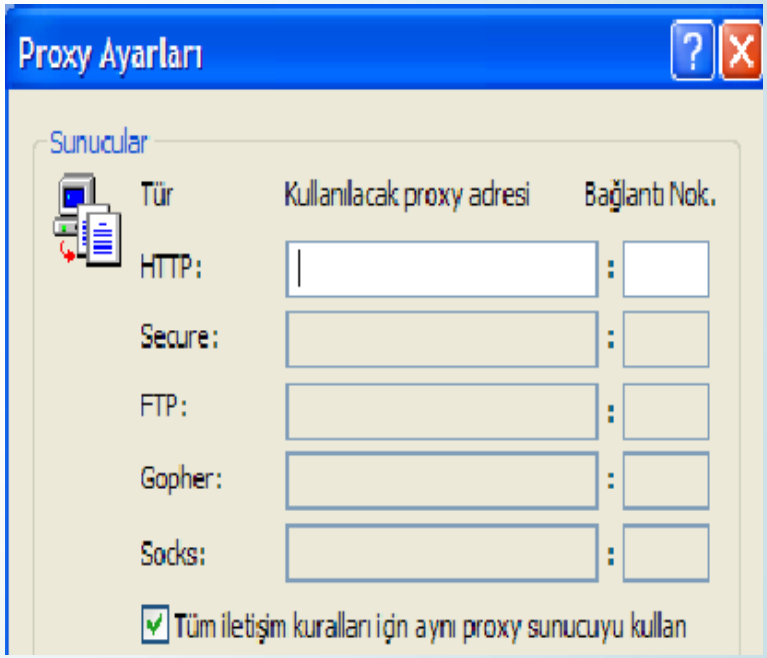
- Uygulama ve işletim sistemlerinin yayınlanmış tüm güncelleme/yamaları uygulanmalı, yeni sürümlerle hizmet verilmelidir.
- Uygulama seviyesinde güvenlik duvarları kullanılmalı.

İNTERNETTE İZİNİZİ BELLİ ETMEYİN

PROXY NEDİR?

PROXY SERVİSİ NEDİR?

BİR PROXY SERVİSİ(SUNUCUSU) SİZİN ADINIZA SİZDEN ALDIĞI BİLGİ ALMA İSTEKLERİNİ YÜRÜTÜR VE SONUCU YİNE SİZE İLETİR.



IE İÇİN PROXY KULLANIMI

- web sitelerinde ip adresinizi çok basit şekilde proxy ile saklayabilirsiniz. önce çalışan proxyler bulmanız gerekiyor, bunun aşağıdaki adreslerden rahatça bulabilirsiniz.

- alive proxy geliştiricilerinden; http://atomintersoft.com/products/alive-proxy/proxy-list/

- google free proxies dizini; http://directory.google.com/top/computers/ınternet/proxies/free/?il=1

PORT KAVRAMI

PORT NEDİR?

144.122.156.104 23

BAZI PORTLAR

80 HTTP

21 FTP

23 TELNET

25 MAİLTO

110 POP3

AÇIK PORTLARIMIZI NASIL ÖĞRENİRİZ?

netstat –a veya

http://www.iana.org/assignments/port-numbers

AÇIK PORTLARIMIZI NASIL KAPATABİLİRİZ?

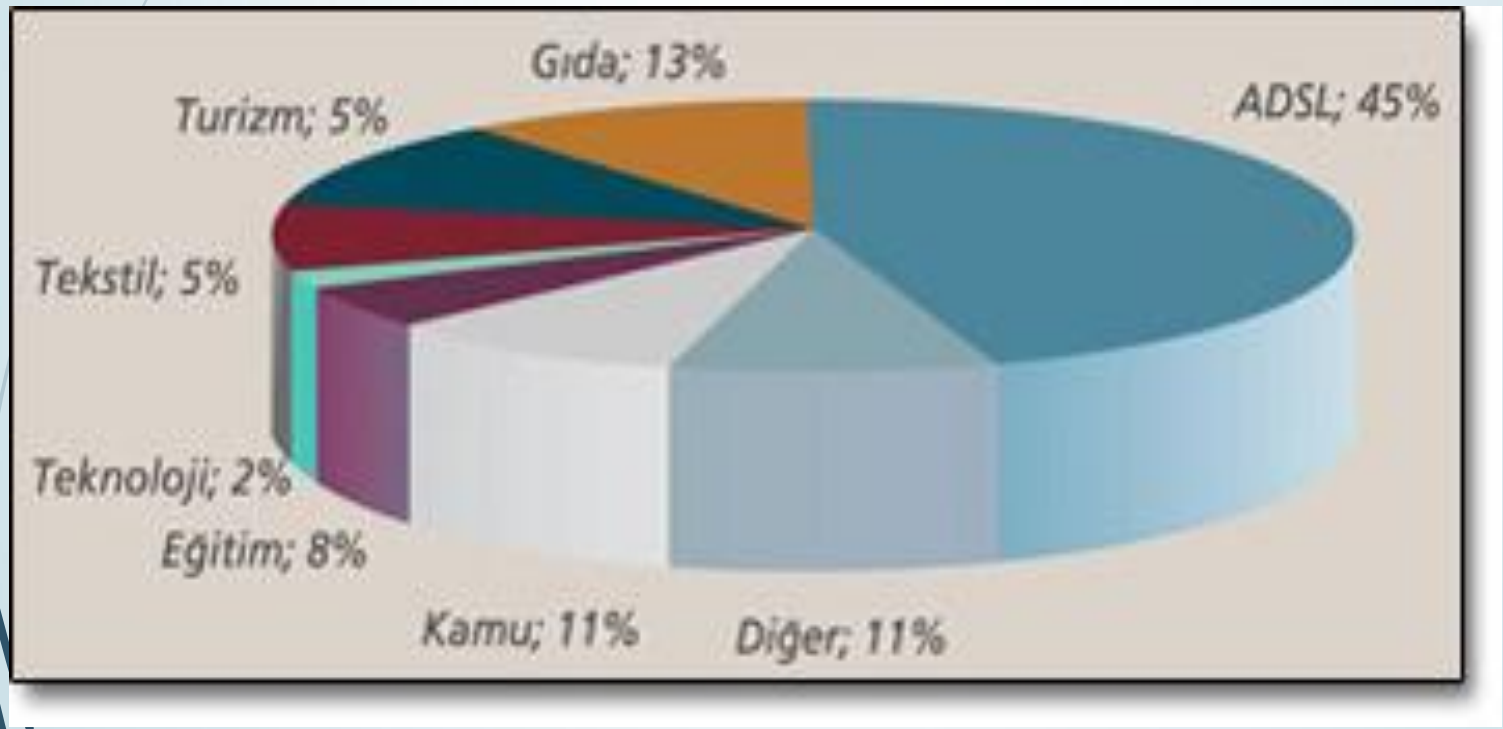
Ağ bağlantılarım sağ tuş özellikler=>et. İnt. Bağ.

Sağ tuş öz.=>tcp/ıp çift =>gelişmiş =>seçenekler=>tcp/ıp süzme işlemi

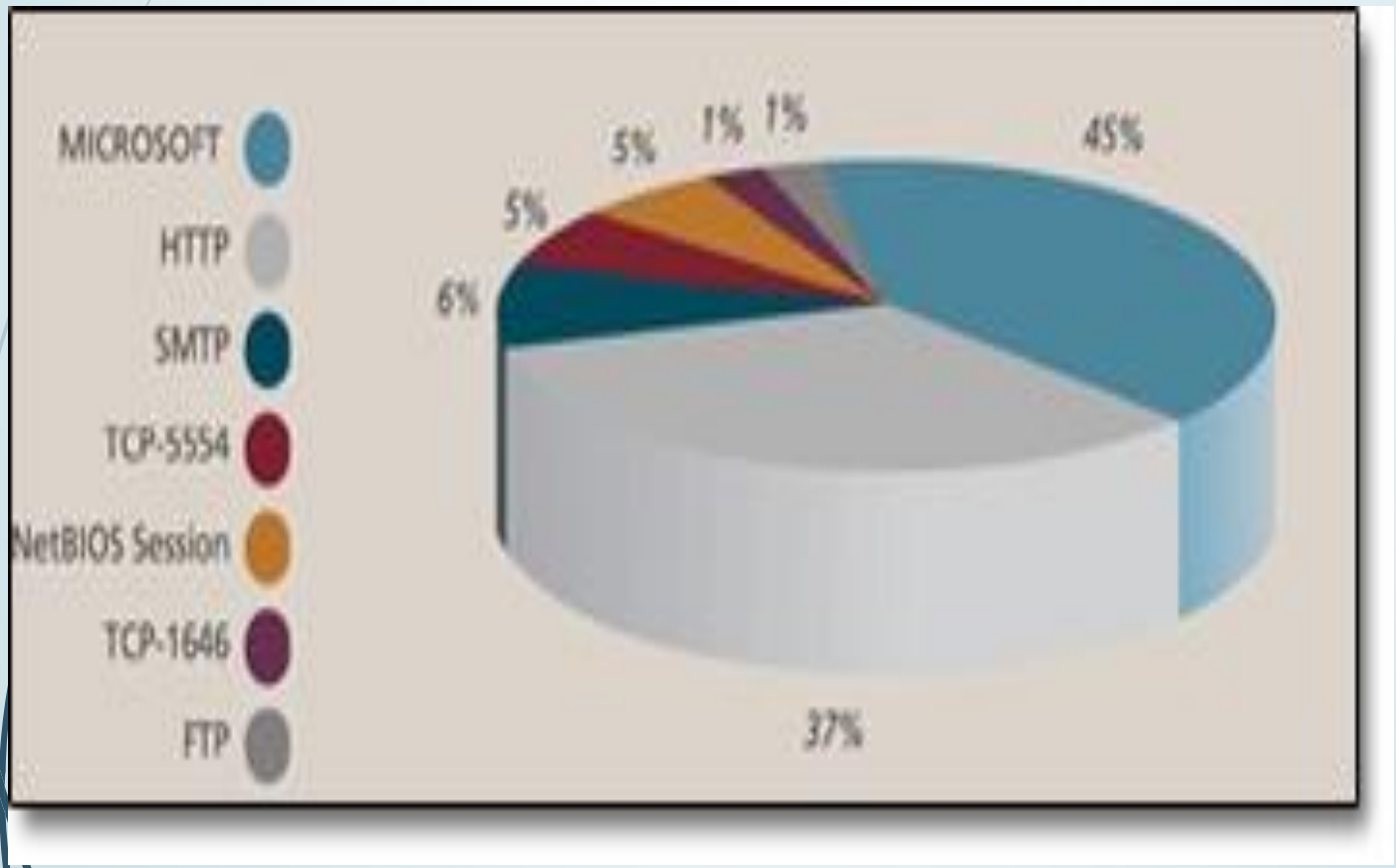
```
C:\>netstat -a

Etkin Bağlantılar

  İl.Kr. Yerel Adres          Yabancı Adres        Durum
  TCP    zalca:http           zalca:0              LISTENING
  TCP    zalca:epmap          zalca:0              LISTENING
  TCP    zalca:https          zalca:0              LISTENING
  TCP    zalca:microsoft-ds   zalca:0              LISTENING
  TCP    zalca:1025           zalca:0              LISTENING
  TCP    zalca:1026           zalca:0              LISTENING
  TCP    zalca:1027           zalca:0              LISTENING
  TCP    zalca:1039           zalca:0              LISTENING
  TCP    zalca:1200           zalca:0              LISTENING
  TCP    zalca:ms-sql-s       zalca:0              LISTENING
  TCP    zalca:1466           zalca:0              LISTENING
  TCP    zalca:1468           zalca:0              LISTENING
  TCP    zalca:1469           zalca:0              LISTENING
  TCP    zalca:1471           zalca:0              LISTENING
  TCP    zalca:1475           zalca:0              LISTENING
  TCP    zalca:1476           zalca:0              LISTENING
```

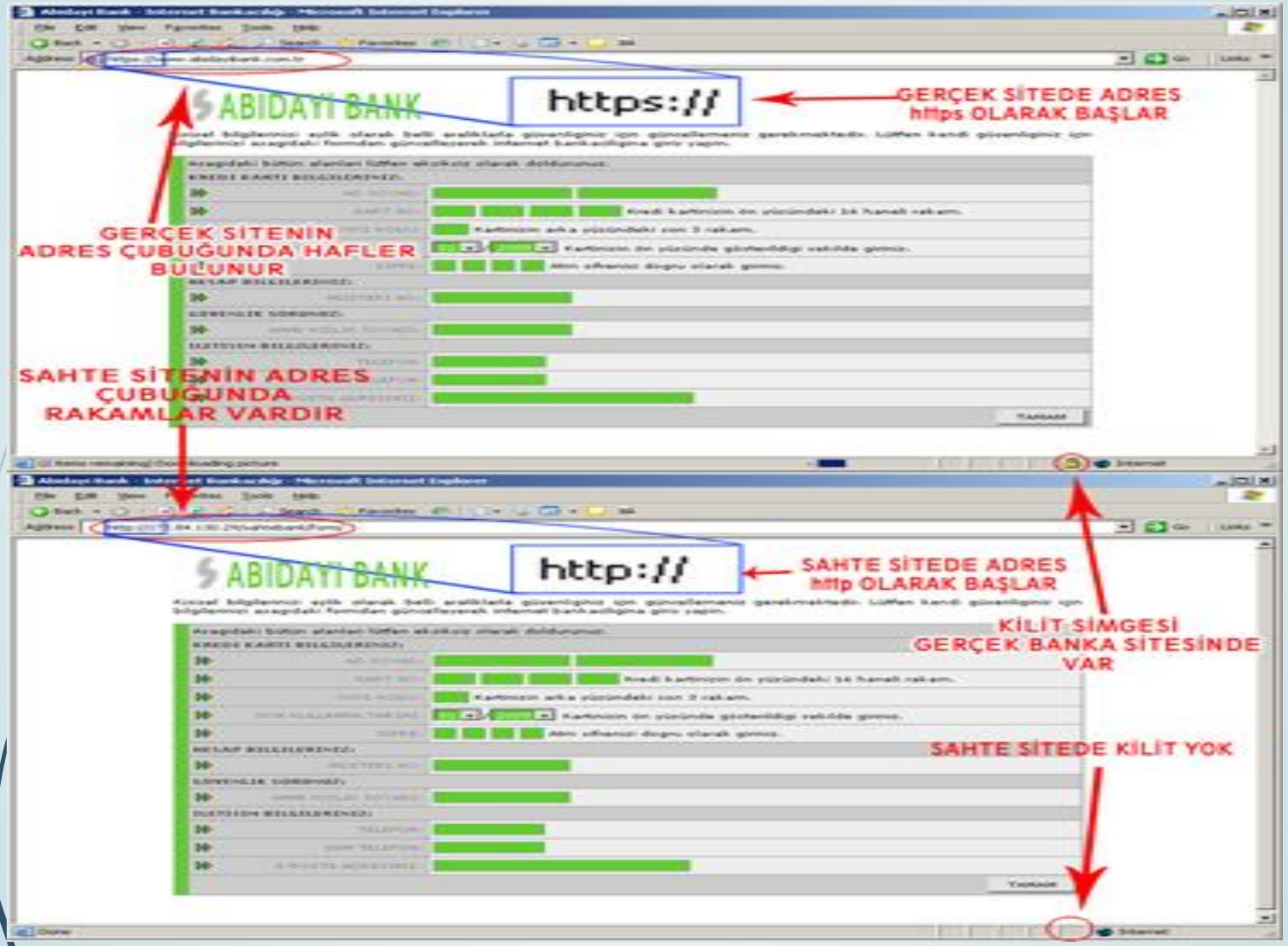
SALDIRI SAATLERİ

ADSL VE SEKTÖRLERE GÖRE SALDIRI ORANLARI



EN ÇOK SALDIRIYA MARUZ KALAN SERVİSLER




https://
GERÇEK SİTEDE ADRES
https OLARAK BAŞLAR
GERÇEK SİTENİN
ADRES ÇUBUĞUNDA HAFLER
BULUNUR
SAHTE SİTENİN ADRES
ÇUBUĞUNDA
RAKAMLAR VARDIR
http://
SAHTE SİTEDE ADRES
http OLARAK BAŞLAR
KİLİT SİMGESİ
GERÇEK BANKA SİTESİNDE
VAR
SAHTE SİTEDE KİLİT YOK

VIRTUAL PRIVATE NETWORK / SANAL ÖZEL AĞ

- VPN nedir?
- VPN çeşitleri
- VPN sistemlerde güvenlik teknikleri
- VPN protokolleri
- VPN sistemlerin çalışma prensibi
- VPN’ in sağladıkları

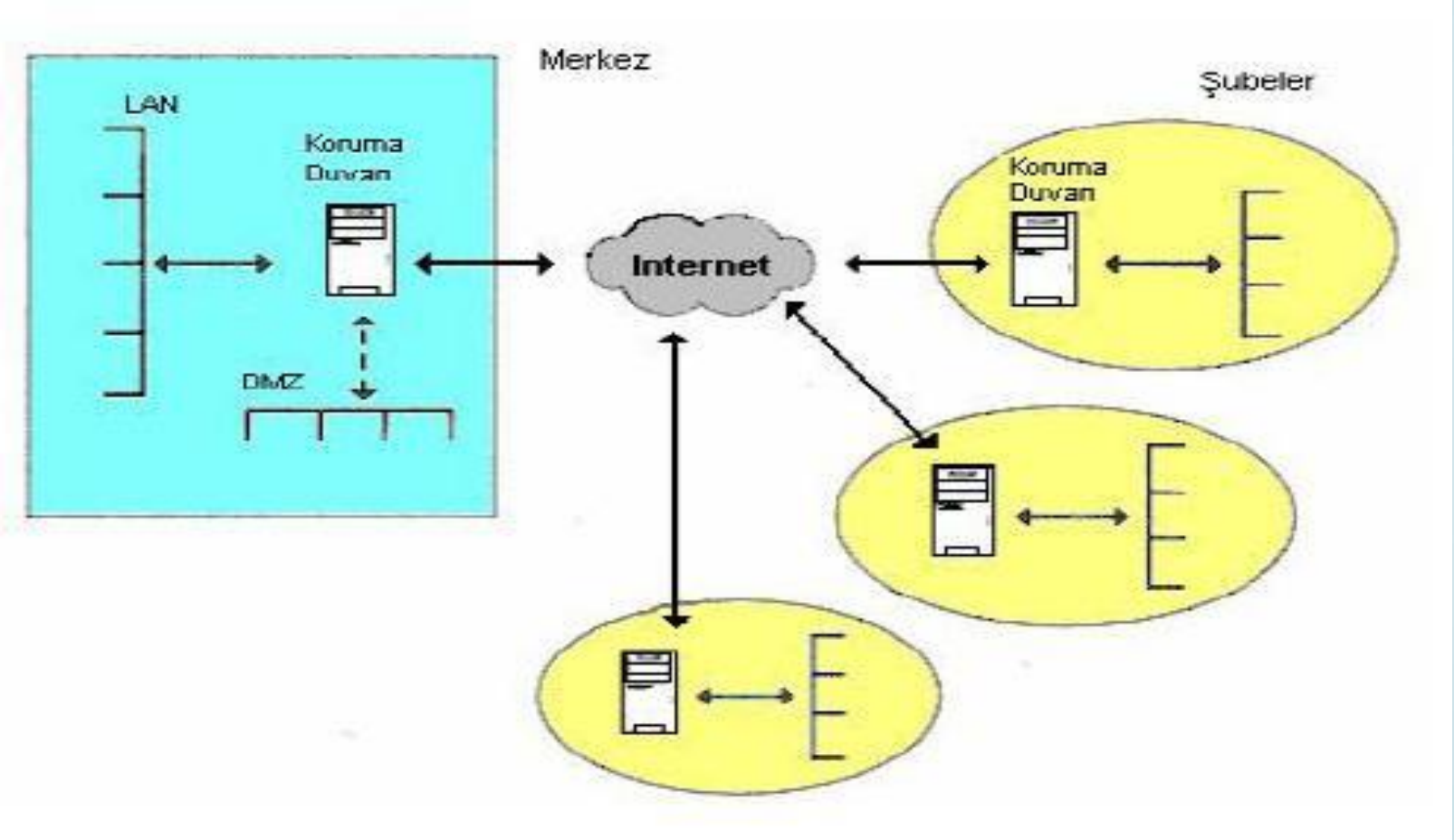
VPN NEDİR?

- İnternet gibi halka açık ağlar üzerinden yani güvensiz ağlar üzerinden güvenli bir şekilde kullanıcıların kendi kurum kaynaklarına erişmelerini sağlayan teknolojidir.

- Güvenlik risklerine karşın, şirketlerin ticari işlemlerini internet üzerinden yürütme isteği, sanal özel ağ kavramını doğurmuştur. Sanal özel ağlar ile şirketler kendilerine, internet üzerinden, erişimi kolay ve ucuz özel bağlantılar oluşturmaktadırlar.

- Büyük kurum ve kuruluşlar uzak yerlerdeki birimleri ile iletişimi internet üzerinden özel bir sanal ağ oluşturarak sağlarlar.

İNTERNET ÜZERİNDEN SANAL ÖZEL AĞ OLUŞTURULMASI



Kaynak: http://www.yozgateml.com/elk/dokuman%5Cmodul%5C18_4.pdf ( )

VPN ÇEŞİTLERİ

- Remote Access VPN (Client to Site)
- Site to Site VPN
  - İntranet VPN
  - Extranet VPN

VPN Çeşitleri

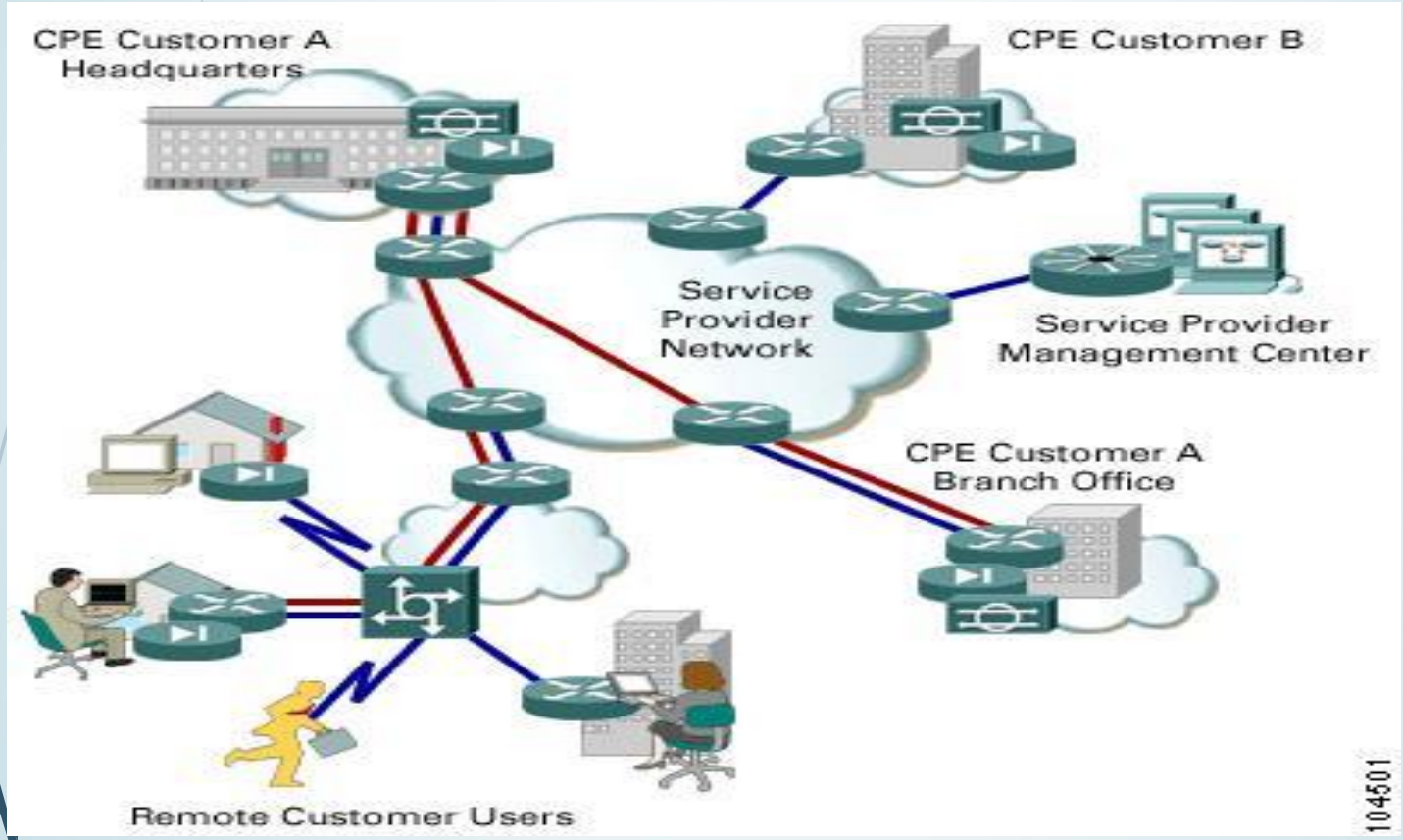
- Remote Access VPN

- Firmaların gezgin çalışanlarının firma ağına her yerden güvenli iletişimlerini sağlamak için kullanılır.

- Büyük bir firmanın farklı yerlerdeki şubelerini merkeze bağlamak için kullanılır.

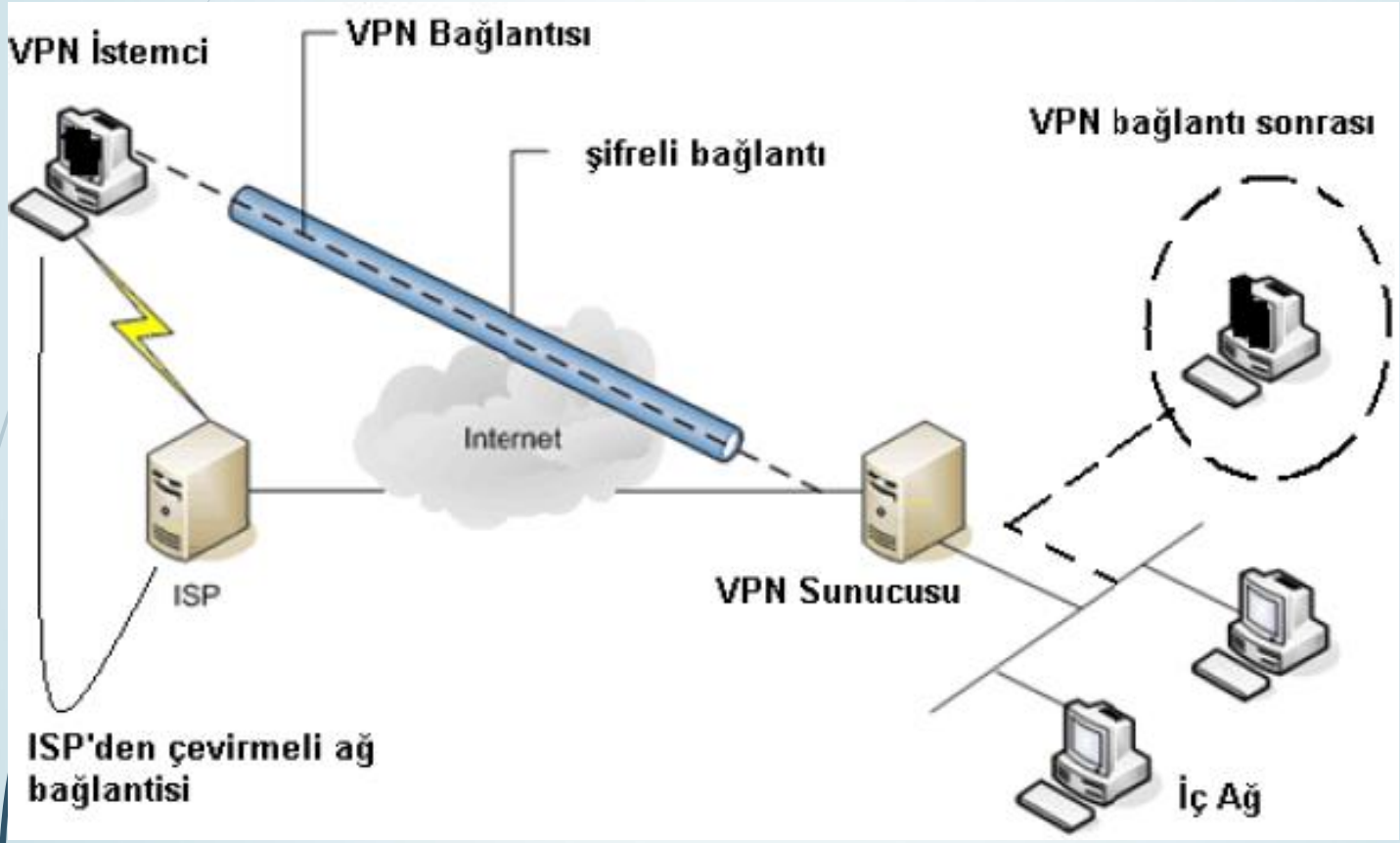
- En önemli özelliği kimlik sorgulaması ile uzak ve gezgin kullanıcıların kimliklerini doğrulamasıdır.

REMOTE ACCESS VPN



Kaynak:
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/3.1/security_management/user/guide/ipsec2.
tml

REMOTE ACCESS VPN

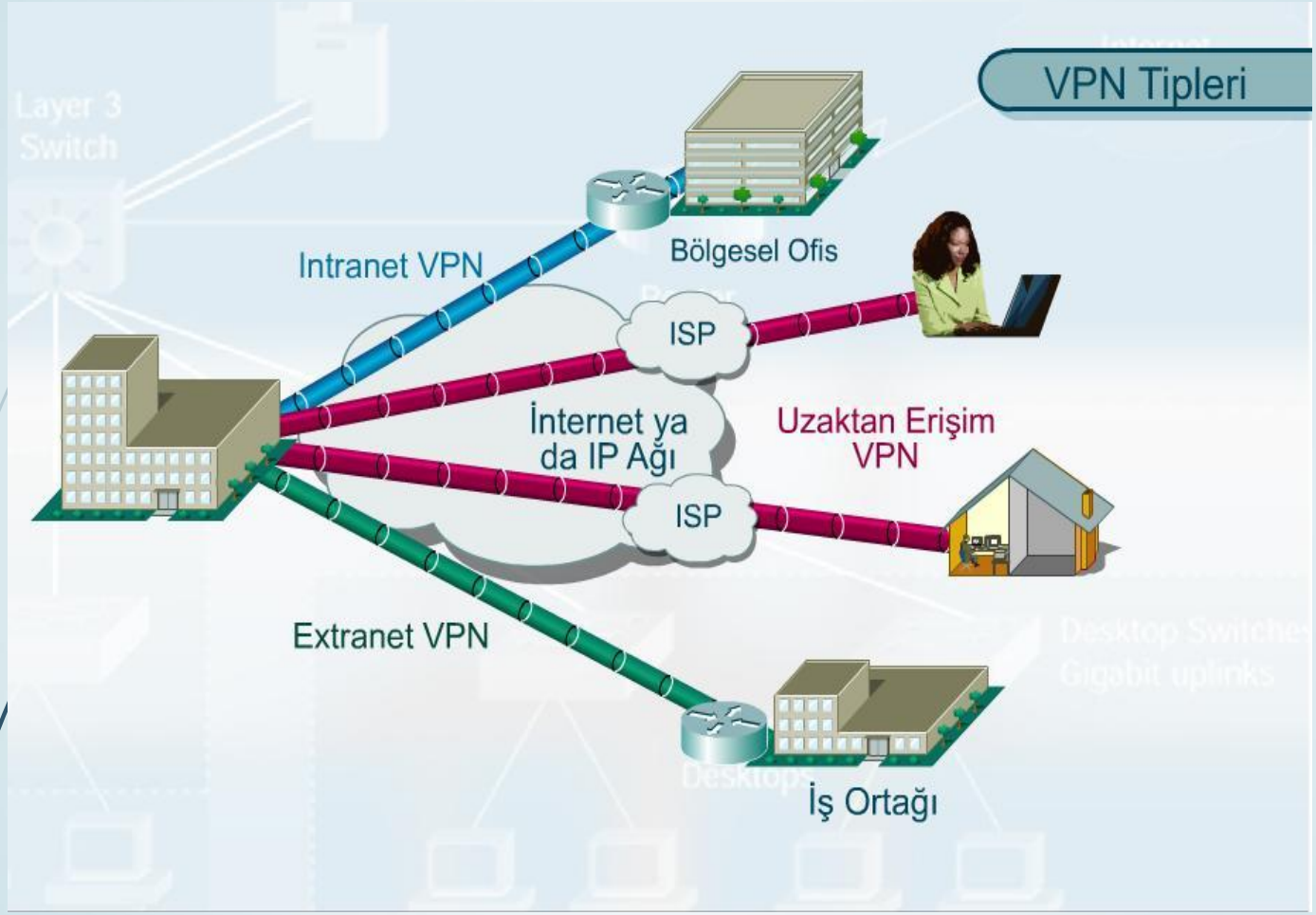


Kaynak: http://www.ozbilen.net/dokumanlar/VPN_virtual_private_network_sevgi_duyen.pdf

SİTE TO SİTE VPN

- Siteden siteye VPN bağlantıları (yönlendiriciden yönlendiriciye VPN bağlantıları olarak da bilinir), kuruluşların farklı ofisler arasında veya diğer kuruluşlarla ortak bir ağ üzerinden yönlendirilmiş bağlantılar kullanabilmelerine olanak verir.

- İnternet üzerinden yönlendirilmiş VPN bağlantısı, mantıksal olarak, adanmış geniş alan ağı (WAN) bağlantısı gibi çalışır.


VPN Tipleri
Intranet VPN
Bölgesel Ofis
ISP
İnternet ya
da IP Ağı
Uzaktan Erişim
VPN
ISP
Extranet VPN
İş Ortağı

VPN GÜVENLİK TEKNİKLERİ

VPN ile üç farklı güvenlik tekniği sağlanır.

- Kimlik Doğrulama (Authentication)
- Şifreleme (Encryption)
- Veri Bütünlüğü (Data Integrity)

VPN GÜVENLİK TEKNİKLERİ

Kimlik Doğrulama (Authentication)

- Sadece yetkili kullanıcıların VPN hizmetini alabilmesini sağlar
- Veriyi gönderenin ve alanın onaylanması.

Veri Bütünlüğü (Data Integrity)

- Kötü niyetli kullanıcıların yolladığınız paketlerin içeriğini değiştirebilmeleri engellenir.

VPN GÜVENLİK TEKNİKLERİ

Şifreleme (Encryption)

- Verinin şifrelenmesi ile gelen ve giden verinin yalnızca iki taraf için anlaşılır olması sağlanır.

- Sisteme dışarıdan girerek veriye ulaşan kişi, veri şifrelenmiş olduğu için hiçbir şey anlamayacaktır.