YEREL BİLGİSAYAR AĞLARININ GÜVENLİK VE PERFORMANSININ ARTTIRILMASI

Hale KESİCİ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR EĞİTİMİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Haziran 1999
ANKARA

Hale KESİCİ tarafından hazırlanan Yerel Bilgisayar Ağlarının Güvenlik ve Performansının Arttırılması adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Halil İbrahim BÜLBÜL
Tez Yöneticisi

Bu çalışma, jürimiz tarafından Bilgisayar Eğitimi Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Başkan : Doç. Dr. Hasan H. ÖNDER

Üye : (Danışman) Yrd. Doç. Dr. H. İbrahim BÜLBÜL

Üye : Dr. Benian TEKİNDAL

Üye : _____

Üye : _____

Bu tez, Gazi Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygundur.

İÇİNDEKİLER

YEREL BİLGİSAYAR AĞLARININ GÜVENLİK VE PERFORMANSININ ARTTIRILMASI

(Yüksek Lisans Tezi)
Hale KESİCİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Haziran 1999

ÖZET

Bilgi çağını yaşadığımız günümüzde en yeni ve doğru bilgiye kısa zamanda ulaşmak oldukça önemlidir. Bilgisayar ve enformatik bilimi bu istekleri kolaylaştırabilmek için sürekli olarak ve çok hızlı bir biçimde gelişmektedir. Bu yoğun bilgisayar kullanım süreci içerisinde ihtiyaç duyulan bilgilere hızlı bir biçimde ulaşabilmek için bilgisayarlarda saklanmaktadır. Bilgisayarlarda mevcut olan bu bilgilerin ve kaynakların daha verimli kullanılabilmesi için iletişim ağlarının kurulması gerekmektedir. İletişim ağları mevcut verilerin, bilgilerin ve kaynakların paylaşımını, haberleşmeyi sağlayan bir yapıdır. Asıl önemli olan da bu yapıyı etkin kullanabilmektir. Günümüzde yerel ağlar bilgisayarların girdiği her yerde vazgeçilmez bir ihtiyaç olarak ortaya çıkmaktadır. Kaynakların paylaşımından çok, kesintisiz şekilde sağlamak önem kazanmıştır. Bunun için kullanılan topolojinin uygunluğu ve verimliliği, bağlantı donanımlarının ayarlanması, kullanılan protokol özelliklerinin iyi tespit edilmesi, güvenliği ve performansı etkileyen faktörlerin bilinmesi gerekir. Bu kapsamda çalışmada yer alan konular, kısaca bilgisayar ağlarında kullanılan yapılar ve yerel ağın iyileştirilmesine yöneliktir.

Bilim Kodu : 5001024
Anahtar Kelimeler : Yerel Bilgisayar Ağı, Performans, Güvenlik
Sayfa Adedi : 97
Tez Yöneticisi : Yrd. Doç. Dr. Halil İbrahim BÜLBÜL

INCREASING OF SECURITY AND PERFORMANCE OF LOCAL AREA NETWORKS
(M.Sc. Thesis)

Hale KESİCİ

GAZİ UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY
June 1999

ABSTRACT

To reach the newest and accurate information has become fairly important in recent years. Computer and enformatik science progress continually and very fast to facilitate obtaining the information that is necessary in a short time. Networks should be established to use information and sources more effectively. These are the structures that enable users to share the existing information and sources available on the separate computers, and to communicate. The power of networks depends on how accurately this structure is used. Today, the use of local area networks is inevitable where computers are used. Providing continuous information has become more important than sharing the sources available on the networks. Availability and proficiency of topology adjustment of the connection hardware, determination of the features of the protocols used and the factors having effect on the security and performance should be precisely known to provide the users with constant share of information. This study focuses on the brief explanation of structures used in the computer networks and the recommendations on the improvement of the networks.

Science Code : 5001024
Key Words : Local Area Network, Performance, Security
Page Number : 97
Adviser : Assist Prof. Dr. Halil İbrahim BÜLBÜL

TEŞEKKÜR

Öncelikle akademik hayata atılmamda büyük desteğini gördüğüm Merhum Doç. Dr. Fazıl DEMİRCİ'yi rahmetle anar, çalışmalarım boyunca yardım ve katkılarıyla beni yönlendiren danışman hocam Sayın Yrd. Doç. Dr. Halil İbrahim BÜLBÜL'e, Sayın Bölüm Başkanım Doç. Dr. Hasan Hüseyin ÖNDER'e, çalışmalarımda teşvik ve desteğini gördüğüm Sayın Dr. Benian TEKİNDAL'a, ayrıca tüm çalışmalarım boyunca her türlü yardım ve özveriden kaçınmayan çok değerli arkadaşım Sayın Araştırma Görevlisi Ahmet KOÇER'e ve bana gösterdikleri sabırdan dolayı çok sevdiğim aileme teşekkürü bir borç bilirim.

ŞEKİLLERİN LİSTESİ

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar

LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
ISO	International Standarts Organization
OSI	Open System Interconnection
UTP	Unshilded Twisted Pair
STP	Shilded Twisted Pair
LLC	Logical Link Control
MAC	Medium Access Control
PDU	Protocol Data Unit
SAPs	Service Access Points
LSAPs	LLC Service Access Points
IEEE	The Institute of Electrical and Electronics Engineers
ARQ	Automatic Repeat Request
ACK	Acknowledged
RR	Receive Ready
REJ	Reject
DBMS	DataBase Management System
HDX	Half Duplex
FDX	Full Duplex
F/FDX	Full/Full Duplex
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection

1. GİRİŞ

İçinde yaşadığımız bilgi çağının bir özelliği olan, en yeni ve en doğru bilgiye en kısa zamanda ulaşma ihtiyacını karşılıyabilmek için bilgisayar ve enformatik bilimi sürekli ve çok hızlı bir biçimde gelişmektedir. Bilgisayarın bir ihtiyaç haline gelmesi, yalnızca iş yerlerinde değil evlerde de yoğun biçimde kullanılmasına neden olmaktadır. Bilgisayarın bu şekilde yoğun kullanılması ve ihtiyaç duyulan bilgilere en kolay ve hızlı bir biçimde ulaşılmasına imkan sağlamasından dolayı bu bilgiler bilgisayarlarda saklanmaya başlanmıştır. Mevcut bilgilerin ve kaynakların daha verimli kullanılması isteği, iletişim ağlarının kurulmasına neden olmaktadır.

Bilgisayar ağı; bilgisayarların birbirleriyle haberleşmeleri, birbirlerine veri aktaramaları için genellikle bir kablo kullanılarak kurulan bağlantıyla oluşturulan sistemdir (Akın, 1996; Çubukcu, 1994; Arslantunalı, 1992).

Ağlarda, veri iletişiminde, iki tarafın da birbirini anlayabilmesi için, önceden kararlaştırılmış bazı kurallara uyması gerekmektedir. Buna iletişim protokolü denir. Fiziksel iletişim, bir kanal olarak kullanılan iletim hattından yapılır. Dört tür hat vardır. Bunlar; Tek yönlü, yarım çift yönlü, tam çift yönlü, tam/tam çift yönlüdür (Intertam, 1997; Erdem, 1996; Collin, 1990).

İletişim ağlarının en yaygın kullanım biçimlerinden biri veri ve bilgi paylaşımını yapabilen sistemler kurmaktır. Bilgi paylaşımında gizlilik ve güvenlilik oldukça önemlidir.

Günümüz bilgisayar ağlarını büyüklüklerine ve kullanım amaçlarına göre: Yerel bilgisayar ağları (Local Area Networks), Metropolitan bilgisayar ağları (Metropolitan Area Networks), Geniş alan bilgisayar ağları (Wide Area

Networks) olarak üç guruba ayrılmaktadır. LAN'lar, bina içerisinde yada bir kaç kilometreden daha büyük alana dağılmamış bilgisayar ağlarıdır. LAN'lara göre daha geniş ve farklı amaçlar için olusturulan MAN'lar; bir şehir yada bir metropolitan üzerine kurulmuş bilgisayar ağlarıdır. WAN'lar ise; ülke kıta hatta dünya çapında kurulmuş olan bilgisayar ağlarıdır. Çünkü geniş çaplı düşünüldüğünde WAN'ların, LAN'lara göre sayısı ve kullanımı azdır. Çünkü LAN'lar bilgisayarın girdiği her yerde artık vazgeçilmez bir ihtiyaç olarak kullanılmaktadır. Bu çerçevede yerel ağların kendi içerisinde hangi sınıfların ve çeşitlerin olduğu tek başına ele alınması gereken bir konudur.

Büyük bilgisayar ağları genellikle onları oluşturan ufak bilgisayar ağlarının özelliklerine sahiptir. Yeni yerel bilgisayar ağları kurulup büyük bilgisayar ağlarının bir parçası oldukça MAN ve WAN'ların da büyüklükleri artar. Bu nedenle, özellikle WAN'ların alt yapı tasarımı çok güç ve çoğu kez plansızdır. Oysa LAN'lar kurulurken detaylı bir çalışma ve analizle bilinçli bir kurulum sağlanmış olur (Arslan, 1995; Networking Technologies, 1994).

Kurulma aşamasında bilgisayar ağının topolojisi, o ağa bağlanacak olan donanımın birbirleri ile matematiksel olarak ne şekilde irtibatlanacağını belirler. Yerel bilgisayar ağlarında kullanılan belli başlı fiziksel topolojiler; yol (bus) topolojisi, halka (ring) topolojisi, yıldız (star) topolojisi, kafes (mesh) topolojisi, hücresel (cellular) topolojisidir (Arslan, 1995; Networking Technologies, 1994; Bilgisayar Pazarı, 1994).

Bir alan içerisinde seçilen uygun bir topoloji kullanılarak ağ oluşturabilmesi için; bağlayıcı (konnektör), ağ iletişim kartları, modemler ayrıca farklı alanlar içeren geniş bir bilgisayar ağı kurulabilmesi için; tekrarlayıcı (repeater), hub, köprü (bridge), çoklayıcı (multiplexer), yönlendirici (router) ve geçit (gateway)'lere ihtiyacı vardır (Networking Technologies, 1994).

Hem yukarıda belirtilen donanım araçlarını hem de bilgisayarları birbirine bağlayan kablolar yapılış tekniğine göre ve yapılan malzemeye göre burgulu çift (twisted pair), korumasız burgulu çift (unshielded twisted pair), korumalı burgulu çift (shielded twisted pair), eş eksenli (coaxiel), fiber optik (fiber optic) olarak farklı isimlerle anılırlar. Bunlardan fiber optik diğerlerine göre bir çok üstünlükleriyle geleceğin teknolojisi olarak görülmektedir (Networking Technologies, 1994; Frank and Derfler, 1996; Bilgisayar Pazarı, 1993).

İletişim ağlarının tasarımını kolaylaştırmak ve farklı standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak amacıyla ISO (International Standarts Organization) tarafından yedi katmanlı bir ağ sistemi olan OSI (Open System Interconnection : Açık Sistem Bağlantısı) referans modeli adı geliştirilmiştir. Ayrıca kullanıcının sahip olduğu donanımın, OSI'nin fiziksel ve veri bağlantı katmanlarını bir standarda sokarak cihazların uyumlu iletişimini sağlayan IEEE (The Institute of Electrical and Electronics Engineers) satandartlarından; IEEE 802.3 CSMA/CD (Carrier-Sense Multiple Access with Collision Detection: Çarpışma Algılamalı Hassas Taşımalı Çoklu Erişim - Ethernet), IEEE 802.4 Token Bus, IEEE 802.5 Token Ring bu çalışmada ele alınmıştır (Stalling, 1993, 1997; Erdem, 1996; Halsall, 1989; Çağıltay, 1995; Tolun, 1994; Oktay, 1997; Bilgisayar Pazarı, 1991).

Yukarıda belirtilen LAN ile ilgili bu ortam erişim teknikleri yani; protokoller veri bloklarının ağ üzerinde iletimiyle ilgilidir. Protokol referans modeli OSI modelinin alt katmanlarıyla ilgilidir ve yüksek katman protokolleri (üçüncü veya dürdüncü katman ve yukarısı) ağ mimarisinden bağımsızdır. Yerel bilgisayar ağları için Mantıksal Bağlantı Kontrol-LLC (Logic Link Control) katmanı diger veri iletim katmalarıyla benzerdir. Diğerleri gibi, LLC de bir "PDU" (protocol data unit)'nun iki istasyon arasında iletimiyle ilgilidir. LLC,

OSI'nin ikinci katman hizmetlerini sağlar. LLC, IEEE 802 protokol modelinin en yüksek katmanıdır. Bu katmanın ilk amacı, yerel ağlar üzerindeki kullanıcıların veri alışverişini sağlamaktır. LLC'nin altında MAC, ağa erişim mantığını sağlar. LLC servisinin farklı çeşitleri, güvenilirlik ve etkili kullanım için oluşturulmuştur. LLC servis biçimleri; onaylanmamış bağlantısız servis, bağlantı modlu servis ve onaylanmış bağlantısız servistir.

Bağlantı (link) kontrol protokollerinde kullanılan çok önemli iki mekanizma; Akış kontrol ve hata kontroldür. Akış kontrol, alıcı tarafın yollayan taraftan etkilenmemesini sağlayan bir tekniktir ve dur ve bekle (stop and wait) ve kayan pencere (sliding window) olmak üzere iki çeşittir. Hata kontrol ise, PDU'ların iletiminde meydana gelebilecek hataların tespitini sağlayan bir tekniktir ve ARQ (Automatic Repeat Request) ile gösterilir. Dur ve bekle (stop and wait) akış kontrolünü destekleyen dur ve bekle ARQ (stop and wait ARQ) ve kayan pencere (sliding window) akış kontrol tekniğine adapte edilmiş N'li geri besleme (go back-N ARQ) olmak üzere iki çeşittir.MAC olarak anılan ortam erişim kontrol tekniğinde kullanılan üç standarda bakmak gerekirse; CSMA/CD, Token Bus, Token Ring'dır. CSMA/CD, yol ve yıldız topolojileri için en geçerli tenkniktir. Bu teknik, ısrarcı olmayan (non-persistent), 1-ısrarcı (1-persistent) ve p-ısrarcı (p-persistent) olmak üzere üç farklı algoritmaya sahiptir. Token Bus için, yol topolojisi üzerindeki istasyonlar mantıksal halka biçimindedir. Fiziksel konumlarına bakılmaksızın mantıksal sıra ve konumlarına bakılarak işlemler yürütülür. Token Ring, halka topolojisi için geçerli bir satandarttır (Stalling, 1997; Schwartz, 1987; Tanenbaum, 1989).

Ayrıca veri bir istasyondan diğerine iletilirken adresleme çok önemlidir. Kullanıcı verisine (sadece veri) LLC'de kontrol bilgileri eklenerek LLC PDU olur, bu PDU MAC'a geçirilir. MAC alıcı istasyonun adresini ekler ve MAC

PDU oluşur, MAC PDU'ya çerçeve (frame) denir (Martin et al., 1994; Stalling, 1993, 1997).

Kapasite, propagasyon gecikmesi, çerçeve (frame) başına düşen bit sayısı, yerel ağ protokolleri, sunulan yük, istasyon sayısı ve kanalın hata oranı LAN performansını etkileyen faktörlerdir.

Her hangi bir yerel bilgisayar ağında sunulan yükün büyüklüğüne bağlı olarak üç işletim bölgesi vardır. Bunlar; ağ boyunca gecikmenin az olduğu bölge, ağ boyunca büyük gecikmelerin olduğu bölge, sınırsız gecikmelerin olduğu bölgedir. Bu işletim bölgelerinden gecikmenin az olduğu bölge kullanıcı tarafından istenen bölgedir (Schwartz, 1987; Stalling, 1993, 1997).

Yerel iletişim ağlarının hızlı gelişiminden dolayı çalışma guruplarının güvenliğini etkileyebilecek unsurlardan kaçınılması gerektiği konusu büyük önem kazanmıştır. Günümüzde her ağın ihtiyaç duyduğu en azından bir güvenlik unsuru vardır. O da yazılım denetimidir. Yazılım denetimi yetkisiz kişilerin yazılımlara (işletim sistemi, uygulama ve hizmet programları vb.) erişmesini önlemeye, dolayısıyla verileri korumaya yönelik bir yöntemdir. Güvenlik konusunda da alınması gereken diğer bir nokta da, ağların güvenliğinin fiziksel olarak aşılmasını önlemek üzere kullanılan donanım birimleri, geri aramalı modemler, fiber optik kablolama, fiziksel korumalı anabilgisayarlar vb. araçlardır. Güvenliğin sağlanabilmesi için hem donanım, hem ağ işletim sistemi, hem de yazılım ayrı ayrı güvenlik barajları kurar. Bunların bir yada bir kaçı aynı anda kullanılarak çok düzeyli ve daha emniyetli iletişim ağlarına sahip olmak da mümkündür. Ancak ne kadar çok düzeyli bir koruma yapılırsa, kurulacak olan ağın maliyetide o kadar artar (Cerit, 1991; Bilgisayar Pazarı, 1991).

2. YÖNTEM VE LİTERATÜR ÖZETLERİ

Bu çalışmada yerel bilgisayar ağlarının güvenlik ve performansının arttırılması ile ilgili mevcut yerli ve yabancı kaynaklar incelenmiştir. Bilgisayar ağının tanımından başlanıp, faydaları, tarihçesi, günümüz bilgisayar ağları ve ağ mimarisini oluşturan ağ topolojileri, kullanılan bağantı donanımları, kablolar ve güvenliği ayrıntılı başlıklar altında incelenmiştir. Daha sonra iletişim ağlarında OSI referans modeli ve donanıma yönelik IEEE 802.X standartları katmanlarıyla incelenip, bu iki standart ilişkilendirilmiştir. Fiziksel katmanın bir üstünde bulunan OSI referans modelinde veri iletim katmanına karşılık gelen LLC ve MAC katmanları; LLC katmanında sunulan servis biçimleri, hata ve akış kontrol mekanizmaları ve bu işlemler için kullanılan algoritmalar verilmiştir. MAC katmanında CSMA/CD, Token Bus ve Token Ring protokollerinde veri iletiminin nasıl yapıldığı incelenmiştir. Yerel ağların performansını etkileyen faktörler ve performans sınırları incelenip, jeton aktarmalı ile CSMA/CD performansları karşılaştırılmıştır.

Konu ile ilgili incelenen literatür aşağıda özetlenmiştir;

Akın (1996), Çubukcu (1994) ve Arslantunalı (1992)'ya göre; Bilgisayarların birbirleriyle haberleşmeleri, birbirlerine veri aktarmaları için genellikle bir kablo kullanılarak aralarında kurulan bağlantıyla oluşturulan bütüne ağ denir.

Arslan (1995) iletişim ağı nedir, niçin gereklidir ? sorusuna;

- Bilginin paylaşımı
- Gizlilik ve güvenlilik
- Kaynakların paylaşımı
- Haberleşme

başlıkları incelemek suretiyle açıklık getirmiştir.

Ön (1994), iletişim ağlarının tarihçesine yani; doğuşu ve gelişimine değinmiş, Erdem (1996) iletişim ağlarının doğuşunun 1960'lı yıllara dayandığını ve bu alandaki gelişmenin çok hızlı yaşandığını belitmiştir.

Ağlarda veri iletişimi ön planda olduğundan, Akgül (1992) ve Şeker (1993), veri iletişimi kısaca bilgisayarlarca kodlanmış bilgilerin bir noktadan diğerine elektiriksel bir iletişim ortamı aracılığıyla taşınması olarak tanımlamışlardır.

Intertam (1997)'da "bilginin değerli olabilmesinin ilk şartı gerektiği zaman kolaylıkla erişebilme isteğine tam anlamıyla cevap verebilmesi" olduğu savunulmuştur. Ayrıca "veri iletiminde, iki tarafın da birbirlerini anlayabilmesi için önceden kararlaştırılmış kurallara iletişim protokolü denildiği" belirtilmiş ve iletim hatlarını şu alt başlıklarada incelemiştir;

Tek yönlü hat
Yarım çift yönlü hat
Çift yönlü yada tam çift yönlü hat
Tam/tam çift yönlü hat.

Collin (1990) ve Erdem (1996) de iletim hatlarını yukarıdaki başlıklar altında toplamışlardır.

Networking Technologies (1994)'de de belirtildiği gibi bilgisayar ağları büyüklüklerine göre ve kullanımlarına göre; yerel bilgisayar ağları, metropolitan bilgisayar ağları ve geniş alan bilgisayar ağları olarak üçe ayrılmaktadır. Buna ek olarak bu eserde yerel bilgisayar ağlarının diğerlerinden farkı ve üstünlüklerine yer verilmiştir.

Bilgisayar Pazarı (1993) ve Networking Technologies (1994)'de bilgisayar ağlarında kullanılan bağlantı donanımları şekillerle tanıtılmıştır. Bağlantıyı sağlayan kablolar resimli bir biçimde; yapılış tekniği, yapıldığı malzeme ve teknik özellikleriyle incelenmiştir.

Ayfer (1996), Oktay (1997), Frank and Derfler (1996) ve Networking Technologies (1994)'e göre; bir parça (segment) içerisinde bir bilgisayar ağı kurabilmek için:

Bağlayıcılar (konnektörler)
Ağ iletişim kartları
Modemler

farklı parçaları (segment) içeren geniş bir bilgisayar ağı kurabilmek için ise ilave olarak:

Tekrarlayıcı (Repeater)
Hub
Köprü (Bridge)
Çoklayıcı (Multiplexer)
Yönlendirici (Router)
Geçit (Gateway)

gibi bağlantı donanımlarına ihtiyaç vardır.

Byte-BBS (1995), bilgisayar ağlarında kullanılan bağlantı donanımlarından modemi her yönüyle ayrıntılı bir şekilde incelemiştir.

Çağıltay (1995), tekrarlayıcı (repeater), köprü (bridge), yönlendirici (router) ve geçit (gateway) gibi bağlantı donanımlarını incelemiştir.

Arslan (1995) ve Oktay (1997) bu baglantı donanımlarını ve bilgisayar ağ topolojilerini incelemiş, ayrıca ISO'nun OSI referans modeline de değinmişlerdir.

Networking Technologies (1994), Pye (1985) ve Langley (1990)'e göre; Bilgisayarları birlirlerine bağlamaya yarayan kablolar yapılış tekniğine ve yapıldığı malzemeye göre;

Burgulu Çift Kablo (Twisted Pair)
Korumasız Burgulu Çift Kablo (Unshielded Twisted Pair)
Korumalı Burgulu Çift Kablo (Shielded Twisted Pair)
Eş Eksenli (Coaxiel)
Fiber Optik (Fiber Optic)

gibi çeşitli isimler alırlar.

Networking Technologies (1994)'de bilgisayar ağ topolojileri şekillerle tanıtılmış, her topolojinin avantaj ve dezavantajları ayrı ayrı belirtilmiştir.

Bilgisayar Pazarı (1994) ve Arslan (1995)'e göre; Bilgisayar ağının topolojisi, o ağa bağlanacak olan donanımın birbiri ile matamatiksel olarak ne şekilde irtibatlanacağıdır. Ağ topoloji çeşitlerini:

Yol (Bus) Topolojisi
Halka (Ring) Topolojisi
Yıldız (Star) Topolojisi
Kafes (Mesh) Topolojisi
Hücresel (Cellular) Topolojisi

olarak incelemişlerdir.

Tolun (1994) OSI referans modelinin, değişik topolojiler ve farklı standartlarda olan bilgisayar ağları arasındaki uyumsuzluğu ortadan kaldırmak amacıyla geliştirildiğini belirtmiştir.

Bilgisayar Pazarı (1991)'de, ISO (International Standarts Organization) tarafından geliştirilen model OSI (Open System Interconnection - Açık Sistem Bağlantısı) referans modelinin; Elektrik mühendisliğinden bilgisayar mühendisliğine uzanan çizgide pek çok kavramı bünyesinde topladığı, iletişim ağlarının tasarımını kolaylaştırmak amacıyla geliştirildiği belirtilmiştir.

Meijer ve Peeters (1983) OSI referans modelinin katmanları olan;

Fiziksel katman
Veri iletim katmanı
Ağ katmanı
Taşıma katmanı
Oturum katmanı
Sunum katmanı
Uygulama katmanı

her biri bir ayrı bölüm olarak incelenmiştir.

Ramos, Schroeder and Beheler (1996) OSI'nin fiziksel ve veri bağlantı katmanlarını bir standarda sokarak cihazların uyumlu iletişimini sağlamak amacıyla, yerel bilgisayar ağları için kablolamayı, topolojileri ve ağ birimlerinin erişim düzenini açıklayan IEEE 802 standartlarının olduğunu belirtmiştir.

Stalling (1993 ve 1997)'in belirttiği gibi "LAN ile ilgili protokoller veri bloklarının ağ üzerinde iletimiyle ilgilidir". Stalling (1993 ve 1997) IEEE 802 modeli ile OSI referans modelini ilişkilendirmiş, LLC ve MAC seviyelerini

ayrı ayrı incelemiştir. Verinin iletiminde adreslemeye genel olarak değinmiştir. LLC seviyesinde yapılan hata ve akış kontrol işlemlerinde kullanılan teknikleri şekillerle tanıtmıştır. MAC seviyesinde ise CSMA/CD (Ethernet), Token Bus ve Token Ring protokollerini ayrı ayrı incelemiştir. Ortam erişimlerinde kullanılan algoritmaları şekillerle tanıtmış, jeton kullanımı ve karşılaşılabilecek durumları örnekleyerek şekillerle anlatmıştır. Verinin taşıdığı adres ve bilgi alanlarını göstermiştir.

Stalling (1993 ve 1997) LAN performansına da değinmiştir. Ayrıca;

Kapasite
Propagasyon gecikmesi
Çerçeve (frame) başına düşen bit sayısı
Yerel ağ protokolleri
Sunulan yük
İstasyon sayısı

performans için önemli faktörler olarak ele almış ve performans sınırlarını üç bölgeye ayırmıştır. Protokolleri performans açısından karşılaştırmış ve çeşitli örneklerle protokollerin etkinliklerini grafiklerle göstermiştir.

Bilgisayar Pazarı (1996) LAN performansını iyileştirmeye yönelik ipuçları vermiştir.

Tanenbaum (1989) genel olarak; LLC servis biçimlerini, hata ve akış kontrol tekniklerini, CSMA/CD (Ethernet), Token Bus ve Token Ring protokollerini ve kullanılan algoritmaları incelemiştir.

Halsall (1989) ve Schwartz (1987) genel olarak; Bağlantı donanımları, ağ topolojileri, OSI referans modeli ve LLC seviyesinde hata ve akış kontrol

teknikleri, CSMA/CD (Ethernet), Token Bus ve Token Ring protokolleri, çerçeve yapısı (frame format) gibi konulara yer vermişlerdir.

Held (1993) ve Naugle (1991) Local Area Networking adlı çalışmalarında yerel ağ protokollerini incelemişlerdir.

Martin, Chapman and Leben (1994) OSI referans modelini IEEE 802 modeliyle ilişkilendirmiş, LLC servis biçimlerine, hata ve akış kontrol tekniklerine yer vermiştir.

Henshall and Shaw S. (1989) LLC ve MAC katmanlarına ayrı ayrı değinmiş, Üstüner (1995) LLC seviyesinde hata ve akış kontrol tekniklerine değinmiştir. Smith ve Udell (1993) hata kontrol tekniklerine yer vermişlerdir.

Cerit (1991) iletişim ağlarının güvenliğinde virüslerden korunmanın önemine değinmiştir. Bilgisayar Pazarı (1991) güvenliğin her ağ için gerekli olduğunu ancak LAN'dan LAN'a farklılıklar gösterebileceği belirtilmiş, güvenlik yazılım ve donanım açısından ayrı ayrı ele alınmıştır.

Aydın (1992) Bilgisayar, Bilgi İşlem ve Telekomünükasyon, Bilişim Sistemleri Sözlüğü adlı eserinde elektronik ve bilgisayar ile ilgili terimlerin kısa açıklamalarını vermiştir.

3. BİLGİSAYAR AĞLARI

Bu bölümde bilgisayar ağının tanımına, doğuşu ve gelişimine, faydalarına değinilmiş olup günümüz bilgisayar ağları tanıtılmış ve birbirlerine göre farklılıkları verilmiştir. Bilgisayar ağlarının mimarisi; Ağ topolojileri ile bu topolojilerde kullanılan bağlantı donanımları tanıtılmıştır. Dördüncü bölümde ilişkilendirilip bir katmanı incelenecek olan OSI referans modeli ve IEEE 802.X standartlarına niçin ihtiyaç duyulduğu hakkında bilgi verilmiştir.

3.1. Ağ Tanımı

Bilgisayarların birbirleriyle haberleşmeleri, birbirlerine veri aktarmaları için genellikle bir kablo kullanılarak aralarında kurulan bağlantıyla oluşturulan bütün, ağ olarak isimlendirilir. Bir başka deyişle bilgisayar ağı, birbirine bağlı (interconnected) bir çok bağımsız bilgisayar anlamına gelir. İki bilgisayarın birbirinin kaynaklarını (diskini yada diskinde yer alan bilgilerini, verilerini, programlarını vb.) ortak kullanabilmesi onların birbirine bağlı olduğunu gösterir. Aradaki bu bağ yani iletişim ortamı, kablo ile olabileceği gibi laser, mikro dalga ve uydular aracılığı ile de olabilir. Ağlar, yan yana duran iki bilgisayar arasında gerçekleştirilebileceği gibi, ülke yada dünya üzerine yayılmış bir çok bilgisayar arasında da gerçekleştirilebilir (Akın, 1996; Çubukcu, 1994; Arslantunalı, 1992).

Başlangıcı çok eskiye dayanmamasına rağmen yerel iletişim ağarındaki gelişmeler çok hızlı yaşandı. 1950'li yıllarda çok pahalı ve az kullanıcıya hizmet eden ilk bilgisayarlar mainframelerdi. Kullanıcının bilgi ve komutlarını bir kart aracılığıyla kabul eden bir sistem vardı. İlgili bilgisayar elemanlarınca girilebilen bu kartlardaki bilgi ve komutların cevabı ertesi gün yazılı döküm

olarak alınabiliyordu. Bir karttaki bir hatalı kodlama günlere mal oluyordu. Bu sistemde yazıcı gibi kaynakların paylaşımı söz konusu değildi.

1960'lı yıllarda zaman paylaşımı kavramının ortaya çıkmasıyla, aptal terminallerin telefon hattı üzerinde modemler aracılığıyla mainframelere bağlanması mümkündü ancak bilgi gönderiminin yavaşlığı sorun olmaktaydı.

1970'li yıllarda bilgisayar fiyatlarının düşmesiyle bir çok yere bilgisayar girmiştir. Aynı bölümde sistem gerektiği gibi çalışıyordu, ancak farklı bölümlere bağlantı yapılması istendiğinde problem çıkıyordu. Sonunda kablo bağlantıları ile bilgisayarlar birbirlerine bağlandı ve birimleri için bağlantı programları yazılmaya başlandı.

1973'de Rank Xeros'un ilk Ethernet'i geliştirmesi ile doğan yerel iletişim ağ teknolojisi, günümüzde en hızlı büyüyen pazarlardan birisi oldu. Bu kadar büyük ilgi görmesinin nedenleri arasında sağladığı yüksek hız, esneklik gibi pek çok istenen özelliği içermesidir. Böylece LAN (Local Area Network) mantığı ortaya çıkmış oldu (Erdem, 1996; Ön, 1994).

Bilgisayar ağlarının faydalarına değinilecek olunursa genel olarak;

Bilginin paylaşımı: İletişim ağlarının en yaygın kullanım biçimlerinden biri veri ve bilgi paylaşımını yapabilen sistemler kurmaktır. Bu amaçla kurulan iletişim ağlarında, merkezi bir bilgisayara yüklenmiş olan bir veri tabanı uzaktaki kullanıcılar tarafından paylaşılır. Ağ seviyesinde pek çok kullanıcı aynı veri veya bilgiye aynı anda ulaşabilir, yetkili kullanıcılar bu veri veya bilgileri değiştirebilir veya yeni veri girişi yapabilirler, yetkisiz kullanıcıların bu veri veya bilgilere zarar vermesi ve hatta ulaşması bile yasaklanabilir. Bu tür iletişim ağları çoğunlukla bir veri tabanı yönetim sistemi (DBMS -

DataBase Management System) ile desteklenir. Veri tabanı yönetim sistemi, uzak kullanıcıların tek bir merkezi veri tabanından yararlanmasını sağlar. Bu sayede böyle bir sistem kurulurken, kullanılan ağ işletim sisteminin, veri tabanı yönetim sistemini destekliyor yada onunla uyumlu çalışabiliyor olmasına dikkat etmek gerekmektedir.

Gizlilik ve güvenlik: Ağa bağlı bir bilgisayarın sabit diskindeki bilgilere sadece o kullanıcı ve ağa bağlı bir kaç kullanıcının erişmesi, diğer kullanıcıların bu bilgilere ulaşamaması sağlanabilmektedir. Güvenliğin sağlanabilmesi için hem donanım, hem ağ işletim sistemi, hem de yazılım ayrı ayrı güvenlik barajları kurar. Bunların bir yada bir kaçı aynı anda kullanılarak çok düzeyli ve daha emniyetli iletişim ağlarına sahip olmak da mümkündür. Ancak ne kadar çok düzeyli bir koruma yapılırsa, kurulacak olan ağın maliyeti de o kadar artar.

Kaynakların paylaşımı: Bir iletişim ağı sayesinde, mevcut kaynakların, yani; bütün bilgisayarlardaki sabit diskler, programlar, yazıcılar, CD-ROM sürücüler gibi tüm yazılım ve donanım öğelerinin, en verimli ve en etkili şekilde kullanılması sağlanır. Mevcut kaynaklar bütün bilgisayarlarda eşit olmayabilir. Bütün bilgisayarlarda kaynak arttırımına gitmek çok büyük masraflara yol açacaktır. Oysa bir iletişim ağında büyük bir sabit diske sahip bir bilgisayar vardır. Bütün programlar bu sabit diske kurulur ve iletişim ağındaki diğer kullanıcılar bu bilgisayardan çalıştırırlar. Böyle bir yapının en önemli iki avantajından birincisi, ağdaki bütün bilgisayarlara büyük birer sabit disk koymak yerine, yalnızca kendi verilerini saklayacakları küçük birer sabit disk koyarak maliyeti azaltmaktır, ikincisi ise; yeni program uyarlamasının güncellenmesini yalnızca bu bilgisayar üzerinde yaparak bütün ağ kullanıcılarının yeni uyarlama programları aynı anda kullanmaya başlamasını sağlamak olacaktır. Bu özellik, yapı içerisinde standardizasyonun sağlanması için önemli bir avantaj sağlar. Bir kullanıcı eski uyarlama program, diğeri yeni

uyarlama program kullanırsa, birbirleri arasında veri aktarımı zorlaşır, hatta bazen imkansız hale gelebilir.

Haberleşme: Artık insanlar birbirleriyle en hızlı şekilde haberleşme ihtiyacı içerisindedir. Zaman, çoğu kez herkesi en çok ilgilendiren birim haline gelmiştir. Böyle bir yaşam süreci içerisinde, insanların birbirleriyle kurdukları iletişimin en hızlı şekilde sağlanması kaçınılmaz bir istek olmuştur. İletişimin çok çeşitli yöntemleri bilgisayar tarafından desteklenir hale gelmiştir. Bilgisayar ağları tanıtım ve reklam için de oldukça önemlidir. Bağlantıları, dünyanın dört bir yanına kadar ulaşmış olan iletişim ağları sayesinde yalnızca büyük firmalar değil, üniversiteler yada kamu kuruluşları da tanıtımlarını yapmaktan geri kalmamışlardır (Çubukcu, 1994; Arslan, 1995).

3.2. Veri İletişimi ve İletim Hatları

Bilginin değerli olabilmesinin ilk şartı gerektiği zaman kolaylıkla erişebilme isteğine tam anlamıyla cevap verebilmesidir. Aksi takdirde dağınık halde bulunan ve gerektiği gibi erişilemeyen bilgi amaca hizmet edemediği için değerini yitirir. Uzak mesafeler arasında hemen hemen anında denebilecek kısa sürelerde bilgi alış verişi sağlanmalıdır.

Veri iletişimi kısaca bilgisayarlarca kodlanmış bilgilerin bir noktadan diğerine elektiriksel bir iletişim ortamı aracılığıyla taşınmasıdır. Uzak mesafeleri mantıksal olarak sıfıra indiren veri iletişim uygulamaları günümüzde bir çok alana girmiştir (Şeker, 1993; Akgül, 1992; Intertam, 1997).

Veri iletişiminde, iki tarafın da birbirini anlayabilmesi için, önceden kararlaştırılmış bazı kurallara uyması gerekmektedir. Buna iletişim protokolü denir.

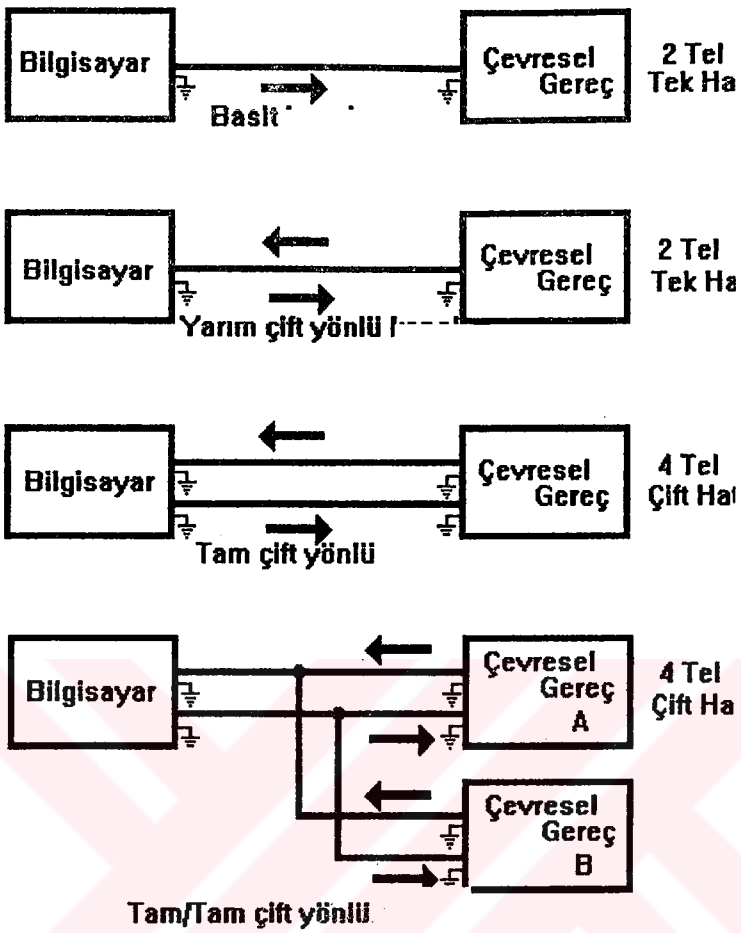
Fiziksel iletim, iletim hattından yapılır. İletim hattı da bir kanal olarak farklı biçimlerde kullanılabilir. Şekil 3.1'de de görüldüğü gibi temelde dört tür hat vardır;

Tek yönlü hat: Bilginin yalnızca tek bir yönde akmasına izin verir. Bilginin alınan çevresel gereç tarafından geriye bilgi göndermesi yoktur. Bu hat noktadan noktaya olduğu gibi merkezden çeşitli noktalara da gönderme yapabilir. İki telli tek hattan oluşur.

Yarım çift yönlü hat (HDX): İki nokta arasında bilgi alışverişi, aynı anda iki yönde olmamakta, yanlız eş zamanlı olarak yapılabilmektedir. Bu da iki telli tek hattan oluşur.

Tam çift yönlü yada çift yönlü hat (FDX veya DX): Bu hatta bilgiler hem iki yönde hem de aynı anda hareket ederler. Bu hatda iletimde herhangi bir kesiklik söz konusu değildir. Çift yönlü haberleşme yapılabilir. Hat sayısı tek yönlü ve yarım çift yönlüye göre iki kattır. Dört telli iki hattan oluşur.

Tam/Tam çift yönlü hat (F/FDX): Aynı anda bilgisayarın çevresel gerece bilgi yollarken başka bir çevresel gerecin bilgisayardan bilgi almasıdır. Yada bilgisayar çevresel gereçten bilgi alırken aynı anda başka bir çevresel gerece bilgi yollaması da olabilir (Intertam, 1997; Erdem, 1996; Collin, 1990).



Şekil 3.1. İletim hatları

3.3. Günümüz Bilgisayar Ağları

Günümüz bilgisayar ağlarını büyüklüklerine ve kullanımlarına göre üç guruba ayırmak mümkündür. Bunlar;

1 - Yerel bilgisayar ağları (Local Area Networks)

2 - Metropolitan bilgisayar ağları (Metropolitan Area Networks)

3 - Geniş alan bilgisayar ağları (Wide Area Networks)

3.3.1. Yerel bilgisayar ağları (Local Area Networks)

Bina içerisinde iletişim cihazları ile birbirine bağlı bilgisayarlar ve yazılımlarını ifade eder. Yerel bilgisayar ağına bağlı bilgisayarlar, bir yada bir kaç kilometreden daha büyük alana dağılmamıştır. Veri iletişim hızı genellikle 1 Mbps hızından daha yüksektir.

3.3.2. Metropolitan bilgisayar ağları (Metropolitan Area Networks)

Bir şehir yada bir metropol üzerine kurulmuş bilgisayar ağıdır. Metropolitan bilgisayar ağları genellikle bir kaç mevcut yerel bilgisayar ağının birleştirilmesi sonucu kurulan ağlardır.

3.3.3. Geniş alan bilgisayar ağları (Wide Area Networks)

Geniş alan bilgisayar ağları ülke, kıta hatta dünya çapında kurulmuş olan bilgisayar ağlarıdır. Ağırlıklı olarak iletişim ve bilgi alış verişinde kullanılır ve mevcut metropolitan ağların birleşmesi ile oluşturulurlar.

Performans açısından yerel bilgisayar ağlarının diğerlerinden en önemli farkı ve üstünlüğü, bilgisayar ağının sahibi olanların bilinçli bir kurulum ve kullanımla LAN performansını yükseltmesi mümkündür.

Hemen hemen bütün yerel bilgisayar ağlarında yüksek hızlı bir omurga (backbone) olur. Omurga bir bilgisayar ağının temel bağlantısını oluşturur ve ne kadar hızlı olursa bilgisayar ağı da okadar hızlı olur. Öte yandan, omurgaya bağlı olan fakat kendi içlerinde omurgadan bağımsız çalışabilme imkanına sahip olan, bilgisayarları birbirine bağlayan hatlara parça manasına gelen "segment" adı verilir.

Bir başka nokta da, hızın kullanıcı sayısıyla ters orantılı olduğudur. Büyük bilgisayar ağlarında daha çok kullanıcı ve bilgisayar ağa bağlı olacağından, bilgisayar ağının hızı da azalacaktır.

Yerel bilgisayar ağlarının diğerlerinden bir başka farkı ise; planlamanın daha ciddi bir biçimde yapılmasıdır. Büyük bilgisayar ağları genellikle onları oluşturan ufak bilgisayar ağlarının özelliklerine sahiptir. Yani yerel bilgisayar ağlarının performansına bağımlıdır. Yeni yerel bilgisayar ağları kurulup büyük bilgisayar ağlarının birer parçası oldukça, MAN ve WAN'ların da büyüklükleri artar. Bu nedenle belki metropolitan ağların değil, özellikle geniş alan bilgisayar ağlarının alt yapı tasarımı çok güç ve çoğu kez plansızdır. Oysa yerel bilgisayar ağı kurulurken, önce detaylı bir çalışma ve mali analiz yapılır. Bu sayede hem bütçeye uygun bir ağ kurulur, hem de kurulacak olan ağ planlı aşamlarla belli bir sistematiğe sahip olur. Böylece en yüksek performans sağlanmış olur (Arslan, 1995; Networking Technologies, 1994; Aydın, 1992).

3.4. Bilgisayar Ağlarında Kullanılan Bağlantı Donanımları

Bir parça (segment) içerisinde bir bilgisayar ağı kurabilmek için aşağıda belirtilen türde donanımlara ihtiyaç vardır:

1- Bağlayıcılar (konnektörler)
2- Ağ iletişim kartları
3- Modemler

Ayrıca farklı parçaları (segment) içeren geniş bir bilgisayar ağı kurabilmek için ise ilave olarak şu tür cihazlar gerekmektedir:

1- Tekrarlayıcı (Repeater)

2- Hub

3- Köprü (Bridge)

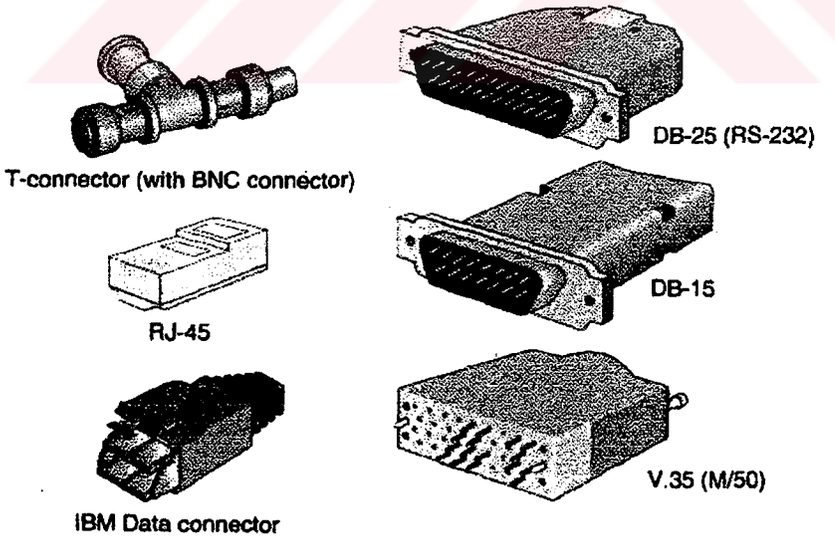
4- Çoklayıcı (Multiplexer)

5- Yönlendirici (Router)

6- Geçit (Gateway)

3.4.1. Bağalyıcılar (konnektörler)

Her ortamda ortama özgün çeşitli sayıda fiziksel bağlayıcılar (konnektörler) kullanılmaktadır. Donanımların bağlantısı yapılırken ilk yapılması gereken işlem, bağlayıcıların kablolara bağlantısının bağlayıcılarla yapılması işlemidir. Ağ bağlantılarında kullanılan çeşitli bağlayıcılar Şekil 3.2'de görülmektedir (Networking Technologies, 1994).



Şekil 3.2. Ağ bağlantılarında kullanılan çeşitli bağlayıcılar

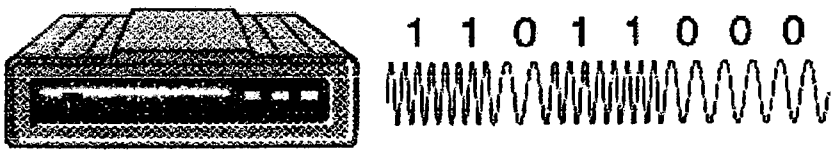
3.4.2. Ağ iletişim kartları

Bir diğer bağlantı cihazı da ağ iletişim kartlarıdır. Teknik olarak bir ağ iletişim kartı kablo ile bilgisayar arasındaki tüm fiziksel ve mantıksal bağlantıları gerçekleştirir. Basit olarak ağ iletişim kartı ağ kablosu ile bağlantı yapabilmek için ağa bağlanacak cihaz içerisine takılan karttır (Networking Technologies, 1994; Frank and Derfler, 1996).

3.4.3. Modemler (MOdulator/DEModulator)

Bilgisayarlarda bulunan sayısal işaretleri (dijital sinyalleri) alıp, telefon hatları yada radyolink (mikrodalga) taşıyıcılarda taşınmak üzere örneksel işaretlere (analog sinyallere) çeviren cihazlardır. Aynı zamanda bunun tersi işlemleri de yerine getirmekle yükümlüdürler. Harici (externel) ve dahili (internal) olmak üzere iki çeşittir. Şekil 3.3'de harici bir modem görülmektedir.

Bir şehrin farklı iki noktasında bulunan bilgisayarları bir birine bağlamak için telefon hatları kullanılır. İşaretleri telefon hattına ulaştırabilmek ve alabilmek için ise modemleri kullanmak gerekmektedir (Networking Technologies, 1994; Halsall, 1989; Modem ve Kullanımı, 1995).

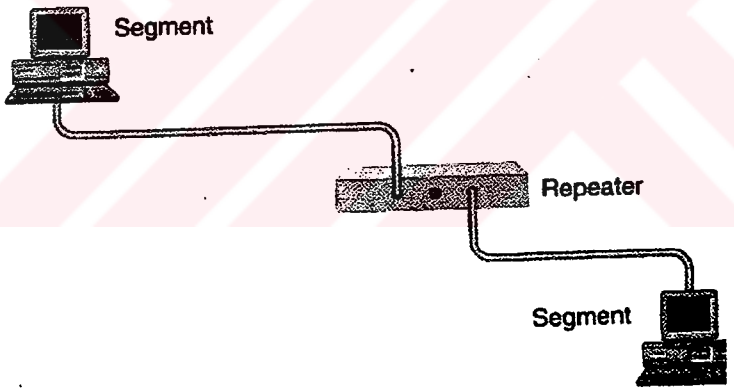


Şekil 3.3. Modem

3.4.4. Tekrarlayıcı (Repeater)

Elektirik işaretleri iletim hattı boyunca yol alırken zamanla zayıf işaretlere dönüşürler. Her kablo tipinde kullanılabilecek değişik aralıklar mevcuttur. Bu mesafe sorununu aşabilmek için tekrarlayıcı (repeater) adı verilen işaret güçlendirici cihazlar kullanılır. Şekil 3.4'de görüldüğü gibi tekrarlayıcı (repeater) sayesinde ağın uçtan uca uzunluğu iki katına uzatılmış olur.

OSI referans modeline göre en alt katman olan fiziksel katmanda çalışır ve bu nedenle ağ üzerindeki bilgisayarlara görünmez ve her hangi bir tampon (buffer) yada sakla-ve-ilet (store-and-forward) özelliği yoktur (Arslan, 1995; Networking Technologies, 1994; Çağıltay, 1995; Aydın, 1992).



Şekil 3.4. Tekrarlayıcı

3.4.5. Hub

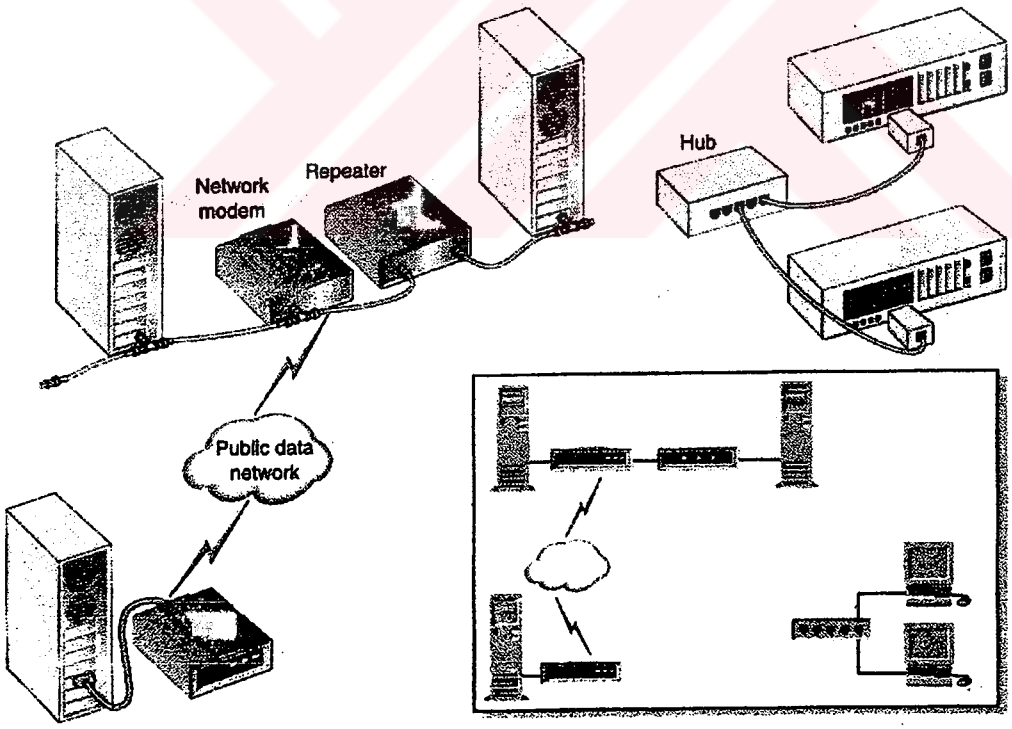
Yıldız topolojisini kullanan bilgisayar ağlarında merkezi bir noktaya ve bu noktada bağlantıların yapılamsını sağlayacak bir cihaza ihtiyaç vardır. Merkezi noktadaki bu cihaza Hub, multiport repeater veya concentrator adı verilir. Şekil 3.5'de bir Hub bağlantısı görülmektedir.

Hubların üç değişik modeli mevcuttur. Bunlar sırasıyla;

Pasif Hublar: Bu tür hublarda yalnızca bağlantı olayı gerçekleştirilir. İşaret güçlendirilmesi veya tekrarlanması yapılmaz.

Aktif Hublar: Pasif hublar gibi bağlantı merkezleridir. Farklı olarak bir çıkışa gelen işaret diğer çıkışlara güçlendirilerek verilir.

Akıllı Hublar: Bu tür hublarda işaret güçlendirmesine ilave olarak ağ yönetimi, akıllı yol seçimi, işaret dağıtımı için yön seçimi ve farklı parça yaratabilme gibi özellikleri de mevcuttur (Networking Technologies, 1994; Oktay, 1997).

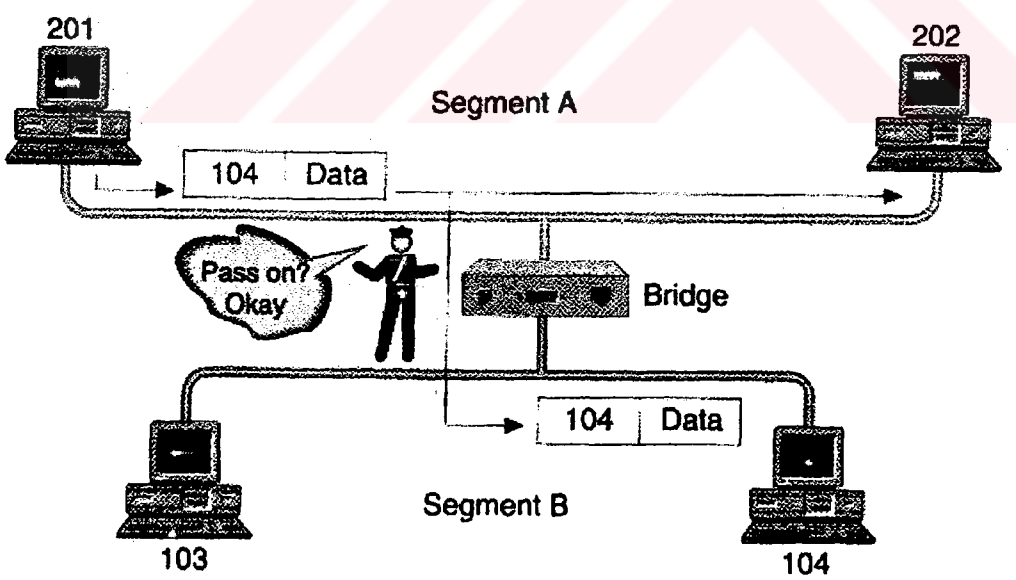


Şekil 3.5. Hub bağlantısı

3.4.6. Köprü (Bridge)

Şekil 3.6'da da görüldüğü gibi köprü (bridge); bir bilgisayar ağını birden fazla parçaya (segment) bölebilmek için kullanılan cihazlardır. Köprüler (bridge) işaretlere bakarak bir parçadan (segment) diğerine geçip geçemiyeceğine karar verirler. Farklı parçaların (segment) oluşturulması ağ trafiğini azaltacağı için ağ performansı da doğal olarak artacaktır.

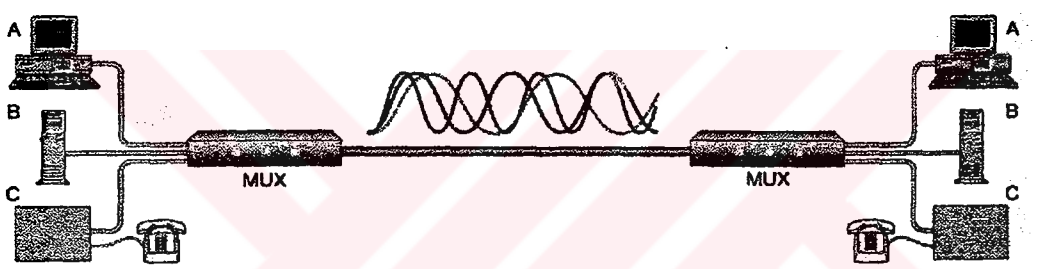
OSI referans modeline göre ikinci katman olan veri iletim katmanında ve sakla-ve-ilet mantığıyla çalışır. Bir parçadan (segment) gelen paketleri saklar, içlerindeki adres bilgilerine bakarak diğer parçaya (segment) gitmesi gereken paketleri geçirir, diğer paketleri geçirmez (Arslan, 1995; Networking Technologies, 1994; Çağıltay, 1995; Aydın, 1992).



Şekil 3.6. Köprü kullanımı

3.4.7. Çoklayıcı (Multiplexer)

Arasıra kullanılan bir ağ iletişim hattının yalnızca bir tek işaret tarafından meşgul edilmesi yerine çoklayıcı (multiplexer) adı verilen cihazlar kullanılarak bu hattın paylaşılabilmesini sağlayabiliriz. Böylece mevcut olan band genişliğini daha tasarruflu olarak kullanabiliriz. Çoklayıcılar (multiplexer) iki yada daha fazla farklı işaretleri bir iletişim hattından geçirebilirler. Çoklayıcı (multiplexer) kullanımı Şekil 3.7'de görülmektedir (Networking Technologies, 1994; Aydın, 1992).

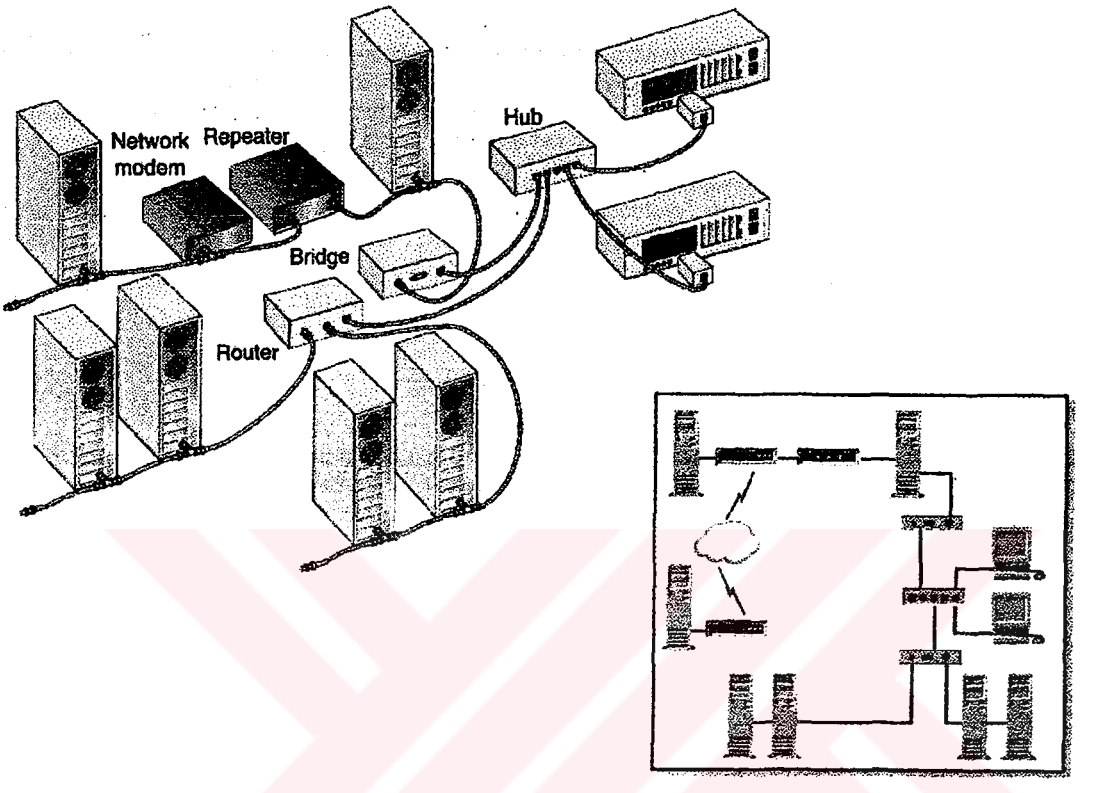


Şekil 3.7. Çoklayıcı

3.4.8. Yönlendirici (Router)

Yönlendiriciler (router) iki yada daha fazla farklı mantıksal ağları bir birine bağlamaya yarayan donanım birimleridir. Görevi, büyük yerel bilgisayar ağlarında paketlerin yollarını kaybetmeden gidecekleri adreslere ulaştırılmasıdır. Yönlendirici (router) kullanımı Şekil 3.8'de görülmektedir.

OSI referans modeline göre üçüncü katman olan ağ katmanda çalışır. Köprüden (bridge) ayrılan en önemli özelliği yönlendiricinin (router) paket uzunluğunu değiştirebilmesidir (Networking Technologies, 1994; Çağıltay, 1995).



Şekil 3.8. Yönlendirici kullanımı

3.4.9. Geçit (Gateway)

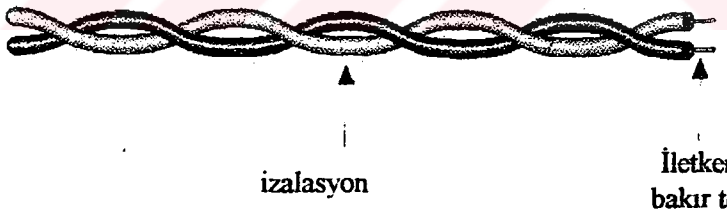
Görevi birbirinden farklı topoloji, veri iletişim yöntemleri, paket uzunluğu ve protokollere sahip ağları birbirine bağlamaktır. Bu sebeple en yaygın kullanımı bir yerel bilgisayar ağının bir geniş alan bilgisayar ağına yada iki geniş alan bilgisayar ağının birbirine bağlanması için kullanılmasıdır. OSI referans modeline göre dördüncü katman olan taşıma katmanında çalışır (Arslan, 1995; Çağıltay, 1995; Ayfer, 1996; Aydın, 1992).

3.4.10. Kablolar

Bilgisayarları birlirlerine bağlamaya yarayan kablolar yapılış tekniğine ve yapıldığı malzemeye göre farklı isimler alırlar.

3.4.10.1. Burgulu çift kablo (twisted pair)

Bu tür bakır tel kullanılarak geliştirilmiş iletişim kablolarında en genel yeri oluşturan kablo türüdür. Bakır teller iyi bir elektron taşıyıcıdırlar. Fakat kapalı bir ortamda elektrik işareti taşıyan iki bakır tel biraraya getirildiğinde ortaya eletromanyetik etkileşim (interference) çıkar. Buna çaprazlaşma (crosstalk) adı verilir. Bu yüzden kablolar sarmal hale getirilerek bu etki azaltılmaya çalışılır. Şekil 3.9'da da görüldüğü gibi burgulu çift (twisted pair) kablolar 22 yada 26 ayar bakır tellerin birbirlerine sarılmasıyla meydana getirilir (Networking Technologies, 1994; Halsall, 1989).



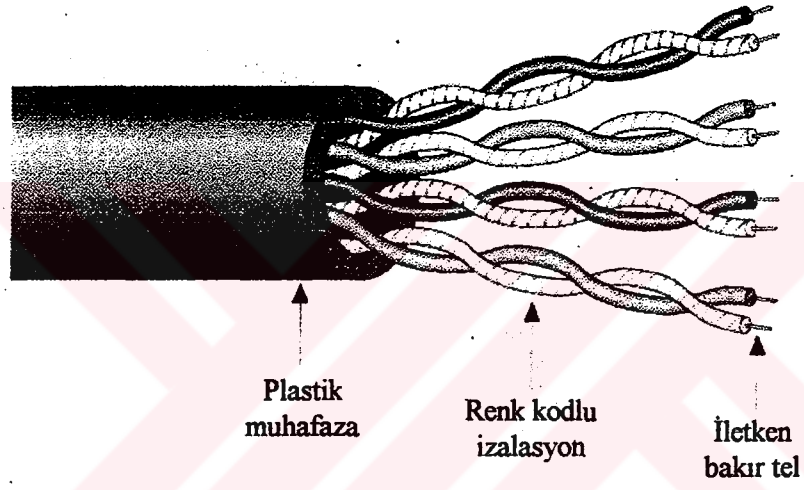
Şekil 3.9. Burgulu çift kablo

3.4.10.2 Korumasız burgulu çift kablo (unshielded twisted pair)

Şekil 3.10'da da görüldüğü gibi bu kablo tipi basit bir plastik muhafaza içerisine çok sayıda burgulu çift (twisted pair) kablo konulmasıyla oluşturulmuş bir kablo türüdür.

UTP adı ile bilinen bu kablo tipi genellikle telefon sistemlerinde de sıkça kullanılmaktadır. Bilgisayar ağlarında tip (category) 3 ve tip (category) 5 UTP kablo türleri yaygın olarak kullanılmaktadır. Tip 5'de ağ performansını artırıcı ilave özellikler (daha fazla sarmal kablo ve daha iyi izalasyon) konulmuştur.

Diğer kablo türlerine göre ucuzdur. Kurulumu oldukça kolaydır. 1 ile 100 Mbit/s veri iletişim hızına çıkabilir. Manyetik dalgalardan etkilenir (Networking Technologies, 1994).



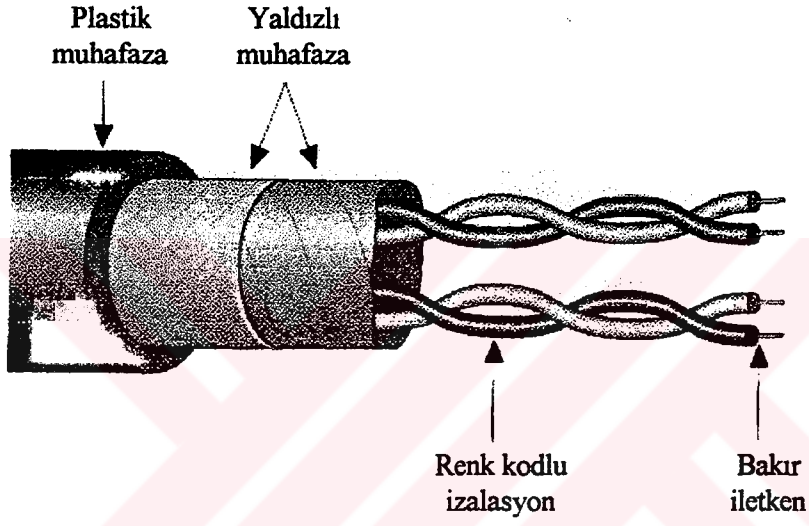
Şekil 3.10. Korumasız burgulu çift kablo

3.4.10.3. Korumalı burgulu çift kablo (shielded twisted pair)

Günümüzde UTP tipi kablolama oldukça yaygın olmasına rağmen STP tipi kablolar da hala mevcuttur.

Şekil 3.11'de görüldüğü gibi bu tip kablolarda sarmallar yaldızlı bir kağıt ile sarılarak koruma altına alınmışlardır. Apple ve IBM'e ait bazı iletişim techizatları bu tür kablo çeşidini kullanmaktadır.

UTP kabloya göre biraz pahalı olmakla beraber thick coax ve fiber kablolardan ucuzdur. Kurulumu UTP'ye göre daha zordur. Teorik olarak 100 metre içerisinde 500 Mbit/s'e kadar çıkabileceği söylenmektedir, fakat bugüne kadar 155 Mbit/s üzerine çıkılmış değildir. Genel olarak 16 Mbit/s olarak kullanılmaktadır. UTP'ye göre manyetik dalgalardan daha az etkilenir (Networking Technologies, 1994; Frank and Derfler, 1996).



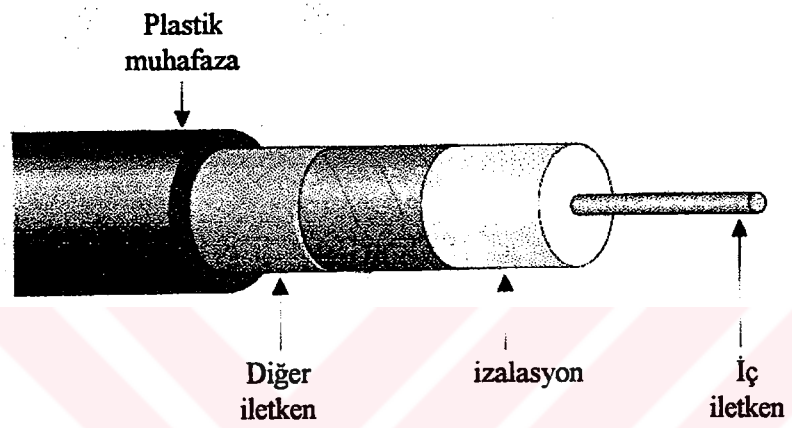
Şekil 3.11. Korumalı burgulu çift kablo

3.4.10.4. Eş eksenli kablo(coaxiel)

Genellikle koaks adı ile anılır. Bir ekseni paylaşan iki taşıyıcı telden imal edilmiştir. (Common axis = "Co", "axis")

Şekil 3.12'de de görüldüğü gibi bu tip kablonun orta kısmında kalın bir plastik muhafaza içerisine alınmış sert bir bakır tel mevcuttur. Bu plastik muhafazanın dışı ikinci bir tel sarmalı tarafından kaplanmıştır. Kablonun tamamı ayrıca bir plastik muhfaza tarafından izole edilmiştir.

Thin coax kablonun maliyeti STP'ye göre, tip 5 UTP kabloya göre ve fiber kabloya göre daha ucuzdur, fakat thick coax kablonun maliyeti STP ve tip 5 UTP'ye göre daha pahalıdır. Kurulumu kolaydır. Kapasitesi 10 Mbit/s'dir. Manyetik alandan ve elektrik alanlarından etkilenir (Networking Technologies, 1994; Halsall, 1989; Pye, 1985).

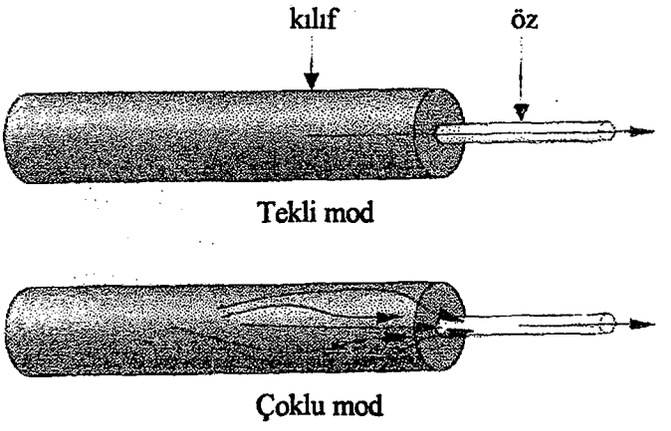


Şekil 3.12. Eş eksenli kablo

3.4.10.5. Fiber optik kablo (fiber optic)

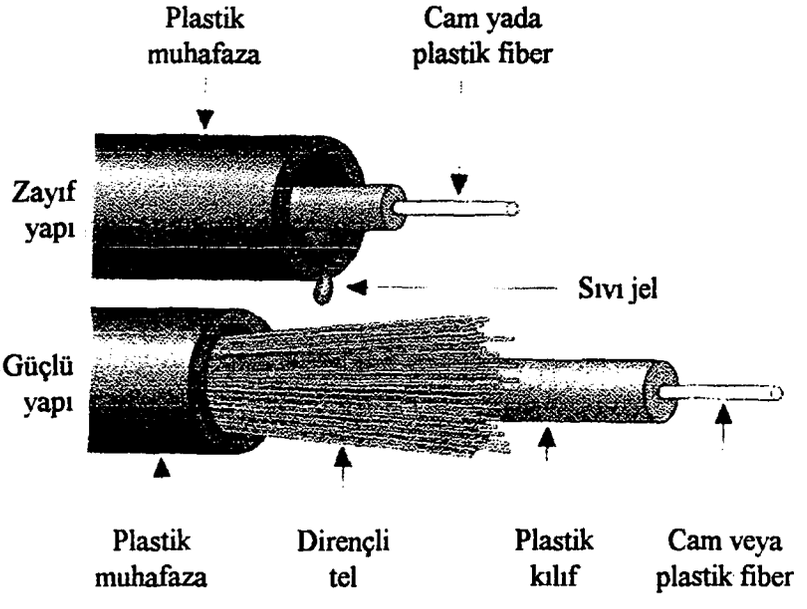
Şekil 3.14'de görülen fiber optik kablolar ışığı taşıma kabiliyeti olan plastik yada cam materyallerden yapılmışlardır. Kablonun merkezinde bulunan çekirdek ışığın ilerleyebileceği bir yol oluşturur. Dış kısım plastik bir muhafaza içerisine alınmıştır. Plastik muhafaza içerisinde bulunan her ışık geçirgen tel ışık geçirmeyen bir materyal yada kılıfla kaplanmıştır.

Şekil 3.13'de de görüldüğü gibi fiber optik kablolar çoklu mod (multi-mode) ve tekli mod (single-mode) olarak ikiye ayrılırlar. Tekli mod (single-mode) fiber optik kablolar yalnızca bir tek ışık yolu oluşturabilecek şekilde tasarlanmışlardır. Çoklu mod (multi-mode) fiber optik kablolar ise birden fazla ışık demetini üzerinden birbirlerine karışmadan geçirebilirler .



Şekil 3.13. Fiber optik kablo çeşitleri

Fiber optik kablolar ve bağlayıcıları diğer kablo tiplerine göre oldukça pahalıdır. Kurulumu oldukça zordur ve uzmanlık gerektirir. 100 Mbit/s ile 2 Gbit/s arasında iletişim hızına sahiptir ve 2 ila 25 kilometre mesafelere kadar kullanılabilir. Manyetik alandan ve elektrik alanlarından kesinlikle etkilenmez. Bu özellikleriyle fiber optik kablolar geleceğin teknolojisi olarak görülmektedir (Networking Technologies, 1994; Langley, 1990; Bilgisayar Pazarı,1993).



Şekil 3.14. Fiber optik kablo

3.5. Bilgisayar Ağ Topolojileri

Bilgisayar ağının topolojisi, o ağa bağlanacak olan donanımın (hizmet cihazları, kullanıcı bilgisayarları, yazıcılar vb.) birbiri ile matematiksel olarak ne şekilde irtibatlanacağını belirler. Yerel bilgisayar ağlarında kullanılan belli başlı fiziksel topolojiler şunlardır:

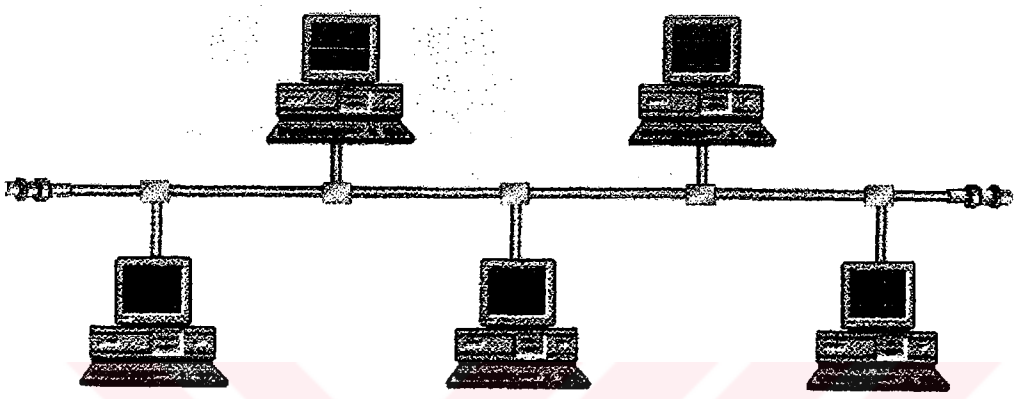
1 - Yol (Bus) Topolojisi
2 - Halka (Ring) Topolojisi
3 - Yıldız (Star) Topolojisi
4 - Kafes (Mesh) Topolojisi
5 - Hücresel (Cellular) Topolojisi (Arslan, 1995; Bilgisayar Pazarı, 1994).

3.5.1. Yol (bus) topolojisi

Şekil 3.15'de görülen fiziksel yol topolojisinde bir adet uzunca kablo kullanılır. Bu kabloya genelde omurga (backbone) adı verilir. Bağlanacak araçlar, kısa bir kablo ile birikte bağlayıcılar kullanılarak omurga (backbone) üzerine girilir. Kullanılan bu kısa kablolara ara kablo (drop cable) adı verilir. Günümüzde yol topolojisinde bilgisayarlar omurga üzerine t-bağlayıcılar (t-konnektörler) kullanılarak bağlanmaktadır. Omurganın (backbone) her iki ucu da terminator veya sonlandırıcı adı verilen aparatlarla mutlaka sonlandırılmalıdır.

Yol topolojisinin kurulumu diğer topolojilere göre göreceli olarak daha kolaydır. Bakımı ortalama olarak daha zordur, çünkü her cihazın omurgaya (backbone) bağlanabilmesi için bağlayıcıların belirli mesafelerle takılması gerekir. Bunların takılabileceği alan kalmadığı takdirde omurganın yenilenmesi

gerekebilir. Sorunları yakalamak pek kolay değildir. Bunun sebebi ise bütün bilgisayarlar tek bir kablo üzerine bağlanmışlardır ve izole etmek oldukça güçtür. Kablo üzerinde bir arıza meydana geldiği zaman bağlı bütün cihazlar bundan etkilenir (Networking Technologies, 1994; Aydın, 1992).



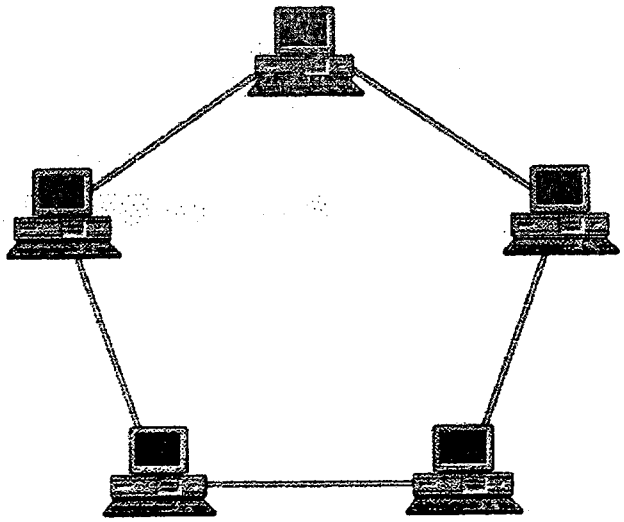
Şekil 3.15. Yol topolojisi

3.5.2. Halka (ring) topolojisi

Şekil 3.16'dan da anlaşılacağı gibi dairesel bir topolojidir. Tüm cihazlar halka üzerine doğrudan yada bir ara kablo (drop cable) vasıtasıyla bağlanır. Elektrik veya elektromanyetik dalgalar bir cihazdan bir cihaza doğru yalnızca bir yönde postalanır. Her cihazda gelen paketleri alan bir alıcı kablo, paketleri göndermek için de bir verici kablo vardır.

Halkalar kapalı bir devre oluşturulması gerektiği için yol tipi yapılara göre daha fazla techizat gerektirirler. Bu tür bir topolojinin bakımı, güncellenmesi oldukça zordur. Hata bulmak oldukça kolaydır. Bunun sebebi ise, her cihaz bir tekrarlayıcı (repeater) olduğu için işareti alamayan veya gönderemeyen cihazı tespit etmek daha kolaydır. Çoğu halka sistemlerinde meydana gelen sorundan tüm cihazlar etkilenir. Fakat çift döngü kullanan halkalar da mevcuttur. Bu

halkalarda döngülerden birinde bir sorun meydana gelirse diğeriyle işleme devam edilebilir (Networking Technologies, 1994; Aydın, 1992).

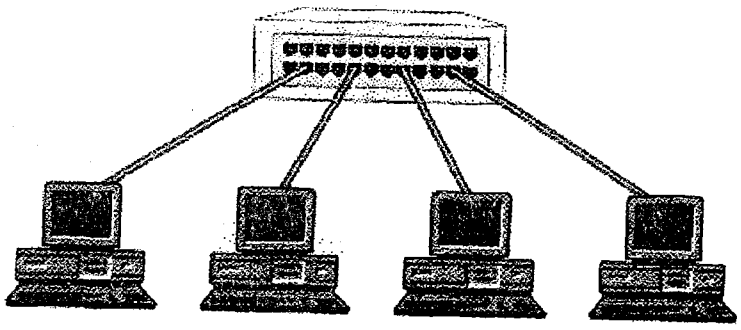


Şekil 3.16. Halka topolojisi

3.5.3. Yıldız (star) topolojisi

Şekil 3.17'de görülen fiziksel yıldız topolojisinde ara kabloların (drop cable) takıldığı merkezi bir cihaz kullanılır. Tüm cihazlar noktadan noktaya bağlantı yapılarak hub adı verilen bir cihaza bağlanır. İlave olarak yıldız topolojisinde iç içe bağlantılar oluşturularak ağaç yapısı meydana getirilebilinir. Yıldız topolojisinde işaret cihazdan huba, oradan da tüm diğer cihazlara gönderilir.

Yıldız topolojisinin kurulumu orta zorluktadır. Zorluğu her cihaza ayrı kablo çekilmesinden kaynaklanmaktadır. Bakımı ve güncelenmesi oldukça kolaydır. Sorunların tespit edilmesi ve çözülmesi oldukça kolaydır. Her hangi bir noktada meydana gelen sorunda sadece o noktaya bağlı cihaz etkilenmektedir (Networking Technologies, 1994; Aydın, 1992).

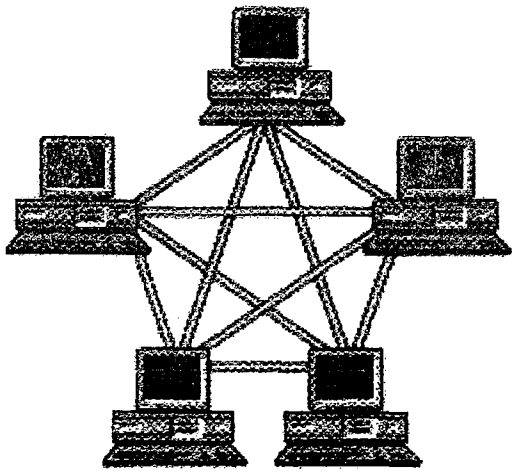


Şekil 3.17. Yıldız topolojisi

3.5.4. Kafes (mesh) topolojisi

Her cihaz bir birine noktadan noktaya doğrudan bağlantı olacak şekilde oluşturulmuş bir bilgisayar ağı topolojisidir. Şekil 3.18'de görülen bu topoloji türünde her bilgisayar diğer bir bilgisayara doğrudan bir hat ile bağlı olması gerektiği için ayrı bir arabirim (interface) kartı gerektirmektedir. Bu yüzden bu topoloji türü pratikte pek fazla uygulanamamaktadır. Bu tür topolojilerde hata toleransı oldukça yüksektir ve her bağlantı sistem performansını doğru orantılı olarak arttırır.

Kafes topolojisinin kurulumu oldukça zordur, çünkü bütün bilgisayarlar birbirlerine teker teker doğrudan bağlanmak zorundadır. Bakımı ve güncellenmesi oldukça zordur. Hata bulma ve düzeltme çok kolaydır. Hata toleransı oldukça yüksektir çünkü bilgisayarlar arasında alternatif pek çok bağlantı söz konusudur (Networking Technologies, 1994; Aydın, 1992).

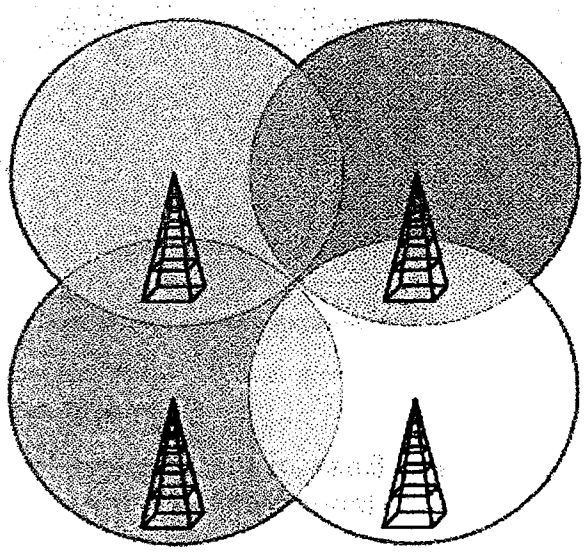


Şekil 3.18. Kafes topolojisi

3.5.5. Hücresel (cellular) topolojisi

Şekil 3.19'da görülen bu tür topolojide telsiz iletişimindeki metodlardan noktadan noktaya (point-to-point) ve çoklu bağlantı (multi-point) stratejileri kullanılarak bilgisayarların bulunduğu alanlar hücreler şeklinde bölünür. Her hücre toplam bilgisayar ağının bir parçasını ifade eder. Cihazlar merkezi bir istasyon veya hub ile iletişim kurarlar.

Hücresel topolojinin kurulumu, merkeze konulacak hubın yerleşimi ile doğru orantılıdır. Eğer hub istenilen yere konulabiliyorsa kurulum oldukça kolaydır, aksi takdirde büyük zorluklarla karşılaşılabilir. Kablosuz bir iletişim söz konusu olduğu için güncellenmesi ve bakımı oldukça kolaydır. Hata tespiti kolaydır. Her hangi bir problem karşısında herkes etkilenir, çünkü ortamda herkes aynı koşullarda çalışmaktadır (aynı oda gibi) (Networking Technologies, 1994; Aydın, 1992).



Şekil 3.19. Hücresel topolojisi

3.6. Bilgisayar Ağlarında OSI Referans Modeli ve IEEE 802 Standartları

Elektrik mühendisliğinden bilgisayar mühendisliğine uzanan çizgide pek çok kavramı bünyesinde toplayan iletişim ağlarının tasarımını kolaylaştırmak amacıyla bir model geliştirilmiştir. ISO (International Standarts Organization) tarafından geliştirilen modele OSI (Open System Interconnection - Açık Sistem Bağlantısı) referans modeli adı verilmiştir.

OSI referans modeli sayesinde değişik bilgisayar firmalarının ürettikleri bilgisayarlar arasındaki iletişimi bir standarda oturtmak ve farklı standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak hedeflenmiştir. OSI referans modelinde, iki bilgisayar sistemi arasında yapılacak olan iletişim problemini çözmek için yedi katmanlı bir ağ sistemi önermiştir. Bir başka deyişle bu temel problem yedi adet küçük probleme parçalanmış ve her bir problem için ayrı ayrı bir çözüm yaratılmaya çalışılmıştır. OSI referans modelini oluşturan yedi katman sunlardır;

1. Fiziksel Katman (physical layer)
2. Veri Bağlantı Katmanı (data link layer)
3. Ağ Katmanı (network layer)
4. Taşıma Katmanı (transport layer)
5. Oturum Katmanı (sesion layer)
6. Sunum Katman (presentation layer)
7. Uygulama Katmanı (application layer)

Bu yedi katmanın en altında yer alan iki katman (1. ve 2.) yazılım ve donanım, üstteki beş katman (3., 4., 5., 6. ve 7.) ise genelde yazılım yolu ile çözülmüştür (Halsall, 1989; Çağıltay, 1995; Tolun, 1994; Oktay, 1997; Bilgisayar Pazarı, 1991; Meijer and Peeters, 1983; Martin et al., 1994).

IEEE (The Institute of Electrical and Electronics Engineers), OSI katmanlarını kullanarak, yerel bilgisayar ağları için; kablolamayı, fiziksel topolojiyi, mantıksal topolojiyi ve ağ birimlerinin erişim düzenini açıklayan bir standartlar takımı geliştirmiştir. Bu satandartlar IEEE 802 olarak anılır ve OSI modelinin en alt iki katmanında kullanılan protokolleri açıklar. Bu katmanların üstündeki katmanlarla bir ilgileri yoktur. IEEE 802 standardının en büyük avantajı kullanıcının sahip olduğu donanımın, OSI'nin fiziksel ve veri bağlantı katmanlarını bir standarda sokarak cihazların uyumlu iletişimini sağlamaktır.

Komite hızlı bir şekilde iki sonuca ulaştı. Birincisi, yerel ağlar arasındaki iletişim işi, yönetilebilir parçalara bölünmesi gerekecek kadar karmaşık bir iştir. İkincisi, hiçbir teknik yaklaşım tek başına tüm gereksinimleri karşılayamaz. IEEE 802 komitesinin çalışmaları, aşağıdaki çalışma grupları halinde organize edilmiştir:

- 802.1: Higher Level Interface (HILI)
- 802.2: Logical Link Control (LLC)
- 802.3: CSMA/CD
- 802.4: Token Bus
- 802.5: Token Ring
- 802.6: Metropolitan Area Network (MAN)
- 802.7: Broadband Technical Advisory Group (BBTAG)
- 802.8: Fiber Optic Technical Advisory Group (FOTAG)
- 802.9: Integrated Services LAN (ISLAN)
- 802.10: Standard for Interoperable LAN Security (SILS)
- 802.11: Wireless LAN (WLAN)
- 802.12: Demand Priority

(Stalling, 1993, 1997; Ramos et al., 1996; Erdem, 1996).

4. YEREL AĞLARDA PERFORMANS VE GÜVENLİK

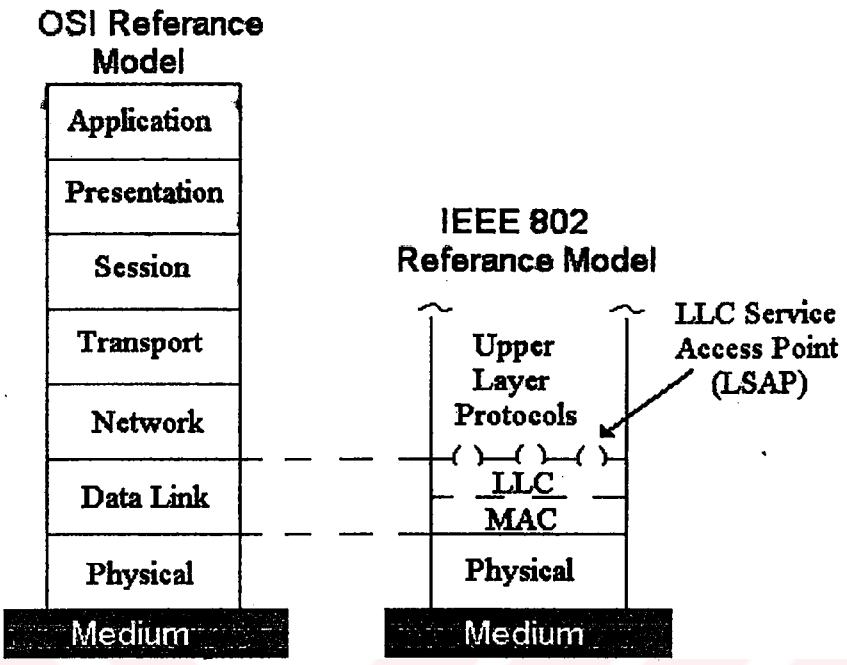
Bu bölümde öncelikle yerel ağların protokol referans modeli incelenmiştir. Bu modelin LLC seviyesinde akış kontrol ve hata kontrol mekanizmaları MAC seviyesinde CSMA/CD, Token Bus, Token Ring protokollerine değinilmiştir. Daha sonra yerel ağlarda performansı etkileyen faktörler ve performans sınırları ele alınmıştır. Yukarıda belirtilen üç protokol performans açısından karşılaştırılmıştır. Son olarak yerel ağlarda güvenliğe değinilmiştir.

4.1. Yerel Ağların Protokol Referans Modeli

LAN ile ilgili protokoller veri bloklarının ağ üzerinde iletimiyle ilgilidir. OSI modelinde, yüksek katman protokolleri (üçüncü veya dördüncü katman ve yukarısı) ağ mimarisinden bağımsızdırlar ve LAN, MAN ve WAN'lara uygulanabilirler. Sonuç olarak protokol referans modeli OSI modelinin alt katmanlarıyla ilgilir.

Şekil 4.1'de IEEE 802 referans modelinin OSI referans modeliyle ilişkilendirilmesi görülmektedir (Martin et al., 1994; Stalling, 1993, 1997).

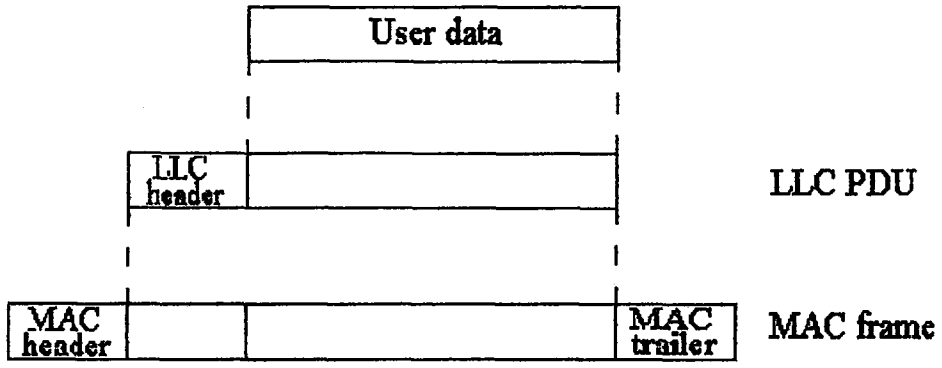
LLC ve MAC seviyeleri için adresleme oldukça önem taşır, çünkü iletişim; süreç, istasyon ve ağla ilgilidir. Buradaki süreçler iki bilgisayar arasında veri değişimi yapan dağıtık uygulamalardır. İstasyonlar ise eşzamanlı olarak bir çok uygulamanın çalışmasına olanak sağlarlar. İstasyonlar bir ağ tarafından birbirlerine bağlanırlar ve veri bir istasyondan diğerine ağ tarafından iletilir. Sonuçta verinin bir süreçten diğerine iletimi için veri önce alıcı sürecin bulunduğu istasyona sonra da bilgisayar içindeki ilgili sürece iletilir.



Şekil 4.1. IEEE 802 referans modelinin OSI referans modeliyle ilişkilendirilmesi

Bütün bunlar için iki seviyeli bir adreslemeye ihtiyaç duyulur. Şekil 4.2 LLC PDU'lar ve MAC çerçeveleri (frame) arasındaki ilişkiyi göstermektedir. Kullanıcı verisi, LLC'ye iletilir ve LLC bir başlık ekler. Başlıkta yerel LLC ile uzaktaki LLC arasındaki protokolü yönetmek için kontrol bilgisi vardır. Kullanıcı verisi ile LLC başlığının bütününe LLC PDU denir. Bu PDU, MAC'a geçirilir. MAC ise hem başlık hem de kuyruk (trailer) ekler ve MAC PDU oluşur. MAC PDU'ya çerçeve (frame) denir.

MAC başlığı alıcı istasyonun adresini içermelidir. Çünkü tüm istasyonlar alıcı adres sahasını okurlar. Bir çerçeve (frame) alındığında ise MAC başlığı ve kuyruk kısımları atılarak, ortaya çıkan LLC PDU, LLC'ye iletilir. LLC başlığı alıcı SAP (Service Access Point) adresini içermelidir. Çünkü LLC veriyi kime dağıtacağını bu adres ile bilir. Bazı durumda ise SAP bir donanım çıkışına karşılık gelir (Stalling, 1993, 1997).



Şekil 4.2. Kullanıcı verisi, LLC PDU'su ve MAC çerçevesinin gösterimi

Şekil 4.3 genel olarak bir MAC çerçevesinin sahalarını göstermektedir. Bunlar:

- MAC *kontrol:* Her türlü protokol kontrol bilgisi. (Örneğin öncelik seviyesi)
- *Alıcı* MAC *adresi*
- *Gönderici* MAC *adresi*
- LLC: Bir üst katmandan gelen LLC verisi
- CRC (Cylic Redundancy Check): Bu; kontrol, adres ve LLC sahalarının bir fonksiyonudur. Gönderici ve alıcı tarafından üretilir. Alıcının sonucu CRC sahasından farklıysa bir iletim hatası oluşmuş demektir (Stalling, 1993, 1997).

MAC Kontrol	Alıcı MAC Adresi	Gönderici MAC Adresi	LLC	CRC

Şekil 4.3. Genel MAC çerçeve yapısı

4.1.1. Mantıksal bağlantı kontrolü (LLC)

LLC (Logical Link Control-Mantıksal Bağlantı Kontrolü), IEEE 802 protokol modelinin en yüksek katmanıdır. IEEE 802 tarafından özelleştirilen bütün MAC (Medium Access Control - Ortam Erişim Kontrolü) standartlarıyla kullanılır. Bu katmanın ilk amacı, yerel ağlar üzerindeki kullanıcıların veri alışverişini sağlamaktır. LLC servisinin farklı çeşitleri, güvenilirlik ve etkili kullanım için oluşturulmuştur (Stalling, 1993, 1997; Held, 1993).

4.1.1.1. LLC servis biçimleri

LLC seviyesinde kullanıcılara sunulan üç çeşit servis biçimi vardır. Bunlar;

- Onaylanmamış bağlantısız servis
- Bağlantı modlu sevis
- Onaylanmış bağlantısız servis

4.1.1.1.1. Onaylanmamış bağlantısız servis

Bu servis öyle ki sadece LLC PDU'larının gönderilip alınmasını sağlar, teslimat garantisi ve hata kontrolü yapmaz. Bu servis "individual", "multicast" ve "broadcast" adreslemeyi destekler.

4.1.1.1.2. Bağlantı modlu servis

Bağlantı modlu LLC servisi, iletişimde bulunan iki LLC kullanıcısının mantıksal bağlantısı için gereken başlangıç ayarlarını aktif (enable) etmek içindir. Bu mantıksal bağlantının kesilmesini yada yeni bağlantı yapılması için kullanıcı isteğini belirtir. Aynı zamanda akış kontrol, sıralama ve hata tespitini de sağlar. Bu servis sadece "individual" adreslemeyi destekler.

4.1.1.1.3. Onaylanmış bağlantısız servis

Bu servis bir bağlantıya gerek duymadan karşı tarafa bir veri yollayarak, bu verinin alındığına dair bir onay sinyali alır. Burada birbirinden bağımsız iki servis vardır. DL-DATA-ACK servisine garantileme servisi de denebilir. Bilgi LLC kullanıcısı tarafından yollanır ve daha sonra bu bilginin gittiğine dair karşı taraftan onay gelir. DL-REPLY servisi garantili cevaptır. Daha önceden hazır olan bir veriyi kullanıcıdan diğer kullanıcıya yollamak yada değiş tokuş yapmak isteği içindir (Stalling, 1993, 1997; Schwartz, 1987; Tanenbaum, 1989; Martin et al., 1994).

4.1.1.2. Bağlantı kontrol protokol mekanizmaları

Bağlantı (link) kontrol protokollerinde kullanılan çok önemli iki mekanizma; akış kontrol ve hata kontrol'dür. Bu mekanizmalar çoğu veri iletim protokollerinde bulunabilir. Akış ve hata kontrol mekanizmaları bağlantı modlu ve onaylanmış bağlantısız modlu LLC protokollerinde kullanılır.

4.1.1.2.1. Akış kontrol

Akış kontrol, alıcı tarafın yollayan taraftan etkilenmemesini sağlayan bir tekniktir. Alıcı taraf iletim için maksimum uzunlukta veriyi bufferına yerleştirir. Veri alındığında, alıcı taraf, verileri takip etmek zorundadır. Eğer akış kontrolü yapılmazsa, alıcının bufferı eski verilerle işlem yaparken yeni veriler taşabilir.

Hatasız akış kontrol mekanizmalarına bakılırsa, Şekil 4.4.a'da zamana göre veri alışı görülmektedir. Her ok iki istasyon arasında iletimde bulunan bir PDU'yu simgeler. Veriler PDU sırasına göre, içerdikleri veri ve kontrol

bilgileri ile gönderilir. Her PDU'nun sağlıklı alındığı farzedildiğinde, iletim hatasız gerçekleşmiştir. Buradaki tek problem her PDU'nun alınmadan önceki gecikme miktarıdır.

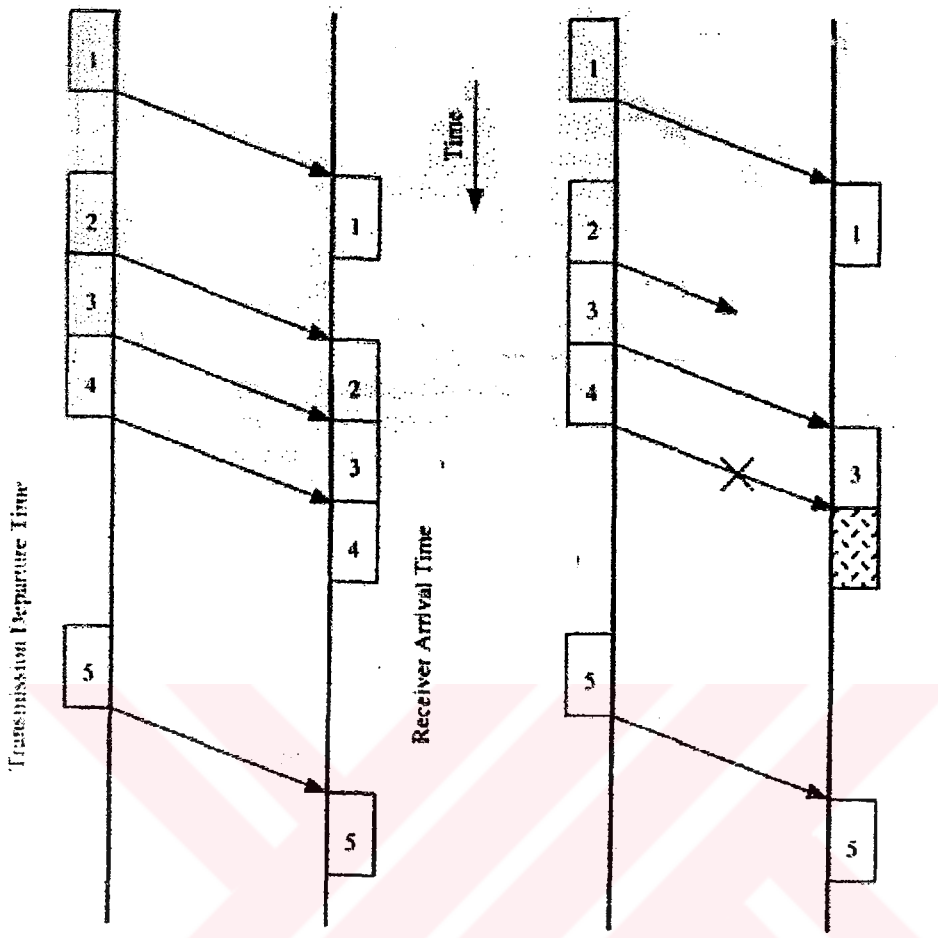
4.1.1.2.1.1. Dur ve bekle (Stop and wait) akış kontrolü

Akış kontrolünün en basit şeklidir. Onaylı bağlantısız LLC servisini destekler ve şöyle çalışır; kaynak cihaz bir PDU iletir. Alımdan sonra hedef cihaz, başka PDU istemini henüz aldığına dair bir onay şeklinde belirtir. Kaynak bir sonraki PDU'yu yollamak için bu onayı beklemek zorundadır. Bu durumda hedef istediğinde veri akışını durdurabilir. Bu kontrol çok iyi çalışır ancak uzun veri iletimlerinde zorluk çıkartabilir. Fakat PDU'yu küçük paketlere ayırmak koşuluyla bu durum aşılabilir. Bu işlemin yapılmasının bir kaç sebebi vardır;

- Alıcının buffeı sınırlı olabilir.

- Uzun iletilerde hata oranı fazla olabilir ve tüm PDU'yu yeniden göndermek gerekebilir, PDU küçükse hata daha önce farkedilerek, daha az veri yeniden gönderilmek zorunda kalınır.

- LAN'lardaki gibi paylaşımlı ortamlarda, tek bir istasyon ortamı sürekli meşgul eder. Bu yüzden diğer istasyonlar beklemek zorunda kalabilir (Tanenbaum, 1989).



a) Hatasız iletim b) Hatalı ve kayıplı iletim

Şekil 4.4. Çerçeve gönderim modeli

4.1.1.2.1.2. Kayan pencere (Sliding-window) akış kontrolü

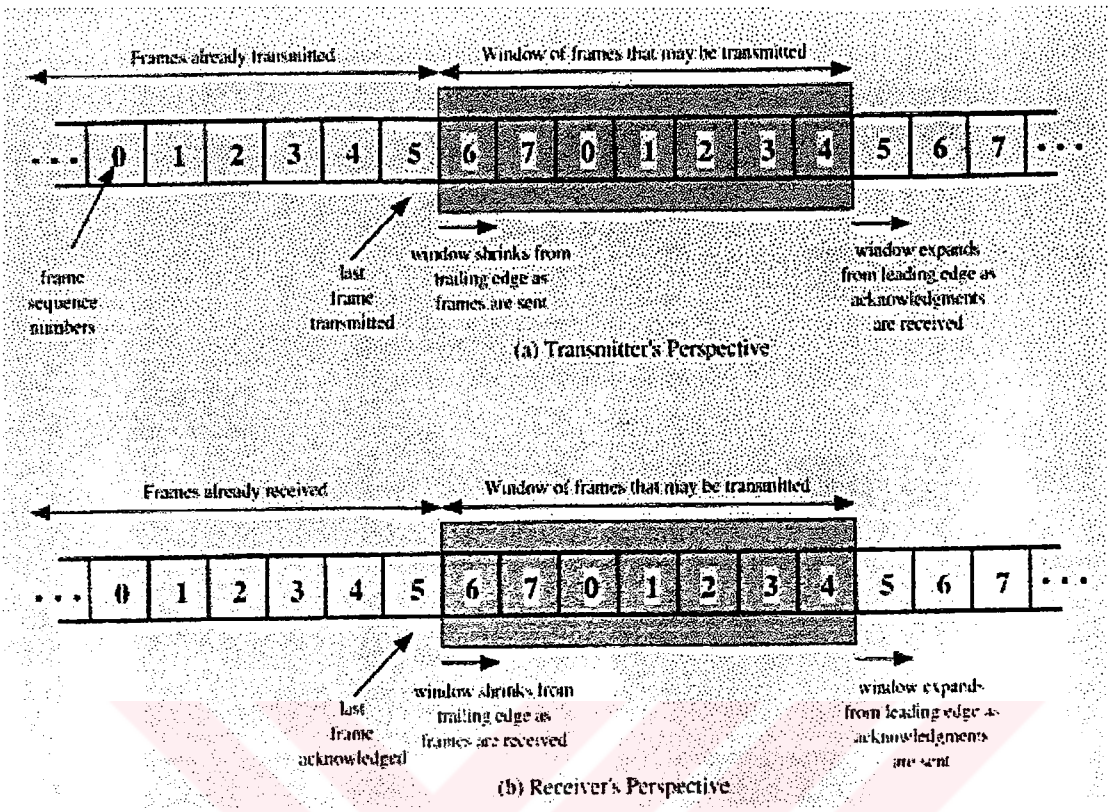
Şekil 4.5'de görülen kayan pencere (sliding-window) akış kontrolü çoklu PDU'yu tek seferde göndermesiyle etkinliğini arttırır. Bunu farklı A ve B istasyonları üzerinde tam çift yönlü bağlantıyla açıklanacak olunursa; tek PDU yerine, B istasyonun bufferında n sayıda PDU için yer ayarlanır. Böylelikle B istasyonu n sayıda PDU'yu kabul eder ve A'ya n sayıda PDU'yu onay beklemeden göndermesi için izin verilmiş olur (Halsall, 1989; Üstüner, 1995; Bilgisayar Pazarı, 1995).

Her PDU'ya hangisinin onaylandığını bilmek için bir sıra numarası verilir. B PDU'yu şöyle onaylar, alınan PDU'dan sonraki numarayı A'ya belirtir. Bu da A tarafından B'nin n sayıda yeni PDU'ya hazır olduğunu gösterir. Örneğin 1,2,3,4,5 numaralı PDU'lar peşpeşe yollandığında ve karşı tarafa 6 numaralı PDU'yu bekliyorum onayı yollandığında, 1,2,3,4,5 numaralı PDU'ların sağlıklı ulaştığı anlaşılır. A göndereceklerini B de almaya hazırlanan PDU'ların sıra numarasını tutar. Bu listelerin herbiri PDU'ların penceresi olarak düşünülür ve bu yüzden kayan pencere (sliding-window) adını alır. Dikkat edilmesi gereken bir nokta daha vardır; sıra numarası gönderilen PDU'da oluşacak kapasite genişlemesinin ayarlanmasıdır (Schwartz, 1987; Tanenbaum, 1989; Stalling, 1993, 1997).

4.1.1.2.2. Hata kontrol

Hata kontrolü PDU'ların iletiminde meydana gelebilecek hataların tespitini sağlayan mekanizmadır. Örneğin Şekil 4.4.b'deki gibi tipik bir hatanın örtülmesinde kullanılabilir. Aynı zamanda yollanan PDU'ların düzenli bir sıra içinde keyfi olmadan yollanmaları ve gecikme miktarlarının dikkate alınmasında kullanılır. Genelde iki tip hatanın olabileceği kabul edilir;

- İletilemeyen PDU kayıpları,
- İletimde bazı bitleri zarar görmüş PDU.



Şekil 4.5. Kayan pencere akış kontrolü

Hata kontrolünde en geçerli bir kaç teknik de şunlardır;

- Hata Tarama: Alıcının hataları taraması ve hatalı olanları çıkarması.
- Pozitif Onaylama: Sağlıklı iletimin alıcı tarafından onaylanması.
- Zaman Bitimiyle Yeniden Yollama: Onaysız şekilde ön karar süresi dolduktan sonra iletilerin yollanması.
- Negatif Onaylı ve Yeniden Tekrarlanan İleti: Olumsuz onaydan sonra PDU'nun tekrar yollanması.

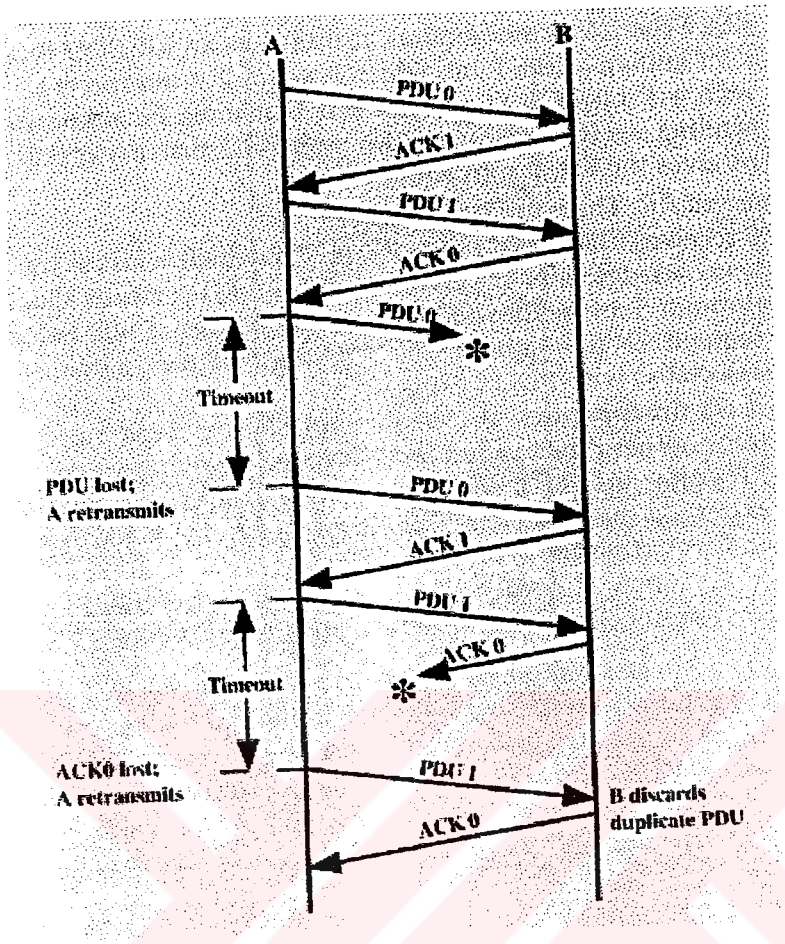
Tüm bu mekanizmalar ARQ (Automatic Repeat Request) ile gösterilir. ARQ güvensiz veri iletimlerini güvenli hale getirebilmek içindir. LLC standartında iki çeşidi bulunur. Dur ve bekle ARQ (stop and wait ARQ) ve N'li geri besleme ARQ (Go-Back-N ARQ) dur (Stalling, 1993, 1997; Halsall, 1989).

4.1.1.2.2.1. Dur ve bekle ARQ (stop and wait ARQ)

Şekil 4.6'da görülen dur ve bekle (stop and wait) akış kontrol tekniğinin taslağıdır. Kaynak istasyon bir PDU iletir ve iletim onayı beklemek zorundadır. Kaynak istasyon verinin ulaştığını onaylamadan başka bir veri yollamamalıdır. Hatalar iki tür oluşur.

Birincisi, PDU hedefe ulaştığında hasarlanmış olabilir. Alıcı hata arama tekniği kullanarak alınan bu PDU'yu tanır ve hata tesbit edildiğinde PDU'u açığa alır. Bu durumdan dolayı kaynağa zaman tanınır. PDU iletildikten sonra kaynak istasyon onay için bekler. Eğer bir zaman süresi sonunda onay alınmazsa, aynı PDU tekrar yollanır. Bu metodla gereken şu ki, iletilen PDU'nun bir kopyasının, alıcıdan bir onay gelinceye kadar tutulması gerektiğidir.

İkinci aşama hatalı onaylamadır. İstasyon A PDU'yu B istasyonuna yollar. B, ACK onayı ile cevap verir. ACK ise iletişim esnasında zarar görebilir ve A tarafından tanınamayabilir. Mesela zaman bitiminde aynı PDU'nun yolladığı bir an olabilir. Bu durumda B istasyonu aynı PDU'dan iki tane almıştır ve bunları ayıramayabilir. Ayrıca bunların farklı etiketlenmesi de mümkündür. 0 ve 1 gibi farklı numaralar verilebilir. Kayan pencerede (sliding window) ACK0 ve ACK1 karşıya onaylanır. Böylece alıcıya yanlış numaranın alındığı bildirilir (Stalling, 1993, 1997; Schwartz, 1987; Smith and Udell, 1993).



Şekil 4.6. Dur ve bekle ARQ

4.1.1.2.2.2. Go-Back-N ARQ

Dur ve bekle ARQ'nun (Stop and Wait ARQ) başlıca avantajı basit oluşudur. Başlıca dezavantajı ise yetersiz bir akış kontrol tekniğine sahip oluşudur. Çünkü bu teknik anca temel hata kontrollerinde kullanılabilir. Kayan pencere (Sliding-window) akış kontrol tekniğine adapte edilmiş hata kontrol tekniği de N'li geri beslene ARQ (Go-Back-N ARQ) olarak isimlendirilmiştir.

N'li geri beslene ARQ'da (Go-Back-N ARQ) istasyon sıra numaralı PDU'ları maksimum değerde yollayabilir. Onaylanmamış PDU'ların numaraları pencere

kapasitesi ile göze çarpan kayan pencere (sliding-window) akış kontrol tekniğini kullanarak belirlenir. Hiçbir hata olmadığında, hedef normal şekilde PDU alabileceğini, RR (receive ready) sinyali ile onaylar. Eğer hedef istasyon PDU'da bir hata saptarsa, bu PDU için kaynağa negatif onay olan REJ (reject) sinyali yollar. Hedef istasyon bu PDU tekrar yollanıncaya kadar, iletimdeki diğer gelebilecek PDU'ları bekletir. Kaynak istasyon REJ aldığında hatalı PDU'yu diğer PDU'larla beraber bu esnada (hedef beklemede iken) yeniden yollamak zorundadır.

A istasyonu PDU'ları B'ye yollar. Her iletişimden sonra A, her PDU'nun iletildiğine dair kendisine onay süresi ayarlar.

Şekil 4.7'de PDU'lar N'li geri beslene ARQ (Go-Back-N ARQ) akışını gösterir. Hattaki propagasyon gecikmesi anında onay, olumlu yada olumsuz yollanan istasyona geri döner. Bu esnada zaten iki PDU bir onay olmasına rağmen yollanmıştır. Böylece REJ, PDU5 olarak alındığında, sadece PDU5 değil PDU'lardan 6 ve 7'de tekrar iletilir. Bu sebepten ileticiler tüm onaysız PDU'ların bir kopyasını saklamak zorundadır (Stalling, 1993, 1997; Schwartz, 1987; Tanenbaum, 1989; Halsall, 1989).

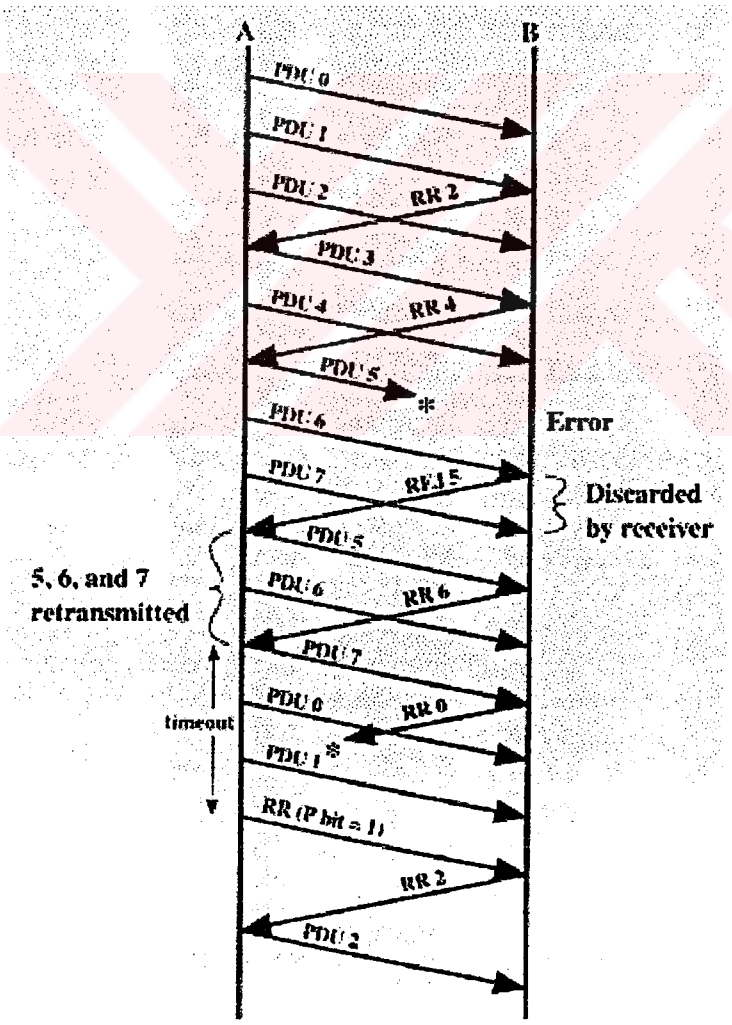
4.1.2. Ortam erişim kontrolü (MAC)

Yerel ağların (LANs: Local Area Networks) yüksek hıza erişmesiyle (100 Mbps) beraber telsiz iletişimin sağlanması gibi uygulamalar da vardır. Tüm bu gelişmelerin 10 Mbps'lik yerel ağlar temel alınarak yapılması IEEE 802 standardında çalışan geleneksel yerel ağların önemini bir kez daha ortaya çıkarmaktadır. Ortam erişim tekniğinde kullanılan üç standarda bakmak gerekirse;

1) CSMA/CD (Carrier-Sense Multiple Access with Collision Detection: Çarpışma Algılamalı Hassas Taşımalı Çoklu Erişim) IEEE 802.3 standardı (Ethernet),

2) Token Bus IEEE 802.4 standardı,

3) Token Ring, IBM'in geliştirdiği IEEE 802.5 standardı (Stalling, 1993, 1997; Tanenbaum, 1989; Naugle, 1991) .



Şekil 4.7. N'li geri besleme ARQ

4.1.2.1. CSMA/CD (Ethernet)

IEEE 802.3 Ethernet'i belirleyen standarttır. Ticarette ve endüstride kullanılmak için tasarlanan bu standart, daha sonra evlerde ve ağır endüstride bile kullanılmıştır. IEEE 802.4 ve IEEE 802.5 ile birlikte bu standart MAC (Medium Access Control-Ortam erişim Kontrolü) ve fiziksel katmanda da tanımlanabilir (Schwartz, 1987; Held, 1993).

Yol ve yıldız topolojileri için MAC ile en geçerli olanı CSMA/CD tekniğidir. MAC'ı incelemeden önce bilinmesi gereken bir kaç nokta vardır;

CSMA/CD'de iletim rasgele erişimle veya çekişme (contention) ile yapılır. Rasgele erişimde ortamdan dolayı bazı sorunlar olabilir. Çerçeve (frame) kanaldaki gürültü miktarının fazlalığından yada aynı zamanda iletilen başka bir çerçeveden (frame) dolayı geçersiz olabilir. Bu durumda iki çerçeve (frame) birbirleriyle karışmış ve *"collision"* olarak bilinen **çarpışma** meydana gelmiştir. Bu durumda alıcı çerçevenin (frame) geçersizliğine karar verebilir ve yoksayabilir.

Şunlara dikkat etmek gerekir ki istasyondan istasyona propagasyon zamanı iyice karşılaştırılmalı, istasyonun yolladığı çerçevenin (frame) ulaşması için geçecek propagosyon zamanından önce karşı taraf bir iletide bulunursa çerçeveler (frame) birbirleri ile karşılaşabilir. Mesafenin fazla olması, bağımsız olarak bir çok istasyonun aynı anda birbirleri ile sağlıklı iletişim kurmasına imkan verir. Çarpışma olmaması için çerçeve (frame) yollayan istasyon gecikme miktarını istasyonlara bildirerek bu sırada iletişime geçmelerine engel olabilir. Başka bir bakışta kısa gecikme zamanı ve iyi bir geri besleme ile verimi arttırmaktır (Halsall, 1989).

CSMA/CD ile istasyon, başka bir istasyonun yürüttüğü işe göre iletim yapıp yapmak istemediğine karar verir. Ortam kullanımda ise istasyon beklemek zorundadır. Eğer değilse iletim yapılabilir. Ancak aynı anda ortamın boşaldığını görüp iletime geçen istasyon olursa meydana gelebilecek çarpışma kaçınılmazdır. Bu durumda iletiyi yollayan istasyonlar karşıdan bir onay gelmediğini farkedince çarpışma olduğuna karar verir ve iletiyi tekrarlar. Normal olarak çerçeve (frame) iletim zamanı, propagasyon gecikmesinden çok fazladır. Çarpışmaya bağlı olarak propagasyon gecikmesi de artar.

Maksimum kullanım çerçeve (frame) uzunluğuna ve propagasyon gecikmesine bağlıdır. Çerçeveler (frame) ve propagasyon gecikmesi azaldıkça kullanım miktarı artar. CSMA/CD ile ortamın meşgul olması durumunda bir algoritmaya ihtiyaç duyulur. Bununla ilgili Şekil 4.8'de üç yaklaşım verilmiştir.

4.1.2.1.1. Israrcı olmayan (Non-persistent)

CSMA/CD algoritmasında iletim yapmak isteyen istasyonların uyması gereken kurallara şunlardır;

1) Ortam boş ise iletime geç değilse 2. kurala uy
2) Ortam meşgul ise, bir süre bekle ve 1. kuralı tekrarla

4.1.2.1.2. 1-ısrarcı (1-persistent)

Çarpışmadan sonra istasyonların tekrar iletime geçmeden önce istasyonların kullandıkları *rasgele gecikme* miktarı çarpışma olasılığını azaltır. Çarpışmadan sonra tekrar iletime geçmek isteyen istasyonlar rasgele gecikme olmasaydı tekrar çarpışmaya sebep olabilecekler ve böylece boşuna zaman harcanacaktı ve iletimden sonra ortam boş kalacaktı. Boş kalmayı engellemek için 1-ısrarcı

(1-persistent) protokolü kullanılır. İletim yapmak isteyen istasyonlar şu kurallara uyarlar;

1) Ortam boş ise iletime geç değilse 2. kurala uy
2) Ortam meşgul ise, boşalıncaya kadar bekle ve iletime geç

4.1.2.1.3. P-ısrarcı (p-persistent)

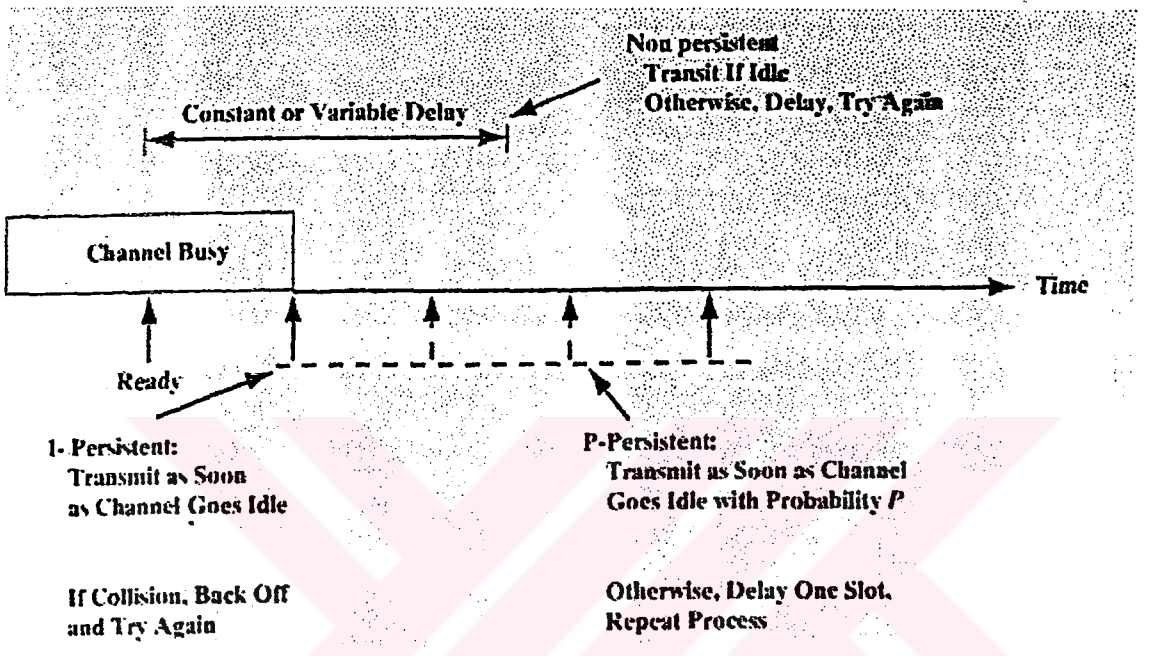
Israrcı olmaya (non-persistent) istasyonları hürmetkar, 1-ısrarcı (1-persistent) istasyonları ise bencildir. İletim için bekleyen iki veya daha fazla istasyon varsa çarpışma kaçınılmazdır. Herşey çarpışmadan sonra şu kurallarla yoluna konur; p-ısrarcı (p-persistent)

1) Ortam boş ise p süresi bekleyip iletim yap ve maksimum propagasyon gecikmesine eşit olan 1-p zaman dilimi bekle

2) Ortam meşgul ise, kanal boşalana kadar bekle ve 1. kuralı tekrarla

P'nin etkili değerinin ne olduğu sorulursa: Ana problem ağır yük altına meydana gelen kararsızlıktır. N sayıdaki istasyon iletimde iken ileti yapmak isteyen istasyon sayısına eşit olabilir veya np eğer 1'den büyükse (np>1), birçok istasyon iletime geçecek ve çarpışma olacaktır. Daha kötüsü istasyonlar çarpışmayı anlayacak ve geri dönmek isteyenler bu sefer çarpışacaktır. Bundan da kötüsü çarpışma sonrası oluşacak yeni iletiler ortalığı daha da karıştıracaktır. Sonuç olarak her istasyon sürekli yollamaya çalıştıkça çarpışma sayısı artacak ve bu durum iletişimi sıfıra bile düşürebilecektir. Bu kargaşayı engellemek için np 1'den az olmalı ve ağır yüklerde p küçük değerde olmalıdır ki bu durumda istasyonlar daha fazla beklemek zorunda kalacaktır. Hafif

yüklemenin olduğu durumlarda bu çok uzun beklemelere sebep olabilir (Tanenbaum, 1989).



Şekil 4.8. CSMA/CD'nin üç değişik algoritması

Israrcı olmayan (non-persistent), 1-ısrarcı (1-persistent) veya p-ısrarcı (p-persistent) adlı algoritmalardan en geçerlisi 1-ısrarcı (1-persistent) olanıdır. Ethernet tarafından kullanılan IEEE 802 standardıdır. Unutmamalıdır ki ısrarcı olmayan (non-persistent) ve p-ısrarcının (p-persistent) performans sorunu vardır. Israrcı olmayanda (non-persistent) kapasite boşuna ayarlanır çünkü iletimin sonunda ancak ortam boşalır. P-ısrarcıda (p-persistent) ise p düşük tutulmalıdır ve bu da kararsızlığa sebep olur. Çarpışa sonrası çarpışma olasılığı düşük de olsa sıfır değildir ve çarpışmadan sonra üretilen rasgele gecikme zamanı her seferinde ikiye katlanır (Stalling, 1993, 1997).

4.1.2.1.4. MAC protokolü

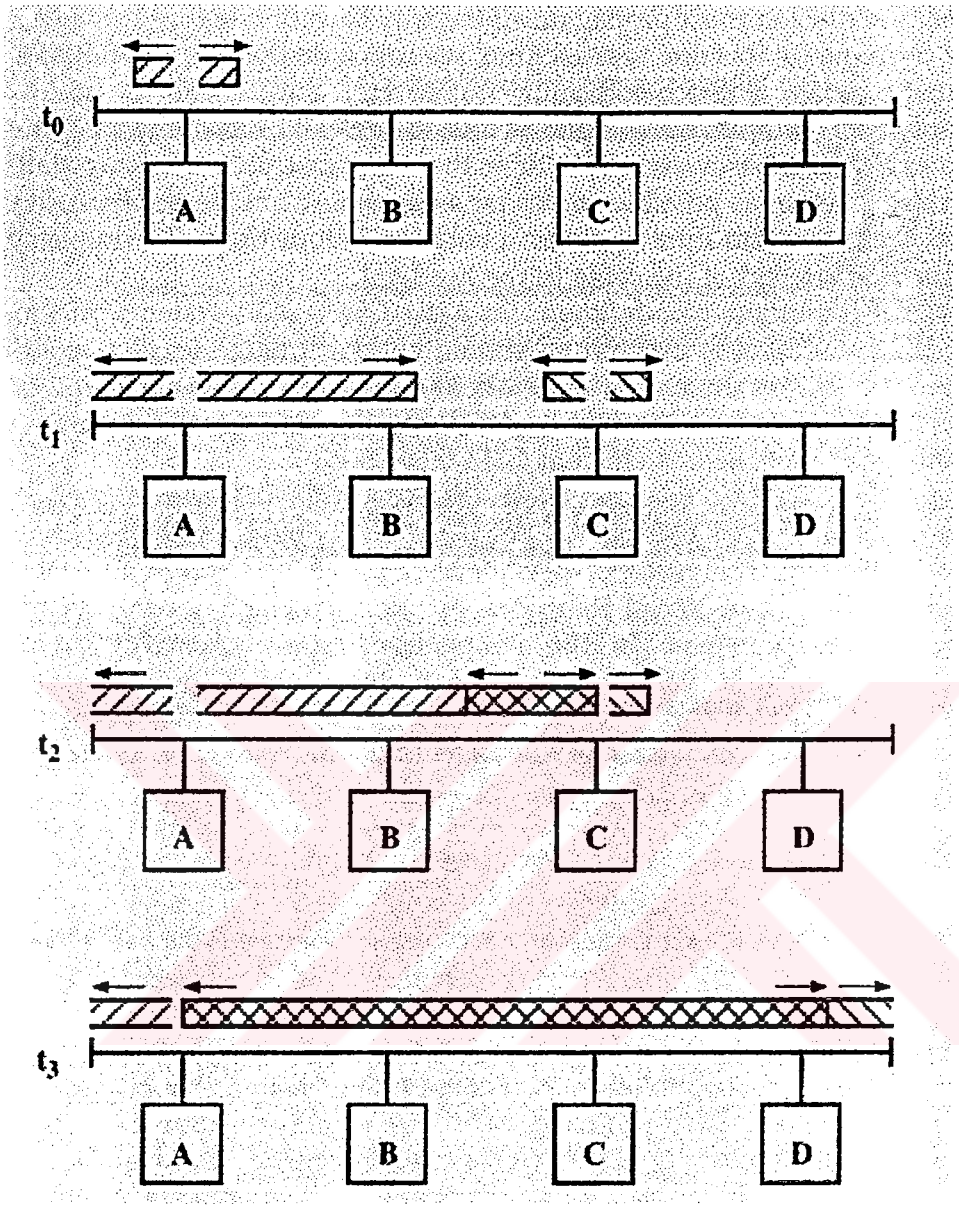
İki çerçeve (frame) çarpıştıktan sonra hasarlı her iki çerçeve (frame) tekrar iletilene kadar ortam kullanılamayacak, uzun çerçeveler (frame) düşünüldüğünde miktar daha fazla olacaktır. Eğer istasyon, iletim süresince ortamı dinlemeyi sürdürürse bu kayıp azaltılabilir. Şu kurallara uyulur;

1) Ortam boş ise iletime geç değilse 2. kurala uy
2) Ortam meşgul ise, boşalıncaya kadar bekle ve iletime geç
3) İleti esnasında çarpışma beklenirse tüm istasyonları bu durumdan haberdar etmek için ortama çakışma (jamming) sinyali yollayarak iletiyi kes
4) Çakışma (jamming) sinyalinden sonra rasgele bir süre bekle ve yeniden ilet

Baseband yol topolojisi Şekil 4.9'dadır. Burada t0 zamanında istasyon A, D'ye bir paket yollamaya başlar ve t1 zamanında B ile C iletiye hazırdır. B ortamda bir ileti olduğunu anlar ve kendi iletisini erteler. Ancak C halen A'nın iletisinden habersizdir ve iletime geçer. A'nın iletisi C'ye t2 zamanında ulaştığında C çarpışmayı anlar ve iletiyi keser. Çarpışma iletisi t3 zamanında bildirilir ve A'da iletiyi keser (Stalling, 1993, 1997; Henshall and Shaw, 1989).

4.1.2.2. Token bus

IEEE 802.4 standardı sadece ofis çevreleri için değil fabrika, endüstri çevreleri ve askeriyede de uygulanır. Bu standart yol (bus) topolojisi kullanılarak yapılır. IEEE 802.4 için MAC protokolü **Token Bus**'tır (Halsall, 1989).

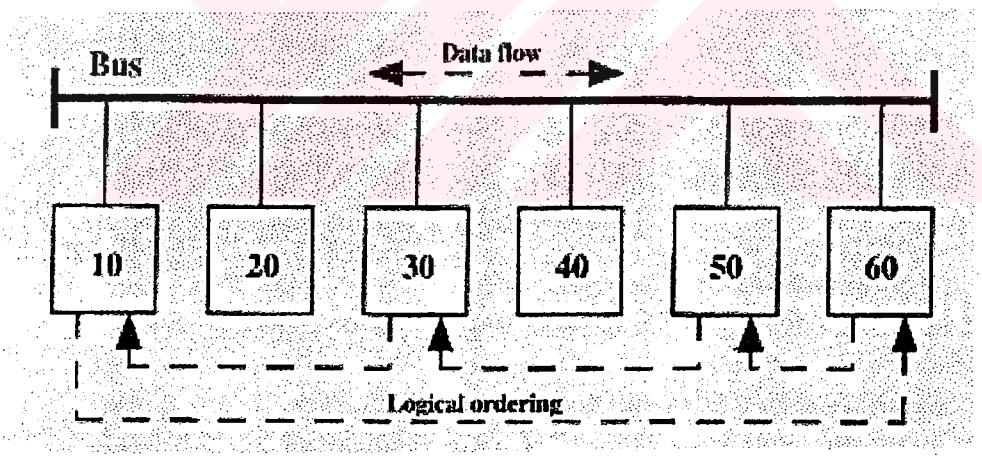


Şekil 4.9. CSMA/CD işlemi

4.1.2.2.1. MAC protokolü

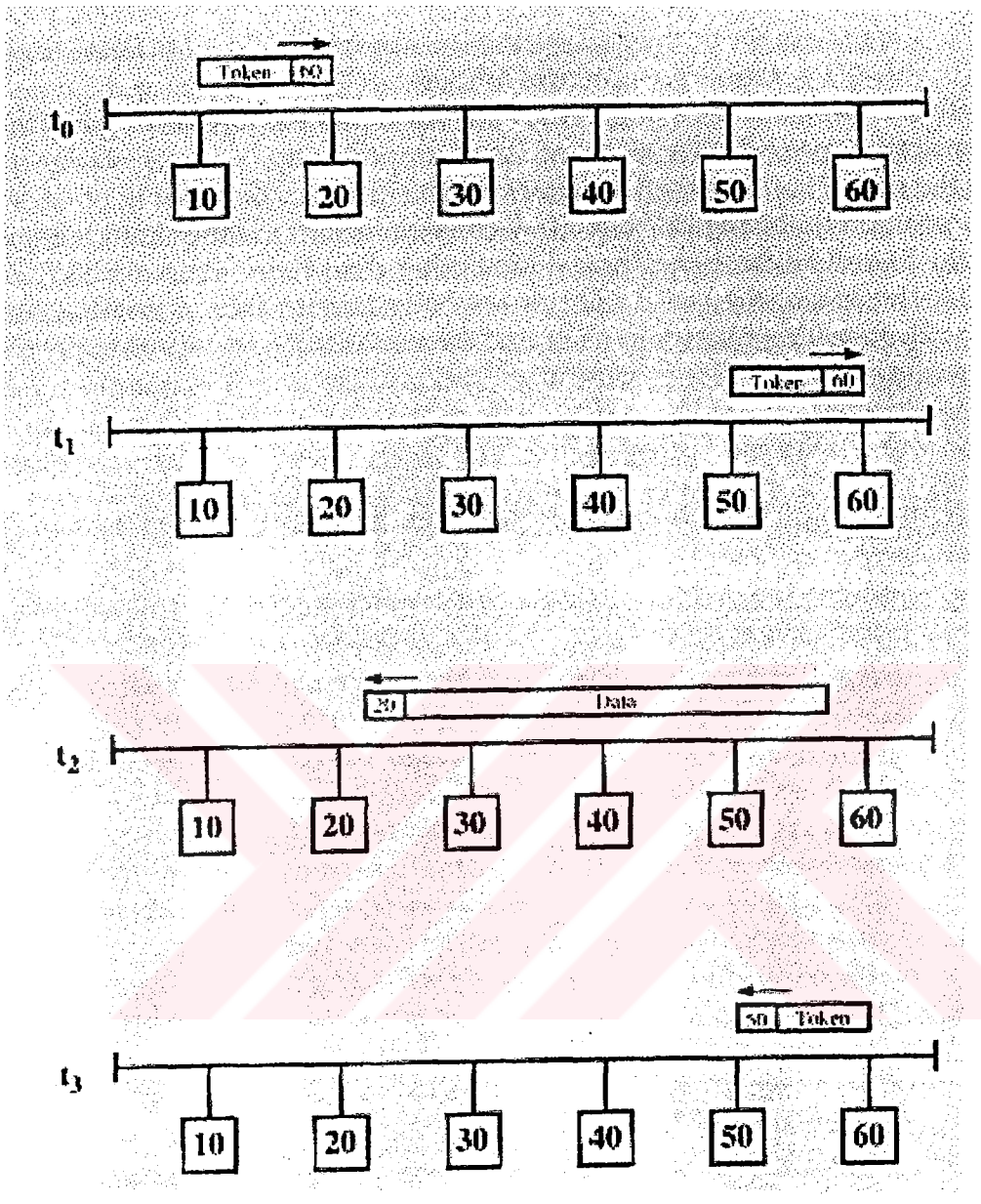
Token Bus için yol topoloji üzerindeki istasyonlar, mantıksal halka biçimindedir. İstasyonlar bir mantıksal sıra ile mantıksal konumlarına bakılarak ve en sondaki baştakini takip edecek şekilde, fiziksel konumlarına bakılmaksızın sıralanabilir. Jeton (token) olarak bilinen çerçeve (frame),

erişimi düzene sokmak için kullanılır. Jetona sahip istasyonlar jetonu salıncaya kadar ortam kontrolünü eline geçirir. İstasyonun jeton ile işi bittiğinde jetonu, mantıksal sıradaki istasyona iletir. Bu sırada diğer istasyonlar ancak onay veya cevaplarını belirtebilirler. Jeton kendilerine gelinceye kadar iletime geçmeleri mümkün değildir. Bu yolla halka yapısına benzer bir yapı oluşturulur ve korunmaya çalışılır. Uç noktadaki istasyonlar hariç istasyonlar birbirlerine azalan adres numaraları ile bağlıdırlar. Şekil 4.10'da verilen örnekte her birim zamanda numarası kesin olan istasyon aktiftir ve jetonla çerçeve (frame) alıp, yollayabilir. Her istasyon bir önceki (pervious station) ve bir sonraki (next station) istasyonu tanır. Yeni katılan bir istasyon bu sayede jetonu alacağı istasyonu ve göndereceği istasyonu belirler. Bu örnekte 60,50,30,10 mantıksal sırası ile tanımlanan istasyonlar 60, 50 numaraya, 50 numaralı istasyon 30 numaraya ve devam eden şekilde jetonu iletebilirler.



Şekil 4.10. Token bus yapısı

Şekil 4.11'de ise önce jeton 10'dan 60'a yollanır. Jetonu alan 60, jeton boş olduğu için 20'ye iletim yapmak istediğinde engel yoktur. 20 mantıksal sırada yer almadığından kendisine yollanan jetonu alabilir fakat kendisi bir iletim başlatamaz. Ancak 60 iletimi bitirdiğinde mantıksal sıradaki 50 numara isterse iletime geçebilir.



Şekil 4.11. Token bus işleyişi

Bu yapıda dikkat edilmesi gereken bazı işlemlere bakılacak olursa;

•Halkaya Eklenme (Addition to Ring): Mantıksal halkaya periyodik olarak isteyenlerin katılması

•Halkadan Silinme (Deletion from Ring): İstasyonun kendisini mantıksal halkadan silebilmesi

•Halka Ayarları (Ring Initialization): Ağ çalıştığında sıra ayarlarının yapılması

•Jetonun Kurtarılması (Token Recovery): İstasyon yada iletim hatasından dolayı kaybedilen jetonun kurtarılması

Halkaya eklemeyi başarabilmek için mantıksal halkadaki her istasyon sorumludur. Yeni istasyon periyodik olarak kabul edilir. Buradaki önemli iki unsur; istasyonun diğer istasyondan düşük adresli olmasının hesaba katılması, istasyonun jetonu yakaladığında yayınladığı başarılı istek çerçevesinin (solicit-successor frame) kendisi ile bir sonraki istasyon arasında geçiş hakkı için doğru sırada olmasıdır. İleten istasyon bir cevap bekledikten sonra dört durum oluşabilir;

1) Cevap yok (No response)
2) Bir cevap (One response)
3) Birden fazla cevap (Multiple responses)
4) Hatalı cevap (Invalid response)

Düşük adresli istasyonun şimdi hesaba katılmasıyla, başarılı istek2 çerçevesi (solicit-successor-2 frame) ve beklenen cevabın istasyonca yollanmasıyla prosedür başlar. Jetonu alandan daha küçük adresli istasyonlar ilk cevap olarak başarılı ayar çerçevesi (set-successor frame) ile yanıt verebilirler. Daha büyük adresli istasyonlar bir cevap beklemek zorundadırlar. Eğer hiçbirşey duyamazsa, cevap yollayabilir yada davete cevap vermeyebilirler.

İstasyon silme, eğer istasyon mantıksal halkadan ayrılmak isterse jetonu alıncaya kadar beklemeli ve başarılı ayar çerçevesi (set-successor frame) yollamalıdır. Böylece yetkili istasyon bu isteğe göre mantıksal halkada güncelleme yapar. Jeton bir tur attıktan sonra yetkili istasyon çıkmak isteyen

istasyonun yolladığı jetona göre davranır. Bu istasyon her zaman jeton alabilir. Böylece istasyon mantıksal halkadan çıkmış olur. Mesela Şekil 4.10'da halkadan çıkmak isteyen 60 nolu istasyon durumunu 60 nolu istasyona 30 numaralı istasyonla bildirir. Bir sonraki durumda jetonu alan 60 numaralı istasyon jetonu 30 numaraya iletir.

Eğer LAN yeni aktif olmuş veya jeton kaybolmuşsa işlem yapılamayacaktır. Zaman bitim değeri kadar bir sürede bu durumu farkeden bir yada daha fazla istasyon halka başlangıç ayarlarını (ring initialization) başlatır. Bu durumu farkeden istasyon jeton istek çerçevesi (claim-token frame) yayınlar. Ardından iletilen sinyale bağlı olarak, belli zaman ve uzunluk ayarlamalarına göre halka yeniden düzenlenir.

Önce jetonun kendisi kaybolabilir yada zarar görebilir. Bu durumda mantıksal halkanın düzenlenme işlemi devreye sokulabilir. Sonra jeton tutulu iken, istasyon başka bir jetonun varlığını hissedebilir. Bu durumda hemen elindeki jetonu yok eder (drop) ve halkadaki dinleyici modunu değiştirir. Bu durum birçok jetonun yada sıfır jetonun oluşmasına neden olabilir. Sonuçta jeton kurtarma işlemi jeton geçişinde yapılabilir. Geçerli jetonu A yayınladığında, B alır ve acilen veri yada jeton yayınlar. Jeton yollandıktan sonra A herşeyin yolunda olup olmadığını dinler ve aşağıdaki işlemler gerçekleşir;

1- Eğer B aktifse, A geçerli jetonu dinler ve dinleyici modunu değiştirir.
2- Eğer A geçerli jetonu dinleyemiyorsa, ikinci kez jetonu B'ye tekrar yollar.
3- Eğer ikinci denemeden sonrada A hala dinleyemiyorsa, B'nin devre dışı (fail) olduğuna karar verir ve B'den sonraki istasyonu

bulabilmek için takip eden kim çerçevesini (who-follows frame) yayınlar. İlgili cevap gelirse adım 1'den işlem devam eder.

4- Eğer takip eden kim çerçevesine (who-follows frame) bir cevap gelmezse ikinci kez dener.

5- Eğer bunda cevap alamazsa tüm adreslere istek çerçevesi (solicit frame) yollar. Eğer bu işlem başarılı olursa, iki istasyon birleştirilmiş olur.

6- Eğer adım 5 başarısız olursa , A büyük bir sorun olduğuna karar verir ve bu noktada yollayacağı verileri ve jetonu yollamaya çalışır. Aksi halde iletişimi keserek hattı dinlemeye geçer (Naugle, 1991).

4.1.2.2.2. Token bus'da üstünlük

IEEE 802.4 servis sınıflarının kullanılmasıyla üstün erişme mekanizması sağlar. Serviste dört sınıf tanımlıdır. Azalan sırayla 6,4,2 ve 0. Her istasyon bir veya daha fazla sınıfa veri yollayabilir. Obje, kanal kapasitesine göre yüksek üstünlüklü çerçeve (higher priority frame) yada düşük üstünlüklü çerçeve (lower priority frame) kullanabilir.

4.1.2.2.3. CSMA/CD ile token bus

Bus topolojisinde MAC tekniği ile kullanılan temel iki eleman CSMA/CD ile Token Bus'dır. Bu iki tekniğin performans ve güvenlik açısından avantaj ve dezavantajı şunlardır;

CSMA/CD kullanıcılar için iyi, güvenilir ve ucuz sayılabilir. Fakat çarpışma algılama sorun teşkil eder. Sinyallerin köşelerde oluşturduğu sinyal değişimleri ve gürültü yüzünden de bunu engellemek güçtür. Küçük çerçevelerin (frame)

kullanılması beraberinde sorun getirebilir veya yük artışlarında yetersiz kalınabilir. Yine de uzun çerçeve (frame) kullanımında iyidir.

Token Bus ise veri yüzdelerinin artmasında ayakta kalabilen bir protokoldür. Kablo uzaması performansını etkilemez. İstasyonlarının çarpışma belirlemesine gerek yoktur. Tek istenen tüm istasyonlara iletilebilecek güçte bir sinyalin sağlanabilmesidir ki bunu güçlendirmeye gerek kalmadan sağlar. Jeton beklemek için zaman kaybedilir fakat bu bekleme istatiksel bir değer içerir. CSMA/CD'deki gibi çarpışma sahibi istasyonun devre dışı kalmasa gibi bir durum yoktur. Bu durum işlem kontrol ve gerçek zamanlı verilerde pek istenmez. Gerçekte hatların belirli bir sınırının olması ve bu yüzden jeton kaybedilmesi bir dezavantajdır. Token Bus'ın en büyük dezavantajı karmaşık oluşudur. Diğer bir dezavantajı da hattın yüklü oluşunda uç kullanıcıların verimsiz şekilde bekleyişte olmalarıdır.

Hangisinin seçilmesi ise ihtiyaçlara ve ücrete bağlıdır. Elbette tüm bunları alıcı, kendi durumunu göz önünde bulundurarak belirler (Stalling, 1993, 1997).

4.1.2.3. Token ring

IEEE 802.5 standardı ticaret ve endüstride kullanılır. IEEE 802.5 için MAC protokolü **Token Ring**'dir.

4.1.2.3.1. MAC protokolü

Token Ring tekniğinde istasyonlar bir halkaya bağlıdırlar. Tek yöne dolaşan bir jeton vardır. Jeton ile küçük iletiler yollar ve jetonu kullanan istasyon dışındakiler beklemek zorundadır. Jeton boşaldığında yakalayan ilk istasyon iletime geçebilir. Çerçeve (frame) içeren jeton kısa bir tur atar, iletilen

istasyon tarafından yakalanır. Eğer yeni bir ileti gerekmiyorsa jeton halkaya bırakılır, boş jetonu alan istasyon aynı şekilde işlemleri sürdürür. Bu esnada iki durumla karşılaşılır;

- Yollayan istasyon, kendi çerçevesinin (frame) iletimini tamamlar.
- İstasyona gelene kadar çerçeveye (frame) yol gösterilir.

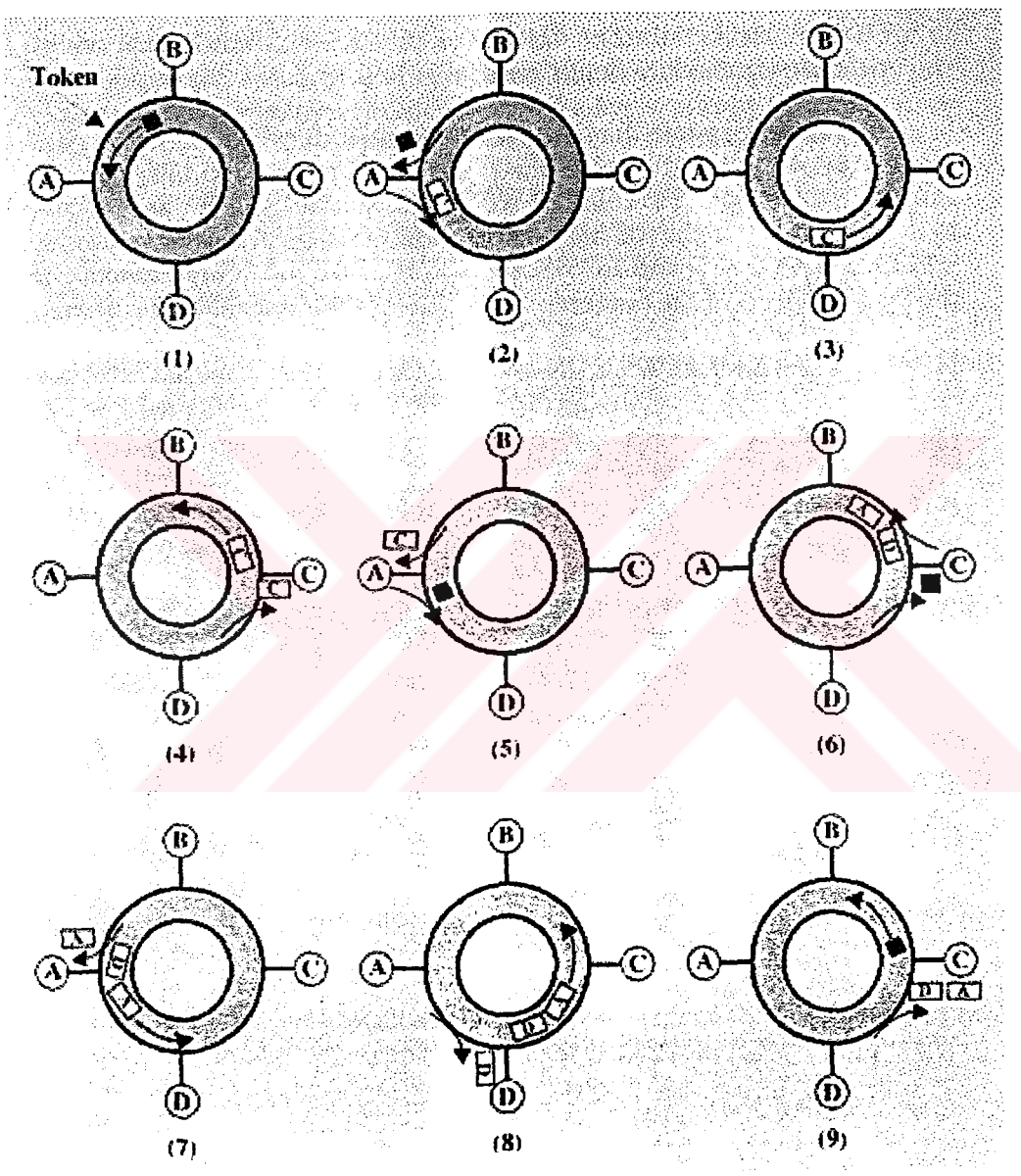
Eğer halkanın bit uzunluğu çerçeve (frame) uzunluğundan azsa ilk durum ikinciyi belirtir. Eğer değilse, istasyon iletimi bittikten sonra jetonu serbest bırakır. Bir seferde ancak tek çerçeve (frame) iletimde olabilir. Halkaya yeni bir jeton atıldığında bir sonraki istasyon bunu değerlendirebilecektir. Şekil 4.12'de A, C'ye paket yollar. C paketi alır ve kendi paketlerini A ve D'ye yollar. Dikkat edilmesi gereken hafif yüklerde etkisizliğin olmasıdır. Çünkü istasyon iletimden önce jetonun turunu beklemek zorunda kalabilir. A, iletimden sonra jetonu salar, ileti yapmak isteyen ilk istasyon D'dir. Eğer D ileti yapmak isterse jetonu yollar bu sefer C sırasını bekler ve işlemler benzer devam eder.

En önemli avantajı erişimde esnek kontrolün olmasıdır. Dezavantajı ise jeton bakımıdır. Çünkü jeton yokluğu iletişimi keser. Jetonların çoğalmasıda halkadaki işlemleri karıştırabilir. Bu yüzden bir istasyon monitör olarak seçilmeli ve jeton bakımıyla ilgilenmelidir.

4.1.2.3.3. Token ring'de üstünlük

IEEE 802.5 standardı üstün seçenekli bir mekanizmaya sahiptir. Sekiz ayrı üstünlük (priority) seviyesi vardır. Bunlar her veri çerçevesi (frame) ve jeton için, iki tane 3 bitlik alan tarafından sağlanır. Bu alan ise üstünlük alanı (priority field) ve reservasyon alanıdır (reservation field).

reserve edilene eşit yada büyük olmalıdır. Eğer üstünlük derecesi fazla olan istasyon kalmazsa, jetonu alan istasyon bu durumda başka üstünlüklü trafik olmayacağından, jetonun seviyesini uygun üstünlüğe ayarlar.



Şekil 4.12. Token ring işleyişi

Şekil 4.13'de şunlar gerçekleşir;

(a) A, B'ye 0 üstünlükte bir veri yolar. Veri bir turdan sonra A'ya geldiğinde bu sefer A jeton çerçeve (frame) yayınlayacaktır. Ancak veri çerçeve (frame), D'ye geçtiğinde D, reservasyon alanını 3'e ayarlayarak, üstünlük 3 seviyesinde reservasyonu yapmış olur.

(b) A, üstünlük 3 seviyesinde bir jeton yayınlar.

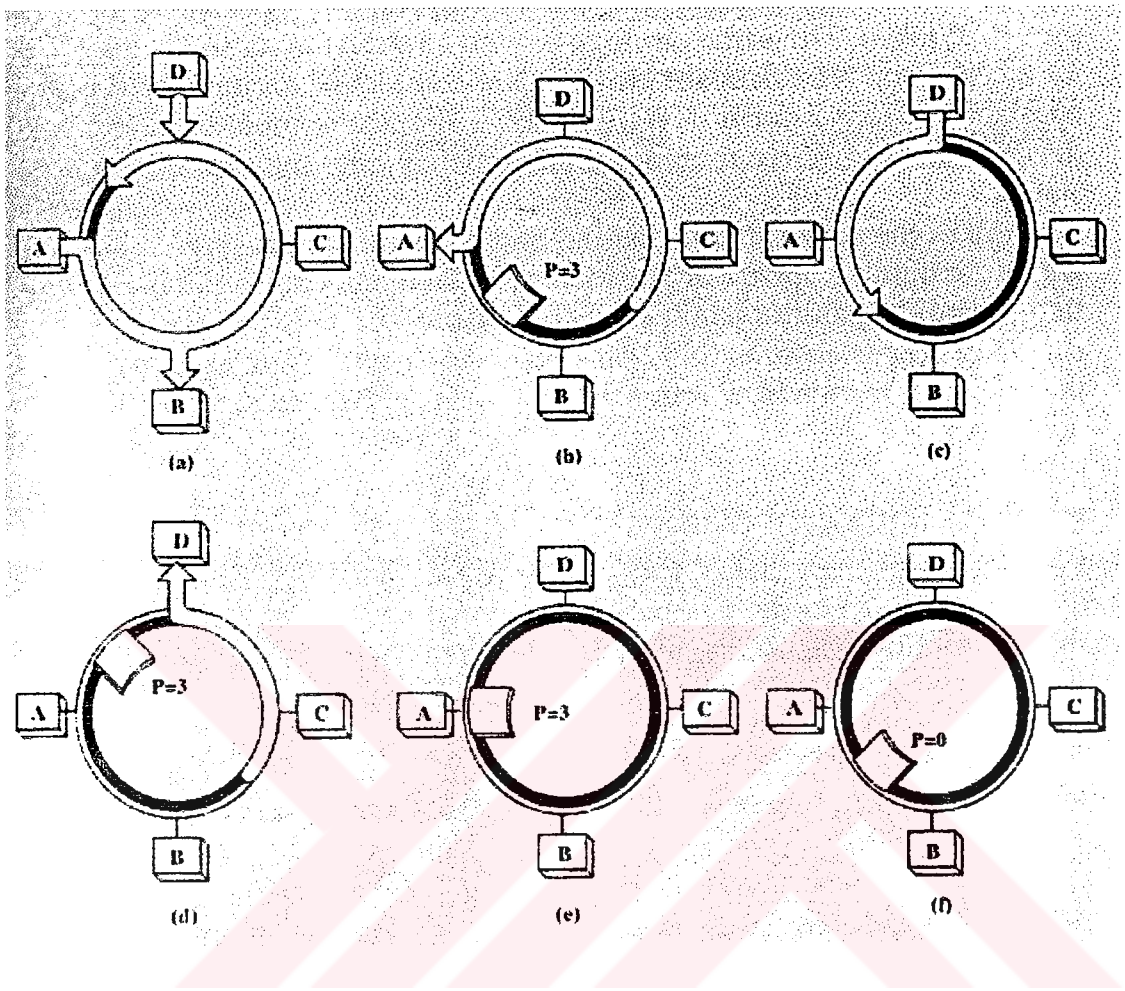
(c) Eğer B ve C'nin üstünlük 3 seviyesinde yada daha büyük seviyede gönderecek bir verisi yoksa , jetonu yakalayamaz ve jeton D'ye döner ve D jetonu yakalayarak veri yollar.

(d) D işlemimi tamamladıktan sonra aynı üstünlük (3) seviyesinde bir jeton yayınlar.

(e) A son yollanan jetonu yollayacak jetonu olmadığı halde yakalar.

(f) A, son üstünlük kademesini dikkate alarak jetonu ayarlar ve yeniden yollar (üstünlük 0)

Dikkat etmek gerekir ki A üstünlük 3 seviyesindeki jetonu gönderdikten sonra, aynı seviyede veya daha büyük seviyede verisi olan bu jetonu yakalayabilir. Bu noktada istasyon C seviyesi 4 olduğundan veri gönderir. C jetonu yakalar ve kendi verisini tarayarak üstünlük seviyesi 3 olan jetonu tekrar yayınlar. D bu zamana kadar jetonu yakalayabilecektir. Üstünlük 3 seviyesindeki jeton A'ya gelinceye kadar 3 veya 3'den büyük olan her istasyon bu veriyi yakalayabilecektir. Son olarak A'nın jetonun seviyesini ayarlaması uygundur (Stalling, 1993, 1997).



Şekil 4.13. Token ring'de üstünlük

4.2. Yerel Ağlarda Performans

Yerel ağların performansı incelenirken performansı etkileyen faktörler ve performans sınırları da ele alınmalıdır. Buna ek olarak IEEE 802 tarafından standartlaştırılmış üç protokolün (CSMA/CD, Token Bus ve Token Ring) performans açısından karşılaştırılması da gerekir.

4.2.1. Performansı Etkileyen Faktörler

Bir LAN'ın performansını etkileyen önemli faktörler şunlardır :

Kapasite (Capacity)

Propagasyon gecikmesi (Propagation delay)

Çerçeve başına düşün bit sayısı (Number of bits per frame)

Yerel ağ protokolleri (Local network protocols)

Sunulan Yük (Offered load)

İstasyon sayısı (Number of stations)

Yerel ağ protokolleri (local network protocols): Fiziksel, MAC ve LLC'den fiziksel katman faktörün çoğu gibi görünmemektedir; genelde iletimlerde ve alımlarda küçük gecikmelerin ötesine pek geçilmez. Bağlantı katmanı (LLC), her çerçeveye (frame) bazı bilgi (overhead) bitleri ekleyecektir. Demek ki, ağ performansını etkileyen kısım ortam erişim (MAC) katmanıdır.

Yukarıda listelenen faktörlerin ağı karakterize ettiği söylenebilir; genelde sabit olarak ele alınırlar veya verilirler. Yerel ağ protokolü, tasarlama çabasına odaklanmıştır, seçim de bu şekilde yapılmaktadır. Son iki faktör, sunulan yük (offered load) ve istasyon sayısı (number of stations), ayrı ayrı ele alınmalıdır. İstasyon başına sabit yük sunulduğu durumda, toplam yükün istasyonların sayısının artışı ile artacağı kesinlikle doğrudur. Aynı artışa, istasyon sayısını sabit tutup, istasyon başına sunulan yükü artırarak da ulaşılabilir. Fakat, görüleceği gibi, ağ performansı bu iki durumda da farklı olacaktır.

Yukarıda listelenmeyen bir faktör: Kanalın hata oranıdır. Çerçeve (frame) iletimindeki bir hata, yeniden iletim gerektirir. Yerel ağlarda çok düşük olmasından dolayı, etkin bir faktör değildir.

4.2.2. Performans sınırları

Herhangi bir LAN'da, sunulan yükün büyüklüğüne dayalı olarak üç işletim bölgesi vardır :

1.Ağ boyunca gecikmelerin az olduğu bölge; kapasite, sunulan yük ile başa çıkabilecek yeterlikten daha fazladır.

2.Ağ boyunca büyük gecikmelerin olduğu bölge; ağ darboğaza girebilir. Bu bölgede, gecikmelerin az olduğu bölgeye kıyasla, ağa erişim denetimi için çok zaman harcanmakta ve gerçek veri iletimine daha az zaman ayrılmaktadır.

3.Sınırsız gecikmelerin olduğu bölge; sunulan yük sistemin toplam kapasitesini aşar.

Son bölge, kolaylıkla tanımlanabilir. Bu üçüncü bölgeden kesinlikle kaçınılmalıdır. Fakat, hemen hemen her zaman, tasarımcı ikinci bölgeye düşmeyi de engellemek isteyecektir. Çünkü ikinci bölge, ağın etkin olmayan kullanımına denk gelir. Ayrıca, ikinci bölgede iken, verilerin ani olarak kabarması, zaten fazla olan gecikmelerin daha da artmasına neden olacaktır. İlk bölgede ağ darboğazda değildir ve belirgin biçimde, uçtan uca gecikmelerin sadece küçük bir kısmına katılır.

Ağ üzerindeki yüke ve ağ özelliklerine dayalı olarak hangi bölgede işleyeceği sorusuna cevap verilecek olursa; Üçüncü bölge kesin olarak tanımlanmıştır ve kaçınılması gerekmektedir. İlk iki bölge arasındaki sınır belirlenmelidir. Ağ bu sınırın altında işlerse, iletişim darboğazına neden olmayacaktır. Sınırın üstünde işlerse, ilgilenilmesi ve yeniden tasarlanması gerekir. Doğru sınırın bulunması ise problemin çözümünde başlangıç noktasıdır; Ağ üzerindeki yük zamanla

değişecek ve sadece tahmin edilebilecektir. Yük tahminlemeleri tam doğru olmayacağından, sınırın tam olarak nerede olduğunun bilinmesine de gerek yoktur. Sınır için iyi bir yaklaşım geliştirilebilirse, tahminlenen yük bu sınırın altında kalacak şekilde boyutlandırılabilir.

4.2.3. Jeton aktarmalı (Token Passing) ve CSMA/CD'nin performans karşılaştırılması

Bu kısmın amacı kullanıcıya, en önemli LAN protokollerinin (CSMA/CD, token bus ve token ring) performansı konusunda bir bakış açısı kazandırmaktır.

Yerel ağın N tane etkin istasyonu olduğu varsayılıyor, jeton aktarımlıda (token passing) gecikme (delay) için ifade türetmek göreceli olarak kolaydır. Bir istasyon (istasyon 1) bir kere ilettiğinde, tekrar iletebilmesi için öncelikle, takip eden şu olayları beklemesi gerekir :

istasyon 1, istasyon 2'ye jeton iletir.
istasyon 2, veri çerçevesini iletir.
istasyon 2, istasyon 3'e jeton iletir.
istasyon 3, veri çerçevesini iletir.
.....
.....
.....
.....
istasyon N-1, istasyon N'e jeton iletir.
istasyon N, veri çerçevesini iletir.
istasyon N, istasyon 1'e jeton iletir.

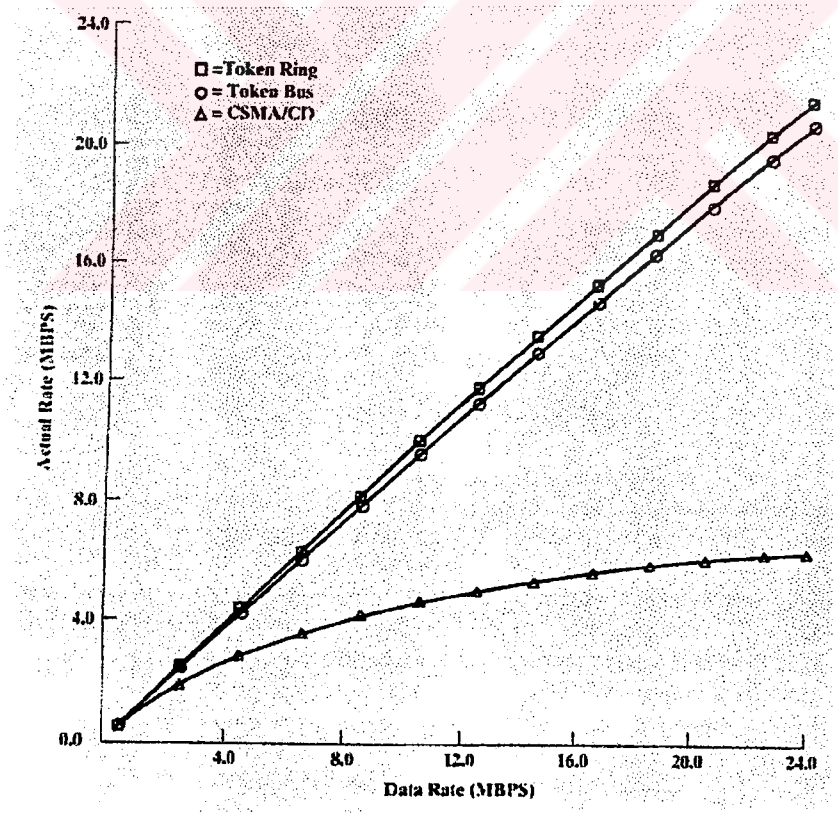
Bu nedenle gecikme, (N-1) devirden oluşmaktadır ve jeton geçirme zamanıdır. Bu nedenle gecikme yük ile doğrusal artar ve sabit sayıda istasyonlardaki gecikme sabittir ve tüm istasyonların her zaman gönderecekleri birşeyler olsa bile sınırlıdır. CSMA/CD gecikmesinin anlatımı zordur ve protokolün kesin doğasına bağlıdır. Genelde, sistem doygunluğa ulaştığında, gecikmelerin de sınırsız artacağı söylenebilir. N arttıkça, daha çok çarpışma ve daha uzun çekişme (contention) aralıkları olacaktır. Tüm istasyonların, (tek tek) çerçevelerinin (frame) başarılı iletim yapabilmeleri için daha çok denemede bulunmaları gerekecektir.

IEEE 802 komitesinin yaptığı daha derin analizin sonuçları anlatılacak olursa; sadece ortalama değerleri dikkate almaya dayalı değil, aynı zamanda gecikme ve mesaj uzunluklarının ikinci momentleri ile de ilgili olduğu görülür. Mesaj varış istatistiklerinin iki durumuna yer verilmiştir. Birincisinde, sadece 100 istasyondan 1 istasyon iletimde bulunacaktır ve her zaman iletime hazırdır. Böyle bir durumda, ağın darboğaza girmeyeceği umulur (sadece bir istasyonlu olma özelliğinin korunması şartı ile). İkinci durumda, 100 istasyondan 100'ü de her zaman iletecek mesaja sahiptir. Bu, tıkanıklığın (congestion) uç bir noktasıdır ve ağın darboğaza gireceği kesin söylenebilir.

Sonuçlar, Şekil 4.14'de gösterilmiştir. Bu, iki km'lik taşıt üzerindeki iletim hızına göre, gerçek veri iletim oranını göstermektedir. 1 istasyon da, 100 istasyon da, ağı tamamı ile kullanılan girdiyi üretebilirler. Grafikler de potansiyel kullanılan toplam kapasite oranının bir ölçüsüdür. Üç sistem incelenmiştir: token ring (istasyon başına 1 bit düşünülerek), token bus ve CSMA/CD. Analiz sonunda şu sonuçlara ulaşılmaktadır:

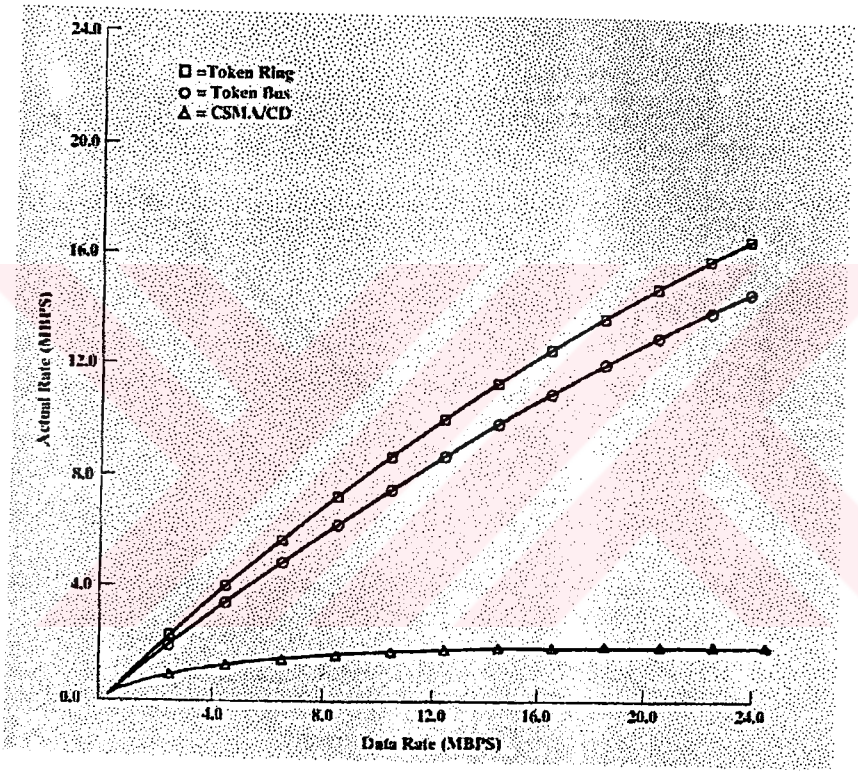
Verilmiş parametreler için, ortalama çerçeve (frame) uzunluğunun küçülmesi, jeton aktarımlı (token passing) ve CSMA/CD arasındaki maksimum ortalama taşınmış olan yük arasındaki farkı büyütmektedir. Token ring, yüke en az duyarlı olanıdır. CSMA/CD hafif yükler altında, en kısa gecikmeyi sağlarken, ağır yük şartlarında en duyarlı olanıdır.

Tek istasyon iletim durumunu düşünürsek, token bus diğer iki protokole göre daha az etkindir. Çünkü, propagasyon gecikmesinin (propagation delay) token ring'dekinden daha uzun olduğu ve jeton işletimindeki gecikmenin token ring'dekinden daha fazla olduğu varsayımı yapılmaktadır.



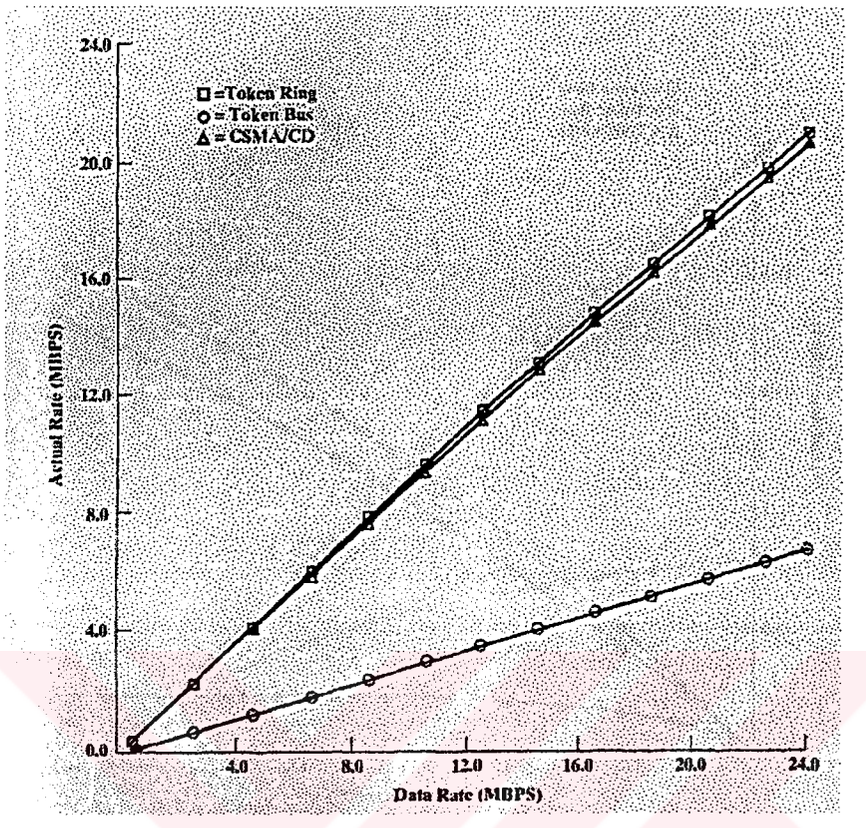
Şekil 4.14. LAN protokolleri için, maksimum potansiyel veri oranı;
a. Paket başına 2000 bit, toplam 100 istasyonun 100'ü de etkin

Dikkate değer diğer bir nokta, Şekil 4.14.b'de açıkça görülmektedir. Bu şartlar altındaki bir CSMA/CD sistemi için, 5 Mbps'de maksimum etkin taşınmış olan yük (throughput) sadece, 1.25 Mbps civarındadır. Beklenen yük 0.75 Mbps ise, bu konfigürasyon uygundur. Bununla birlikte, yükün 2 Mbps'ye çıkarılabileceği beklense de, ağ veri oranını 10 Mbps veya 20 Mbps'ye çıkarmaya ayak uyduramaz.

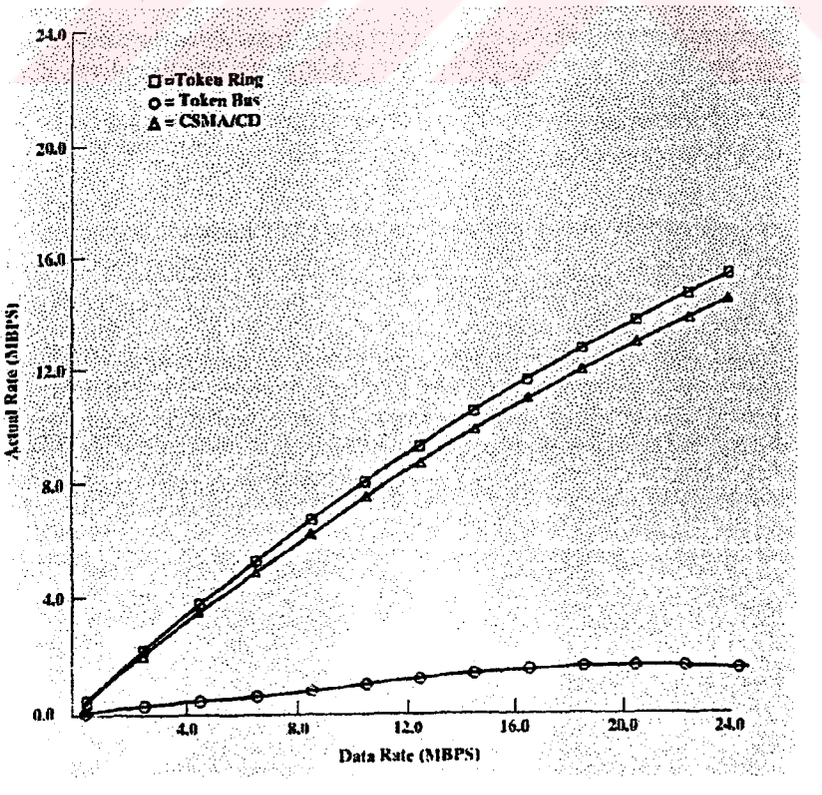


Şekil 4.14.b. Paket başına 500 bit, toplam 100 istasyonun 100'ü de etkin

Bu bölümde sunulan diğer sonuçlarda olduğu gibi, bunlar yapılan varsayımların doğasına bağlıdır ve gerçek dünyadaki yüklerin doğasını tam olarak yansıtmamaktadır. Buna rağmen, çarpıcı bir şekilde CSMA/CD'nin değişkenliğinin doğasını ve token ring ve token bus'ın aşırı yüklü şartlarla yüzleştiğinde, işletimine iyi bir şekilde devam edebilme yeteneğini göstermektedirler (Stalling, 1993, 1997; Bilgisayar Pazarı, 1996; Bilgisayar Pazarı; 1996, Bilgisayar Pazarı; 1996).



Şekil 4.14.c. Paket başına 2000 bit, toplam 100 istasyonun 1'i etkin



Şekil 4.14.d. Paket başına 500 bit, toplam 100 istasyonun 1'i etkin

4.3. Yerel Ağlarda Güvenlik

Yerel iletişim ağlarının (LAN) gelişimi hızlı oldu. Çalışma gruplarının basit araçları olarak başlayan serüven büyük kuruluşların bilgi kullanımında vazgeçemedikleri parçalar haline geldi. Bu yüzden iletişim ağlarının güvenliği üzerinde dikkatle durmak gerekir.

Aslında güvenlik hemen her ağ için gereklidir. Ancak güvenliğin türü bir LAN'dan diğer LAN'a büyük farklılıklar gösterebilir. Günümüzde her ağın gereksinim duyduğu en azından bir güvenlik unsuru vardır; yazılım denetimi. Yazılım denetimi yöntemleri, bir ağda biriktirilen verilerin bütünleşikliği için kaçınılmaz bir öğedir ve bu yöntemlerin uygulanması da bir ağ yöneticisinin en önemli amacı olmalıdır.

Kullanıcıların sayısı ve paylaşılan verilerin ilişkili olduğu birimlerin sayısı arttıkça, denetimsiz yazılımların yol açacağı sorunların sayısı da artacaktır. Verilerin güvenli saklanmaması zaman zaman verimliliğin düşmesine neden olacaktır.

Yazılım denetimi yetkisiz kişilerin yazılımlara (iletişim sistemi, uygulama ve hizmet programları vb.) erişmesini önlemeye, dolayısıyla verileri korumaya yönelik bir yöntemdir. Birçok ağ yöneticisi, kullanıcıların bağımsız olarak ağa yazılım kurmasını engeller. Ancak kurulmuş yazılımlara yetkisiz erişimin de engellenmesi henüz yeni yürürlüğe giren bir uygulamadır.

Yönetim politikası ne olursa olsun, yazılımların yeni uyarlamalarının yapılması yada güncelleştirilmesi her yerde karşılaşılan bir gereksinim ve soru işaretleri yaratan bir noktadır. Yazılım düzeyleri ile uğraşmak, yeni düzeylerin kullanım bilgilerinin ağ çevresinde dağıtılmasını ve eski düzeylerle uyum

sorununun çözülmesini gerektirdiğinden, özellikle zaman ve emek olarak pahalı bir iştir.

Yine de yazılım düzeylerine ilişkin sorunlar, yetkisiz erişimin yol açacağı kadar korkutucu değildir. Gerçek bir koruma yoksa, ağ işletim sistemi ve yönetsel hizmet programlarından başka uygulama programları da yetkisiz kişilerin yaptığı değişikliklerden ve virüslerden etkileneceklerdir. Yetkisiz yazılımları kullanmak ne kadar kolay olursa şifre düzeylerini aşmak ve kullanıcı erişim hakları gibi yönetsel işlevleri değiştirmek o kadar kolay olacaktır. Sorumsuz bir kullanıcı yönetsel denetimi eline aldığı anda şifreleri değiştirebilir, verilere ulaşabilir, hatta verileri değiştirebilir. Ayrıca virüs içeren yazılımları yükleyebilir.

Ağ virüslerinin bilinen bir özelliği veri akışını yavaşlatarak ağın performansını düşürmeleridir. Ayrıca virüsler tarafından ana bilgisayarda yapılan yoğun disk işlemleri sonucu donanım da ısınarak zarar görebilir. Virüsler ve solucanlar (bir iletişim ağında kendini bir düğümden diğerine aktararak yayılmayı amaçlayan virüslerdir), yaptıkları zarar sonucu ağdaki her servisin ve her kullanıcının yeniden yaratılmasını gerektirebileceğinden bu ağ yöneticileri için istenmeyen bir durumdur.

Yerel iletişim ağlarını virüslere karşı korumak için en etkili yöntem yazılım denetimidir. Diğer güvenlik önlemleriyle birlikte, ağa yetkisiz erişimi önlemeye yönelik bir duvar örülür. Ardışık şifreler, geçerliliği zamana bağımlı şifreler ve verileri şifreleme gibi yöntemler gelişmiş koruma yüntemleridir. Parmak izine, sese ve hatta gözün retinasındaki damar yapısına göre kullanıcıyı tanıyan ve erişim izni veren sistemler daha güvenilir olmakla birlikte yüksek bedelleri nedeniyle daha az kullanılan yöntemlerdir.

Güvenlik konusunda ele alınması gereken diğer bir nokta da ağların güvenliğinin fiziksel olarak aşılmasını önlemek üzere kullanılan geri-aramalı modemler, fiber optik kablolama, fiziksel korumalı ana bilgisayarlar vb. araçlardır. Bütün bunlar iyi yöntemler olmakla beraber yine de aşılabilirler. Yetkisiz bir kullanıcı bu önlemi aştığı anda ağ verilerine korumasız ulaşacaktır.

Yazılım denetimi yöntemleri, iyi programları içeride, kötü programları dışarıda tutarak uygulama programlarının kararlılığını arttıracak dolayısıyla verileri koruyacaktır. Yazılım denetimi yöntemlerinin belkide en kolayı fiziksel yaklaşımlardır; bilgisayarlardaki disket dürücülerini kullanım dışı bırakarak kullanıcıların ağdan veri çıkarmalarını ve ağa yazılım yüklemelerini önlemek gibi. Bu yöntem çoğu zaman etkin olsa bile bir koruyucu yöntemdir ve başka yollarla, örneğin modem bağlantısı ile aşılabilir.

Yaygın olan bir başka yaklaşım da kullanıcıların işletim sistemine erişimini engellemektir. Bu bir menüler sistemi ile kolayca başarılabilir. Menüler başlangıçta ağda, işlemlerin rahat bir şekilde yapılmasını sağladıkları için yaygınlık kazanmışlardı. Ama şimdi güvenlik aracı durumuna geldiler. Kullanıcı erişim yetkisine bağlı olarak kişiselleştirilmiş menüler kullanıcının erişebildiği olanakları kısıtlayarak işletim yazılımına ulaşmasını engeller.

Bugün ticari yazılım denetimi ürünlerinin çoğunda bulunan yazılım gözleme yöntemi daha iyi bir koruyucu önlemdir. Bu ürünler sürekli olarak ağ düğümlerindeki etkinlikleri denetler, bir kullanıcı yetkisi olmayan bir etkinlikte bulunursa onun düğümünü ağ dışında bırakarak ağ yöneticisine alarm verirler. Böylece ağ yöneticisinin onaylamadığı programların yüklenmesi engellenir.

Program tanıma daha karmaşık bir yazılım denetimi yöntemidir. Bazı yazılım denetimi ürünleri bir program çalıştırılacağı zaman onu asıl kopyası ile karşılaştırılarak bozulup bozulmadığını denetlerler. Bu karşılaştırma tabi ki birebir değil, çalıştırılacak programa ait bazı parametrelerin hesaplanarak ana programa ait olan verilerle aynı olup olmadıklarına bakarak yapılır. Böylece o programa bir virüsün bulaşıp bulaşmadığı belirlenebilir.

Yazılım denetiminin hem engelleyici hem de tanımaya dayalı yöntemlerle gerçekleştirmek en idealidir. Böylece ağ yöneticisi ağa yüklenen ve ağda çalıştırılan tüm yazılımlardan haberdar olur, dolayısıyla verilerin güvenlikli bir ortamda saklanması sağlanır.

Güvenlik yazılımları ağ yönetiminde daha yüksek bir düzeye gelmelidir. Ağ yöneticileri de bu alanda sürekli gelişmelerin olmasını beklemeli ve istemelidirler. Ağlara bağımlı insanların sayısı artarken güvenlik ve bütünleşiklik, iletişim ağlarının en önemli öğesi olmalıdır (Cerit, 1991; Bilgisayar Pazarı, 1991).

5. SONUÇ

Bilgi çağını yaşadığımız günümüzde en yeni ve doğru bilgiye kısa zamanda ulaşmak oldukça önemlidir. Bilgisayar ve enformatik bilimi bu istekleri kolaylaştırabilmek için sürekli olarak ve çok hızlı bir biçimde gelişmektedir. Mevcut bilgilerin ve kaynakların daha verimli kullanılması isteği iletişim ağlarının kurulmasına neden olmuştur. Bir iletişim ağı sayesinde mevcut kaynakların, yani tüm yazılım ve donanım birimlerinin, en verimli ve en etkili şekilde kullanımı sağlanır. Bütün bilgisayarlarda kaynak arttırmasına gitmek çok büyük masraflara yol açar. Oysa bir iletişim ağında büyük bir sabit diske sahip bir bilgisayar vardır. Bütün programlar bu sabit diske kurulur ve iletişim ağındaki diğer kullanıcılar bu bilgisayardan çalıştırırlar. Böyle bir yapının en önemli iki avantajından birincisi, ağdaki bütün bilgisayarlara büyük birer sabit disk koymak yerine, yalnızca kendi verilerini saklayacakları küçük birer sabit disk koyarak maliyeti azaltmaktır, ikincisi ise; yeni program uyarlamasının güncellenmesini yalnızca bu bilgisayar üzerinde yaparak bütün ağ kullanıcılarının yeni uyarlama programları aynı anda kullanmaya başlamasını sağlamak olacaktır. Bu özellik, yapı içerisinde standardizasyonun sağlanması için önemli bir avantaj sağlar. Bir kullanıcı eski uyarlama program, diğeri yeni uyarlama program kullanırsa, birbirleri arasında veri aktarımı zorlaşması hatta bazen imkansız hale gelme problemi de çözülmüş olur (Akın, 1996; Çubukcu, 1994; Arslantunalı, 1992; Arslan, 1995)

Büyüklüklerine ve kullanım alanlarına göre LAN, MAN ve WAN'dan; LAN olarak adlandırılan yerel bilgisayar ağlarının performans açısından diğerlerinden en önemli farkı ve üstünlüğü, bilgisayar ağının sahibi olanların bilinçli bir kurulum ve kullanımla LAN performansını yükseltmesi mümkündür.

Hemen hemen bütün yerel bilgisayar ağlarında yüksek hızlı bir omurga (backbone) olur. Omurga bir bilgisayar ağının temel bağlantısını oluşturur ve ne kadar hızlı olursa bilgisayar ağı da okadar hızlı olur.

Bir başka nokta da, hızın kullanıcı sayısıyla ters orantılı olduğudur. Büyük bilgisayar ağlarında daha çok kullanıcı ve bilgisayar ağa bağlı olacağından, bilgisayar ağının hızı da azalacaktır.

Yerel bilgisayar ağlarının diğerlerinden bir başka farkı ise; planlamanın daha ciddi bir biçimde yapılmasıdır. Büyük bilgisayar ağları genellikle onları oluşturan ufak bilgisayar ağlarının özelliklerine sahiptir. Yani yerel bilgisayar ağlarının performansına bağımlıdır. Yeni yerel bilgisayar ağları kurulup büyük bilgisayar ağlarının birer parçası oldukça, MAN ve WAN'ların da büyüklükleri artar. Bu nedenle belki metropolitan ağların değil, özellikle geniş alan bilgisayar ağlarının alt yapı tasarımı çok güç ve çoğu kez plansızdır. Oysa yerel bilgisayar ağı kurulurken, önce detaylı bir çalışma ve mali analiz yapılır. Bu sayede hem bütçeye uygun bir ağ kurulur, hem de kurulacak olan ağ planlı aşamlarla belli bir sistematiğe sahip olur. Böylece en yüksek performans sağlanmış olur (Arslan, 1995; Networking Technologies, 1994; Aydın, 1992).

Yerel bilgisayar ağının hangi topolojiye göre kurulduğu, yani; donanımın matematiksel olarak ne şekilde bağlandığı oldukça önem taşır;

Yol topolojisinin kurulumu diğer topolojilere göre göreceli olarak daha kolaydır. Bakımı ortalama olarak daha zordur, çünkü her cihazın omurgaya (backbone) bağlanabilmesi için bağlayıcıların belirli mesafelerle takılması gerekir. Bunların takılabileceği alan kalmadığı takdirde omurganın yenilenmesi gerekebilir. Sorunları yakalamak pek kolay değildir. Bunun sebebi ise bütün bilgisayarlar tek bir kablo üzerine bağlanmışlardır ve izole etmek oldukça

güçtür. Kablo üzerinde bir arıza meydana geldiği zaman bağlı bütün cihazlar bundan etkilenir.

Ringler kapalı bir devre oluşturulması gerektiği için yol tipi yapılara göre daha fazla techizat gerektirirler. Bu tür bir topolojinin bakımı, güncellenmesi oldukça zordur. Hata bulmak oldukça kolaydır. Bunun sebebi ise, her cihaz bir tekrarlayıcı (repeater) olduğu için sinyali alamayan veya gönderemeyen cihazı tespit etmek daha kolaydır. Çoğu halka sistemlerinde meydana gelen sorundan tüm cihazlar etkilenir. Fakat çift döngü kullanan halkalar da mevcuttur. Bu halkalarda döngülerden birinde bir sorun meydana gelirse diğeriyle işleme devam ediler.

Yıldız topolojisinin kurulumu orta zorluktadır. Zorluğu her cihaza ayrı kablo çekilmesinden kaynaklanmaktadır. Bakımı ve güncelenmesi oldukça kolaydır. Sorunların tespit edilmesi ve çözülmesi oldukça kolaydır. Her hangi bir noktada meydana gelen sorunda sadece o noktaya bağlı cihaz etkilenmektedir.

Kafes topolojisinde; her bilgisayar diğer bir bilgisayara doğrudan bir hat ile bağlı olması gerektiği için ayrı bir arabirim (interface) kartı gerektirmektedir. Bu yüzden bu topoloji türü pratikte pek fazla uygulanamamaktadır. Bu tür topolojilerde hata toleransı oldukça yüksektir ve her bağlantı sistem performansını doğru orantılı olarak arttırır. Kafes topolojisinin kurulumu oldukça zordur, çünkü bütün bilgisayarlar birbirlerine teker teker doğrudan bağlanmak zorundadır. Bakımı ve güncellenmesi oldukça zordur. Hata bulma ve düzeltme çok kolaydır. Hata toleransı oldukça yüksektir çünkü bilgisayarlar arasında alternatif pek çok bağlantı söz konusudur.

Hücresel topolojinin kurulumu, merkeze konulacak hubın yerleşimi ile doğru orantılıdır. Eğer hub istenilen yere konulabiliyorsa kurulum oldukça kolaydır,

aksi takdirde büyük zorluklarla karşılaşılabilir. Kablosuz bir iletişim söz konusu olduğu için güncellenmesi ve bakımı oldukça kolaydır. Hata tespiti kolaydır. Her hangi bir problem karşısında herkes etkilenir, çünkü ortamda herkes aynı koşullarda çalışmaktadır (aynı oda gibi) (Networking Technologies, 1994; Aydın, 1992).

Yerel bilgisayar ağlarında, bilgisayarlar birbirlerine bağlanırken kullanılan kablolardan UTP, diğer kablo türlerine göre ucuzdur. Kurulumu oldukça kolaydır. 1 ile 100 Mbit/s veri iletişim hızına çıkabilir. Manyetik dalgalardan etkilenir. Bilgisayar ağlarında tip 3 ve tip 5 UTP kablo türleri yaygın olarak kullanılmaktadır. tip 5'de ağ performansını artırıcı ilave özellikler (daha fazla sarmal kablo ve daha iyi izalasyon) konulmuştur.

STP kablo ise; UTP kabloya göre biraz pahalı olmakla beraber thick coax ve fiber kablolardan ucuzdur. Kurulumu UTP'ye göre daha zordur. Teorik olarak 100 metre içerisinde 500 Mbit/s'e kadar çıkabileceği söylenmektedir, fakat bugüne kadar 155 Mbit/s üzerine çıkılmış değildir. Genel olarak 16 Mbit/s olarak kullanılmaktadır. UTP'ye göre manyetik dalgalardan daha az etkilenir.

Eş eksenli kablonun kurulumu kolaydır. Kapasitesi 10 Mbit/s'dir. Manyetik alandan ve elektrik alanından etkilenir (Networking Technologies, 1994; Frank and Derfler, 1996; Halsall, 1989; Pye, 1985).

Fiber optik kablolar ve bağlayıcıları diğer kablo tiplerine göre oldukça pahalıdır. Kurulumu oldukça zordur ve uzmanlık gerektirir. 100 Mbit/s ile 2 Gbit/s arasında iletişim hızına sahiptir ve 2 ila 25 kilometre mesafelere kadar kullanılabilir. Manyetik alandan ve elektrik alanından kesinlikle etkilenmez. Bu özellikleriyle fiber kablolar geleceğin teknolojisi olarak görülmektedir (Networking Technologies, 1994; Langley, 1990; Bilgisayar Pazarı,1993).

Değişik bilgisayar firmalarının ürettikleri bilgisayarlar arasındaki iletişimi bir standarda oturtmak ve farklı standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak amacıyla ISO (International Standarts Organization) tarafından yedi katmanlı OSI (Open System Interconnection - Açık Sistem Bağlantısı) referans modeli geliştirilmiştir.

Ayrıca, IEEE (The Institute of Electrical and Electronics Engineers), OSI katmanlarını kullanarak, yerel bilgisayar ağları için; kablolamayı, fiziksel topolojiyi, mantıksal topolojiyi ve ağ birimlerinin erişim düzenini açıklayan bir standartlar takımı geliştirmiştir. Bu satandartlar IEEE 802 olarak anılır ve OSI modelinin en alt iki katmanında kullanılan protokolleri açıklar. Bu katmanların üstündeki katmanlarla bir ilgileri yoktur. IEEE 802 standardının en büyük avantajı kullanıcının sahip olduğu donanımın, OSI'nin fiziksel ve veri bağlantı katmanlarını bir standarda sokarak cihazların uyumlu iletişimini sağlamaktır.

Komite hızlı bir şekilde iki sonuca ulaştı. Birincisi, yerel ağlar arasındaki iletişim işi, yönetilebilir parçalara bölünmesi gerekecek kadar karmaşık bir iştir. İkincisi, hiçbir teknik yaklaşım tek başına tüm gereksinimleri karşılayamaz.

IEEE 802 standartlarından CSMA/CD, Token Bus, ve Token Ring için şunlar söylenebilir; Yol ve yıldız topolojileri için MAC ile en geçerli olanı CSMA/CD tekniğidir. Rasgele erişimde iki çerçeve (farme) karışır ve çarpışma meydana getirebilir, şunlara dikkat etmek gerekir; istasyondan istasyona propagasyon zamanı iyice karşılaştırılmalı, istasyonun yolladığı çerçevenin (frame) ulaşması için geçecek propagosyon zamanından önce karşı taraf bir iletide bulunursa çerçeveler (frame) birbirleri ile karşılaşabilir. Mesafenin fazla olması, bağımsız olarak bir çok istasyonun aynı anda birbirleri ile sağlıklı iletişim kurmasına imkan verir. Çarpışma olmaması için çerçeve (frame)

yollayan istasyon gecikme miktarını istasyonlara bildirerek bu sırada iletişime geçmelerine engel olabilir. Başka bir bakışta kısa gecikme zamanı ve iyi bir geri besleme ile verimi arttırmaktır (Halsall, 1989).

Normal olarak çerçeve (frame) iletim zamanı, propagasyon gecikmesinden çok fazladır. Çarpışmaya bağlı olarak propagasyon gecikmesi de artar. Maksimum kullanım çerçeve (frame) uzunluğuna ve propagasyon gecikmesine bağlıdır. Çerçeveler (frame) ve propagasyon gecikmesi azaldıkça kullanım miktarı artar.

CSMA/CD'de kullanılan üç değişik algoritma ısrarcı olmayan (non-persistent), 1-ısrarcı (1-persistent) ve p-ısrarcı (p-persistent)'dır. En geçerlisi 1-ısrarcı (1-persistent)'dır. Ethernet tarafından kullanılan IEEE 802 standardıdır. Unutmamalıdır ki ısrarcı olmayan (non-persistent) ve p-ısrarcı (p-persistent)ın performans sorunu vardır. Israrcı olmayanda (non-persistent) kapasite boşuna ayarlanır çünkü iletimin sonunda ancak ortam boşalır. p-ısrarcıda (p-persistent) ise p düşük tutulmalıdır ve bu da kararsızlığa sebep olur. Çarpışa sonrası çarpışma olasılığı düşük de olsa sıfır değildir ve çarpışmadan sonra üretilen rasgele gecikme zamanı her seferinde ikiye katlanır (Stalling, 1993, 1997; Martin et al., 1994).

Yol topolojisinde kullanılan Token Bus olarak bilinen IEEE 802.4 protokolünün bir üstünlügü, servis sınıflarının kullanılmasıyla üstün erişme mekanizması sağlar. Serviste dört sınıf tanımlıdır. Azalan sırayla 6,4,2 ve 0. Her istasyon bir veya daha fazla sınıfa veri yollayabilir. Obje, kanal kapasitesine göre yüksek üstünlüklü çerçeve (higher priority frame) yada düşük üstünlüklü çerçeve (lower priority frame) kullanabilir.

Token bus ve CSMA/CD tekniklerinin avantaj ve dezavantajları şunlardır; CSMA/CD kullanıcılar için iyi, güvenilir ve ucuz sayılabilir. Fakat çarpışma algılama sorun teşkil eder. İşaretlerin köşelerde oluşturduğu işaret değişimleri ve gürültü yüzünden de bunu engellemek güçtür. Küçük çerçevelerin (farme) kullanılması beraberinde sorun getirebilir veya yük artışlarında yetersiz kalınabilir. Yine de uzun çerçeve (frame) kullanımında iyidir.

Token Bus ise veri yüzdelerinin artmasında ayakta kalabilen bir protokoldür. Kablo uzaması performansını etkilemez. İstasyonlarının çarpışma belirlemesine gerek yoktur. Tek istenen tüm istasyonlara iletilebilecek güçte bir işaretin sağlanabilmesidir ki bunu güçlendirmeye gerek kalmadan sağlar. Jeton beklemek için zaman kaybedilir fakat bu bekleme istatiksel bir değer içerir. CSMA/CD'deki gibi çarpışma sahibi istasyonun devre dışı kalmasa gibi bir durum yoktur. Bu durum işlem kontrol ve gerçek zamanlı verilerde pek istenmez. Gerçekte hatların belirli bir sınırının olması ve bu yüzden jeton kaybedilmesi bir dezavantajdır. Token Bus'ın en büyük dezavantajı karmaşık oluşudur. Diğer bir dezavantajı da hattın yüklü oluşunda uç kullanıcıların verimsiz şekilde bekleyişte olmalarıdır.

Hangisinin seçilmesi ise ihtiyaçlara ve ücrete bağlıdır. Elbette tüm bunları alıcı, kendi durumunu göz önünde bulundurarak belirler.

Token ring olarak bilinen ve istasyonların bir halkaya bağlı bulunduğu IEEE 802.5 standardının en önemli avantajı erişimde esnek kontrolün olmasıdır. Dezavantajı ise jeton bakımıdır. Çünkü jeton yokluğu iletişimi keser. Jetonların çoğalmasıda halkadaki işlemleri karıştırabilir. Bu yüzden bir istasyon monitör olarak seçilmeli ve jeton bakımıyla ilgilenmelidir (Stalling, 1993, 1997).

Bir LAN'ın performansını etkileyen önemli faktörler şunlardır :

- Kapasite (Capacity)
- Propagasyon gecikmesi (Propagation delay)
- Çerçeve başına düşün bit sayısı (Number of bits per frame)
- Yerel ağ protokolleri (Local network protocols)
- Sunulan Yük (Offered load)
- İstasyon sayısı (Number of stations)

Yerel ağ protokolleri (local network protocols): Fiziksel, MAC ve LLC'den fiziksel katman faktörün çoğu gibi görünmemektedir; genelde iletimlerde ve alımlarda küçük gecikmelerin ötesine pek geçilmez. Bağlantı katmanı (LLC), her çerçeveye (frame) bazı overhead bitleri ekleyecektir. Demek ki, ağ performansını etkileyen kısım ortam erişim (MAC) katmanıdır.

Yukarıda listelenen faktörlerin ağı karakterize ettiği söylenebilir; genelde sabit olarak ele alınırlar veya verilirler. Yerel ağ protokolü, tasarlama çabasına odaklanmıştır, seçim de bu şekilde yapılmaktadır. Son iki faktör, sunulan yük (offered load) ve istasyon sayısı (number of stations), bu iki değişkenin fonksiyonu olarak performansı belirleme ile ilgilidir. Bu iki değişken ayrı ayrı ele alınmalıdır. İstasyon başına sabit yük sunulduğu durumda, toplam yükün istasyonların sayısının artışı ile artacağı kesinlikle doğrudur. Aynı artışa, istasyon sayısını sabit tutup, istasyon başına sunulan yükü artırarak da ulaşılabilir. Fakat, görüleceği gibi, ağ performansı bu iki durumda da farklı olacaktır.

Yukarıda listelenmeyen bir faktör: Kanalın hata oranıdır. Çerçeve (frame) iletimindeki bir hata, yeniden iletim gerektirir. Yerel ağlarda çok düşük olmasından dolayı, etkin bir faktör değildir.

Herhangi bir LAN'da, sunulan yükün büyüklüğüne dayalı olarak üç işletim bölgesinden; üçüncüsü olan sınırsız gecikmelerin olduğu bölgeden kesinlikle kaçınılmalıdır. Fakat, hemen hemen her zaman, tasarımcı ikinci olan ağ boyunca büyük gecikmelerin olduğu bölgeye düşmeyi de engellemek isteyecektir. Çünkü ikinci bölge, ağın etkin olmayan kullanımına denk gelir. Ayrıca, ikinci bölgede iken, verilerin ani olarak kabarması, zaten fazla olan gecikmelerin daha da artmasına neden olacaktır. Birinci olan ağ boyunca gecikmelerin az olduğu bölgede ağ darboğazda değildir ve belirgin biçimde, uçtan uca gecikmelerin sadece küçük bir kısmına katılır.

Ağ üzerindeki yüke ve ağ özelliklerine dayalı olarak hangi bölgede işleyeceği sorusuna cevap verilecek olursa; Üçüncü bölge kesin olarak tanımlanmıştır ve kaçınılması gerekmektedir. İlk iki bölge arasındaki sınır belirlenmelidir. Ağ bu sınırın altında işlerse, iletişim darboğazına neden olmayacaktır. Sınırın üstünde işlerse, ilgilenilmesi ve yeniden tasarlanması gerekir. Doğru sınırın bulunması ise problemin çözümünde başlangıç noktasıdır; Ağ üzerindeki yük zamanla değişecek ve sadece tahmin edilebilecektir. Yük tahminlemeleri tam doğru olmayacağından, sınırın tam olarak nerede olduğunun bilinmesine de gerek yoktur. Sınır için iyi bir yaklaşım geliştirilebilirse, tahminlenen yük bu sınırın altında kalacak şekilde boyutlandırılabilir.

Token Bus, Token Ring ve CSMA/CD arasında yüke en az duyarlı olanı Token Ring'dir. CSMA/CD hafif yükler altında, en kısa gecikmeyi sağlarken, ağır yük şartlarında en duyarlı olanıdır (Stalling, 1993, 1997).

Tek istasyon iletim durumunu düşünürsek, token bus diğer iki protokole göre daha az etkindir. Çünkü, propagasyon gecikmesinin (propagation delay) token ring'dekinden daha uzun olduğu ve jeton işletimindeki gecikmenin token ring'dekinden daha fazla olduğu varsayımı yapılmaktadır.

Güvenlik her ağ için gereklidir. Ancak güvenliğin türü bir LAN'dan diğer LAN'a büyük farklılıklar gösterebilir. Günümüzde her ağın gereksinim duyduğu en azından bir güvenlik unsuru vardır; yazılım denetimi. Yazılım denetimi yöntemleri, bir ağda biriktirilen verilerin bütünleşikliği için kaçınılmaz bir öğedir ve bu yöntemlerin uygulanması da bir ağ yöneticisinin en önemli amacı olmalıdır.

Yazılım denetimi yetkisiz kişilerin yazılımlara (iletişim sistemi, uygulama ve hizmet programları vb.) erişmesini önlemeye, dolayısıyla verileri korumaya yönelik bir yöntemdir. Gerçek bir koruma yoksa, ağ işletim sistemi ve yönetsel hizmet programlarından başka uygulama programları da yetkisiz kişilerin yaptığı değişikliklerden ve virüslerden etkileneceklerdir. Yetkisiz yazılımları kullanmak ne kadar kolay olursa şifre düzeylerini aşmak ve kullanıcı erişim hakları gibi yönetsel işlevleri değiştirmek okadar kolay olacaktır.

Ağ virüslerinin bilinen bir özelliği veri akışını yavaşlatarak ağın performansını düşürmeleridir. Ayrıca virüsler tarafından ana bilgisayarda yapılan yoğun disk işlemleri sonucu donanım da ısınarak zarar görebilir.

Diğer güvenlik önlemleriyle birlikte, ağa yetkisiz erişimi önlemeye yönelik bir duvar örülür. Ardışık şifreler, geçerliliği zamana bağımlı şifreler ve verileri şifreleme gibi yöntemler gelişmiş koruma yüntemleridir. Parmak izine, sese ve hatta gözün retinasındaki damar yapısına göre kullanıcıyı tanıyan ve erişim

izni veren sistemler daha güvenilir olmakla birlikte yüksek bedelleri nedeniyle daha az kullanılan yöntemlerdir.

Güvenlik konusunda ele alınması gereken diğer bir nokta da ağların güvenliğinin fiziksel olarak aşılmasını önlemek üzere kullanılan geri-aramalı modemler, fiber optik kablolama, fiziksel korumalı ana bilgisayarlar vb. araçlardır.

Yazılım denetiminin hem engelleyici hem de tanımaya dayalı yöntemlerle gerçekleştirmek en idealidir. Böylece ağ yöneticisi ağa yüklenen ve ağda çalıştırılan tüm yazılımlardan haberdar olur, dolayısıyla verilerin güvenlikli bir ortamda saklanması sağlanır.

Güvenlik yazılımları ağ yönetiminde daha yüksek bir düzeye gelmelidir. Ağ yöneticileri de bu alanda sürekli gelişmelerin olmasını beklemeli ve istemelidirler. Ağlara bağımlı insanların sayısı artarken güvenlik ve bütünleşiklik, iletişim ağlarının en önemli öğesi olmalıdır (Cerit, 1991; Bilgisayar Pazarı, 1991).

KAYNAKLAR

Akgül, M. K., (1992) Bilgisayar Ağları ve Bilgi İletişimi. **Bilgisayarın Uygulamalarda Etkin Kullanımı Semineri,** Milli Prodüktivite Merkezi, Ankara.

Akın, C., (1996) **Her Yönüyle Internet.** Alfa Basım Yayım Dağıtım, İstanbul.

Arslan, A., (1995) İletişim Ağı Nedir, Niçin Gereklidir ? **Bilgisayar Pazarı** (83) 56-59, İstanbul.

Arslan, A.,(1995) Bilgisayar Ağlarının Yapısı. **Bilgisayar Pazarı** (84) 36-46, İstanbul.

Arslantunalı, M., (1992) **Herkes İçin Ansiklopedik Kişisel Bilgisayar Klavuzu.** PcWorld, İstanbul.

Aydın, E.D., (1992) **Bilgisayar, Bilgi İşlem ve Telekomünükasyon, Bilişim Sistemleri Sözlüğü.** Doruk Yayınları, Saydam Matbaacılık, Ankara.

Ayfer, C. U., (1996) **Kim Korkar Internet'ten ?** Pusula Yayıncılık ve İletişim Ltd., İstanbul.

Bilgisayar Pazarı (1991) İletişim Ağlarında OSI Referans Modeli. **Bilgisayar Pazarı,** (30), 18-19, İstanbul.

Bilgisayar Pazarı (1991) İletişim Ağlarında Güvenlik. **Bilgisayar Pazarı,** (30), 38-39, İstanbul.

Bilgisayar Pazarı (1993) Tüm Yönleriyle İletişim Ağları. **Bilgisayar Pazarı,** (59) 88-98, İstanbul.

Bilgisayar Pazarı (1994) Lan'ın Ardında Neler Gizleniyor ? **Bilgisayar Pazarı,** (63) 78-80, İstanbul.

Bilgisayar Pazarı (1996) Lan Performansını İyileştirme. **Bilgisayar Pazarı,** (92) 30-34, İstanbul.

Bilgisayar Pazarı (1996) Lan Performansını İyileştirme 2. **Bilgisayar Pazarı,** (93), 40-46, İstanbul.

Bilgisayar Pazarı (1996) Lan Performansını İyileştirme 3. **Bilgisayar Pazarı,** (94), 62-67, İstanbul.

Bratt, C., (1992) **Tele-Communications Data Network 1.** Ericssons, Televerket and Student Litteratuur, Sweden.

Cerit, B., (1991) İletişim Ağlarında Güvenlik Sorunu. **PcWorld** (6) 88-90, İstanbul.

Collin, S., (1990) **Computer Interfaces and Communication Network.** Printice-Hall Inc., USA.

Çağıltay, K., (1995) **Herkes İçin Internet.** Tübitak Matbaası, 2.Baskı, Ankara.

Çubukcu, F., (1994) **Novell NetWare İşletim Sistemi.** Türkmen Kitabevi, İstanbul.

Erdem, A., (1996) **Bilgisayar Ağları ve Uygulamaları.** Erbek Ltd.Şti., Ankara.

Frank, J.&Derfler, J., (1996) **Network Sistemleri ve Bilgisayar Bağlantı Klavuzu.** Sistem Yayıncılık, İstanbul.

Halsall, F., (1989) **Data Communications, Computer Network and OSI.** Addison- Wesley Publishing Company, 2nd Edition, USA.

Held, G., (1993) **Understanding Data Communications.** SAMS, 3rd Edition, USA.

Henshall, J., Shaw S., (1989) **OSI-Explained.** Ellis Horwood Ltd. 2nd Edition, England.

Intertam (1997) **OfisLog Ürün Fiyat ve Satış Katoloğu.** Intertam A.Ş., İstanbul.

Langley, G., (1990) **Telecommunications Primer.** Pitman Publishing Company, 3rd Edition, UK.

Martin J., Chapman K. K., Leben, J., (1994) **Local Area Networks Architectures and Implementation.** Printice-Hall Internation Inc. 2nd Edition, USA.

Meijer, A., Peeters, P., (1983) **Computer Network Architectures.** Pitman Publishing, 2nd Edition, UK.

Modem ve Kullanımı. **Byte-BBS**, Modem Eki, 1995, İstanbul.

Naugle, M. G., (1991) **Local Area Networking.** McGraw Hill Inc, USA.

Networking Technologies. Novell Education , Novell Inc., 1994, USA.

Oktay, D., (1997) Networking Dersleri. **Network World** (12), 63-65, İstanbul.

Oktay, D., (1997) **Kim Korkar Network'ten ?** Pusula Yayıncılık ve İletişim Ltd., 2. Baskı , İstanbul.

Ön, N., (1994) Yerel İletişim Ağları. **Bilgisayar Ağları ve İletişim Semineri,** Türkiye Bilişim Derneği, Antalya.

Pye, C., (1985) **Networking with Microcomputers.** NCC Publications, Manchester, England.

Ramos, E., Schroeder, A., Beheler, A., (1996) **Computer Networking Concepts.** Von Hoffman Press Printice Hall Inc., New Jersey, USA.

Schwartz, M., (1987) **Telecommunication Networks Protokols Modeling and Analysis.** Addison-Wesley Publishing Company, USA.

Smith, B., Udell, J., (1993), Linking LANS. **Byte,** (19) 66-90

Stalling, W., (1997) **Local&Metropolitan Area Network.** Mcmillan Publishing Company, 5th Edition, New York USA.

Stalling, W., (1993) **Local&Metropolitan Area Network.** Mcmillan Publishing Company, 3rd Edition, New York USA.

Şeker, S., (1993) **İletişim Sistemlerinin Planlanması.** Boğaziçi Üniversitesi Matbaası, İstanbul.

Tanenbaum ,A. S., (1989) **Computer Networks.** Printice-Hall Inc., USA.

Tolun, R., (1994) Bilgisayar Ağı ve İletişim Kavramları. **Bilgisayar Ağları ve İletişim Semineri,** Türkiye Bilişim Derneği, Antalya.

Üstüner, I. Ş., (1995) Bilgisayralar Arası Asenkron İletişimde Hata Arama, Bulma, Giderme. **Bilgisayar Pazarı,** (84), 90-96, 1995, İstanbul.

ÖZGEÇMİŞ

Hale KESİCİ 7 Mayıs 1973 tarihinde Ankara'da doğdu. İlk okul eğitimini Yalçın Eski Yapan İlk Okulu'nda, ortaokul eğitimini Namık Kemal Ortaokulu'nda tamamladı. Bir yıl hazırlık sınıfı olmak üzere toplam dört yıllık Gazi Osman Paşa Anadolu Meslek Lisesi Bilgisayar bölümünden mezun oldu.

1991 yılında Gazi Üniversitesi Endüstriyel Sanatlar Eğitim Fakültesi Bilgisayar Eğitimi Bölümü'nü kazandı. 1993-94 ve 1994-95 Öğretim Yıllarında iki kere fakülte birincisi oldu. Fakülteyi 1995 yılı bahar döneminde bitirdi.

Eylül 1995 döneminde Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Eğitimi Anabilim Dalı'nda Yüksek Lisans'a başladı. Aynı dönemde Gazi Üniversitesi Endüstriyel Sanatlar Eğitim Fakültesi Bilgisayar Eğitimi Bölümü'nde Araştırma Görevliliğine atandı. Halen bu göreve devam etmektedir.