T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR AĞLARI ve GÜVENLİK

YÜKSEK LİSANS TEZİ

Elektrik ve Elektronik Müh. Cüneyt BERGEL

Enstitü Anabilim Dalı : **Elektrik ve Elektronik Müh.**
Enstitü Bilim Dalı : **Elektrik**
Tez Danışmanı : **Doç. Dr. İsmail Hakkı CEDİMOĞLU**

NİSAN 2004

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR AĞLARI ve GÜVENLİK

YÜKSEK LİSANS TEZİ

Elektrik ve Elektronik Müh. Cüneyt BERGEL

Enstitü Anabilim Dalı : Elektrik ve Elektronik Müh.
Enstitü Bilim Dalı : Elektrik
Tez Danışmanı : Doç. Dr. İsmail Hakkı CEDİMOĞLU

Bu tez 22/ 04 / 2004 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Doç. Dr. İ.Hakkı CEDİMOĞLU	Yrd. Doç. Dr. İbrahim ÖZÇELİK	Prof. Dr. Şerafettin Özbey
Jüri Başkanı	Jüri Üyesi	Jüri Üyesi

TEŞEKKÜR

Bu çalışmanın başlangıcından bitimine kadar her aşamada çalışmayı yönlendiren, özverili yardımlarını esirgemeyen Doç. Dr. İsmail Hakkı Cedimoğlu'na, tezin biçimlenmesinde değerli katkılarını aldığım çalışma arkadaşlarım Sistem Müh. Turgay Çavdar, Volkan Günaydın ve Yalçın Doğan'a teşekkürü bir borç bilirim.

Cüneyt BERGEL

NİSAN 2004

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

ÖZET

Anahtar Kelimeler: Bilgisayar Ağları, Network, LAN, Token Ring, 100VG-AnyLAN, Jetonlu Yol, FDDI, WAN, ADSL, ISDN, Frame Relay, ATM, Sistem Güvenliği.

Gelişmiş ve gelişmekte olan ülkelerde haberleşmenin artan öneminin iyice kavranması ve iş dünyasının iletişim ihtiyacındaki hızlı artış nedeni ile sayısal iletişim gün geçtikçe vazgeçilemez bir haberleşme ortamı haline gelmiştir. Dünyadaki teknolojik gelişmelere paralel olarak daha iyi ses kalitesi, yüksek hızda veri iletimi, az data kaybı vs. gibi nedenlerden dolayı iletişim analog yapıdan sayısal yapıya dönüştürülmektedir

Kurumsal ve kişisel haberleşmeyi sağlamak için bilgisayar ağları geliştirilmiştir. Bilgisayar ağlarının temelleri, askeriyede kullanılan bilgisayarların birbirleri ile haberleşmesiyle atılmıştır. DIX (Digital Intel Xerox) tarafından geliştirilen Ethernet teknolojisi artık bir standart haline gelmiştir. Günümüzde Ethernet teknolojisi LAN teknolojisinde maliyet, kolay kurulum nedeniyle daha yaygın olarak kullanılmaktadır. Diğer LAN teknolojileri olarak Token Ring, 100VG-AnyLAN ve FDDI'yi sayabiliriz. LAN'ların uzak mesafe bağlantıları sağlayamamaktadır. Bu nedenle de uzak uçların birbirine bağlanması için WAN teknolojileri geliştirilmiştir. ADSL, ISDN, Frame Relay ve ATM, WAN'da en yaygın kullanılan teknolojilerdir. İnternet'in yaygınlaşması ile kurum ve şirketlerin web siteleri, online alış-veriş hizmetleri ve bankacılık hizmetlerinin internet üzerinden yapılması güvenlik problemleri de gün yüzüne çıkmaya başlamıştır. Bu nedenle ağlar oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Ağların bu zayıflıkları, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur. Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hala büyük bir tehlike oluşturmaktadır.

Güvenlik sorunlarının ortaya çıkması ile güvenlik ürün ve cihazlarıda geliştirilmeye ve kullanılmaya başlanmıştır. Bir kurum güvenlik sistemi kurmadan önce güvenlik politikalarını belirlemelidir. Bu politikalar içerisinde hangi güvenlik cihazlarının ne kadar kullanılacağı, hangi rollerin verileceği, şifre yönetiminin ve fiziksel yönetiminin nasıl sağlanacağı bu politikalarda belirtilmelidir. Firewall ve IDS'ler kurumlar tarafından en çok kullanılan güvenlik ürünleridir. Güvenlik sistemini kurdukdan sonra mutlaka güvenlik testleri yapılmalıdır. Sistem yöneticisi bu test sonuçlarına göre sistemi gözden geçirmeli, gerekli gördüğü değişiklikleri anında yapmalı ve her zaman sistemi gözlemlemelidir.

İnternetin tüm dünyada yaygın kullanımı, güvenlik tehlikelerini de artırmaktadır. Önemli bir bilgi kaybı olabilir, gizlilik ihlal edilebilir (kredi kartı numarasının

bulunması gibi) veya saatler hatta günler süren yükleme zamanları ortaya çıkabilir.

İnternetteki bu tür güvenlik açıkları, insanları internete karşı güvensizleştirebilir ve web tabanlı şirketlerin sonunu hazırlayabilir. Bu yüzden şirketler, güvenliklerini her geçen gün arttırmakta ve yeni tehditlere karşı önlem almak amacıyla yatırımlarını sürdürmek zorundadırlar.

COMPUTER NETWORKS AND SECURITY

SUMMARY

Keywords: Computer Networks, Network, LAN, Token Ring, 100VG-AnyLAN, Jetonlu Yol, FDDI, WAN, ADSL, ISDN, Frame Relay, ATM, System Security.

Understanding of the importance of telecommunication on developing and developed countries and rapid increasing demand of business world's communication has contributed digital communication the most important platform. The telecommunication has been changed from analog to digital form because of the technological improvements on sound quality, high speed data transmission, low data loss.

Computer networks have been developed to provide instutional and personel communication. The basics of computer networks have been started with the communication of military computers. For example, the ethernet technogy that has been developed by DIX (Digital Intel Xerox) is a standart now. Nowadays, the ethernet technology, LAN, is being used very popular because of the cost, and easy deployment. The other technogies are Token Ring, 100VG-AnyLAN and FDDI. LANs can not connect long distances. For this reason, the other technogy, WAN, has been developed. The WAN technogies are ADSL, ISDN, Frame Relay, and ATM.

The security problems increased as internet has become most popular platform, and also online shopping and online banking services have most ratings. For this reason, the networks are more vulnerable now. Because of the vulnerabilities on networks the companies have had severe damages, and more downtimes on production environments. Computer viruses, DoS (Denial of Service) attacks, and company computer users' faults are still most important danger.

Because of this security concerns, the security devices and programs are developing and using more than ever now. A company must make security policies known before setup the security system. These security policies are, which security devices how often will be used, which roles will be deployed, how to fullfil password management, and physical management of the system, etc. Firewalls and IDSs are the most used products on companies today. After the setup of security system, the tests of the system must be took in place. Then, Systems Engineer have to realize the system regarding the test results, take the correct aciton and monitor the system everytime.

Common usage of the Internet in the world has inreased the potential of security threats. As a result of this, there has been important information losses, privacy can be comprimised, or there has been long time downtimes. In the end, those security vulnerabilities can affect people's trust to the Internet and as a result those companies who have internet based gone to end. Finally, Companies have to increase theirsecurity levels gradually, and continue to their investments about preventing new threats.

BÖLÜM 1. VERİ HABERLEŞME SİSTEMLERİ

Bu bölümde; genel işaretleşme kavramları, modülasyon teknikleri ve iletim oranlarına genel bir giriş yapılmıştır. Ek olarak, veri haberleşme kodları ve makinelerin birbirlerine iletim yaparken eş zamanlamanın nasıl sağlandığı konularına değinilmiştir.

1.1 Verinin İletilmesi

Veri bir bilgisayarda saklanır ve bir haberleşme sistemi üzerinden ikilik tabanda (0 ve 1' ler biçiminde) iletilir.

Bir bilgisayardaki bitler elektrik işaretinin polarizasyon seviyeleri ile gösterilirler. Bir bilgisayardaki saklama elemanı içindeki yüksek seviye işareti 1'i ve alçak seviye işareti 0'ı gösterebilir. Bu elemanlar birlikte dizilerek belirlenmiş kodlara göre sayı ve karakterleri oluştururlar.

Veri; haberleşme yolu üzerinden (örneğin telefon hattı) bilgisayar yönlendirmeli cihazlar arasında elektrik işaretleri ve bit katarları ile iletilir. Bu elektrik işaretleri ve bit katarları harf ve karakterleri belirtir. Bazı durumlarda, veri ışık işaretleri ile gösterilir (fiber optik hatlarda). Bit dizileri kullanıcı verisini ve kontrol verisini tanımlar. Kontrol verisi, haberleşme ağını ve kullanıcı verisi akışını yönetmek için kullanılır.

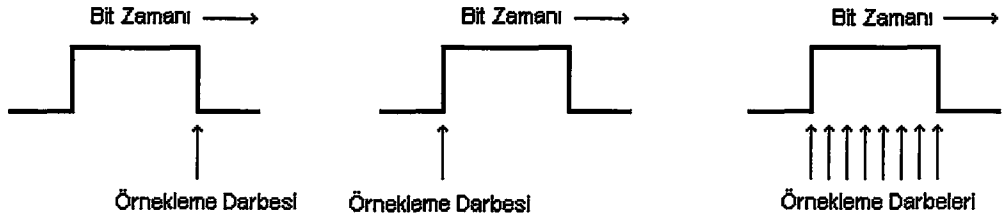
Saniye başına bit (bit/sn) terimi, iletim hızını belirtmek üzere kullanılır. Bu terim haberleşme yolu veya parçası üzerinden saniyede iletilen bit sayısını verir. Örneğin 2400 bit/sn'lik bir hat, bir sayı veya karakteri belirtmek için 8-bit'lik kodlar

kullanıyorsa, saniyede iletilen karakter sayısı 300 (2400 / 8) olur. Haberleşme hızı genelde bit/sn oranı ile verilir. [1]

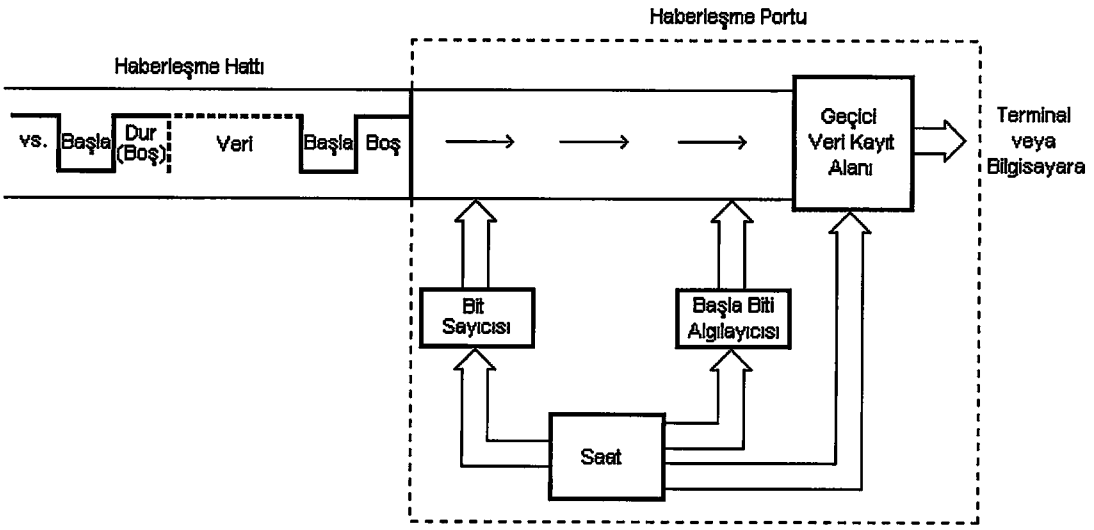
1.2 Eşzamanlı ve Eşzamansız İletim

İletilen bitler birbirlerini tam olarak eşit zaman aralıkları ile izlemektedirler ve alıcı taraftaki algılama ve zamanlama mekanizmaları ile ölçülmektedirler. Başla biti, veri karakterinin önünde gelir ve alıcı tarafa verinin yolda olduğunu belirtir (başla bitinin algılanması). Başla biti gelmeden önce yol veya hat 'boştur' denir ve bir başla biti gelene kadar hat boş konumunda kalır. Boş konumda kaldığı sürece, hat akım çeker. Bu seviyeden düşük işaret seviyesine geçiş; alıcı cihazdaki örnekleme, sayma ve veri biti katarı alıcısı (bit sayıcısı) mekanizmalarını başlatır. Veri bitleri akım varsa mark (ikilik 1), akım yoksa space (ikilik 0) olarak algılanır.[3]

Kullanıcı veri bitleri, register veya tampon (buffer) gibi geçici bir saklama alanına aktarılır. Daha sonra da bu bitler işlenmek üzere bilgisayara veya terminale aktarılır. Dur biti, bir yada daha fazla mark işaretinden oluşur ve alıcı tarafa (eski cihazlarda) sıradaki karakter için mekanizmasını hazırlayacak bir zaman aralığı sağlar. Dur bitinden sonra işaret boş seviyesine geçer ve sıradaki karakterin 1-0 geçişi ile başlamasını garanti eder. Eğer önden gelen karakter hep 0'lardan oluşursa ve dur biti, gerilim yüksek veya boş seviyeye alınarak gösterilmezse, başla biti algılayıcısı şaşıracaktır.[2]



Şekil 1.2 Bit Örnekleme



Şekil 1.2 Eşzamansız iletim süreci

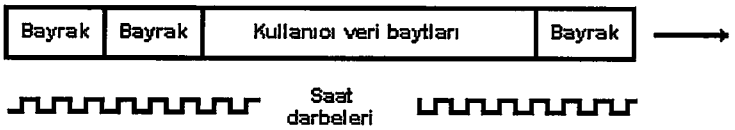
Alıcı ve verici arasında sürekli bir eşzamanlama olmadığı için bu haberleşmeye eşzamansız iletim denmektedir. Bu iletim veri karakterinin, ön bir zamanlama işaretine bakılmaksızın, herhangi bir anda iletilebilmesini sağlamaktadır. Zamanlama işareti veri işaretinin bir parçasıdır. Eşzamansız iletim genelde yazıcılarda ve düşük hızlı bilgisayar terminallerinde kullanılır. Birçok kişisel bilgisayar eşzamansız iletimi kullanır. Eşzamansız iletimin avantajı basit olmasıdır. [2]

Saat cihazı bir veri haberleşme sisteminin en önemli unsurlarından biridir. Kullanılma amacı, hat üzerinde önceden tanımlanmış işaret seviyelerinin varlığını veya yokluğunu sürekli olarak incelemek ve örneklemektir. Ayrıca tüm iç parçaların eşzamanlamasını sağlamaktadır. Saatin hızı, bir saniyede ürettiği darbe sayısı ile belirlenir. Şunu da not edelim ki saat, sistemi oluşturan diğer elemanlara da bağlanarak tüm elemanların tutarlı bir biçimde zamanlamasını sağlar.[2]

Gerçekte, örnekleyici saat haberleşme hattını gelen veriden daha hızlı bir oranda örnekleme işlemini gerçekleştirir. Örneğin; veri 2400 bit/sn'de gelirken zamanlama mekanizması belki de saniyede 19,200 kere (gelen işaretin 8 katı) örnek almaktadır. Daha sık örnek almak, alıcının 1-0 ve 0-1 geçişlerini daha erken algılamasını sağlar. Bu sayede alıcı ve verici cihaz daha yakın bir eşzamanlılıkta tutulmaktadır. [3]

Örnekleme hızının önemi Şekil 1-1'de açıkça görülebilmektedir. 2400 bit/sn hızındaki bir hatta bit zamanı 416 msn olur. Saniyede yalnızca 2400 örnek alınırsa

bitin başlangıcında ve sonunda bitten örnek alınabilir. Her iki durumda da bit algılanmaktadır. Ancak, bir işaretin hafifçe değişmesi ve hat üzerinde daha kısa veya daha uzun bir süre bulunması muhtemeldir. Yavaş bir örnekleme oranı hat üzerindeki durum değişimini doğru zamanda örnekleyemez ve işaret sürüklendikçe, bitler alıcı istasyondan doğru olarak alınamaz. [1]



Şekil 1.3 Eşzamanlı iletim süreci (Kısa mesafelerde çalışan devrelerde)

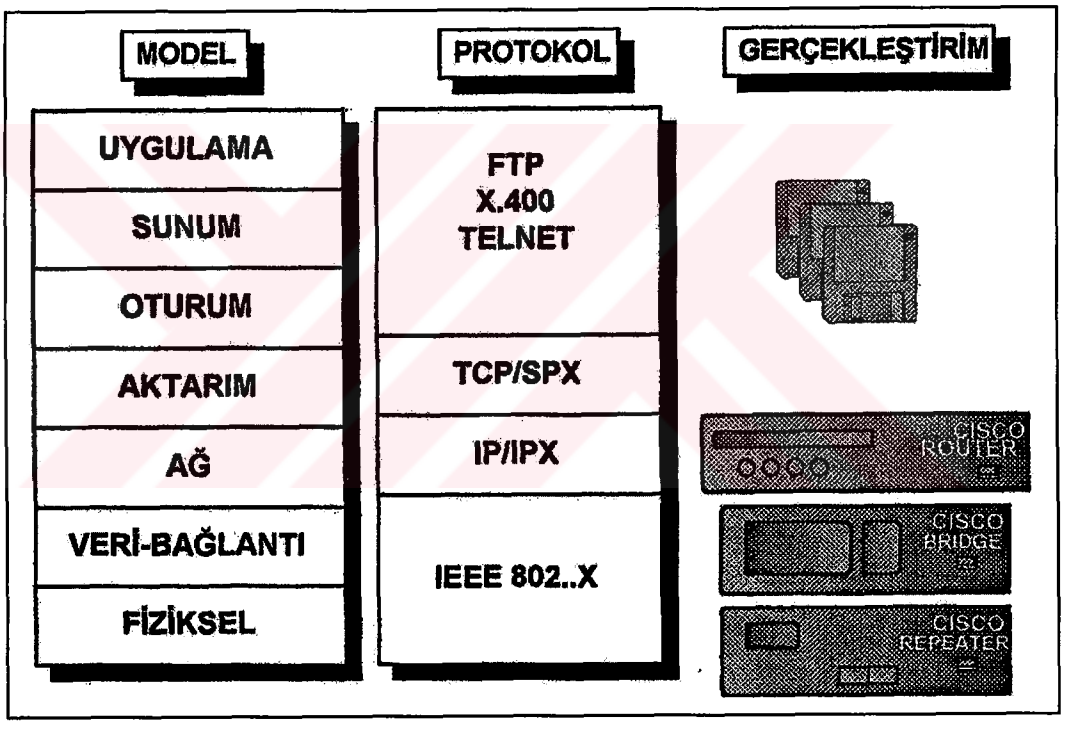
Daha etkin bir yöntem olan eşzamanlı iletimde, alıcı ve verici istasyonlarda ayrı zamanlama işaretleri vardır. Şekil 1.3'de eşzamanlı iletim şeması görülmektedir. Bu yöntemle veri, kontrol bitleri arasına yerleştirilmektedir. Bu bitlere genelde bayrak (flag) denir. Bunlar alıcıya mesajın geldiğini haber verirler. Kısa mesafeli devrelerde cihazlar arası zamanlama işaretlerini sağlamak üzere ayrı bir kanal kullanılabilir.[2]

Eşzamansız iletimde olduğu gibi, alıcı cihaz bayrak bitlerini arar, ancak yerel olarak zamanlama işareti üreterek, gelen işareti ne zaman ve ne sıklıkta örnekleyeceğine karar verir. Zamanlama işareti, alıcıdaki ve vericideki zamanlama cihazlarının eşzamanlamasını sağlar. Cihazlar arasında eşzamanlama bir kez sağlandı mı artık cihazlar bu konumda kalırlar. Saatler biraz kayabilir, fakat sıradan osilatör saatleri 1/100,000 çözünürlükte çalışırlar. Yani bu osilatörler 100,000 sn süresinde 1 sn şaşırmaktadırlar. Böylece saniyede 2500 kez örnekleme yapan bir osilatör belirli saniyeler boyunca eşzamanlı kalmaktadır. Eşzamanlama için kullanılan bir başka yöntem de, özel kodlar ile periyodik aralıklarla eşzamanlamayı yeniden sağlamaktır. Bu kodlara zamanlama kodları denir.[2]

Alıcı, bayrağı kullanıcı verisinden ayırabilmelidir. Üreticiler bu işareti, farklı bit katarları kullanarak belirtirler. Yaygın bir yaklaşım bir bayrağı göstermek için 8 bitlik 01111110 değerini kullanmaktır. [2]

BÖLÜM 2. MODEL, PROTOKOL VE GERÇEKLEŞTİRİM KAVRAMLARI

Genelde OSI referans modeli, bilgisayar ağı protokolleri ve cihazları arasındaki farkları karıştırılmaktadır. LAN/WAN birimlerini tasarlamadan ve seçmeden önce bunların arasındaki ayrımın iyi bilinmesi gerekmektedir.



Şekil 2.1 Modeller, Protokoller ve Gerçekleştirimler

Model, verinin A noktasından B noktasına taşınması için yol göstermeler, genel kavramları içerir. Model, verilmesi gereken servisleri ve bu servislerden hangi adımların (katmanların) sorumlu olduğunu tanımlar.

Protokol, donanım ve yazılımı ilgilendiren belirli kurallar serisidir. Üreticiler tarafından kullanılan ve ağ servislerini gerçekleştirmek ve veriyi ağ ortamında taşımak için tasarımlardır. Her protokol, model tarafından belirtilen servislerden

birisini gerçekleştirir.

Gerçekleştirim, protokole bağlı kalınarak, ürünlerin gerçekleştirilmesidir. Farklı üreticilerin ürünleri görünüş olarak farklı olacaktır ancak eğer protokol tanımına uygun gerçekleştirim yapılırsa birbirileri ile uyumlu olmaması için bir neden yoktur.

2.1 Bilgisayar Ağları Modelleri ve Protokolleri

Bina endüstrisinde olan durumun aynısı bilgisayar ağları endüstrisinde de bulunmaktadır.

2.1.1 Bilgisayar ağları modelleri

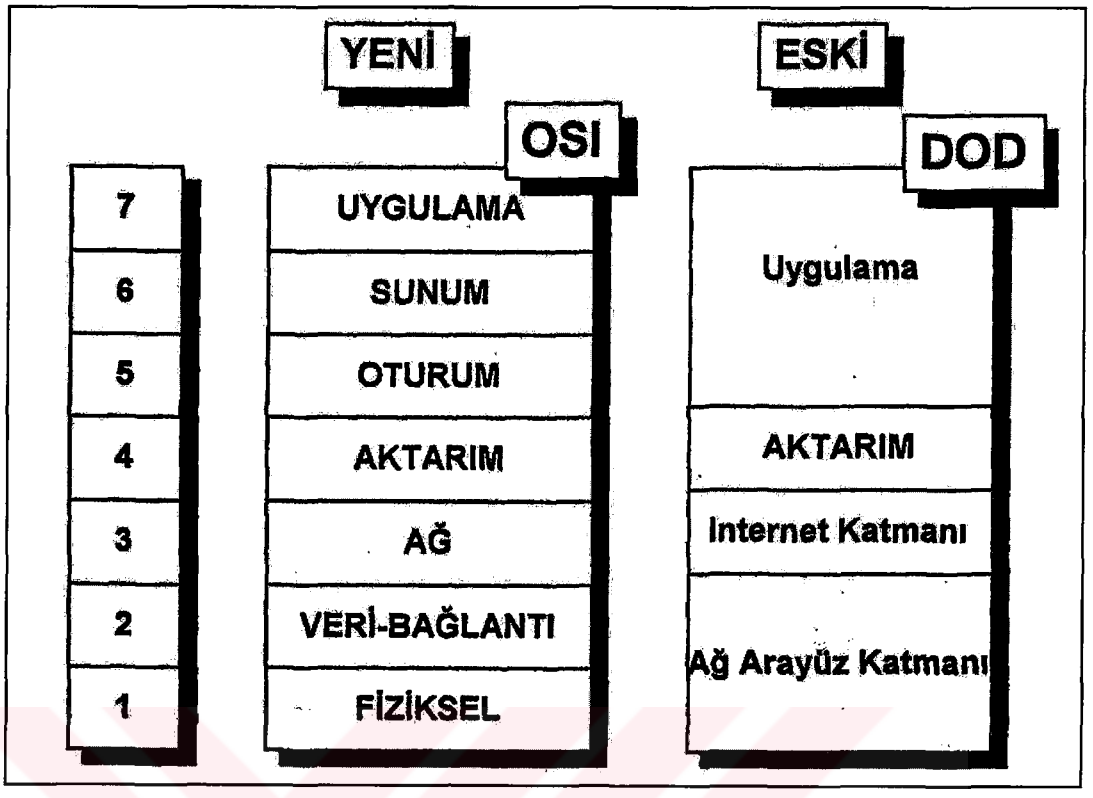
Modeller, bilgisayar ağı protokollerinin sağlaması gereken servisleri tasarlamaktadır. En popüler olan model ISO tarafından tasarlanan yedi katmanlı OSI modelidir. OSI modelinden önce tanımlanan bir model, Birleşik Devletler Savunma Bakanlığı, (Department of Defence) tarafından geliştirilmiş olan (DoD) modelidir. Bu model, 1970'lerin ortasında geliştirilmiş TCP/IP protokol suite'in modelidir.

2.1.1.1 Bilgisayar ağları protokolleri

Bilgisayar ağları protokolleri, servis ve sorumlulukların detaylı olarak planlanmasıdır. Bu tanımlamalar, protokol aileleri (suite) olarak anılır. Bazı protokol aileleri, TCP/IP, ISO, Appletalk, IEEE802, XNS, Netware, SNA ve DECnet'dir.

2.1.1.2 Bilgisayar ağları gerçekleştirimleri

Yazılım ve donanım mühendisleri, protokolleri gerçekleştirerek ürünler yaratmaktadırlar. Belli bir protokolü birden fazla firma gerçekleştirse bile aralarında farklılıklar olacaktır. Ancak protokoller, doğru olarak gerçekleştirilirse, farklı ürünlerin aynı protokol ile birbirlerinin iletişimi problem olmayacaktır.



Şekil 2.2 Eski ve Yeni Modeller

Örneğin, Ethernet ağ kartları üreten bir firma, fiziksel ve veri-bağlantı katmanı için IEEE 802.3 tanımlamalarını gerçekleştirimini yapmış olsun. Bu üretici, 802.3 adaptörlerinin verimliliğini arttırmak için yeni bir algoritma geliştirmiş olsun. Bu algoritma, kart üzerinde geniş alanda bir buffer kullanarak, rakiplerinden daha hızlı erişim sağlamaktadır. Bu üreticinin kartı diğerlerinden farklı olacaktır. Ancak temelde adaptör IEEE 802.3 standartına uygun olarak frame'leri göndermekte ve almaktadır.

2.2 OSI Referans Modeli

Modern bilgisayar ağları yapısal olarak tasarlanmıştır. Tasarım karmaşıklığını azaltmak için birçok ağ her biri diğeri üzerine inşa edilmiş bir seri tabaka şeklinde organize edilmiştir.

OSI Referans Modeli International Standards Organization (ISO) tarafından sunulan bir model üzerine geliştirilmiştir. Bu model ISO OSI (Open Systems

Interconnection) Referans Modeli olarak anılır zira açık sistemlerin yani diğer sistemlerle haberleşmeye açık sistemlerin bağlantısı ile ilgilenir. OSI modeli yedi tabakadan oluşur. Bu tabakaların oluşturulmasında uygulanan prensipler: [5]

1-Değişik seviye bir ayırım gerektiğinde bir tabaka oluşturulmalıdır.
2-Her tabaka iyi tanımlanmış bir fonksiyonu yerine getirmelidir.
3-Her tabakanın fonksiyonu uluslararası standartlaştırılmış protokoller açısından seçilmelidir.
4-Tabaka sınırları arabirimler arası bilgi akışını en aza indirecek şekilde seçilmelidir.
5-Tabakaların sayısı belirgin fonksiyonların aynı tabakalar üzerinde atlama yapmayacak kadar geniş, mimariyi hantallaştırmayacak kadar az olmalıdır.

2.2.1 Yedi tabakalı model

Tanımlanan yedi tabaka:

7) Uygulama : Uygulamalara değişik servisler sağlar
6) Sunum : Bilgi formatını çevirir
5) Oturum : Haberleşme ile ilgili olmayan problemlerle ilgilenir.
4) Taşıma : Uçtan uca haberleşme kontrolünü sağlar
3) Ağ : Ağ üzerinde bilgiyi yönlendirir
2) Veri Bağlantısı : Bağlı uçlar arasında hata denetimi sağlar
1) Fiziksel: İletim ortamına bağlantıyı sağlar

Open System Interconnect (OSI) modeli, bilgisayar ağı protokolleri geliştirilirken belirli kalıpları ortak olarak sağlayabilmeleri için oluşturulmuş ve geniş kabul görmüştür. OSI, bilgisayar ağı protokollerinin tanımlandığı ve bu protokollerin organize edildiği yedi katmanlı bir yapı sağlamaktadır.

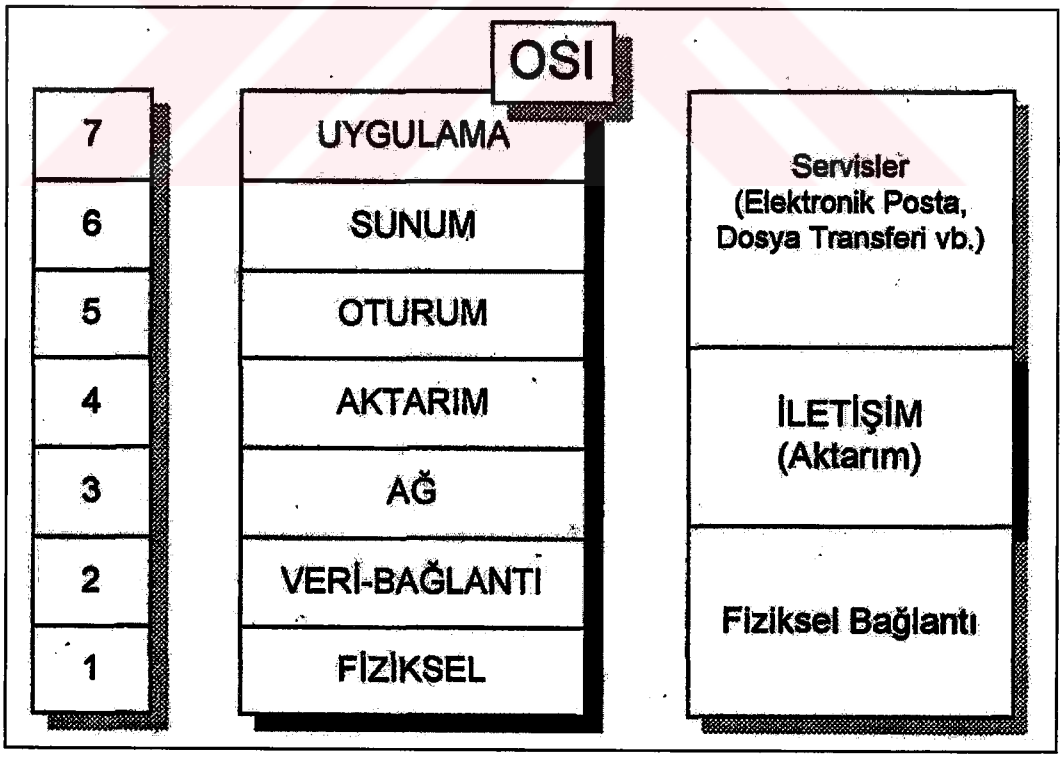
OSI modelinin katmanlarını anlamak, bilgisayar endüstrisinde kullanılan protokoller, kavramlar ve tanımlar açısından önemlidir.

Günümüzün büyük ağlarını tasarlamak, gerçekleştirmek ve yönetmek için, bilgisayar ağları tasarımcısı olarak bilgisayar ağ modelleri, protokoller ve bu protokollerin gerçekleştirimlerini aralarındaki farkları anlamak gerekmektedir.

2.2.2 OSI modeli

International Organization for Standardization (ISO)'in tanımlamış olduğu OSI modeli, bilgisayar ağı iletişimi için büyük problemleri, küçük, daha kolay yönetilebilir parçalara bölerek işlevsel bir tanım verir. Model, ağ ile ilgili tartışmalarda bir referans oluşturmaktadır. [5]

OSI modeli yedi katmana bölünmüştür. Her katman için belirli sorumluluklar ve servisler tanımlanmıştır. Alıcı ya da göndericideki katman, karşısındaki katman ile iletişim kurar. Her katman komşu katmanlardan işlevsel olarak bağımsızdır. Örneğin, Ağ katmanındaki bir protokol gerçekleştirimi, diğer katmanların işleyişini değiştirmeden başka bir ağ katmanı gerçekleştirimi ile yer değiştirebilir. [5]



Şekil 2.3 OSI Referans Modeli

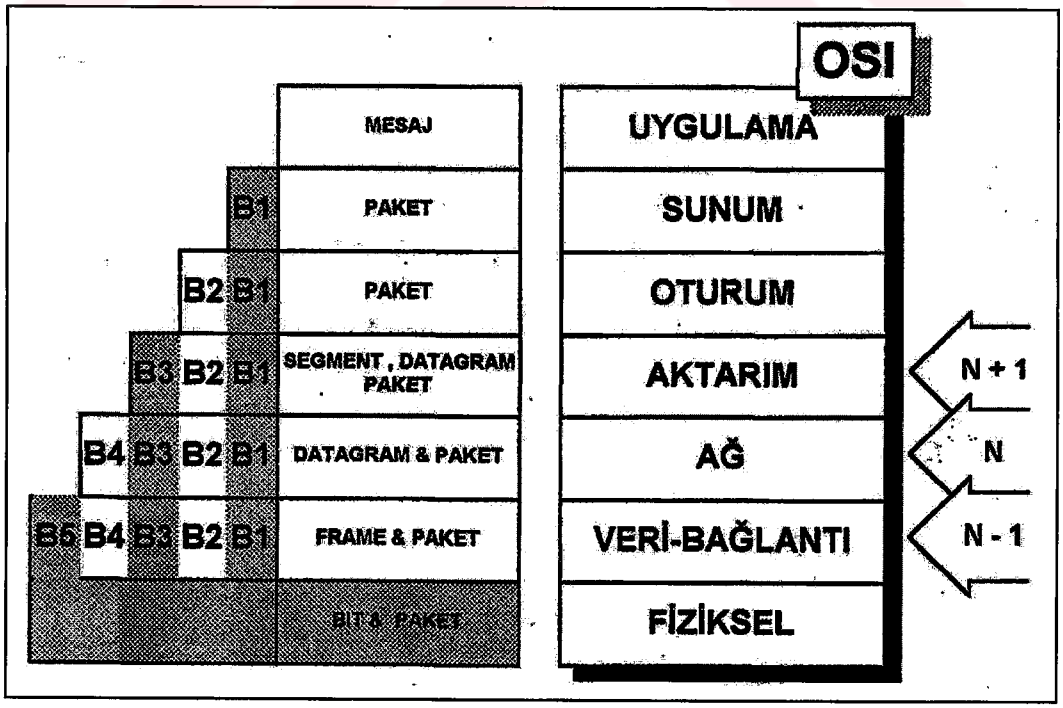
2.2.3 Katmanlar arası iletişim

OSI sadece bir model olduğu için katmanlar herhangi bir işlev gerçekleştirmezler. Ancak, protokol gerçekleştirimleri (yazılım ve donanımdan oluşan) OSI referans modelde ilgili tanımlamalara göre işlevlerini gerçekleştirirler.

Model'e göre, gerçekleştirimdeki her bir katmana karşı gelen protokol, diğer bilgisayardaki aynı düzeydeki katmanla konuşur. Ancak mesajın doğrudan karşı katmana iletemeyeceğinden, mesajını aynı düzeydeki bir alt katmana ileterek bu mesajın fiziksel ortam üzerinden karşı bilgisayara ulaşmasını sağlar.

Diğer bir deyişle, N katmanı N-1 katmanının servislerini kullanır ve N+1 katmanına servis sağlar. Katmanlar bu iletişimi Servis Erişim Noktaları (Service Access Point) aracılığı ile gerçekleştirir.

Alıcı durumda olan katman, aynı düzeydeki gönderen katmanın ne istekte bulunduğunu nasıl anlayacaktır? Her katman kendi denetim bilgisini mesajın başına ekleyerek, karşı katmana isteğini/bilgisini iletir. Bu denetim bilgisine Başlık (Header) denilir. [3]



Şekil 2.4 Katmanlar arası iletişim

Alıcı bilgisayarda, mesaj aşağıdan yukarıya katmanlarda iletildikçe, her katman kendine ilişkin Başlık bilgisine bakarak gönderen bilgisayarın ne istekte bulunduğuna anlar ve ona göre tavır alır. Gelen mesaj ya bir üst katmana iletilir ya da başka bir yere gönderilmek üzere alt katmana iletilir.

2.2.4 OSI fiziksel katman

OSI Fiziksel katman protokol gerçekleştirimleri bitlerin aktarımındaki kuralların düzenlemesini gerçekleştirir. Fiziksel katman şunları tanımlar:

- Fiziksel ağ yapıları,
- Aktarım ortamının kullanımındaki mekanik ve elektriksel belirlemeler,
- Bit aktarım kodlama ve zamanlama kuralları.

Fiziksel katman, aktarım ortamının tanımını içermez. Bunun yanında fiziksel katman protokol gerçekleştirimleri aktarım ortamına özeldir. Aşağıdaki ağ bağlantı birimleri fiziksel katmanın kapsamındadır:

- Yoğunlaştırıcı, hub, repeater gibi elektriksel sinyal üreten birimler,
- Birimlerin aktarım ortamıyla bağlantısını sağlayan, aktarım ortamı bağlantı donanımları,
- Sayısal-analog çevrimi yapan modem ve codec'ler.

OSI Fiziksel katmanı, ağ üzerinde birimlerin birbirlerine göre nasıl yerleştiklerini ve fiziksel aktarım ortamından bitlerin ne şekilde aktarılacağını belirler. Fiziksel katman içinde, bağlantı türleri, fiziksel topoloji, Sayısal ve Analog sinyal kodlama teknikleri, band kullanımı, bit senkronizasyonu ve multiplexing önemli kavramları oluşturmaktadır.[3]

2.2.5 OSI veri-bağlantı katmanı

Veri-Bağlantı katmanının amaçları aşağıda açıklanmıştır.

- Fiziksel katmanın bitlerini frame olarak adlandırılan mantıksal birimler halinde gruplandırır (Byte gibi frame de sürekli devam eden bitler serisidir),

• Hata kontrolü (ve bazen düzeltilmesi),
• Veri akış kontrolü,
• Ağ üzerindeki bilgisayarların tanınması.

Diğer katmanların çoğu gibi Veri-Bağlantı katmanı da kendi kontrol bilgisini veri paketinin başına ekler. Bu başlık alanında, kaynak ve hedef adres bilgisi (fiziksel ya da donanımsal), frame boyu bilgisi ve kapsanan üst katmanlar bilgisi içerilir. [3]

Aşağıdaki ağ bağlantı elemanları Veri-Bağlantı Katmanı kapsamındadır.

- Bridge'ler,
- Akıllı hub'lar (intelligent hubs),
- Ağ arabirim kartları (Network interface boards).

Veri-Bağlantı Katmanının fonksiyonları genelde aşağıdaki iki alt katman arasında bölünmüş biçimde anılır.

Mantıksal bağlantı kontrolü (Logical Link Control - LLC)
Ortam erişim kontrolü (Media Access Control - MAC)

2.2.5.1 Mantıksal bağlantı kontrolü (Logical Link Control -LLC)

LLC alt katmanı bir cihazdan bir diğerine veri aktarımı amacıyla bağlantının kurulmasından ve devam ettirilmesinden sorumludur. [3]

2.2.5.2 Ortam erişim kontrolü (Media Access Control -MAC)

MAC alt katmanı vericilerin tek bir aktarım kanalını nasıl paylaştığını kontrol eder. MAC fonksiyonları ortam erişimi adlı alt başlık altında açıklanacaktır. [3]

2.2.6 OSI ağ katmanı

Ağ katmanın temel görevi verinin, ağın belirli konumlarına aktarılmasını sağlamaktır. Bu işlev Veri-bağlantı katmanının fiziksel adresler üzerinden yaptığına benzerdir. Ancak Veri-bağlantı katmanın yaptığı işlem tek bir ağ üzerindedir. Ağ

katmanı, internetwork olarak adlandırılan birbirinden bağımsız bir çok ağ arasındaki veri alış verişini düzenler.

Veri-bağlantı katmanı adreslemesi tek bir ağa veri iletimini sağlar ve alıcılara ulaşan verinin onlar için bir anlam ifade ettiği varsayımına dayanır. Buna karşılık Ağ katmanı internetwork içerisinde veriyi belirli bir ağa yönlendirir ve ilgili olmayan ağlara veri göndermez. Ağ katmanı bu işlemi anahtarlama, adresleme ve yol belirleme algoritmaları kullanarak gerçekleştirir. Ağ katmanı aynı zamanda bir internetwork içerisinde aynı niteliklere sahip olmayan ağlar arasında doğru rota(yol) belirlenmesinden de sorumludur. [3]

2.2.7 OSI aktarım katmanı

Aktarım Katmanı ağın karmaşıklığını üst katman işlevlerinden gizlemek için tasarlanmıştır. Yüksek düzey mesajları segmentlere bölümler ve segmentleri güvenilir biçimde Oturum ya da daha üst katmanlara iletir.

Aktarım Katmanı genelde güvenilir veya bağlantı-tabanlı servislerin yokluğunu dengelemektedir. Güvenilir kelimesi tüm verinin her zaman ulaştırılabileceği anlamına gelmemektedir. Örneğin eğer kabloda bir kopukluk olursa Aktarım Katmanı verinin ulaştırılmasını garanti edemez. Halen, güvenilir Aktarım Katmanı protokol gerçekleştirimleri genelde verinin alındığı onaylar ya da reddeder. Eğer alıcı birimde veri düzgün biçimde alınamamışsa, Aktarım Katmanı verinin yeniden gönderilmesini başlatabilir ya da üst katmanları haberdar eder. Üst katmanlar gerekli düzeltme işlemini gerçekleştirebilir ya da kullanıcıya bazı seçenekler sunabilir. [3]

2.2.8 OSI oturum katmanı

Oturum katmanı, değişik makinelerdeki kullanıcıların birbirleri arasında oturumlar açmasını sağlar. Bir oturum taşıma katmanının yaptığı gibi sıradan veri taşıma işini gerçekleştirdiği gibi, bazı uygulamalarda çok yararlı gelişmiş hizmetler de sunar. Bir oturum bir kullanıcının uzaktaki zaman paylaşımlı bir sisteme bağlanmasını (Log on, log in) veya iki makina arasında dosya transferi yapmasını sağlar.

Oturum katmanın sunduğu hizmetlerden biri de sistemlerin karşılıklı iletimlerinin yönetimidir. Oturumlar aynı anda tek yönlü veya aynı anda çift yönlü veri akışına izin verebilirler. Eğer trafik tek yönlü ise oturum katmanı iletim sırasının kimde olduğu konusunda yardımcı olur.

İlgili diğer bir oturum hizmeti token yönetimidir. Bazı protokoller için, her iki tarafın aynı anda aynı işlevi yerine getirmeye çalışmaması çok önemlidir. Bu aktiviteleri yönetmek için oturum katmanı taraflar arasında değiştirilebilecek tokenlar sağlar. Token' a sahip taraf kiritik uygulamayı çalıştırma hakkına sahip olur.

Diğer bir oturum servisi senkronizasyondur. Oturum katmanı veri akımının içine kontrol noktaları yerleştirir böylelikle bir çökmeden sonra en son kontrol noktasından sonraki veri gönderilir. [3]

2.2.9 OSI sunum katmanı

Sunum katmanı, kullanıcıların problemleri kendi başlarına çözüm bulmaları yerine onlara yeterli bir genel çözüm sunar. Kısaca, diğer alt katmanların aksine, bit' leri bir uçtan diğerine güvenilir bir biçimde iletimleri ile ilgilenmek yerine oturum katmanı iletilen bilginin söz dizimi ve semantiği ile ilgilenir. [3]

Sunum servislerine tipik bir örnek standart, üzerinde anlaşılan bir şekilde veriyi kodlamaktır. Birçok kullanıcı programları rast gele bit dizilerini kendi aralarında değişimini gerçekleştirmez. Şahız adları, tarih, para gibi şeyleri değişirler. Bu başlıklar, karakter dizileri, tamsayılar, kayan nokta numaraları gibi daha basit veri yapıları olarak ifade edilirler. Değişik bilgisayarlar karakter dizileri ve tamsayıları ifade etmek için değişik kodlar kullanırlar. Bu bilgisayarlar arasında veri değişimini standartlara uygun olarak yerine getirmek sunum katmanının işidir. [3]

Sunum katmanı ayrıca bilginin sunulmasının diğer yönleri ile de ilgilidir. Örneğin veri sıkıştırması iletilmesi gereken bir sayısını artırmak için kullanılabildiği gibi kriptografi güvenlik ve kullanıcı doğrulaması için sık sık kullanılır.

2.2.10 OSI Uygulama Katmanı

Kullanıcı tarafından çalıştırılan tüm uygulamalar bu katmanda tanımlıdırlar. Bu katmanda çalışan uygulamalara örnek olarak, FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), e-mail uygulamalarını verebiliriz. [3]

BÖLÜM 3. BİLGİSAYAR AĞLARINDA KULLANILAN TEKNOLOJİLER

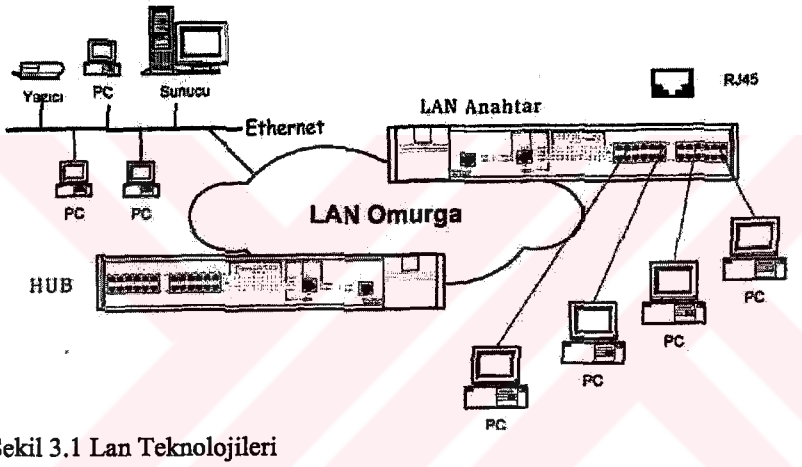
Yerel alan ağları (LAN), aynı çalışma ortamında birbirleriyle ilgili işlerde çalışan bir topluluk içinde veri alış verişi ve bilgisayarların CPU, disk gibi kaynaklarının ve yazıcı, çizici gibi cihazların paylaşması amacıyla geliştirilmiştir. LAN'larda temel özellik, sistemlerin aynı ortamda veya birbirlerine yakın mesafede olmasıdır. Bu nedenle sistemler arasında kullanılacak kabloların seçiminde büyük esneklik vardır ve kablolama alt yapısı bir kez kurulduktan sonra maliyetsiz bir iletişim ortamı sağlar. Ethernet, Jetonlu Halka (Token Ring), Jetonlu Yol (Token Bus), 100VG-AnyLAN , ATM ve FDDI bilgisayar ağlarında kullanılan teknolojilerdir.

LAN uygulamasında kablolama altyapısı oldukça önemlidir; kablo türü, seçilecek teknolojiyi,ağın yayılabileceği fiziksel genişliği ve portlar arasındaki iletişim hızını belirlemede baskın parametrelerdir. İletişim ağı uygulamasında UTP , STP ve koaksiyel bakır kablolar ile fiber optik (FO) kablo türleri kullanılır. Bakır kablolar daha çok anahtar HUB gibi ağ cihazlarına, kullanıcı (client) durumdaki bilgisayarların bağlanması için kullanılırken, fiber optik kablolar ağ cihazları arasındaki bağlantıda veya yüksek hız gerektirip bakır kablolar ile gidilmeyen mesafe sorunu olan bağlantılarda tercih edilir. Kablosuz (wireless) iletişim kablo çekme kısıtlaması veya zorluğu olan uygulamalarda bir seçenek olmaktadır. LAN uygulamasında oldukça yüksek hızlara çıkabilir; hızı 2-5 Mbps' ten başlayıp Gbps' ler mertebelerine çıkabilir.

LAN uygulamalarında yoğun olarak kullanılan birkaç teknoloji vardır. Bunlardan Ethernet teknolojisi ucuzluğu, kurulum kolaylığı, değişik hızlarda uygulama çeşitliliği olması ve bu teknolojiyi içeren ürünlerin çokluğu açısından yoğun olarak kullanılmaktadır. Ethernet teknolojisinin yetersiz kaldığı LAN uygulamalarında ise ATM veya FDDI teknolojileri devreye girmektedir; çoğu zaman komple büyük bir

LAN içerisinde bu teknolojilerin hepsini bir arada uygulamak mümkündür. Örneğin, ağın omurgası için ATM teknolojisi, bilgisayarların doğrudan bağlandığı anahtarlarda Ethernet teknolojisi kullanılabilir ve ağ içinde bulunan sunucu konumundaki bilgisayarlara FDDI veya ATM ile bağlanabilir.

Yerel alan ağları, daha küçük parçalarından oluşan alt ağlara (subnetwork) ayrılabilir. Uygulamanın gerekliliğine göre veya performansın arttırılmasını sağlamak amacıyla alt ağlar birbirlerine köprü, anahtar veya yönlendirici üzerinden bağlanırlar. Bir LAN temel olarak aşağıdaki şekilde görüldüğü gibi olur.



Şekil 3.1 Lan Teknolojileri

3.1 Lan Teknolojileri

3.1.1 802.x ailesi ve protokolleri

IEEE , 1980 yılı başlarında LAN standartlarını belirlemeye başlamış ve günümüzde yoğun olarak kullanılan standartların temelini atmıştır. IEEE 802.x ailesi bu çalışmalarının sonucu olarak ortaya çıkmış LAN teknolojileri ailesidir. Bu teknoloji standardında her tanımlamaya 802.3 benzeri bir numara verilmiştir. Örneğin 802.3 bilinen ünlü Ethernet teknolojisinin numarasıdır. Jetonlu Halka için 802.5, Fast Ethernet için 802.3u, Gigabit Ethernet için 802.3z, Jetonlu Yol için 802.1 kullanılır.

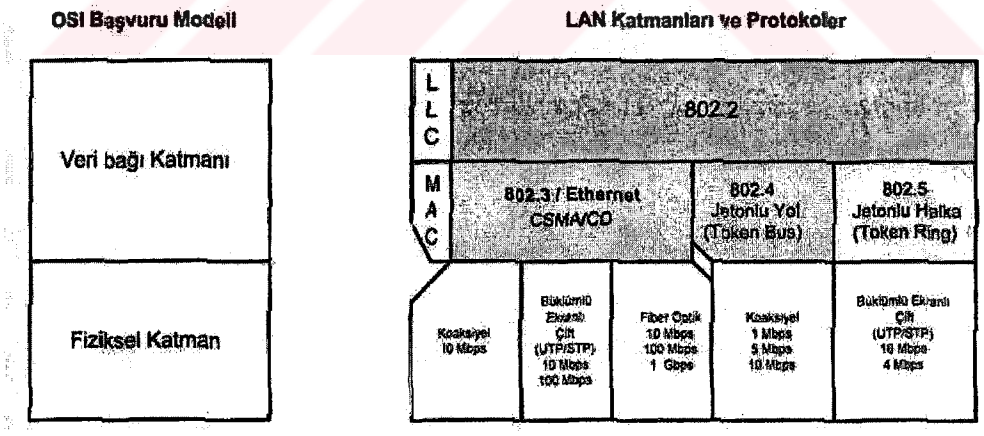
IEEE, fiziksel katmanın hemen üzerinde bulunan veri bağı katmanını ortama Erişim Alt Katmanı (MAC- Medium Access Sublayer) ve Mantıksal Bağ Denetim Alt Katmanı (LLC- Logical Link Control Sublayer) olarak iki alt katman şeklinde

tanımlanmıştır. Bu 2 katman bir arada OSI başvuru modelinin 2. Katmanına (Veri Bağı Katmanı) düşer. [3]

Protokol Adı	Açıklama
802.1	Ağlar ve sistem yönetimi hakkında genel tanımlamalar
802.2	LLC alt katmanını tanımlar
802.3	Ethernet - CSMA/CD yol erişim yöntemi
802.3u	Fast Ethernet
802.3z	Gigabit Ethemet
802.4	Jetonlu Yol (Token Bus) tanımlaması
802.5	Jetonlu Halka (Token Ring) tanımlaması
802.13	100VG-anyLAN
802.xx	...

Tablo 3.1 8Q2.x ailesi protokolleri

- MAC (Media Access Control)
- LLC (Logical Link Control)



Şekil 3.2 OSI başvuru modeline göre IEEE LAN Standartları

802'ye dayalı tüm IEEE LAN'larda benzer LLC alt katmanı bulunur. Böylece üst katmanların, ağ donanım yapısı ve türüne bakmaksızın aynı ara birimle çalışması sağlanmış olunur. Şekil'de IEEE 802 ailesinin OSI başvuru modeline göre temel durumu gösterilmiştir. MAC alt katmanı standartları ise birden fazladır. CSMA/CD (Carrier Sense Multiple Access with Collision Detect), Jetonlu Halka (Token Ring)

bunlardan en yaygın kullanılanlarıdır. Bu iki alt katman, ağ düğümleri arasında hatadan arındırılmış iletişimin koparılması amacıyla beraber çalışır. MAC alt katmanı aktarım ortamına erişimi koparırken, LLC alt katmanı bağlantı kurulması , bağlantı akış kontrolü,hata düzeltme ve çerçeve sıralanması gibi işlevleri yerine getirir. [3]

3.1.2 Ethernet (IEEE 802.3)

Ethernet ilk olarak ,deneysel çalışmaların sonucu olarak ortaya çıkmıştır. İlk Ethernet LAN 2.94 Mbps hızında idi. Ancak günümüzde bilgisayar haberleşmesine olan gereksinim artması ve mikroelektronik teknolojinin gelişmesine paralel olarak daha yüksek hızlara, 10 Mbps, 100 Mbps ve 1000 Mbps gibi hızlara kadar çıkılmıştır. Günümüzde Ethernet ve türevleri olan Fast Ethernet ,Giabit Ethernet LAN tarafında vazgeçilmez (de Facto) bir standart haline gelmiştir. [3]

Bir IEEE standart olan 802. 3 ile Ethernet aslında birbirlerinden farklı standartlardır. Ancak ikisi arasındaki fark o kadar çok değildir ve genelde Ethernet ile 802.2 aynı şeylermiş gibi bahsedilir; farklardan biri çerçeve yapılarıdır.

3.1.2.1 CSMA / CD

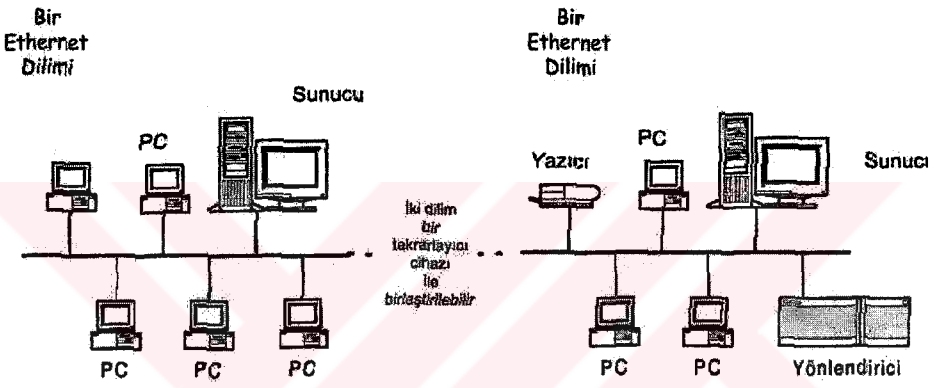
IEEE 802.3 ve Ethernet standartlarında yola erişim yöntemi olarak kullanılan CSMA/CD' de, bir Ethernet düğüm veri aktarmadan önce yolu dinler, eğer yol, o anda diğer düğümler tarafından veri aktarmak için kullanılıyorsa, yolda bir taşıyıcı (carrier) olduğunu sezer ve kendi verisini yola çıkarmaz, bir süre bekler. O anda yolda aktarılan veri paketinin son bitinden itibaren en azından 9. 6 μs bekler. Eğer bir düğüm o anda yolda taşıyıcı olduğunu sezdiği halde, yola verisini çıkarırsa çatışma (collision) oluşur. Veri aktarımı gerçeklenmez. [3]

3.1.2.2 Ethernet topolojisi

Ethernet ağların temel topolojisi ortak yol şeklindedir. Yani ağa bağlı her bilgisayar aynı yolu paylaşırlar. En temel uygulaması bir koaksiyel kablo dolaştırıp var olan bilgisayarların bu kabloya bağlanması şeklinde olabilir. Bu tür uygulama başlarda

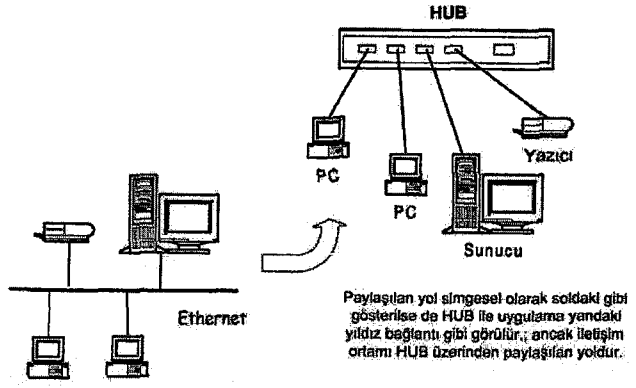
oldukça fazla kullanılmıştır. Ancak günümüzdeki Ethernet uygulamasında pek fazla kullanılmamaktadır. Günümüzde paylaşılan yol ortamı olarak HUP cihazları veya bunu başarım (performans) açısından daha ileri götüren ve portlarına bağlı sistemlerle anahtarlamalı yol sunan anahtar (switch) cihazları kullanılmamaktadır.

Koaksiyel kablolu ethernet uygulamasında bilgisayarların aynı yola bağlanması için ' tap' olarak adlandırılan fiş kullanılır. Her istasyon, özel bir adrese sahiptir ve ortak yol üzerinde, yalnızca kendini adresleyen veri paketlerini okur.



Şekil 3.3 Ortak yol topolojisi

Veri parçalarını içeren Ethernet çerçeveleri paylaşılan bir yol üzerinden yolu ele geçirebilmesi ölçüsünde aktarılır. Aynı anda iki çerçeve yola çıkarsa çatışma oluşur.



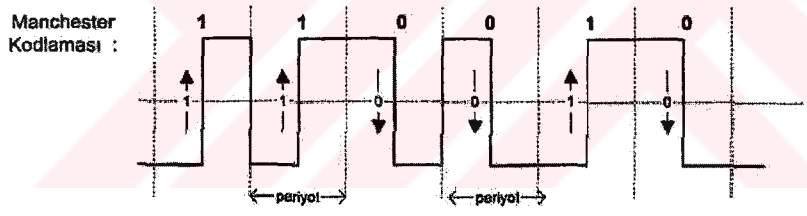
Şekil 3.4 Ortak yolun HUB ile uygulaması

Paylaşılan yol ortamında aynı anda yalnızca bir tek gönderici etkin olabilir. Aynı anda iki veya daha fazla göndericinin ağı kullanmaya kalkması çatışmaya yol açar. Bunun nedeni Ethernet teknolojisinin fiziksel katmanından temel band (baseband)

kullanılıyor olmasıdır. Yani, yol aynı anda tek bir işaret tarafında kullanılır ve yolun tüm band genişliği onu kullanan işaret tarafından harcanabilir. Şekil 3.3'de verilen örnek, tipik olarak koaksiyel kablolu uygulamayı gösterir. Şekil 3.4 ise Ethernetin HUB ile uygulaması görülmektedir; bağlantı şekli yıldız topolojisi gibi görünse de mantıksal olarak ortak yol şeklindedir. [3]

3.1.2.3 CSMA / CD fiziksel katmanı

CSMA / CD fiziksel katman topolojisi ilk zamanlar pasif ortak yoldan ibaretti. Ancak anahtar (switch) cihazların uygulamada yaygınlaşmasıyla birlikte yıldız anahtarlamalı yolda kullanılmaktadır. 802.x ailesi LAN fiziksel katmanlarında çoğunlukla Manchester kodlaması veya 4B5B diye adlandırılan kodlama tekniği kullanılır. Manchester kodlamasında bit süresinin ortasında çıkan yada düşen kenar, bitin 1 yada 0 olarak değerlendirilmesini sağlar. Çıkan kenar 1, düşen kenar 0 anlamındadır. [3]



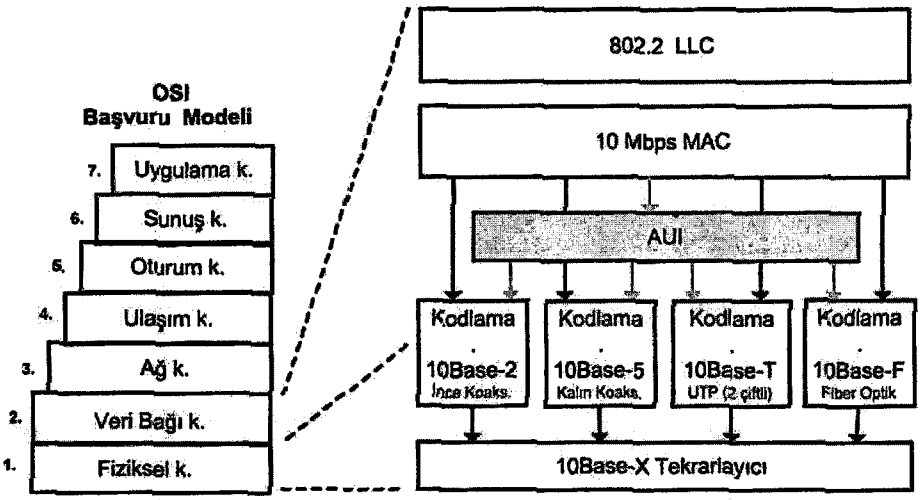
Şekil 3.5 Manchester Kodlaması

Yukarıdaki şekilde görüleceği gibi Manchester kodlaması ile ne iletirse iletilsin, hat üzerinde her zaman bir titreşim olur ve bu titreşim sayesinde herhangi bir düğüm hattın meşgul yada boş olduğunu kolayca ayırt edebilir. Hattaki titreşim bir taşıyıcı işareti andırdığı için 802.3 türü LAN için taşıyıcı sezmeli (carrier sense) sözcüğü kullanılır. [3]

3.1.2.4 Ethernet'in OSI başvuru modelindeki yeri

Ethernet içerisinde bulunan alt birimler şekil 3.6'da OSI başvuru modeline göre görülmektedir. OSI'nin ilk katmanına sahip olan Ethernet'te , en üstte LLC ve MAC birimleri, hemen altında kotlama birimi vardır. Şekilde görüleceği gibi, MAC birimi

ile kodlama birimi arasında AUI diye adlandırılan bir birim vardır. AUI birimi, Ethernet'e esnek bir fiziksel ara yüz desteği sağlamak amacıyla araya koyulmuş ara birimdir. En altta ise tekrarlayıcı ara birim vardır. [3]



Şekil 3.6 Ethernet'in OSI Başvuru Modelindeki yeri

Ethernet portlu bazı ağ cihazları (örneğin yönlendiriciler) tekrarlayıcı birimine sahip olmaksızın doğrudan AIU portlu olarak üretilir. Bu port kısmen Ethernet portudur. Ancak bağlantı yapılabilmesi için araya ortam dönüştürücü (transceivers) takılmalıdır. 10Base–X ortam dönüştürücü cihazların bir tarafı AUI ara yüze, diğer tarafı ise gereksinim duyulan kablolama yapısına göre bakır için BNC, RJ 45 ve fiber optik kablo için ST , SC konnektörlü arayüze sahip olurlar.[3]

3.1.2.5 Kabloma standartları

802.3 ve Ethernet ağlarda kullanılabilecek kablo türleri standartlar ile belirlenmiştir. Bu standartlar, kablo türünü, bağlantı topolojisini, mesafe bilgilerini, aktarım hızını ve fiziksel katmanda kullanılan priz/fiş yapısını belirler. Tüm bunlardan amaç, standart ile belirlenen hızın ve başarının garanti altında tutulmasıdır. [3]

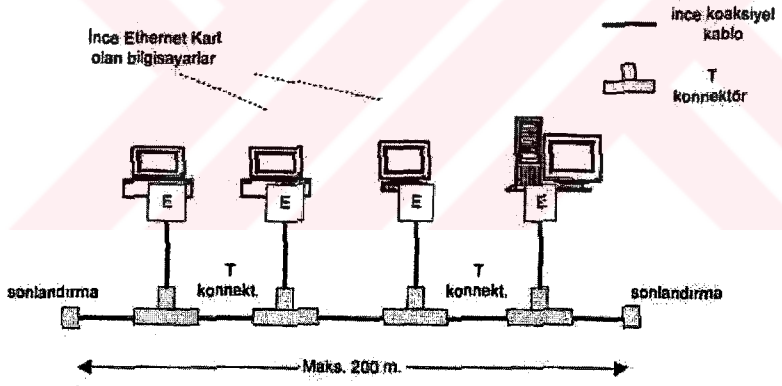
İlk 10 Mbps hızında 802.3 gerçekleştirilimi kalın koaksiyel kablo kullanılımına dayanılarak yapılmıştır ve 10Base5 diye adlandırılmıştır. Buradaki 10 hızı, Base sözcüğü aktarımda temel band (base band) kullanıldığını ve 5 rakamı ise ağ dilimlerinin (segments) 500 metre olabileceğini gösteriyor. Kalın koaksiyel kablo uygulaması, zamanında pahalı bir çözüm olmuştur. Onun daha ucuz bir uygulaması

olan 10Base2, ince koaksiyel kablo kullanılmasına dayanır. 10BaseT, bakır büklümlü çift (twisted pair); 100BaseF, fiber optik kablo kullanılmasına dayanan standartlardır.

- 10Base-2 - İnce (thin) koaksiyel kablo
- 10Base-5 - Kalın (thick) koaksiyel kablo
- 10Base-T - UTP , STP (bakır) kablo

3.1.2.6 İnce koaksiyel kablo (10Base-2)

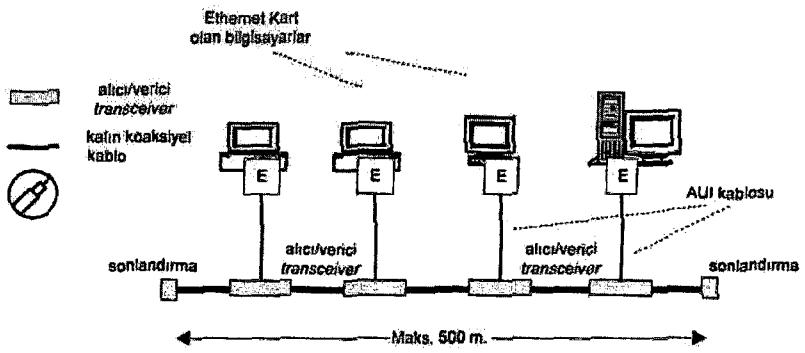
İnce koaksiyel kablo uygulaması (10Base-2) ortak yol topolojisine dayanır ve band genişliği 10 Mbps'dir. 1 ağ dilimi en fazla 185 m. ve bir dilim içinde en fazla 30 düğüm olabilir. Ağ dilimleri arasına tekrarlayıcı cihazlar koyularak genişlik 925 m.'ye kadar çıkabilir. En fazla 4 tekrarlayıcı koyulabilir. 10Base-2 uygulaması, 10Base-5'in daha ucuz çözümü için geliştirilmiş olup mesafesi ve bir dilime eklenecek düğüm sayısı daha azdır. [3]



Şekil 3.7 İnce koaksiyel kablo (10Base-2) uygulaması ve topolojisi.

3.1.2.7 Kalın koaksiyel kablo (10Base–5)

Kalın koaksiyel kablo uygulaması 802.3'ün ilk halidir. Hız 10 Mbps olup adı üzerinde kalın koaksiyel kablo (50Ω) kullanılmasına dayanır. Topoloji ortak yol şeklindedir ve bilgisayarların kabloya bağlanması için alıcı/verici (transceiver) birimi kullanılır. Bir ağ dilimi en fazla 500 m. , bir dilim içinde en fazla 100 düğüm (bilgisayar vs.), alıcı/verici birimi ile bilgisayar arasındaki kablo en fazla 50 m. olabilir. Ağ dilimleri tekrarlayıcılar (en fazla 4 tane) ile bağlanarak ağ genişliği 2500 m. ye çıkarılabilir. Ağ içerisindeki toplam düğüm sayısı 1024'ü aşmamalıdır. [3]



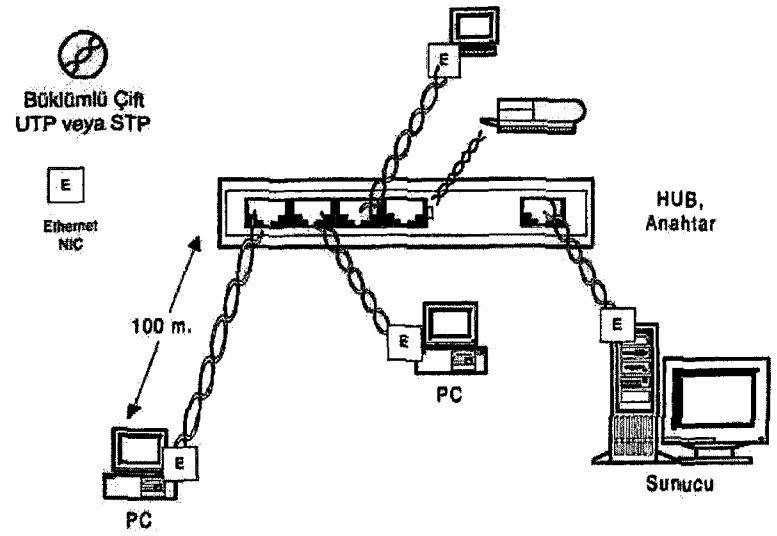
Şekil 3.8 Kalın koaksiyel kablo (l0Base-5) uygulaması ve topolojisi.

3.1.2.8 Çift büklümlü (UTP , STP) kablo (10Base – T)

Çift büklümlü bakır bir kablo türüdür. Veri haberleşmesi uygulamasında ekranlı (STP) ve ekransız (UTP) diye adlandırılan türü kullanılır. Ekranlı olan , yani STP kablo UTP'ye oranla daha pahalı ve döşemesi, sonlandırılması daha uğraştırıcıdır. Ancak ekranlı yapısı çevre şartlarından oluşan gürültü etkisini azalttığından, gürültünün çok olduğu ortamlar için iyi sonuç verir. Bunun dışında UTP kablo daha ucuz çözümdür. [3]

Uygulamada UTP ve STP'yi destekleyen anahtar, HUB gibi ağ cihazları aynıdır. Yalnızca, bağlantıların yapılacağı portlarda STP kablolar için ekranlamanın sonlandırılacağı metal bir kısım vardır ve konnektörleri farklıdır.

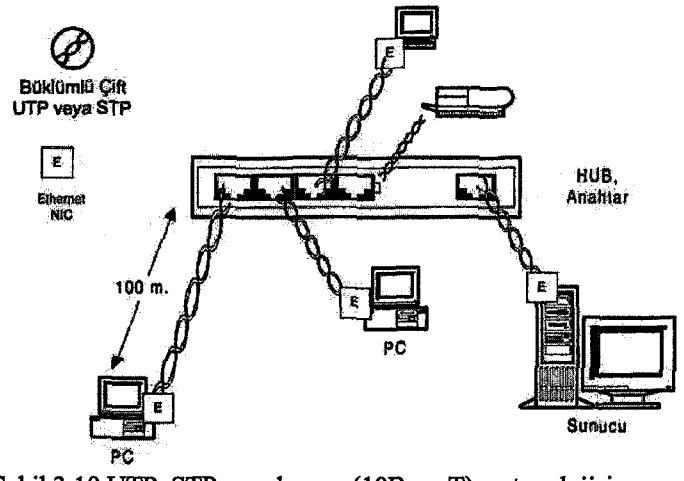
Büklümlü çift kullanılan 10Base-T uygulamasında topoloji, fiziksel olarak yıldız, ancak mantıksal olarak ortak yol şeklindedir. Ağ uygulamasındaki gelişmeler sonucu 100Base–T4, 100Base–TX, 100Base–FX ve 100Base-SX, gibi bir çok türevi çıkarılmıştır. Genel olarak baştaki 10, 100 gibi sayılar hızı, base sözcüğü temel bandın kullanıldığını ve sondaki T,TX , F gibi harflerde kablo türünü gösterir. Şekil 3.9'da verilen mesafe değerleri 10Base-T için yapılmıştır. Mesafe değerleri her bir türev için farklı farklıdır. [3]



Şekil 3.9 UTP, STP uygulaması (10Base-T) ve topolojisi.

3.1.2.9 Fiber optik kablo (10Base – F)

Bu standart fiber optik (FO) kablo kullanılmasına dayanır ve topolojisi bakır olan standartlar gibi fiziksel görünüm olarak yıldız, mantıksal olarak ortak yol şeklindedir. Fiber optik kabloların tek modlu (Single Mode Fiber, SMF) ve çok modlu (Multi Mode Fiber, MMF) olan her iki türü de veri haberleşmesinde kullanılır. FO kablo kullanmanın yararı, daha uzak mesafelere gidilebilmesi, ortam şartlarından daha az etkilenmesi (veya etkilenmemesi) ve daha yüksek hızlara çıkılabilmesidir. Ağ cihazları üzerindeki FO kablo portları ve kabloyu sürecek devre SMF ve MMF için farklıdır ve SMF kablolarla çok daha uzak mesafelere gidilebilir. Bu nedenle Türk Telekom gibi Telco şirketleri sahip oldukları ağ cihazlarını tek modlu fiber (SMF) ile bağlarlar. [3]



Şekil 3.10 UTP, STP uygulaması (10Base-T) ve topolojisi.

Yukarıdaki bağlantı gruplarının her birine dilim (segment) denir. Dilimler bazı sınırlar çerçevesinde bir birine bağlanarak daha büyük bir ağ veya altağ oluşturabilir.

3.1.2.10 Ethernet Adresi

Her Ethernet kartın MAC adresi olarak adlandırılan 6 sekizlik (48 bitlik) özel bir adresi vardır (00- 23- c3 – 45 – 00 – b3 gibi) ve bu adres tektir. LAN içerisindeki yerel değişimler, gerçekte bu adresler kullanılarak gerçekleştirilir.

3.1.3 Yüksek hızlı ethernet (Fast and gigabit ethernet)

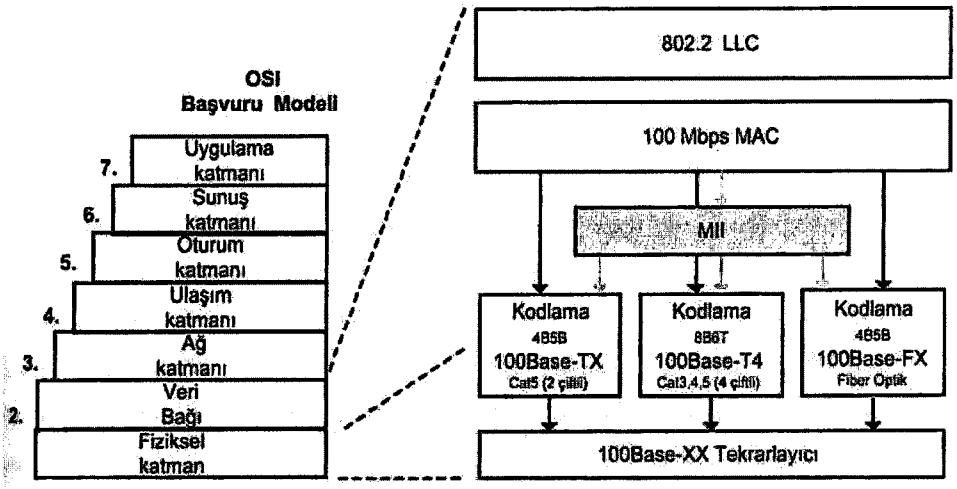
Ethernet ilk olarak kalın koaksiyel kablo üzerinden 10 Mbps hız için tanımlanmıştır. Daha sonra bazı sınırlamalar dahilinde, daha ekonomik olan ince koaksiyel uyarlaması yapılmıştır. Ancak, bakır büklümlü çift (UTP veya STP) ve fiber optik (FO) kabloların veri iletişiminde kullanılması, fiziksel olarak yıldız topolojinin yaygınlaşması ve her geçen gün daha yüksek hızlara olan gereksinimden dolayı yüksek hızlı Ethernet teknolojileri ortaya çıkmıştır. Fast Ethernet ve Gigabit Ethernet olarak adlandırılan bu teknolojiler sayesinde, 100 Mbps vel Gbps hızlara çıkılmaktadır. [3]

3.1.4 Fast ethernet (100Base-TX, 100Base-T4, 100Base-FX)

Yüksek hızlı Fast Ethernet teknolojisi genel olarak 100Base-T olarak gösterilir. Kablolama gereksinime göre 100Base-TX, 100Base-T4 ve 100Base-FX türevleri vardır. Bu türevlerin gereksinim duyduğu kablo türü, konnektör sonlandırılması (uç bağlantıları), kablo uzaklığı ve kodlama yöntemleri faklıdır. Şekil 3.11'de Fast Ethernet' in birimleri OSI başvuru modeli ile karşılaştırılmalı olarak verilmiştir. Ethernet'te var olan AUI verimi için Fast Ethernet'te MII ara birimi vardır. MII portlu bir ağ cihazına isteğe göre ortam dönüştürücüler takılarak değişik türde fiziksel port elde edilebilir. [3]

Ağ genişliği, bakır kablo ile 205 m., FO ile 325 m. ve çift yönlü (full dublex) FO ile 2 Km. olabilir. Bir uç düğüm ile HUB, anahtar (SWITCH) gibi cihazlar arası en fazla

100 m. olabilir. Kullanılan kablo türüne (Cat3, Cat4, Cat5) ve kablo içindeki kaç çiftin kullanıldığına göre alt sınıflara ayrılır.



Şekil 3.11 Fast Ethemet'in OSI başvuru modelindeki yeri

Her bir türevin gereksinim duyduğu kablolama ve kodlama teknikleri farklıdır:

- 100Base-TX: 2 çiftli Cat5 UTP, STP, yarı çift yönlü veya çift yönlü iletişim.

- 100Base-T4: 4 çiftli Cat3, Cat4, Cat5 UTP, yarı çift yönlü iletişim.

- 100Base-FX: SM veya MM fiber optik, yarı çift yönlü ve ya çift yönlü iletişim.

- 100Base-TX: Bu standartta UTP kablo için Cat5, STP için tybe 1 türünde kablo kullanılmalıdır. 100Base–TX, Cat5 kablolama gerektirir. Cat3 kablolama üzerinde garanti edilen sınırlar içinde çalışamaz. UTP veya STP kablo içindeki 4 çiften yalnızca 2 çifti kullanılır. Kablo bağlantısı 10Base-T ile aynıdır. Dolayısıyla 10Base-T için yapılan kablolamada, herhangi bir değişiklik yapılmadan 100Base-TX standardında cihazlar kullanılabilir. UTP kabloların sonlandırılması için DB–9 konnektör kullanılır. Yarı çift yönlü (half duplex) veya tam çift yönlü (full duplex) iletişim yapılabilir. Fiziksel katmanda Manchester kodlaması yerine daha elverişli olan 4B/5B kodlama tekniği kullanılır.

▪ 100Base-T4: Bu standart Cat3 kablolama alt yapısıyla 100Base–T'yi desteklemek için tanımlanmıştır. Ancak, UTP kablonun 4 çifti de sonlandırılmalıdır. 10Base–T için yapılan sonlandırma da UTP'nin iki çifti kullanıldığı için aynı sonlandırma ile 100Base-T4 çakışmaz, ancak sonlandırması 2 çiften 4 çifte yükseltilirse aynı kablolama alt yapısıyla (Cat3, Cat4 veya Cat5) çalışır. Yarı çift yönlü (half duplex) iletişim yapıla bilir. Kodlamada 8B/6T tekniği kullanılır.

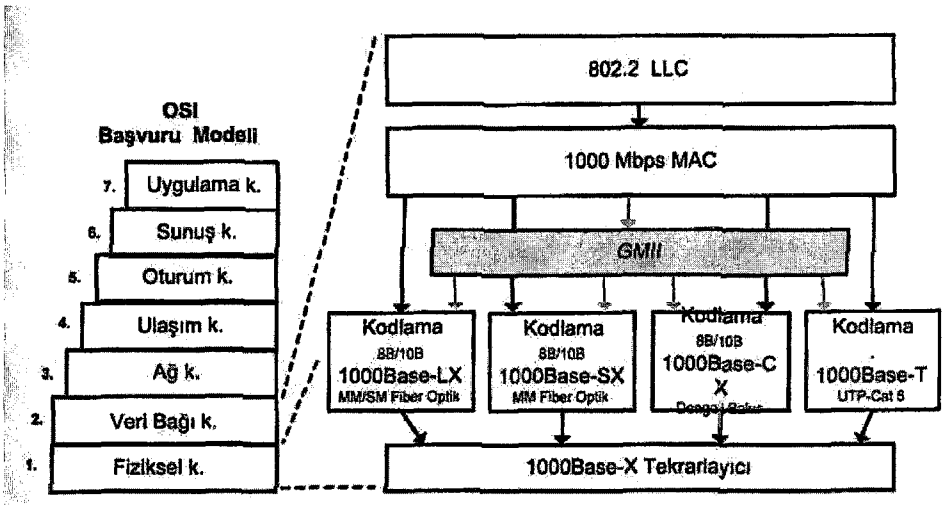
▪ 100Base-FX: Bu standart fiber optik kablonun kullanılmasına dayanır. Bakır kablolar ile erişilmeyen uzaklıklara gidilebilir. Yarı çift (half duplex) yönlü çalışmada 450 m. , tam çift yönlü (full duplex) çalışmada 2 Km.'ye kadar gidilebilir. Fiziksel katmanda 4B/5B kodlaması kullanılır.

3.1.5 Gigabit ethernet

Gigabit Ethernet, 10Mbps'lik 10Base–T'ye göre 100 kat daha hızlı Ethernet teknolojisidir. Gigabit Ethernet kablolaması için, başlangıçta FO kablo (802.3z) düşünülmüş olsa da daha sonra Cat5 UTP bakır kablo (802.3ab) üzerinde çalışacak türevi de tanımlanmıştır. Gigabit Ethernet ile alışagelen Ethernet teknolojileri üzerinde birkaç değişiklik yapılarak çok yüksek hızlara çıkılmıştır. Değişiklerden en önemlisi kodlama tekniği ve fiziksel katmandaki kablolama gereksinimidir. [3]

Şekil 3.12'de Gigabit Ethernet'in birimleri OSI başvuru modeli ile karşılaştırılmalı olarak görülmektedir. En üstte diğer Ethernet'lerde olduğu gibi LLC ve MAC (1000 Mbps için) birimleri vardır. Bu birimlerinde altında kodlama ve fiziksel ara yüz birimi bulunur. Gigabit Ethernet'e sahip portları olan ağ cihazlarına fiziksel arayüz esnekliği kazandırmak için GMMI ara birimi (Ethernet'teki AUI, Fast Ethernet'teki MII'ın karşılığı olarak) vardır. [3]

Gigabit Ethernet ailesinin FO kablo için 1000Base–LX, 1000Base-SX ve 1000Base-CX (bunlar 802.3z ile tanımlanmıştır); UTP bakır kablo için 1000Base–T (802 .3ab ile tanımlanmıştır) olarak adlandırılan türevi vardır. [3]



Şekil 3.12 Gigabit Ethemet'in OSI başvuru modelindeki yeri

▪ 1000Base-LX: FO Kablo kullanılmasına dayanır. Tek modlu fiber (Single Mod Fiber, SMF) veya çok modlu fiber (Multi Mod Fiber, MMF) kablo kullanılabilir. SMF kablo ile 3 Km. mesafede bağlantı yapılabilir. 50μ MMF kablo ile 550 m., 62.5μ MMF kablo 440 m.'ye kadar gidilebilmektedir. Yarı çift yönlü (half duplex) veya tam çift yönlü (full duplex) çalışabilir. Kodlama olarak 8B/10B tekniği kullanılır.

▪ 1000Base-SX: MMF Kablo kullanılmasına dayanır. 50μ MMF kablo ile 550 m., 62.5μ MMF kablo ile 260 m. uzaklığa gelinebilir. 1000Base–LX ile daha çok uzak mesafede bağlantılar amaçlanmış iken, 1000Base–SX ile daha ucuz yatay kablolama ve çok uzakta olmayan omurgaya bağlantı amaçlanmıştır. Kodlamada yine 8B/10B tekniği kullanılır.

▪ 1000Base-CX: Bakır kablo (copper twinax) kullanılmasına dayanır. Genel olarak çok yakın (25 m.'ye kadar) mesafedeki bağlantılar için tanımlanmıştır. 8B/10B kodlama tekniği kullanılır.

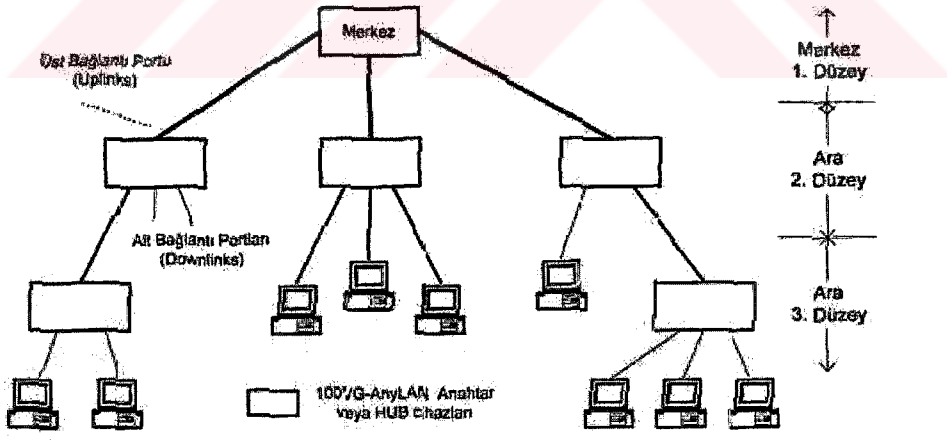
▪ 1000Base-T: Bu standart ile gigabit Ethernet' in alışılagelen Cat5 UTP kablolama (4 çiftli) alt yapısı üzerinde çalışması amaçlanmıştır. Daha önceki LX, SX ve CX tanımlamaları 802.3z altında toplanmışken; 1000Base–T, 802.3ab adı altında tanımlanmıştır. Bu standartta bağlanılacak iki uç arası 100 m.' ye kadar olabilir. Ağın çapı ise 200 m.' ye kadar çıkabilir.

Gigabit Ethernet yüksek band genişliği gerektiren ağ cihazlarının bir birine bağlanmasında ve yüksek hızlı Ethernet omurga ağ kurulmasında seçim olabilecek bir teknolojidir.

3.1.6 100VG –AnyLAN

100VG-AnyLAN, IEEE'nin 802.12 komitesi tarafından tanımlanmış yüksek hızlı bir LAN teknolojisidir. 100Base–T gibi 100Mbps'lik bir iletim ortamı sunar. Bu teknolojide yola erişim için Ethernet'te olduğu gibi CSMA/CD yöntemi kullanılmaz. CSMA/CD'ye göre erişim zamanı daha öngörülebilir bir yöntem olan DPMA (Demand Priority Access Medhod) yöntemi kullanılır. DPAM, CSMA/CD'de çatışmalardan dolayı oluşan zaman kaybını yok eden ve portlara merkezi denetimli erişim sağlayan bir yöntemdir. [3]

100VG–AnyLAN teknolojisinde topoloji Şekil 3.13'de görüldüğü gibi hiyerarşik (yıldız) yapıdadır. Bir tane merkez cihaz vardır. Hiyerarşik yapı en fazla 3 düzeyli olabilir. Aralarda bulunan HUB, anahtarlar gibi cihazların 1 tane üst bağlantı (uplink), birden çok alt bağlantı (downlink) portları olur.



Şekil 3.13 100VG-AnyLAN topolojisi ve uygulaması

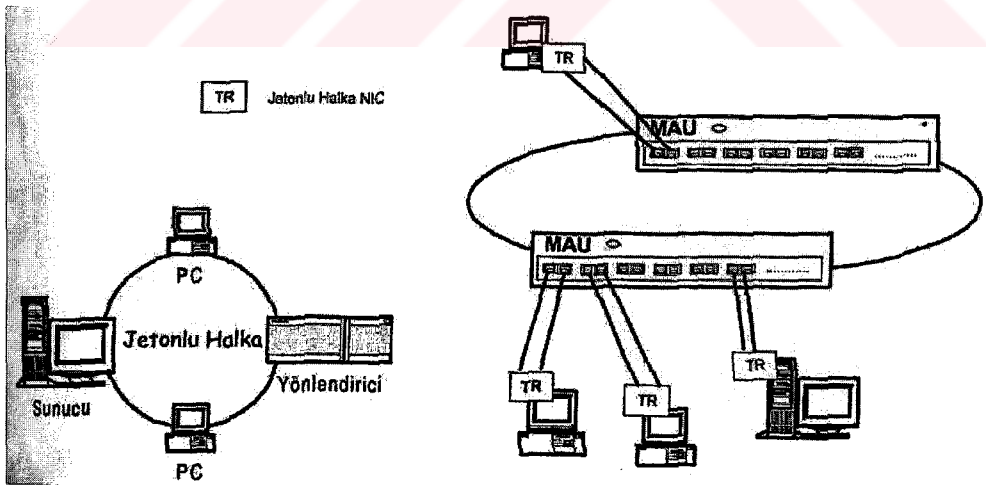
100VG-AnyLAN ağ cihazlarının portları, normal ve gözleme (monitor) olarak adlandırılan 2 moddan birinde çalışırlar. Normal modda çalışan port kendisine gelen çerçeveler adresine göre uygun yere aktarırken, gözleme modunda çalışan port, gelen tüm çerçeveleri aktarır. Normal mod uç düğüm ve alt bağlantılarda kullanılırken, gözleme mod yönlendirici, anahtar gibi cihaz bağlantılarında kullanılır. Yola erişim için kullanılan DPAM , portlara erişim hakkı tanımak için Round–Robin yoklama

(polling) tekniği kullanılır. Bu teknikte ağ cihazı portlarına bağlı sistemleri sırayla yoklar. Her yoklamada çerçeve göndermek isteyen sistemlerin birer çerçeveleri aktarılır. Bir uç sistem bir yoklama çevriminde, diğer uç sistemlerin gönderecekleri çerçeveleri olduğu sürece birden fazla çerçeve göndermez. Yola erişim için öncelikli yapı kullanılmaktadır. Öncelikli aktarım istekleri, merkezi cihaz tarafından daha öncelikli değerlendirilir.[3]

100VG–AnyLAN teknolojisinde bilinen kablo türleri kullanılır; Cat3, Cat4, Cat5 UTP kablolar, STP kablo ve FO kablo seçenekleri vardır. Bakır kablo ile kullanımda iki düğüm arası mesafe 100 m.'ye, FO kablo ile bağlama 2 Km.'ye kadar olabilir. Kodlamada 5B/6B tekniği kullanılır. [3]

3.1.7 Jetonlu halka (Token ring)

İlk olarak IBM firması tarafından (1970'li yıllarda) geliştirilen Jetonlu Halkada (Token Ring, TR) düğümler birbirlerine Şekil 3.14'de görüldüğü gibi halka biçiminde bağlanırlar. Aktarım hızı olarak 4 ve 16 Mbps olan iki uygulaması vardır.



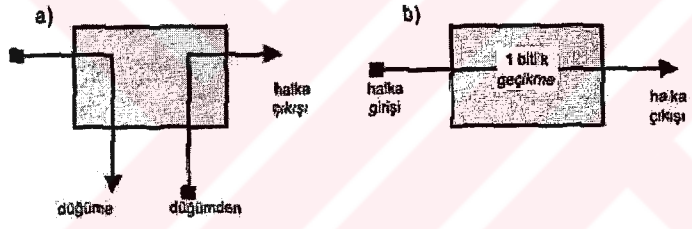
Şekil 3.14 Jetonlu Halka Yapısı

Jetonlu Halka IEEE 802.3 standardı ile hemen hemen özdeş tanımlamadır. Aralarındaki birkaç farktan biri, jetonlu halkada düğümler birbirlerine mantıksal olarak halka biçiminde, fiziksel görünüm olarak yıldız topoloji ile bağlıdırlar. 802.5'te ise bağlantı için bir topoloji tanımı yapılmamıştır. [3]

Düğümlerin bir birlerine halka biçiminde bağlanmasından dolayı, her düğüm fiziksel olarak komşu 2 düğüme bağlıdır. Veri iletimi halkada tek yönlüdür. Bir t anında halkada en fazla birtek çerçeve olabilir. Çerçeveler düğümlerden geçerken, her düğümde 1 bitlik bir gecikmeye uğrar.

Jetonlu Halka ağının kurulması MAU (Multistation Access Unit) olarak adlandırılan ve üzerinde uç sistemleri bağlanması için birden çok TR portu olan cihazlar kullanılır. Ağı oluşturan MAU cihazlarına bağlanacak cihazlar üzerinde hızına göre 4 veya 16 Mbps hızında TR NIC'ler olmalıdır. Bunlar adaptör kablolarla MAU'ya bağlanır. Şekil 3.15'de Jetonlu Halkanın tanımsal topolojisi solda, fiziksel gerçekleştirilmesi ise sağda görülmektedir. [3]

Jetonlu Halka ağda her düğümün fiziksel ara yüzü (halka arayüzü) iki moddan birinde bulunur. Fiziksel arayüz dinleme modunda ya da aktarım modundadır.

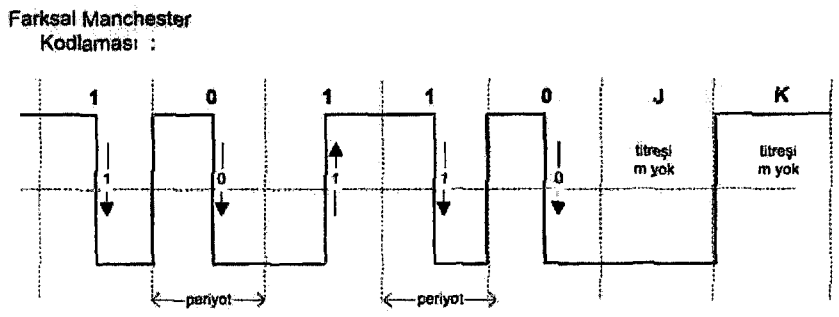


Şekil 3.15 Halka arayüzü a) Dinleme modu, b)Aktarım modu

3.1.7.1 Jetonlu halka fiziksel katmanı

Jetonlu Halkda fiziksel işaretler farksal Manchester kodlamasına göre oluşturulur. Bu kodlamada bit süresinin tam ortasında ya düşen ya da çıkan kenar vardır.

Lojik l'e karşı düşen işaretin başındaki seviye ile bir önceki işaretin seviyesi aynıdır. lojik 0'a karşı düşen işaretin başındaki seviye ise, bir önceki işaretin sonundaki seviyenin tersidir. Bit ortasındaki geçişler, alıcı tarafta bit senkronizasyonu sağlanması içindir. Çerçeve baş ve sonunu ayırt etmek için J ve K ile gösterilen bit desenleri kullanılır. J ve K'da bit süresinin ortalarında geçiş yapılmaz. J'de bit başındaki işaretin seviyesi bir önceki işaretin sonundaki düzey ile aynıdır. K'da ise tersidir. [3]



Şekil 3.16 Farksal manchester kodlaması

3.1.7.2 Jetonlu halka kablolama standartları

Jetonlu Halka ağların kablolama alt yapısında genel olarak 3 tür kablolama standardı kullanılır. Her birinde kullanılan çift sayısı farklıdır. Kablo türlerine göre TR ağda uç sayısı ve uzunluk değerleri şöyledir. [3]

Özellik	Tür 3 (Type 3)	Tür 2, 1 (Type 2, 1)
Hız	4 Mbps	16 Mbps
Sistem sayısı/Halka	96	260
Maksimum MAU sayısı	2	12
İki MAU arasındaki uzaklık	120 m	200 m
Uç sistem MAU arası uzaklık	100 m' 45 m"	300 m' 100 m"

Tablo 3.2 Jetonlu Halka Kablolama Standartları

3.1.8 Jetonlu yol (Token bus)

Jetonlu Yol (Token Bus) fiziksel topoloji olarak ethernetin ilk hali (IEEE 802.3) gibi ortak yola dayanır. Ancak bir jeton geçirme yöntemi yardımıyla düğümlerin her biri belirli bir süre içinde ortama erişmeleri garanti edilir. Jetonlu yolda, düğümler birbirlerine ortak yol üzerinden bağlıdırlar. Ancak yola erişim ethernette kullanılan CSMA/CD yöntemiyle değil de, düğümler arasında dolaşan bir jetonun ele geçirilmesiyle yapılır. Jetonu ele geçiren düğüm verisini gönderebilir. Bir düğüm jetonu ele geçiremediği sürece bekler. Jetonu ele geçiren ve verisini gönderen bir düğüm, daha sonra bu jetonu diğer düğümlere atar. Burada Jetonlu Halkada olduğu gibi komşu kavramı yoktur. Jeton ağ içindeki herhangi bir düğüme gönderilebilir. [3]

Düğümlere sırasıyla iletim hakkı tanınması için jeton (token) adı verilen bir denetim çerçevesi tanımlanmıştır. Bir düğüm kendi adresini taşıyan bir jetonu yolda gördüğü zaman 2 şeyden birini yapmak zorundadır:

• Göndereceği bir verisi varsa, bunları veri çerçevesi şeklinde yola çıkarır ve verisi bitene kadar peş peşe çerçeveler çıkararak sürdürür.

• Göndereceği bir verisi yoksa ya da kalmamışsa, bir sonraki düğüme onun adresini taşıyan bir jeton gönderir.

3.1.8.1 Jetonlu yolda ortama erişim

Düğümler arasındaki jeton aktarımı mantıksal bir halka oluşturur. Yalnızca gönderme hakkı olan düğümlerin adresleri jetonlarda yer alır. Gönderme hakkı olmayan, yalnızca dinleme yapan düğümlere jeton geçirilmez. Her düğüm tüm verisini yola çıkardıktan sonra mutlaka son bir iş olarak kendisinden sonraki düğümün adresini taşıyan bir jeton üretir. [3]

İletim yapan düğüm veri çerçevesinin denetim alanındaki yanıt istek bitini (request with response) 1 yaparak, çerçevenin yanıtını, gönderdiği düğümden hemen talep edebilir. Bu durumda çerçeveyi alan düğüm bir yanıt çerçevesi üretir ve iletim sırası yeniden yanıt isteğinde bulunan düğüme geçer. Bu çalışma şekli çerçevenin doğru alındığının teyid edildiği bir hizmete de uygundur.

Jetonlu yol uygulamasında ağ üzerinde bir jeton dolaşmalıdır. Jetonun kaybolması veya bozulması iletişimi tamamen keser. Bu nedenle jeton ağ üzerindeki düğümler belirli aralıklarla jetonun varlığını sınarlar. Eğer belirli bir süre jetonun varlığı hakkında bilgi edinemezlerse yola yeni jeton çıkarmalıdırlar. [3]

Jetonlu yolda, topoloji olarak ortak yol seçilmesine karşın, yola erişmek için 802.2'de kullanılan CSMA/CD yöntemi kullanılmaz. 802.4'ün kendi fiziksel ve MAC katmanları vardır. Fiziksel katmanda elektriksel işaretin aktarılması için koaksiyel kablo üzerinden geniş band kullanılır. Aktarım hızı olarak 1 Mbps, 5 Mbps ve 10 Mbps uygulamaları vardır.

Jetonlu yol ilk olarak General Motors firmasının 1980 yılında uygulamaya koyduğu MAP (Manufacturing Automation Protocol) örnek alınarak hazırlanmıştır.

3.1.9 FDDI (Fiber distributed data interface)

FDDI, iki yollu halka topolojiye sahip türevine göre 100 ile 2 Mbps'e kadar band genişliği sunan ve temelde fiber optik kablo kullanılmasına dayanan bir ağ teknolojisidir. Bir LAN teknolojisi olarak geliştirilmesine karşın, Ethernet ve Jetonlu Halka tabanlı LAN'ların daha ucuz çözüm sunmaları ve uygulamada baskın olmalarından dolayı, FDDI daha çok Omurga (Backbone) ağ oluşturmak için kullanılmıştır. FDDI'ın ilk uyarlaması 1980'li yılların ortalarında ANSI'nin X3T9.5 standart komitesi tarafından ortaya atılmış olup daha sonra ISO tarafından uluslararası tanımlaması yapılmıştır. [3]

FDDI ilk olarak fiber optik kablo üzerinden 100 Mbps'lik band genişliği sağlayacak bir LAN teknolojisi olarak düşünülmüştür. Ancak daha sonraları Ethernet teknolojisi üzerindeki gelişmeler, Ethernet'in başlangıçta 2-5 Mbps olan band genişliğini sırasıyla 10, 100 ve 1000 Mbps'e çıkarmış ve diğer teknolojilere göre daha az maliyetli bir çözüm olmuştur. Dolayısıyla çokta büyükçe olmayan LAN uygulamalarında Ethernet çözüm olagelmiştir. FDDI ise, daha çok büyükçe LAN uygulamalarında veya kampüs uygulamalarında omurga ağ kurulması için seçenek olmuştur. [3]

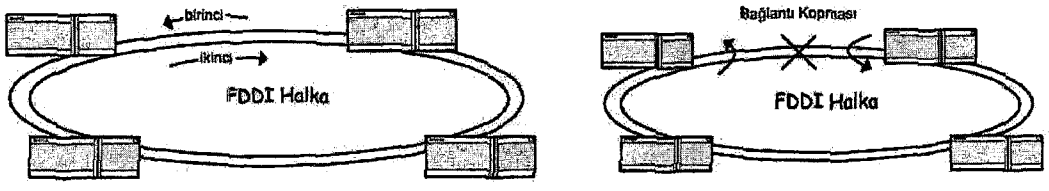
FDDI, LAN'ları birbirine bağlayan omurga uygulaması için hala en güvenilir teknolojidir denilebilir. Özellikle türevleri olan FDDI-II ve FTOL teknolojileri, çoklu medya veya gerçek zaman uygulamalarının gereksinim duyduğu servis kalitesini (QoS) garanti etmektedirler. FDDI'ın fiber yerine bakır kablolar üzerinde çalışan türevi ise CDDI olarak adlandırılır.

3.1.9.1 FDDI teknolojisi

FDDI fiziksel iletim ortamı (transmission medium) olarak fiber optik (FO) kablonun kullanılmasına dayanır. Yola erişilmesi için Jeton Geçirmeli (Token Passing) algoritma kullanır. İletimin güvenirliğini sağlamak için biri yedek sayılabilecek iki halka yol (dual-ring) vardır ve 100 Mbps'lik band genişliği sunar. Birçok açıdan Jetonlu Halka ile benzer özelliklere sahiptir, ancak ondan daha hızlıdır. [3]

FDDI'ın sahip olduğu iki yoldan biri aktif olarak verilerin aktarılması, diğeri de yedek anlamındadır. Trafik, halkalarda ters yönde akar. Bu durum iletişimin güvenilirliğini güçlü kılar ve ağ üzerindeki herhangi bir bilgisayar veya düğümün bozulması, devreden çıkması durumunda iletişim kesintisiz devam eder. Normal iletişimde trafik birinci (primary) halkadan akar. Bir arıza olduğunda ikinci (secondary) halka da kullanılarak devre tamamlanır. Bu durum diğer teknolojilere göre FDDI'ın güçlü yanıdır. Özellikle kritik ana bağlantılarda veya güçlü sunucu sistemlerin omurgaya bağlanmasında FDDI'ın tercih edilmesini sağlamaktadır. [3]

FO kablo üzerinden aktarılacak sayısal veri önce ışına modüle edilir. Ardından FDDI ağ üzerinden alıcısına ışın olarak gider. Alıcı ışına modüle edilmiş veriyi demodüle ederek yeniden elektriksel hale getirir. Fiziksel iletim ortamı olarak fiber kablonun kullanılması, ağın daha geniş bir alana yayılmasını mümkün kılmıştır. 2 aktif düğüm (ağ cihazı veya bilgisayar) arası 2 Km.'ye kadar çıkabilir.



Şekil 3.17 FDDI halka yapısı ve bağlantı kopması durumu

FDDI standardında tek modlu (SM) ve çok modlu (MM) fiber optik kablo desteklenmektedir. Tek modlu üzerinden yapılan iletişimde, çok modluya göre daha yüksek band genişliği ve daha uzak mesafeler söz konusu olur. Bu özelliklerinden dolayı tek modlu fiber, genelde, birbirine çok uzakta binalar arasındaki bağlantıda

kullanılırken ve çok modlu fiber ile bina içi veya birbirine yakın mesafede olan binalar arası bağlantıda kullanılır. [3]

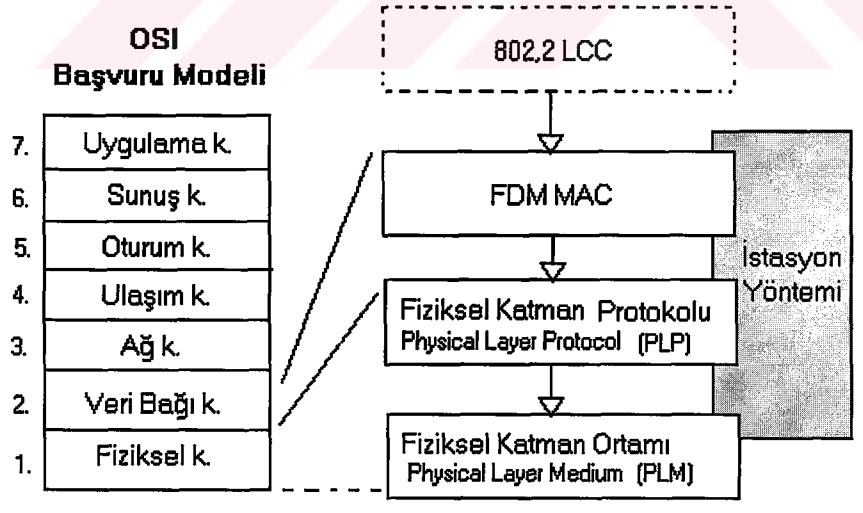
3.1.9.2 FDDI mimarisi

FDDI standardında, OSI başvuru modeline göre fiziksel katman ve veri bağı katmanının ilk yarısı olan MAC alt katmanı tanımlıdır. Şekil 3.18'de FDDI birimleri OSI başvuru modeline göre görülmektedir. [3]

FDDI MAC, iletim ortamına nasıl erişileceğini tanımlar. Çerçeve formatı, jeton geçirme yönetimi, hata düzeltme, CRC hesabı ve adresleme gibi işleri derler.

Fiziksel Katman Protokolü, verinin kodlama ve çözülmesi, saat işareti gereksiniminin karşılanması, çerçeveleme gibi işleri tanımlar.

Fiziksel Katman Ortamı, fiziksel iletim yoluna yapılacak bağlantıyı tanımlar; FO kablo ve konnektör türü, gerilim düzeyleri, optik birimler bu alt katmanda tanımlıdır.



Şekil 3.18 FDDI mimarinin OSI başvuru modeline göre durumu

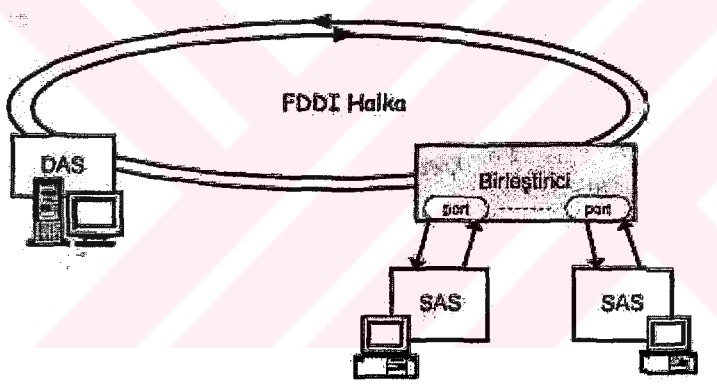
İstasyon Yönetimi, halka konfigürasyonu, statiksel bilgilerin toplanması, halka denetim şeklini ve ağa yeni düğüm ekleme, çıkarma gibi işlerin nasıl gerçekleştirileceğini tanımlar.

3.1.9.3 FDDI ağ cihazları / arayüzleri

FDDI ağ oluşturmak veya var olan bir ağa bir sistem eklemek için DAS (Dual Attachment Station-Çift Bağlantılı Arayüz), Birleştirici (Concentrator) ve SAS (Single Attachment Station-Tek Bağlantılı Arayüz) olarak adlandırılan üç temel cihaz/arayüz kullanılır. [3]

3.1.9.3.1 DAS - Çift bağlantılı arayüz (Dual attachment station)

DAS arayüzü ile bir istasyon, iki halkaya da bağlanır. Bu FDDI'ın orjinal durumudur. Eğer birinci halkada bir sorun olursa, sorun olan noktanın her iki tarafındaki cihazlar olayı sezer ve iletişimi sürdürecek şekilde kendilerini ayarlarlar. Böylelikle sorun olan nokta ağdan yalıtılarak ağın iletişim güvenilirliği sağlanır. [3]



Şekil 3.19 FDDI ağ cihaz ve arayüzleri

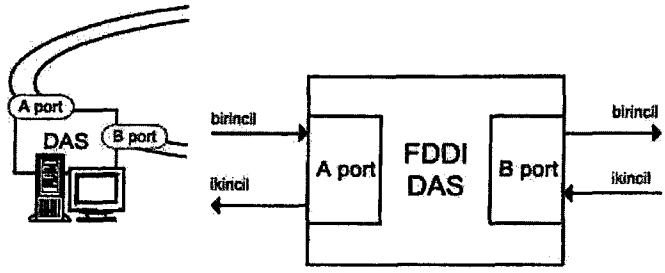
3.1.9.3.2 Birleştirici (Concentrator)

Birleştiricinin en az iki tane DAS bağlantısı vardır. Kullanım amacı FDDI olmayan cihazları veya SAS arayüzlü cihazları, sistemleri FDDI ağa eklemektir. FDDI HUB cihazı olarak da adlandırılır.

3.1.9.3.3 SAS - Tek bağlantılı arayüz (Single attachment station)

SAS arayüzle FDDI ağa bağlı bir sistem yalnızca birinci halkaya bağlıdır. Aynı anda iki halkaya bağlı değildir. SAS ile birleştirici arasında bir sorun oluşursa birleştirici yalnızca ilgili SAS'ı devreden çıkarır.

FDDI DAS arayüzünün her birinde de birinci ve ikinci halkaya bağlantı yapılacak, A ve B olarak adlandırılan 2 portu vardır.



Şekil 3.20 FDDI DAS portları

3.1.9.4 FDDI trafik türleri

FDDI, asenkron ve senkron olmak üzeri iki tür trafiği destekler. Senkron trafik gerektiren uygulamalarda, 100 Mbps'lik band genişliğinin bir kısmı öncelikli olarak kullanılırken, asenkron iletişim, senkron trafikten artan kısmı veya sınırlı bir band genişliğini kullanır. FDDI asenkron iletim, ses ve video bilgileri gerçek zaman uygulamalarını kesintiye uğratabilir. Özellikle ağ üzerindeki trafik yoğun olduğu zaman kabul edilmeyecek düzeyde gecikme oluşabilir. Bu tür uygulamalar için senkron iletim daha iyi sonuç verir. Ancak senkron iletim de bile uçtan uca devre anahtarlama yapılmadığı, paket anahtarlama yapıldığı için gerçek anlamda QoS'ten söz edilemez. Ancak FDDI-II'de devre anahtarlamalı erişim şekli kullanıldığı için, Çoklu ortam uygulamalarının gereksinim duyduğu trafik gereksinimi iyi bir şekilde karşılanmaktadır. [3]

Asenkron trafikte 8 düzeyli öncelik kullanılır. Her İstasyona bu düzeyden biri verilir. İstasyonlar kendilerine verilen öncelik düzeyine göre halkaya erişirler. Ancak, asenkron iletişim yapan istasyonlar karşılıklı anlaşarak geçici olarak tüm asenkron band genişliğini kullanabilir.

3.1.10 FDDI-II

FDDI-II, FDDI'ın bir sonraki türevidir. Daha çok yalın FDDI'ın eksik kaldığı noktaları gidermek için tanımlanmıştır denilebilir. Band genişliği yine 100 Mbps'dir. Yalın FDDI'da yalnızca asenkron ve senkron trafik desteklenirken, FDDI-II'de Isokron trafik de desteklenmektedir. Özellikle, aynı ağ üzerinden ses ve veri

tümleştirilmesi yapılan uygulamalarda Isokron trafik gereksinimi vardır. Örneğin sayısal telefon santrallerinin birbirine ağ üzerinden bağlanması, etkileşimli gerçek zaman uygulamaları Isokron iletim ortamına ihtiyaç duyarlar. [3]

FDDI-II birimleri, genel olarak biri temel (basic) diğeri karışık (hybrid) mod olarak adlandırılan iki moddan birinde çalışır. Temel modda çalışan bir FDDI-II birimi yalın FDDI birimi gibi davranır. Asenkron ve senkron trafik desteklenir, ancak Isokron desteklenmez. Karışık mod temel modu desteklediği gibi Isokron iletimi de destekler. Temel mod paket anahtarlamalı, karışık mod ise devre anahtarlamalı çalışır. [3]

FDDI-II'da Isokron iletimi desteklemek için her 125μ saniyede çevrim (cycle) olarak adlandırılan özel bir çerçeve üretilir.

3.1.10.1 FFOL (FDDI follow-On lan)

FFOL temelde, FDDI veya FDDI-II ile kurulmuş ağları birbirine bağlamak amacıyla geliştirilmiş bir omurga teknolojisidir. Ancak daha sonra 802.x ailesi, ATM, ve bazı yüksek hızlı WAN teknolojileriyle uyumlu olacak şekilde gelişme göstermiştir. Omurga band genişliği olarak 155 Mbps'den başlayıp 2.4 Gbps'e kadar çıkılabilmektedir.

3.1.10.2 CDDI (Copper distributed data interface)

CDDI fiziksel iletim ortamı olarak bakır kabloyu kullanır. FDDI'ın fiber optik yerine bakır kablo üzerindeki uygulamasıdır. CDDI'ın geliştirilmesindeki ana amaç, uç sistemlere kadar fiber optik kabloların çekilmesinin, UTP veya STP kablolara göre getirdiği yüksek maliyeti azaltarak FDDI standardında bir ağ oluşturulmasıdır.

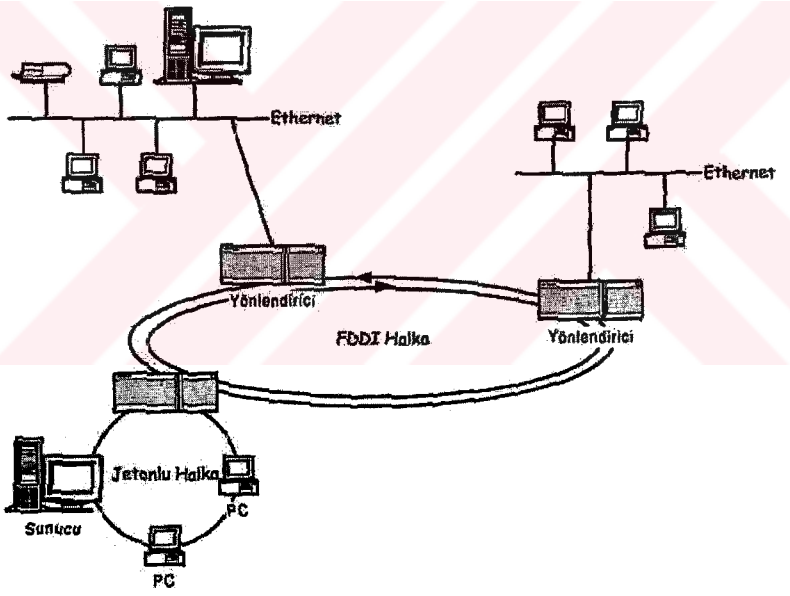
3.1.11 FDDI Uygulamaları

FDDI tipik olarak omurga ağ oluşturulmasında veya doğrudan uç sistemlerin FDDI ağa bağlanmasında uygulama bulmaktadır.

3.1.12 Omurga ağ oluşturulması

Omurga iki veya daha fazla ağın birbirine bağlanarak, ağlar içindeki sistemlerin birbiriyle görüşmesini, iletişimde bulunmasını sağlayan yapıdır; Birbirine bağlanacak LAN'ların sayısı fazla ise hızlı, kritik bir uygulama ise güvenilir olması beklenir. Omurga gerektiren uygulamalar genel olarak birbirinden uzak ve genişçe bir alana yayılmış ve ayrı binalarda bulunan ağların bağlanması için kullanılır. FDDI böyle bir durumda seçilebilecek teknolojilerden biridir. [3]

Uzaklık açısından FDDI ile ulaşılabilecek maksimum mesafe 200 Km.'dir. Ağ içerisinde iki düğüm arası uzaklık ise en fazla 2 Km. olabilir. FDDI omurga yapısının diğer bir olumlu yanı omurgaya eklenecek yeni LAN'larda herhangi bir değişiklik yapılmasına gerek duyulmamasıdır. [3]

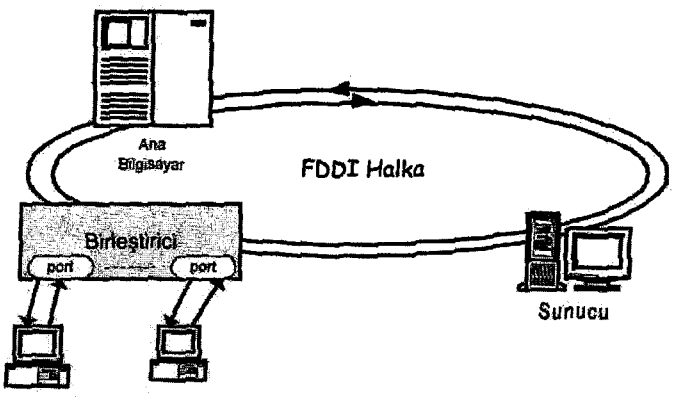


Şekil 3.21 FDDI tabanlı omurga ağ

3.1.13 Uç sistemlerin doğrudan FDDI ağa bağlanması

Bilgisayar, iş istasyonu ve sistemdeki sunucular doğrudan FDDI ağa bağlanabilir. Bunun için bu tür uç sistemlere FDDI ağ arayüz kartı (FDDI NIC) takılmalıdır. Ancak uygulamada, FDDI NIC'lerin pahalı olması ve uç sistemlere kadar, bakır olanlara göre daha pahalı olan fiber optik kabloyla gidilmesi gerekliliği, bu tür uygulamayı kısıtlamıştır. Kullanıcıların çalıştığı bilgisayarların doğrudan FDDI ağa

bağlanması ekonomik olmamıştır, ancak sunucuların bağlanması, güçlü ve hızlı yapısından dolayı seçim olmaktadır. [3]



Şekil 3.22 Uçtan uca FDDI ağ

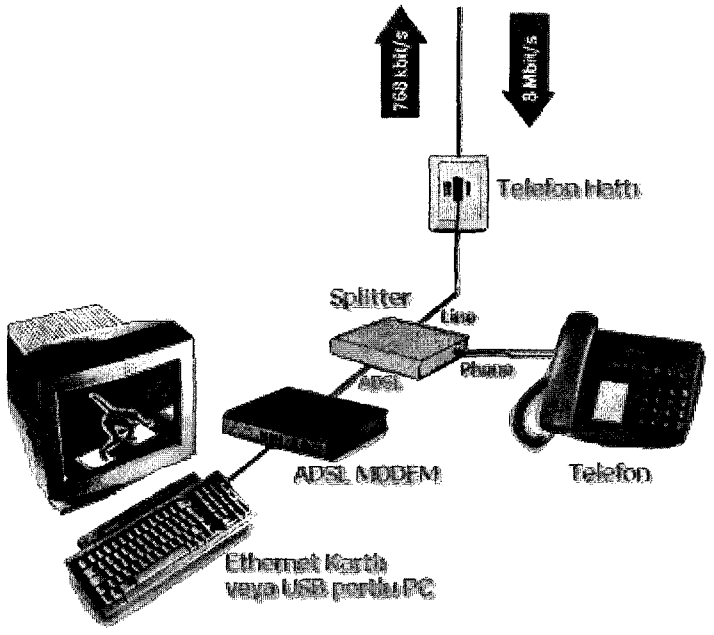
FDDI ağların diğer bir kullanım alanı da, ilk tasarlandığı yıllarda bir temel uygulama alanı olarak görülen IBM, DEC veya benzeri güçlü bilgisayarlar Jetonlu Halka ve Ethernet gibi teknolojilerden daha güvenilir bir erişim ortamının sağlanması üzerinedir. [3]

3.2 Wan Teknolojileri

3.2.1 ADSL (Asymmetric digital subscriber line)

ADSL (Asymmetric Digital Subscriber Line), mevcut telefon altyapısında kullanılan bakır teller üzerinden yüksek hızlı veri, ses ve görüntü iletimini sağlayan bir erişim teknolojisidir. Kullanıcılar bu servisler üzerinden internete erişebilirler, şirket LAN'larını birbirine bağlayabilirler, video ve ses gibi uygulamaları çalıştırabilirler.[23]

ADSL, varolan telefon hattınınızı kullanarak, daima açık olan bir internet erişimi sağlar .Özel ADSL modemler ve filtreler kullanılarak bakır tel üzerindeki frekans bandı, daha yüksek hızlara çıkmaya imkan vermektedir. ADSL, 0 KHz ile 4 KHz arasındaki bandı telefon servisi, 20KHz ile 2.2MHz arasındaki bandı ise ADSL servisi için kullanır. ADSL, asimetrik transfer yöntemini kullanır. Buna göre, yapılan bilgi transferinden daha hızlıdır. [23]



Şekil 3.23 ADSL Bağlantı

ADSL, hat uzunluğu, hatta kullanılan bakır kablonun çapı, hattın kapasitansı, hattaki sinyal kaybı (dB olarak), servis sağlayıcının servis verebildiği maksimum hız ve kullanılan modemin tipine bağlı olarak 8 Mbps downstream'a (kullanıcıya) ve 1 Mbps upstream'a kadar hız sağlar. Türkiye'de yalnızca Türk Telekom tarafından verilen ADSL servisi maksimum 2 Mbit hıza kadar verilmektedir.

ADSL, ATM teknolojisine dayanmaktadır. ATM, iki nokta arasında data transferi için kullanılan bir protokoldür. Internet, iletişim için TCP/IP protokolünü kullanır. Dolayısıyla ADSL hattı üzerindeki data, ATM üzerinden TCP/IP formuyla çalışır. TCP protokolü, data kısmına ekstradan %3 başlık bilgisi ekler. ATM ise %10'dan fazla başlık bilgisi ekler.S onuç olarak satın alınan hız miktarı başlık bilgilerinden dolayı %13 civarında düşer. Örnek olarak 128 Kbit hızında ADSL servisi alındı ise, gerçekte hız 111 Kbit olacaktır.Yani internetten bir dosya indirirken, 16 KBps yerine maksimum 13-14 KBps hızlarını görülecektir. [23]

Avantajları:

-Tek telefon hattı üzerinden aynı anda internet ve ses/fax özelliği (kabiliyeti),
-Kesintisiz, yüksek hızlı internet erişimi,
-Müşteriye efektif bant kullanımı sağlaması,

-Yeni bir altyapıya gerek duymadan mevcut PSTN hattı üzerinden yüksek hızda iletişimin sağlanmasıdır.

ADSL Sinyal Kalitesi:,

Sinyal kalitesi aşağıdaki kriterlere bağlıdır;

Devrenin hızı: Geçerli devre hızı, 1472Kbps/256Kbps. Bu değer FCC tarifelerine göre , izin verilen maksimum hızdır.

Erişilebilir Hız: Maksimum ADSL devre hızı 8 Mbps/1.5 Mbps civarındadır.Eğer erişilebilir hız, bu değerlere ulaşabiliyorsa bu iyi bir devredir.

SNR (Sinyal Gürültü Oranı): ADSL sinyal gücünün , devre üzerindeki gürültüye oranıdır.Bu değer ne kadar büyükse devre o kadar sağlıklıdır.ADSL devresinin alışabilmesi için minimum SNR değeri 6 dB olmalıdır.

Zayıflama: DSLAM (Telekom ucunda modemlerin sonlandığı çoğullayıcı) ve ADSL modem arasındaki sinyal zayıflamasının ölçüsüdür. Bu durumda düşük değer daha iyidir. Çalışılabilir bir devre için maksimum zayıflama 60-65 dB olmalıdır

Sinyal Çıkış Gücü: Her bir modemin kullandığı güç miktarını belirtir. Güç seviyesi arttıkça devrenin çalışabildiği mesafe de artar. Fakat sinyal çıkış gücü 15-16 dB' den fazla olursa devre sık sık kararsız duruma düşebilir. [23]

3.2.2 ADSL modülasyon teknikleri

ADSL teknolojisinde iki tip modülasyon tekniği kullanılmaktadır. Bunlar ANSI ve ETSI standartlarında kabul edilmiş olan DMT (Discrete Multi Tone) ve standart olmayan CAP (Carrierless Amplitude and Phase Modulation) modülasyonlarıdır. (ANSI T1.413, ITU G992.1 (G.dmt), ITUG.992 (G.Lite)) [24]

3.2.2.1 DMT

ITU G992.1 standartı olarak kabul edilen G.DMT denilen geleneksel ADSL protokolüdür. DMT modülasyon tipinde bakır hattın üzerinde 1 MHz frekans spectrumu 256 kHz'lik alt katmanlara bölünüyor ve böylece gürültü ve girişimden etkilenmemesi için bu katmanlarda bit yoğunluğunu değiştiriyor. DMT iyi kanallarda throughput değerini yükseltme kabiliyetinden dolayı gürültülü hatlarda CAP'den daha iyidir. Ayrıca DMT rate adaptive olmasından dolayı hattın kalitesine göre hız ayarlanıyor ve böylece daha esnek bir yapıya sahip oluyor. DMT'de çok fazla taşıyıcılar olmasından dolayı, işlem hacmi fazladır. [24]

3.2.2.2 CAP

Standartı olmayan bir modülasyon tipidir. Tek taşıyıcı bulunduğu için işlem hacmi düşüktür. [24]

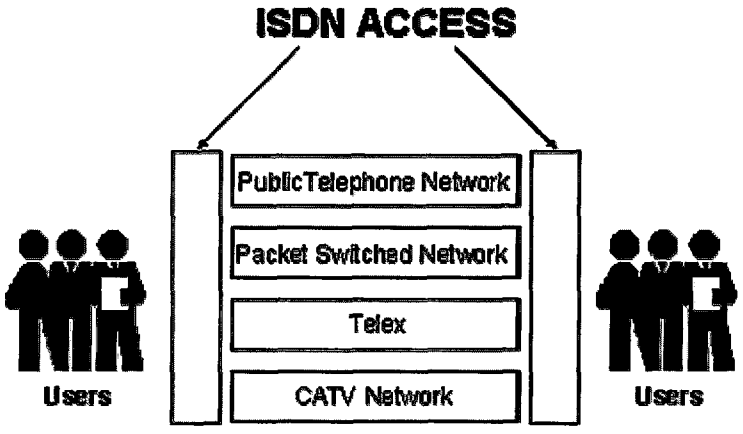
3.2.3 ISDN (Integrated services digital network)

ISDN (Integrated Services Digital Network-Tümleşik Hizmetler Sayısal Şebekesi); ses, görüntü, veri gibi her türlü bilginin sayısal bir ortamda birleştirilip aynı hat üzerinden iletilmesinin sağlandığı bir haberleşme ağıdır. İletim kalitesi normal telefon hattından daha yüksektir. ISDN hata oranı düşük, güvenli ve sınırsız bir haberleşme sağlar. [20]

ISDN'in 3 çeşidi vardır:

3.2.3.1 IDSL

IDSL (ISDN Digital Subscriber Line) 2-tel kiralık hat üzerinden 2B1Q hat kodlaması, 2 bitli bir kodlanma tekniği ile 5,5 km'de full-duplex 128Kbps BRI veri oranı sağlayan bir DSL teknolojisidir. [20]



Şekil 3.24 ISDN erişimi

3.2.3.2 EURO-ISDN

Avrupa Topluluğu ülkelerinin kurduğu ve Türkiye'nin de üye olduğu Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), üye ülkelerin ortak kullanımı için standartları Euro-ISDN adıyla belirlemiştir. Euro-ISDN Avrupa'daki birçok iletişim uygulaması için evrensel ve standart bir çözüm haline gelmiştir. Bu standartlara göre hizmet veren ISDN de Euro-ISDN olarak isimlendirilmektedir. [20]

Kullanıcılar Euro-ISDN şebekesine iki şekilde erişebilirler: [21]

3.2.3.3 Temel erişim (Basic access, BA)

2 telli hatlar üzerinden 64 kbit/s'lik hıza sahip iki bilgi kanalı (B kanal) ile işaretleşme bilgisinin taşınması için 16 kbit/s'lik hıza sahip bir işaretleşme kanalı (D kanal) kullanıcının hizmetine sunulmuştur. Ayrıca paket modlu bilgi transferini (9.6 kbit/s) D kanalı üzerinden gerçekleştirme imkanı da mevcuttur. [21]

3.2.3.4 Primer erişim (Primary rate access, PRA)

ISDN PABX ve LAN kullanıcıları, primer erişim sayesinde her biri 64 kbit/s'lik 30 B kanalı ve 64 kbit/s'lik bir D kanalı ile 30 servisi aynı anda kullanma imkanına sahip olmaktadır. [21]

3.2.3.5 Broadband ISDN

ISDN PRI'dan daha büyük band kullanan ISDN servislere Genişband ISDN denir. Başka bir deyişle hızı 2 Mbit/s'den (2 Mbit/s hariç) başlayıp 1 Gb/s'e kadar olan ISDN servislerdir. Broadband ISDN denince akla özellikle bir teknoloji gelmez, sadece ATM gelir. ATM teknolojisi ISDN genişband'ta anahtarlama alt yapısı olarak kullanılır. Başka bir deyişle bir köprü düşünülürse bir bacağı darband ISDN, diğer bacağı ATM (Genişband ISDN)'dir. [20]

3.2.4 Frame Relay

Frame Relay, kurumlara geniş alan ağları üzerinden yüksek hızlarda servis alma imkanı veren, esnek bantgenişliği kullanımını sağlayan, kiralık hatlara göre daha verimli ve ucuz bağlantı imkanı sağlayan bir servistir.

Frame Relay, uç noktalar ve ağ arasında veri taşınması ve sinyalleşmesi ile ilgili arayüzü tanımlar. Bu arayüz birden fazla kullanıcının haberleşme kaynaklarını paylaşması esasına dayanır ve ağa bağlanan tek bir fiziksel hat aracılığıyla birden fazla nokta ile görüşmelerine olanak tanır. Bu noktada artık iki uç arasında sürekli ayrılmış bantgenişliği yerine gereksinim duyuldukça kısa zaman aralıklarında kullanılan daha yüksek bantgenişlikleri söz konusudur. Bu fiziksel hat üzerinden birden fazla nokta ile yapılacak sanal bağlantılar değişik topolojilere sahip ağlardaki kiralık devrelerle karşılaştırıldığında, gereksinim duyulan devre sayısının azalması ile maliyet etkin bir alternatif olarak kullanılmaktadır.

Patlamalı (bursty) trafik profiline sahip bir LAN (Local Area Network-Yerel Alan Ağı) kullanıcısının kiralaması gereken bantgenişliği, zaman zaman da olsa gereksinim duyduğu maksimum trafik gereksinimine göre hesaplanır. Ancak kullanıcının gün içinde ihtiyaç duyduğu ortalama bantgenişliği, bu uç trafik gereksiniminden daha düşük olduğundan, alınan kiralık hat günün bazı saatlerinde verimli kullanılsa da, diğer saatlerde atıl olarak kalır ve kullanıcı, kullanmadığı bu bantgenişliği için para ödemeye devam eder.

Diğer tarafta, bölgelerini kiralık hatlar üzerinden birbirine bağlayan bir kurum, şehirlerarası veya ülkelerarası kiralık hat tarifesi üzerinden ücretlendirilirken, ağa eklenen her bir yeni bölge için, çoklu erişimi sağlamak üzere, bu tarifeler üzerinden bir ya da birden fazla kiralık hat alması gerekebilir. Bu tip bir ağın maliyet giderleri oldukça yüksek olacaktır.

Frame Relay, kurumların geniş alana çıktıklarında ihtiyaçları olan yüksek bantgenişliğini sağlamak ve patlamalı trafik profilini en iyi şekilde taşıyabilmek için geliştirilmiş, yüksek hızlı bir iletim teknolojisidir. Düşük hızlardan başlayarak, 2 Mbps, 34 Mbps, 50 Mbps'ye varan hız seviyelerinde servis vermektedir.

Frame Relay, günümüzün iyileştirilmiş hat kapasitesi ve uç kullanıcı cihazları (PC, iş istasyonları vs.) üzerindeki TCP/IP temelli uygulamaların hata denetim ve düzeltme mekanizmaları dikkate alınarak, X.25'deki çoğu denetleme fonksiyonu en aza indirilerek geliştirilmiş ve bu nedenle Frame Relay servisi ile çok yüksek işlem hızlarına çıkmak mümkün olmuştur.

Frame Relay, pazarının çoğunu LAN trafiği oluşturmaktadır. Kullanıcıların Frame Relay'in kiralık hatlara karşı %30-%15 indirim sağladığını görmesiyle bir dönem LAN-LAN bağlantısı neredeyse Frame Relay pazarında tek uygulama haline gelmiştir. Kullanıcıların Frame Relay teknolojisini daha iyi tanımasıyla birlikte, 1994 yılından itibaren SNA kullanıcıları tarafından tercih edilen bir servis olmuştur. Günümüzde; Frame Relay internet erişiminde oldukça yaygın olarak kullanılmaktadır. Özellikle yüksek hızlı servis sağlayıcı WWW bağlantıları Frame Relay servisi kullanılarak yapılmaktadır. Birçok servis sağlayıcının temel ağı Frame Relay teknolojisi ile kurulmuştur. Frame Relay üzerinden ses iletimi de hızla büyümesi beklenen bir pazardır. Frame Relay'in ATM teknolojisine açık oluşu, Frame Relay - ATM servislerinin birlikte çalıştığı bu servisi cazip kılan diğer bir konudur. [22]

3.2.4.1 Servis özellikleri

Frame Relay servisi, bir kalıcı sanal devre (PVC) veya anahtarlamalı sanal devre (SVC) üzerinden iki kullanıcı cihazı arasında (router) veri çerçevelerini aktarır. Frame Relay, veri bağı (data link) katmanı adreslemesiyle aynı fiziksel hat üzerinden değişik kullanıcı veri akışlarını taşır. Aynı fiziksel hat üzerinden taşınan her bir kullanıcı veri akışı, veri bağı bağlantısı (Data Link Connection-DLC) olarak adlandırılır. Aynı fiziksel hat üzerinde değişik DLCI (Data Link Connection Identifier) numaraları ile PVC/SVC'ler kullanılarak farklı yerlere bağlantılar yapılabilir ve veri aktarımı süresince belirli bir bağlantıya ait tüm frame'ler aynı DLCI numarasına ait kanal üzerinden sıralı olarak iletilir.

Frame Relay servisinin iki ana trafik bileşeni vardır: CIR (Committed Information Rate - Taahhüt Edilen Bilgi Oranı) ve EIR (Excess Information Rate - Fazla Bilgi Oranı). [22]

CIR: Ağın belli koşullar altında bir PVC veya SVC üzerinden taşımayı taahhüt ettiği bilgi oranıdır, CIR=Bc/Tc olarak tanımlanır. Toplam patlama büyüklüğü, Bc kullanıcının bir ölçüm ağırlığı (Tc) içinde gönderebileceği toplam veri miktarı olarak tanımlanabilir. Bc bir kredi mekanizmasına benzetilebilir, kullanıcı bir Tc zamanı içinde Bc byte'ı istediği şekilde kullanır, bu yöntemle DLC'nin kendine tahsis edilen CIR değerine ulaşmadığı zamanlara ait kredileri saklı tutarak gerektiği zamanlarda harcamasına olanak sağlanır ve zaman zaman CIR'dan yüksek değerlerde veri gönderilebilir. [22]

EIR: Kullanıcının hattı üzerinde kullanılabilir bantgenişliği olması durumunda ağın koşulları uygun olduğu sürece CIR'ın üzerinde gönderebileceği fazla bilgi oranıdır. EIR'da CIR gibi bir oranla tanımlanır, EIR=Be / Tc.Be, fazla patlama büyüklüğü, bir Tc zamanı içinde kullanıcının Bc kredisine ek olarak kullanabileceği ek kredi miktarı olarak tanımlanabilir. Ancak Be byte bilgi ağ üzerinde yeterli bantgenişliği olması durumunda gönderileceğinden, bu frame'ler DE (Discard Eligibility - Atılabilir) işaretli taşınır ve tıkanıklık durumunda atılır. Bu bilgilerin taşınacağı taahhüt edilmediğinden, EIR trafik tarifesi oldukça düşük tutulur. [22]

CIR ve EIR her bir veri iletim kanalı, DLC için ayrı ayrı tanımlanır. Kullanıcı isterse hiç EIR istemeden sadece CIR trafiği taşıyabilir. Tek bir DLC için tanımlanan CIR+EIR oranları toplamı hat hızını geçmemelidir, ancak her DLC'nin aynı anda aktif olmayacağı varsayımı ile tek bir hat üzerinde tanımlanan birden fazla DLC için verilen toplam CIR+EIR oranı hat hızını aşabilir.

Frame Relay, kullanıcılara bantgenişliğinin esnek kullanımı sağlamaktadır. Ancak CIR ve EIR değerleri belli mühendislik kriterlerine göre seçilmez ve ağ kaynakları iyi ayarlanmaz ise ağ üzerinde "tıkanıklık" oluşabilir, bantgenişliği sıkışıklıkları yaşanır.

3.2.4.1.1 Erişim hızının seçilmesi

Erişim hızı kullanıcının ağa bağlandığı fiziksel hızdır, ortalama hız ise ihtiyacı olan ortalama veri iletim hızıdır. Bir Frame Relay kullanıcısının erişim hızı/ortalama hız oranı ne kadar yüksek olursa servis performansı o kadar yüksek olacaktır (yüksek verim, düşük gecikme) ve kullanıcı, bantgenişliğini patlamalı trafik gereksinimleri uyarınca daha etkin kullanabilecektir. Ancak ağ performansı düşünüldüğünde bu oranının 2 ve 4 arasında tutulması tavsiye edilmektedir. [22]

Bir erişim hattı üzerinde birden fazla DLCI kullanılıyorsa, toplam kullanımın (tüm DLC'ların aynı anda kullanılması durumunda) %50'nin altında olmaması koşuluyla aynı kural her bir DLCI için uygulanır.

Ancak istenise, aynı erişim hattı üzerinden taşınan birden fazla DLC'ye ait toplam hız (toplam CIR) erişim hızının 2 katı olabilir. Pratikte bu durum, "Aşırı yükleme" olarak tanımlanır ve kullanıcılara, ağ performansını etkilemeden, oldukça iyi ekonomik koşullar sağlar. Tüm DLC'ler aynı anda aktif olmayacağı ve olanlar arasında da bantgenişliğinin istatistiksel olarak paylaşılacağı düşünüldüğünde bu çözüm oldukça iyi bir alternatif oluşturur.

3.2.4.1.2 CIR seçilmesi

CIR, DLC üzerindeki ortalama trafik hızını kontrol eder, ancak patlamalı LAN trafik profili gözönüne alındığında, CIR'ın ortalama trafik gereksiniminden %10, %20 daha yüksek tutulması, bantgenişliğinin daha esnek kullanıma olanak verir. "Erişim hızı / ortalama hız oranı" yüksek seçilen hatlarda CIR'da ortalama hıza göre daha yüksek seçilebilir. [22]

Erişim hızı / Ortalama hız = 2
CIR = 1.1* ortalama hız
Erişim hızı / Ortalama hız = 4
CIR = 1.2* ortalama hız

Erişim hattında birden fazla DLC olması durumunda her bir CIR için "erişim hızı / ortalama hız" oranı 4'ten daha yüksek olabilir, bu da ilgili DLC'lerden akan trafiğin aşırı patlamalı olmasına izin verir (tavsiye edilen maksimum "erişim hızı / ortalama hız oranı 4'tür). Ancak bu DLC'lere ait patlama hat üzerindeki diğer DLC'ler tarafından dengelenecektir ve erişim hattına yansıyan toplam patlama ağ performansını etkilemeyecek şekilde olacaktır.

3.2.4.1.3 Bc belirlenmesi

Bc bir "Kredi Akümülatör"ü olarak düşünülebilir. DLC, kendine ait CIR'ın tümünü kullanmadığı zaman Bc byte'a kadar kredisi saklı tutulur. Bu krediler daha sonra, DLC'den akan trafik CIR oranını aşmak istediği zamanlar kullanılır. Bc, her bir DLC için patlamalı trafik profili dikkate alınarak belirlenir. [22]

Etkileşimli trafik, zaman zaman gönderilen kısa frame'lerden oluşur, bu frame'lerin ortalama 50 byte olduğu varsayımı ile Bc şu şekilde belirlenebilir:

Bc= 20* ortalama frame uzunluğu (50 byte), Bc = 1000 byte
Dosya transfer uygulamalarında Bc ortalama boyutu ile orantılı olarak seçilir. Patlama boyutunun belirlenemediği durumlarda, ortalama değer 4 kbyte olarak alınırsa;

Bc = 20* ortalama patlama boyutu (4 kbyte), Bc = 80 kbyte

Olarak hesaplanabilir. Bu değerler kullanıcı ihtiyaçları doğrultusunda belirlenir, ancak düşük erişim hızlarında, çok yüksek Bc değerleri seçilmemelidir. Örneğin; 64 kbps'lık bir erişim hattı üzerinde 80 kbyte'lık patlama boyutunun tanımlanması hattı 10 saniye meşgul edecektir ve ağ kaynaklarını zorlayabilecektir, bu gibi durumlarda CIR'ın yükseltilmesi, Bc'nin ise düşürülmesi tavsiye edilir. Normal koşullar altında Bc 2 saniyelik zaman aralığı ile tanımlanır.

Bc = CIR* Tc (2 saniye)

3.2.4.1.4 EIR seçilmesi

EIR kullanıcının belirli zaman aralığında Bc'nin üstünde gönderebileceği bir Be byte miktarı ile tanımlanır (EIR = Be / Tc). Be, Bc gibi bir kredi akümülatörü olarak düşünülebilir, ancak Be kredisiyle gönderilen frame'ler DE işaretlidir. EIR maksimum erişim hızına eşit seçilebilir. Eğer erişim hızı CIR'dan çok yüksek değilse (2 veya 4 katını aşmaması durumu), EIR, ağ performansını etkilemeden, "Erişim Hızı-CIR" olarak seçilebilir. [22]

3.2.5 ATM (Asynchronous transfer mode)

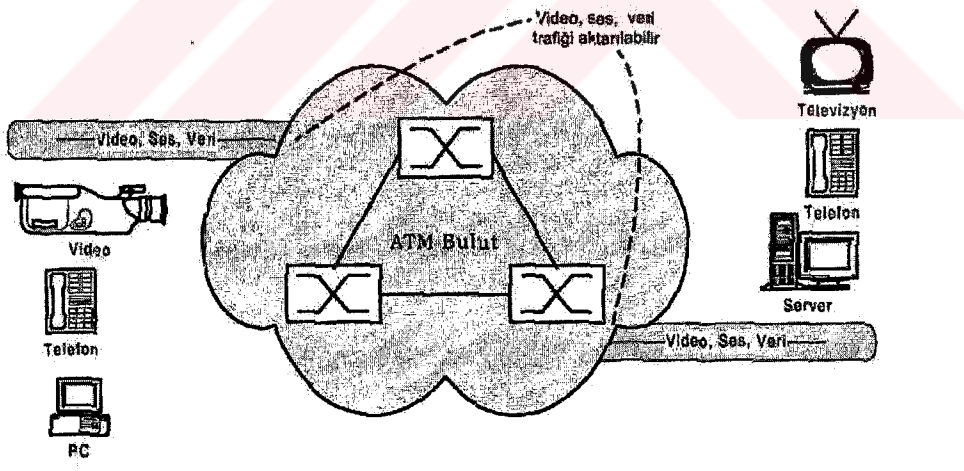
ATM, ses, veri, resim ve video gibi değişik türde bilgilerin aynı ortamdan hızlı bir şekilde aktarılması olanağı sağlayan bir anahtarlama/çoğullama teknolojisidir. LAN, WAN ve Kampüs uygulamalarında omurga ağ olarak, hızlı ve başarımı yüksek (performanslı), kullanıcı sayısından bağımsız bir ağ çözümü sunar. Güçlü bir başarım, güçlü bir anahtarlama alt yapısı ve farklı türde trafik gereksinimi olan uygulamaların tek bir ağ üzerinde çalışabilmelerine verdiği destekle kendisine sayısal iletişim ve ağ uygulamalarında önemli bir yer bulmaktadır.

ATM, son yıllarda birçok üretici firmanın desteklediği, üzerinde yoğun olarak çalışılan ve firmaların ürettikleri ATM ağ cihazlarının karşılıklı çalışabilmeleri için

yeni yeni standartların eklendiği bir konudur. ATM üzerine standart belirleyen ve her biri farklı açılara odaklanmış üç grup vardır. Bunlardan ITU-TSS, ATM'in protokollerini ve arayüzlerini tanımlamış ve orijinal standartları (1990 yılında) belirlemiştir; ATM Forum'un (daha çok üretici firmaların üye olduğu bir çalışma grubudur) ana amacı ITU-TSS tarafından tanımlanan standartları geliştirmek ve tüm üyelerinin uyacağı, ürünlerine yansıtacağı standardı belirlemektir. IETF, genel olarak ATM üzerinden IP trafiğinin taşınabilmesi (IP over ATM) üzerine olmaktadır.

3.2.5.1 Hücre, ses ve veri aktarımı

ATM teknolojisinin en önemli birkaç özelliği, aktarımda, hücre (cell) olarak adlandırılan küçük boyutlu ve sabit uzunlukta veri paketleri kullanılması; ses, veri, ve video uygulamalarının gereksinim duyduğu farklı türde hizmet (service) sınıflarını desteklemesi ve yine bu tür uygulamaların gereksinim duyduğu hizmet kalitesini sunmasıdır. Bunlara ek olarak, ağ içindeki kullanıcı sayısından bağımsız, güçlü bir başarım sunması büyük boyutlu uygulamalarda önemli bir nokta olarak ortaya çıkar.



Şekil 3.25 ATM ağ ses, veri ve video bilgisi aktarılması

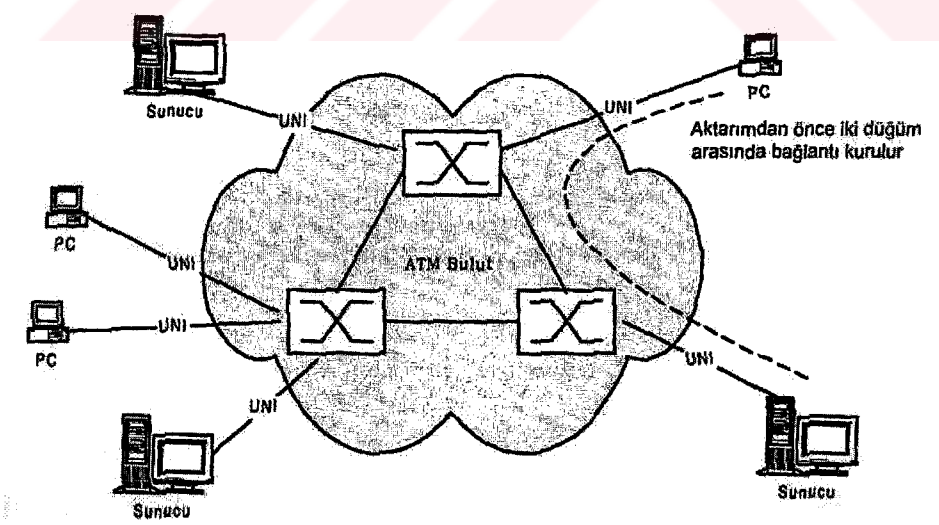
ATM, uygulamalara hizmet kalitesi sunan ve farklı türde trafik gereksinimini karşılayan hizmet sınıflarına (Class of service, CoS) sahip hücre tabanlı bir ağ teknolojisidir. Hücre tabanlı olduğundan, yani aktarım için kullanılan paketlerin sabit uzunlukta olmasından dolayı daha hızlı aktif cihazlar daha az donanım karmaşıklığıyla tasarlanabilmekte ve aktif cihazların portlarına tampon (buffer) amacıyla koyulan belleğin daha verimli ve başarımı arttıracak şekilde

kullanılabilmesini sağlamaktadır. Üstelik, bu tasarım kriterlerine göre üretilmiş cihazlarda porttan porta olan gecikmeler ve herhangi iki uç düğüm arasındaki gecikme hesaplanabilir olmakta ve oluşacak toplam gecikme öngörülebilmektedir.

ATM teknolojisinde bir fiziksel hat üzerinden aynı anda birden çok uygulamaya ait hücre aktarımı yapılabilir. Yani bir fiziksel yol birçok uygulama arasında paylaşılabilir. Yolun aktarım kapasitesinden bir kısmı bazı uygulamalara öncelikli olarak kullandırılabilir.

3.2.5.2 Bağlantı gereksinimi

ATM, bağlantıya yönelik bir aktarım protokolüdür. İki düğüm arasında aktarım yapılabilmesi için, önce düğümler arasında bağlantı kurulur. Aynı telefon konuşması yapılabilmesi için karşı tarafla bağlantı kurulması gerektiği gibi ATM'de de iki düğüm arasında önceden bağlantı kurularak aktarım süresince veri paketleri/veya hücrelerinin izleyeceği bir yol belirlenir. Daha sonra aktarılacak veri paketleri bu yol üzerinden, izlenecek yörünge belirli olduğu için alıcı ve verici adresleri veri paketlerinin içerisine koyulmadan gönderilir.



Şekil 3.26 ATM ağda bağlantı kurulması

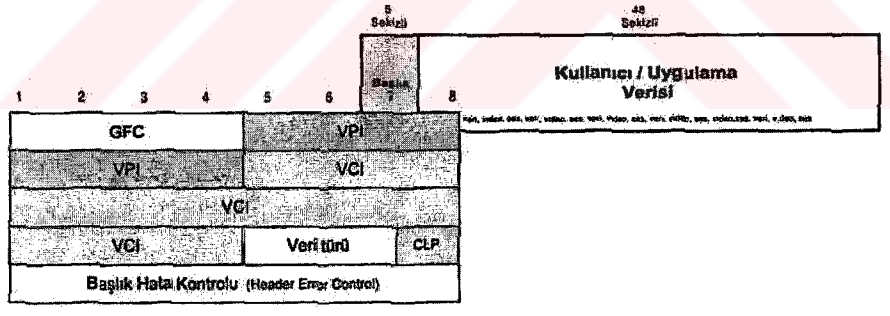
Hizmet kalitesi (Çuality of Service, QoS) özellikle zamana duyarlı gerçek zaman uygulamalarında kendisini hissettiren önemli bir faktördür.

3.2.5.3 Temel aktarım paketi/hücre (Cell)

ATM protokolünde aktarım için kullanılan temel paket sabit uzunlukta hücrelerdir. Toplam 53 sekizli olan hücrelerin 5 sekizlisi başlık, 48 sekizlisi de aktarılacak veri içindir. Başlık bilgisi oldukça kısadır, ancak aktarım için gerekli bağlantı önceden kurulduğundan dolayı bu kadar başlık bilgisi hücrenin alıcısına doğru olarak ulaşmasına yetmektedir. Aktarım için kullanılan veri paketinin, yani hücrelerin sabit uzunlukta olması daha hızlı ve donanım karmaşıklığı daha az olan ATM anahtarlama cihazlarının tasarlanabilmesine imkan verir.

3.2.5.4 GFC (Generic flow control)

Bu alan ilerisi için saklı tutulmuş olup, genel olarak, birden çok cihazın tek bir UNI'ı kullanmasını desteklemesi amacıyla düşünülmektedir. Standart belirleyen gruplar tarafından bu alan için henüz bir şey tanımlanmamıştır.



Şekil 3.27 Hücre yapısı ve başlık bilgisi içindeki alanlar

3.2.5.5 VPI (Virtual path identifier)

Hücrenin üzerinden geçeceği sanal yol (Virtual Path Identifier) numarasını içerir. (8 Bit)

3.2.5.6 VCI (Virtual channel identifier)

Hücrenin içerisinden geçeceği sanal kanal numarasını içerir. (16 bit)

3.2.5.7 Veri Türü (Payload type identifier)

Hücrelerin içinde taşınan verinin kullanıcı bilgisi, ağ bilgisi, yönetim bilgisi gibi ne tür bilgi içerdiğini gösterir. Aynı zamanda iletim anında tıkanma meydana geldiğinin belirtilmesi için de kullanılır. (3 bit)

3.2.5.8 CLP (Cell loss priority)

Bu 1 bitlik alan ilgili hücrelere öncelik vermek için kullanılır. Eğer değeri 1 ise önceliği düşük, 0 ise önceliği yüksektir. İletim anında tıkanma oluşursa düşük öncelikli hücreler yoldan çıkarılır. (1 bit)

3.2.5.9 Başlık hata kontrolu (HEC - Header error control)

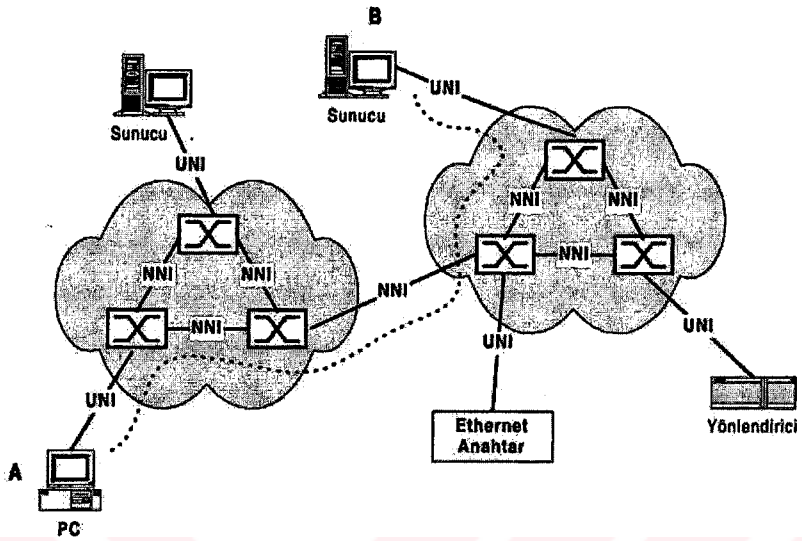
Hücrenin başlık kısmı için hata kontrolü yapmak için kullanılır. Hata kontrolünde CRC algoritması kullanılır.

3.2.5.10 Bağlantı arayüzleri (UNI ve NNI)

ATM ağlar için iki tür bağlantı arayüzü tanımlanmıştır. Biri, ATM portu olan (ATM NIC, Ethernet Anahtar veya Yönlendirici gibi) bir uç sistemin ATM ağa bağlanması için kullanılır ve UNI (User-to-Network Interface) olarak adlandırılır. Diğeri, ATM bulutu oluşturan Anahtarların birbirine bağlanması için kullanılır ve NNI (Network-to-Network Interface) olarak adlandırılır. ATM hücrelerin başlık bilgisi, bağlantının UNI ve NNI olmasına göre farklıdır. Şekilde gösterilen başlık bilgisi UNI için olanıdır. NNI bağlantıda başlık bilgisi GFC alanı içermez. Bu alan VPI alanına eklenerek VPI alanı 12 bit'e çıkartılmıştır.

Diğer şekilde de iki ayrı ATM bulut, onların içerisindeki ATM anahtarlar ve uç sistemlerin buluta bağlantısı görülmektedir. Dikkat edilirse, bulut içerisindeki anahtarlar birbirlerine NNI ile bağlıdır. Aynı zamanda iki bulutu birbirine birleştiren bağlantı da NNI'dır (çünkü iki bulut birbirlerine ATM anahtar üzerinden bağlıdır).

Ancak, ATM portu olan Ethernet anahtar, yönlendirici ve ATM NIC (ATM ağ kartı) ATM ağa UNI ile bağlıdır.

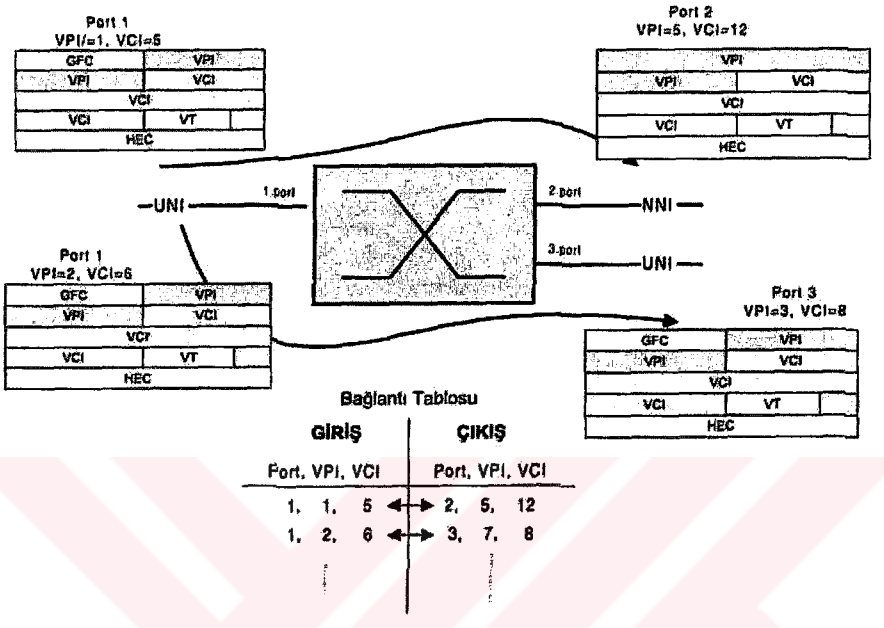


Şekil 3.28 UNI ve NNI bağlantı arayüzleri

Yukarıdaki örnekte, A düğümünden B düğümüne bir bağlantı kurulduktan sonra, buradan akacak hücreler, birden çok ara düğümden geçer. Verilen çizimde 5 ara yol, 4 ara düğümden geçmektedir. A düğümünden çıkan hücreler önce UNI arayüzü üzerinden bir ATM anahtara, oradan NNI arayüzü üzerinden bir başka ATM anahtar ve oradan da, sırasıyla NNI, NNI, UNI ara yüzlü bağlantılarını izleyerek B düğümüne ulaşır. Atlama sayısı, bu örnek için 5 olur. En kısa atlama sayısı, iki uç düğüm aynı ATM anahtara bağlı ise olur ve 2'dir.

ATM hücreleri düğümden düğüme atlarken, başlık kısmı içerisinde bulunan VPI ve VCI numaralan değişir. Eğer atlama UNI ile NNI arasında oluyorsa değişen VPI/VCI ikilisine ek olarak başlık formatı da kısmen değişir. Hücre başlığı UNI bağlantıda kullanılan format olup NNI bağlantıda geçerli olan formatta GFC alanı yoktur. GFC için kullanılan bitler VPI alanına eklenmiştir. Aşağıda, Şekil 3.29'da, bir ATM anahtar üzerinde iki bağlantı kurulmuştur. Birinci bağlantı 1.port ile 2.port arasında (UNI-NNI dönüşümü var), ikinci bağlantı 1.port ile 3.port arasındadır. Birinci bağlantı için, 1.porta VPI/VCI numarası 1/5 ile gelen hücreler 2.porttan VPI/VCI numarası 5/12 olarak çıkarlar (aynı zamanda GFC alanı çıkartılıp VPI alanına eklenmiştir). İkinci bağlantıda hücreler 1.porta 2/6 VPI/VCI numaraları ile girip

3.porttan 3/8 numaraları ile çıkmaktadır. Bu değiştirme işlemleri anahtar tarafından yapılır. İki düğüm arasında hangi VPI/VCI numaraları kullanılacağı sanal bağlantı kurulması sırasında belirlenir ve ATM anahtarlarda bulunan tabloya koyulur.



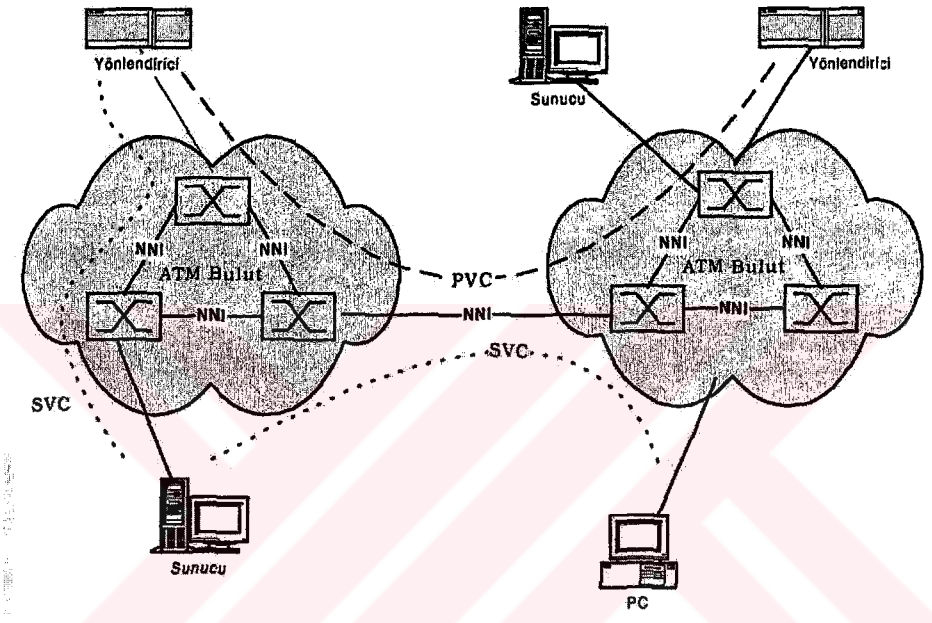
Şekil 3.29 Hücre aktarımda VPI/VCI numarası ve başlık formatı değişimi

3.2.5.10.1 Sanal devreler (Virtual circuits)

ATM ağda hücre aktarımı sanal devreler (virtual circuit) üzerinden gerçeklenir. Yani, iletişimde bulunacak iki düğüm arasında aktarım işlemi yapılabilmesi için, önceden, ilgili iki düğüm arasında sanal devre kurulmuş olmalıdır. Sanal devrelerin oluşturulmasında iki farklı yol izlenmektedir. Birisi, iletişimden hemen önce sanal devrenin kurulması ve aktarım işlemi bittikten sonra kaldırılması şeklinde olurken, diğer yöntemde, sanal devre sistem konfigürasyonu aşamasında kurulur ve silinmediği sürece öyle kalır. Birinci yöntem anahtarlamalı sanal devre (Switched Virtual Circuit, SVC), ikinci yöntem ise kalıcı sanal devre (Permanent Virtual Circuit, PVC) olarak adlandırılır.

SVC, yöntem olarak dial-up bağlantıyı andırırken, PVC kiralık hat uygulamasını andırır. Her iki yöntemin de seçimlik veya en uygun olduğu durumlar vardır.
İletişimi başlatmak isteyen bir uç düğüm karşı düğüm ile aralarında sanal bir bağlantı (Virtual Connection, VC) kurulması işlemini başlatmalıdır. İki düğüm arasında sanal

bağlantının kurulmasıyla beraber, o bağlantının uçtan uca güzergahını belirten birtakım yol ve kanal numaraları atanır. Daha sonra o bağlantı yolu üzerinden aktarılacak hücreler bu numaraların kullanılmasına dayanarak anahtarlanır ve alıcısına gider. Temel olarak, ATM adresleri hücrelerin aktarılması için kullanılmaz, yalnızca sanal bağlantının kurulması için kullanılır. Hücrelerin aktarılması sürecinde, hücre başlığı içinde bulunan sanal yol numarası ve sanal kanal numarası kullanılır.



Şekil 3.30 ATM ağ üzerinde sanal devre kurulması

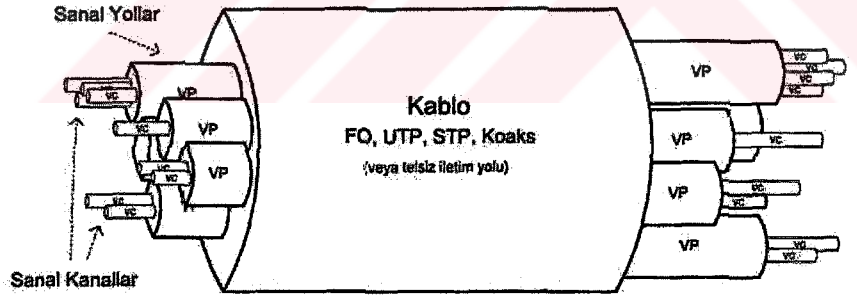
SVC - Anahtarlamalı sanal devre (Switched virtual circuit): Anahtarlamalı sanal devre, gerektiği anda kurulur ve işi bitince sonlandırılır. Böylelikle düğümler arasında esnek iletişim kanalları oluşturulması sağlanır. ATM ağ içindeki her düğüm gerektiği anda bir başka düğümle arasında SVC kurar ve iletişimini kotarır.

PVC - Kalıcı sanal devre (Permanent virtual circuit): Kalıcı sanal devre, sistem konfigürasyonu sırasında veya sistem konfigürasyonu düzeyinde önceden kurulur ve sistem işletilmeye başladığı andan itibaren sürekli kalır. Böylece aralarında PVC tanımlı düğümler birbirleriyle haberleşmek istediğinde halihazırda aralarında sanal devre olduğu için doğrudan aktarıma başlarlar. Bu yöntemde sanal devre kurulması için zaman harcanmaz. Ancak, her PVC'nin önceden sistem konfigürasyonu düzeyinde yapılması ve gerekmediği anda da bellek gibi sistem kaynaklarını kullanması nedeniyle genel olarak, çok fazla kullanılmaz. Böyle olmasına rağmen,

kullanılması kaçınılmaz olan durumlar da vardır. Örneğin birbirini ATM ağ üzerinden görmesi gereken iki yönlendirici arasında PVC tanımlaması kaçınılmaz olabilir.

Sanal yol (Virtual path-virtual channel) : ATM ağda, iki düğüm arasında sanal bağlantı kurulması demek, aslında, iki düğüm arasında sanal yol ve onun da içerisinde sanal kanal oluşturulması anlamına gelir. Temel aktarım birimi olan hücreler bu sanal kanallar içerisinden akar. Bu demektir ki, gerçekte aktarım yapılan ortam sanal yol içerisindeki sanal kanallardır. Sanal kanallar bir otobandaki şeritlere ve sanal yol da birden çok şeriti içeren anayola benzer.

Her ATM anahtar üzerinde, hangi portları arasında hangi sanal devrelerin kurulmuş olduğunu tutan birer tablo vardır. Anahtar üzerindeki bir porta gelen hücrelerin nereye (hangi porta) anahtarlanacağı bu tabloya bakılarak değerlendirilir. Tablo, her sanal bağlantı için bir sanal yol numarası (Virtual Path Identifier, VPI) ve bir sanal kanal numarası (Virtual Channel Identifier, VCI) içerir

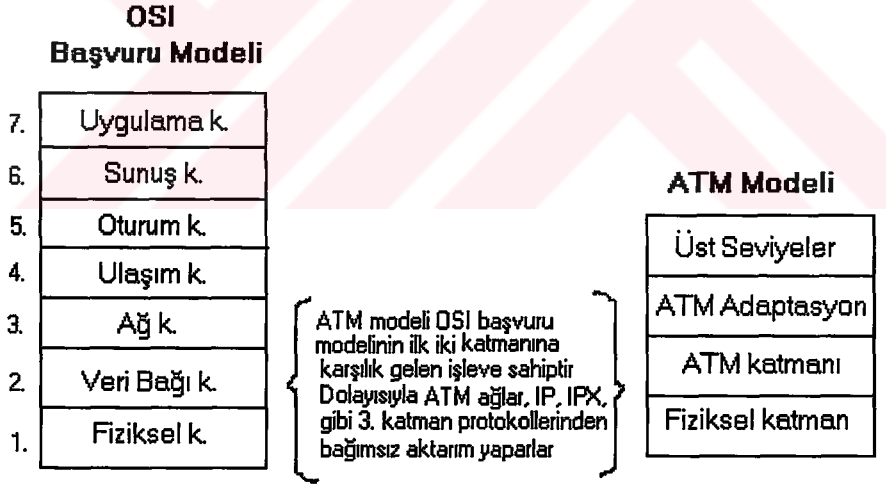


Şekil 3.31 Sanal Yol ve Sanal Kanal

Şekil 3.31'de görüleceği gibi uçtan uca iki düğüm arasında kalıcı (PVC) veya anahtarlamalı (SVC) sanal devre kurulurken, devre birden çok ATM switch veya ATM portlu cihaz üzerinden geçebilmektedir. Burada dikkat edilmesi gereken nokta iki düğüm arasında sanal bağlantı kurulduğunda, o bağlantı için atanan VPI ve VCI değerleri tüm bağlantı boyunca aynı değildir. Herhangi bir VPI/VCI ikilisi yalnızca birbirine komşu iki düğüm arasındaki bağlantıyı gösterir.

3.2.5.11 ATM mimarisi

ATM teknolojisinin genel yapısı diğer ağ protokol kümelerinde/teknolojilerde olduğu gibi katmanlı bir mimariye sahiptir; OSI'nin 7 katmanlı başvuru modelinde olduğu gibi ATM'de de tüm yapı katmanlara (3 katmana) ayrılmış ve her bir katmana ait görevler bu konuda standart oluşturan gruplar tarafından belirlenmiştir. Bu standartlara göre ATM mimarisi temelde 3 katmandan oluşmaktadır. En altta, diğer ağ başvuru modellerinde olduğu gibi veri paketlerinin aktarım ortamı üzerinden bit düzeyinde aktarılması işini kotaran fiziksel katman bulunur; hemen üstünde ATM katmanı ve onun da üzerinde ATM adaptasyon katmanı vardır. Bu üç katman, işlevsel olarak OSI başvuru modelinde ilk 2 katmana karşılık gelir ve dolayısıyla OSI'nin 3.katmanı olan ve IP, IPX gibi protokol bazında denetimlerin, yönlendirmelerin gerçeklendiği ağ katmanını kapsamaz. Bu nedenle ATM ağ, protokol bağımsız, her türlü trafiği aktarabilecek saydam bir yapıya sahiptir.



Şekil 3.32 ATM ve OSI başvuru modeli

3.2.5.11.1 Fiziksel katman

Fiziksel katman, temel aktarım birimi olan hücrelerin ağ ortamı üzerinden nasıl aktarılacağını belirtir ve bununla ilgili bağlantı arayüzlerini, arayüzlerin sahip olacağı aktarım hızlarını (Mbps) tanımlar. ATM tanımlarında arayüz olarak daha önce hücre tabanlı teknolojiler için tanımlanmış olan arayüzlerin kullanılacağı varsayılarak yeni arayüz tanımlamaları yapılmamıştır, onların kullanılması önerilmiştir.

ATM ağa, bir uç cihazın bağlanması için kullanılan arayüz tanımlaması UNI'dır. UNI için 3.0 ve 3.1 olarak numaralanan iki uyarlama vardır. Fiziksel katman protokolleri aşağıda belirtildiği gibidir:

Fiziksel katman kendi içerisine fiziksel ortam (Physical Medium, PM) ve aktarım dönüşümü (Transmission Convergence, TC) olarak adlandırılan iki alt katmana ayrılmıştır

PM alt katmanı doğrudan iletişimin yapıldığı aktarım ortamı ile çalışma şeklini belirler ve genel olarak bit zamanlaması (bit timing) ile hat kodlama (line coding) işlevini yerine getirir. Kodlama şekli ve bağlantılarda kullanılacak konnektörler bu katmanda belirlenmiştir:

• MM fiber
•100Mbps TAXI (4B/5B kodlaması)
• 155 Mbps - SONET STS-3c
• 622 Mbps - SONET STS-12c
• SM fiber
• 155 Mbps - SONET STS-3c

• UTP
• 52 Mbps, Cat3 veya Cat5
• 155 Mbps, Cat5

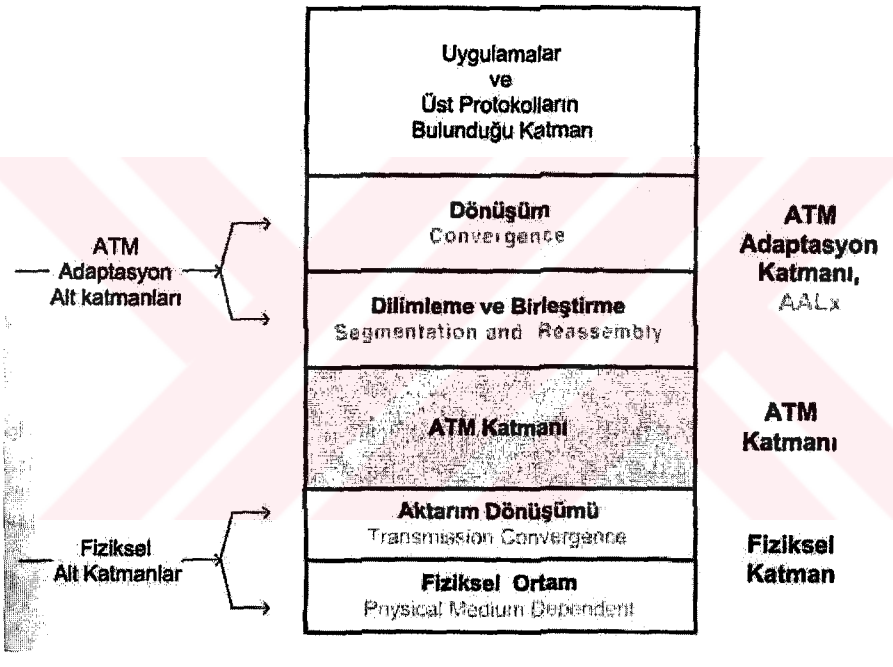
• STP
• 25.6 Mbps
• 155 Mbps - SONET STS-3c

• Coaksiyel
• 45 Mbps -DS3

TC alt katmanı, hemen altında bulunan PM alt katmanıyla hemen üstünde bulunan ATM katmanı arasında adaptasyon sürecini kotarır ve genel olarak başlık hata sınaması için gerekli işlevlere ve hücrelerin aktarım ortamına geçirilmesi için gerekli adaptasyon işlevlerini yerine getirir; zaman kriterlerini sağlamak için çerçeve içine boş hücreler yerleştirir.

3.2.5.11.2 ATM katmanı

ATM katmanı bir üst katmandan gelen bilgiyi, ona bir katma değer eklemeksizin alıcısına ulaştıran yalın bir aktarım ortamı sunar. ATM katmanı hücrelerin içerisinde taşınan bilgi türüyle ilgilenmez. Temel olarak bağlantı kurulması, akış kontrolü ve hücrelerin hızlı bir şekilde anahtarlanması işini kotarır. Anahtarlama işlemi genel olarak donanıma dayalı gerçeklendiği için çok yüksek hızlarda ATM anahtarlar gerçeklenebilmektedir. Hücrelere ait sekizliler artan sırada gönderilirken, sekizlilere ait bitler azalan sırada aktarılır.



Şekil 3.33 ATM başvuru modelinin alt katmanları

3.2.5.11.3 ATM adaptasyon katmanı (ATM adaptation layer – AAL)

ATM Adaptasyon katmanı (kısaca AAL), uygulama programları ve servislerinin gereksinim duyduğu farklı türde trafiklerin ATM katmanı üzerinden aktarılması işini sağlar. Örneğin ses haberleşmesi uygulaması ile veri haberleşmesi veya video aktarımı birbirinden farklı özelliklerde aktarım kriterleri ister. Ses ve video haberleşmesi zamana duyarlı iletişim ortamı isterken, veri haberleşmesinin böyle bir gereksinimi yoktur. Her uygulama türünün kendine has gereksinimleri vardır. AAL bu gereksinimleri karşılar. Bu amaçla değişik türde hizmet sınıflarına sahiptir. Bunlar

AALl, AAL2, AAL3/4 ve AAL5 olarak adlandırılır ve her biri değişik kriter gereksinimi olan uygulamalara hizmet sunar. Tablo-4.3'de bu servis sınıflarının sunduğu özellikler ve diğer bir sınıflamaya göre yeri gösterilmiştir.

ATM adaptasyon katmanı, fiziksel katman gibi kendi içerisinde 2 alt katmana ayrılmıştır. Biri, dönüşüm (Convergence Sublayer, CS), diğeri ise dilimleme ve birleştirme (Segmentation and Reassembly, SR) alt katmanları olarak adlandırılır. Dönüşüm alt katmanı genel olarak, ATM ile ATM olmayan bağlantıda format dönüşümü yapan fonksiyonları yerine getirir. Dilimleme ve birleştirme alt katmanı, adı üzerinde bir hücrenin veri alanından büyük veri parçalarını dilimleyerek 48 sekizliden oluşan küçük dilimlere ayırır veya tersine, kendisine gelen 48 sekizli uzunlukta olan dilimlerden, bir üstünde bulunan dönüşüm katmanının kabul edeceği büyüklükte veri parçalarını elde eder.

3.2.5.12 Hizmet sınıfları (Class of services – CoS)

ATM adaptasyon katmanının hizmetleri üç farklı parametreye dayanılarak dört farklı sınıfta toplanmıştır. Sınıflamada kullanılan üç parametre şöyledir:

- Gönderen ile alıcı arasında zamana duyarlılık gereksinimi - var/yok
- Bit akışı (Bit rate) - sabit/değişken
- Bağlantı modu (Bağlantı mode) - bağlantıya yönelik/bağlantısız

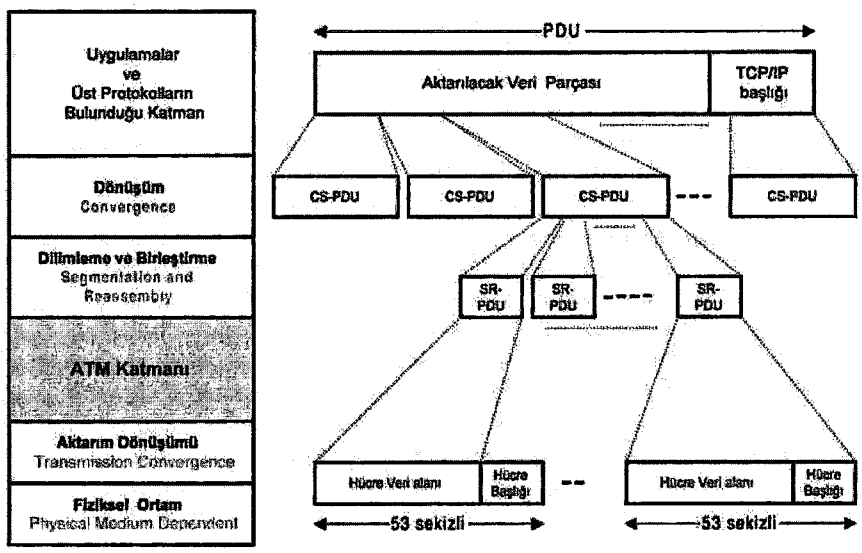
Tüm hizmet sınıfları bu üç parametre baz alınarak yapılır. Örneğin ses aktarımının, zamana duyarlılık gereksinimi vardır ve sabit bit akışı gerektirir. Veri aktarımının zamana duyarlılığı yoktur ve değişken bit akışıyla gerçeklenebilir. A, B, C ve D diye adlandırılan hizmet sınıflarının gereksinimi Tablo-4.3'de verilmiştir.

Aşağıdaki tabloda gösterilen hizmet sınıflarının her biri genel olarak farklı uygulamalar için daha uygundur. Örneğin A sınıfı hizmet, zamana duyarlı, sabit bit akışını sağlayan ve bağlantıya yönelik bir ortam sunar; bu tür hizmet sınıfı ses ve video aktarımı için uygundur. Buna karşın C sınıfı hizmet veri aktarımı için uygun düşer. Kısacası, ATM üzerinden klasik LAN verilerinin aktarılması için AAL5 (C ve D sınıfı) hizmeti, PBX gibi sistemlerin bilgileri aktarılırken AALl (A sınıfı) hizmet kullanılır.

Servis Sınıflan	Zamana Duyarhlık	Bit Akışı	Bağlantı Modu	AAL Türü	
A Sınıfi	Var	Sabit	Bağlantıya yönelik	AALl	
B sınıfi	Var	Değişken	Bağlantıya yönelik	AAL2	
C Sınıfi	Yok	Değişken	Bağlantıya yönelik	AAL3	AAL5
D Sınıfi	Yok	Değişken	Bağlantısız	AAL4	

Tablo 3.3 AAL'in sunduğu hizmet sınıflan ve özellikleri

PDU olarak adlandırılan ve üst düzey protokollerden veya uygulamalardan gelen veri paketleri, ATM adaptasyon katmanından geçerken, önce, kullanılan AAL hizmet türüne göre dönüşüm alt katmanında (CS) parçalanır ve CS-PDU olarak adlandırılan parçalar elde edilir. Daha sonra bu parçaların içerisine ilgili AAL'in başlık ve kontrol bilgileri yerleştirildikten sonra, bir altında bulunan dilimleme ve birleştirme alt katmanına (SR alt katmanına) aktarılır. Dilimleme alt katmanı, kendisine gelen CS-PDU paketlerini 48 sekizliden oluşan ve hücrelerin veri alanına koyulacak küçük dilimlere ayırır (tersi durumda, gelen dilimleri birleştirerek CS-PDU'yu elde eder). ATM katmanı, bu dilimlere hücre başlık bilgileri ekler alıcısına iletilmesi için fiziksel katmana verir...



Şekil 3.34 Veri paketinin AAL üzerinden geçişi

ATM hizmetleri bit akışına göre de sınıflanarak, sınıflamada ikinci bir tanımlama yapılmıştır. Bu tanımlamaya göre ATM hizmetleri şöyle sınıflanmıştır:

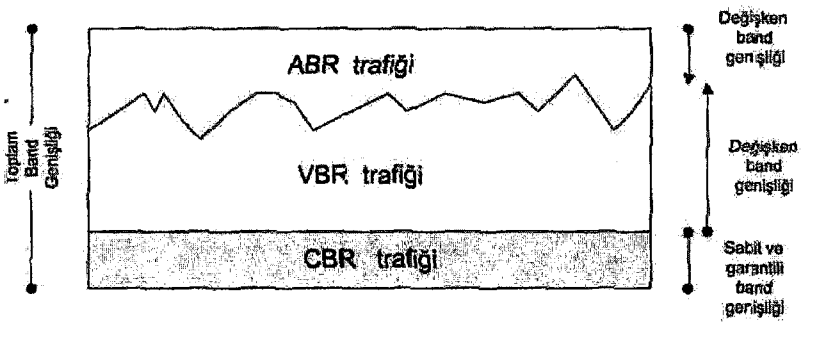
- CBR (Continuos Bit Rate)
- VBR (Variable Bit Rate)
- ABR (Available Bit Rate)
- UBR (Unspecifled Bit Rate)

3.2.5.12.1 CBR

Sabit bit akışı gereksinimi olan video ve ses aktarımlarında kullanır. Uçtan uca sabit bir band genişliği garanti eder. Sayısal telefon santralı olan PBX1er bu hizmet sınıfı üzerinden birbirlerine aktarım yapabilir.

3.2.5.12.2 VBR

Bit akışının birden arttığı ve sonra azaldığı, ne zaman ne kadar artacağı belli olmayan, ancak arttığı zaman aktarılması gereken uygulamalar için kullanılır. Örneğin iki uç sistem arasında trafik aktarımı birden çok artıyorsa (örneğin transaction prosesler) bu tür hizmet sınıfını kullanmalıdır. VBR kendi içinde, biri rt-VBR (real time VBR), diğeri nrt-VBR (non-real-time VBR) olmak üzere iki alt sınıfa ayrılır.



Şekil 3.35 Bit Akışına göre trafik özellikleri

3.2.5.12.3 ABR

Önceliği az olan ve band genişliği garantisini en az veren hizmet sınıfı ABR'dır. Genel olarak diğer hizmet sınıflarından kalan boş band genişliği kullanılır. Bu hizmet

sınıfı LAN'ların klasik verisini aktarmak için uygundur. Uçlarda koşan uygulamalara belirli bir band genişliği vermez, ancak onların minimum gereksinimlerini karşılayacak (oturumların kopmaması vs. gibi) iletişim garantisi verir. ABR hizmetinde, bir tıkanma oluşması durumunda hücre kaybı olmaması için tıkanma kontrolü de yapılır.

3.2.5.12.4 UBR

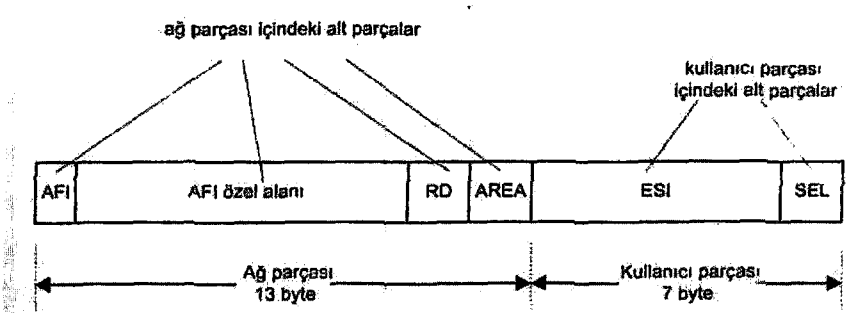
Bu hizmet sınıfında akış kontrolü yapılmaz ve iletişimde garanti yoktur.

3.2.5.13 ATM adresleri

ATM adresleri 20 sekizli uzunluğundadır ve ağ içerisinde bulunan ATM cihazlara kimlik kazandırmak için kullanılır. Genel olarak, iletişim yapılması için gerekli olan sanal bağlantının kurulması sırasında kullanılır. ATM ağa UNI ile bağlı bir uç cihaz, iletişim yapma gereksinimi duyduğunda, karşı tarafla aralarında bir PVC yoksa, dinamik bağlantı kurma yöntemi olan SVC'nin kurulması isteğinde bulunmalıdır. SVC kurulurken, o bağlantı için VPI/VCI değerleri belirlenir ve o oturum için aktarılacak tüm hücreler bu VPI/VCI değerleri kullanılarak aktarılırlar. Yani, aktarım anında ATM adresleri kullanılmaz, yalnızca VPI/VCI değerleri kullanılır. Dolayısıyla 20 sekizli gibi uzun bir adres yapısına sahip olan ATM teknolojisinde, adreslerin bu kadar uzun olması başarımı etkilemez.

ATM adresleri, temel olarak 2 parçaya ayrılır. Biri ağ parçası (network prefix), diğeri kullanıcı parçası (user part) olarak adlandırılır. Ağ parçası bir ATM ağ için aynı olup ağı temsil ederken, kullanıcı parçası, o ATM ağ içerisindeki ATM cihaza ait özel bir değerdir ve onun kimliği niteliğindedir. Ağ ve kullanıcı parçaları da kendi içlerinde alt parçalara ayrılarak adresleme de güçlü bir hiyerarşik yapı elde edilmesi yoluna gidilmiştir. Küçük boyutlu bir ATM ağda, ATM adreslemenin sağladığı güçlü hiyerarşik yapı kendini hissettirmez iken, büyük boyutlu global ATM ağlarda önemini ortaya koyar.

ATM adresleri için halihazırda var olan ve, DCC, E-164 ve ICD formatı olarak bilinen 3 tür format şeklinden biri kullanılır. Adresin ilk sekizlisi hangi tür formatın kullanıldığını gösterir ve bu sekizlinin ne olacağı aşağıda verilmiştir:



Şekil 3.36 ATM adres formatı ve alt parçaları

- DCC formatı → 39 ; DDC (Data Cauntry Code)
- E-164 formatı → 45 ; E-164 (ISND de kullanılan numaralandırma formatı)
- ICD format → 47 ;ICD (İnternational Code Designer)

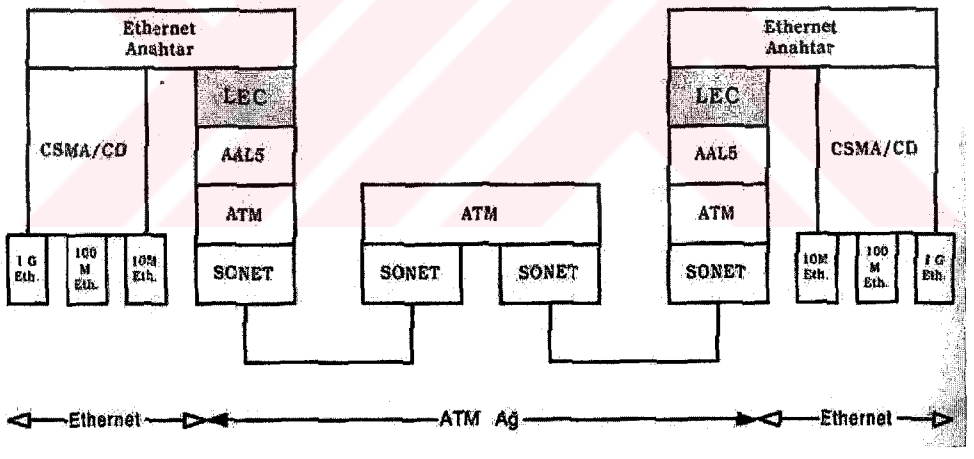
Ağ parçası içinde bulunan AFI (Authority Format Identifier) kullanılan format türünü, AFI özel alanı ATM cihazı üreten firmanın özel kodunu içerir. RD (Routing Domain) ve AREA parçaları ise ATM ağ içerisinde anahtarlamanın etkin bir şekilde sağlanması için alt ağ ve bölgeler oluşturmak amacıyla kullanılır. Kullanıcı parçasında bulunan ESI (End Station Identifier) bir uç cihaza ait adres parçasını gösterirken, SEL (SELector Field) için henüz bir tanımlama yapılmamıştır.

3.2.5.14 LAN emülasyonu (LANE)

LAN emülasyonu, kısaca LANE diye anılır, paket aktarımına dayanan Ethernet, Jetonlu Halka, FDDI gibi ağ ortamlarının ATM buluta eklenmesi ve o ortamdan iletişim yapabilmelerini sağlar. Bu sayede bu tür teknolojilere dayanan ortamlarda bulunan sistemlerin birbirleriyle veya ATM bağlı sistemlerle görüşebilmeleri, iletişim yapabilmeleri sağlanır.

Yalnızca ATM'den oluşan bir ağ içerisinde LAN emülasyonuna gerek yoktur. Ağ içindeki her şey, yani uç sistemler ve anahtarlar ATM olduğu için tüm ağda yalnızca ATM standartları ve arayüzleri vardır. Böyle bir ağa yalın ATM ağ denir. Ancak günümüz uygulamalarında yalnızca bir teknolojiyi içeren yalın bir ağ ile iletişim gereksinimin sağlanması mümkün olamayacağı için birden çok teknolojinin birbirleriyle bütünleşik olarak çalışması zorunludur.

Şekil 3.37'de ATM ağ ile Ethernet teknolojinin bütünleştirilmesi durumu, katmanlar düzeyinde görülmektedir; ortada bir ATM düğüm, iki kenarda ise üzerinde ATM portu olan birer Ethernet Anahtar vardır. Ethernet Anahtarın Ethernet portları tarafında, Ethernet'in dayandığı CSMA/CD protokolü, ATM portu tarafında ise ATM'in 3 katmanına ek olarak LEC olarak adlandırılan bir katman daha vardır. Bu LEC katmanı Ethernet paketlerinin ATM ortamı üzerinden aktarılmasını ve onun üzerinde koşan uygulamaların ATM ağ üzerinden karşılıklı çalışabilmelerini sağlar.

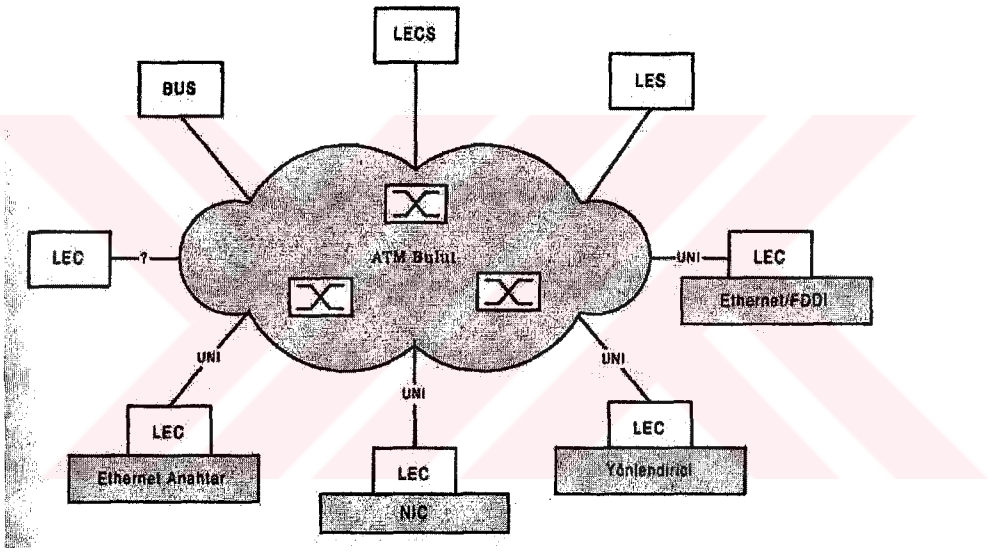


Şekil 3.37 ATM ile Ethernet ağların bütünleştirilmesi ve katmanlar

LANE, ATM ağ ile diğer ağ teknolojilerin karşılıklı çalışabilmesini sağlayan bir tanımlama, bir özelliktir. Böylece, 802.x ailesi kapsamındaki LAN protokolleri, üzerlerinde herhangi bir değişiklik yapılmadan ATM ağa birleştirilebilir. Normalde, bu tür paket anahtarlamalı protokoller üzerinde koşan uygulama programlarına ait iletişim paketleri ATM ağ üzerinden de aktarılır.

LEC, yalnızca, LAN Emülasyonu'nun gerçeklenmesi için tanımlanmış olan parçalardan birisidir. LEC'e ek olarak LECS, LES ve BUS olarak adlandırılan

parçaları da vardır. LANE'nin LEC (LAN Emulation Client) parçası, ATM ağa bağlanacak (Paket anahtarlama tabanlı) uç cihazların üzerinde olan kısmıdır. Bu tür uç cihazlar üzerinde en az bir tane LEC olmalıdır; birden çok da olabilir. Şekil 3.38'de bir ATM ağda bulunacak LANE parçaları görülmektedir. LECS, ATM ağda bir tane bulunur ve ağ ile ilgili tüm konfigürasyon işleri buradan kotarılır. LES, ATM ağ üzerinde tanımlı her vLAN için bir tane bulunur ve ilgili vLAN üzerinde tanımlı uç sistemlerin ağa erişmesi işini kotarır. BUS, 802.x ailesine dayanan LAN teknolojilerinde kullanılan yayın türü (broadcast) aktarımın ATM üzerinden de gerçeklenmesini sağlar ve her vLAN için bir tane olur.



Şekil 3.38 LAN Emülasyonu parçaları (LEC, LECS, LES ve BUS)

3.2.5.14.1 LEC (LAN emulation cilent)

LEC, ATM ağa LANE üzerinden bağlanan uç sistemlerde bulunur. Genel olarak adres çözümlemesi ve kontrol işlemlerini kotarır. Uç sistem ilk açıldığında genel olarak aşağıdaki işleri yerine getirir.

1-LECS ile iletişimde bulunur. ILMI veya bilinen VPI/VCI numaraları kullanır.
2-LECS'ten kendisinin üyesi olacağı vLAN'ın LES adresini alır.
3-Üyesi olacağı LES'e bağlanarak, kendisini tanıtır ve o vLAN'ın BUS adresini öğrenir.

4-BUS ile bağlantı kurar.

LECS'e kendisini kaydettirmiş ve LES, BUS adreslerini öğrenmiş bir LEC artık iletişim için gerekli bağlantıyı kurmaya hazır demektir.

3.2.5.14.2 LECS (LAN emulation configuration server)

LECS, LAN Emülasyonu kapsamında tüm ATM ağ hakkında gerekli konfigürasyon bilgilerini tutar ve ATM ağa bağlanacak uç sistemlerin gereksinim duyduğu bilgileri verir. Bir uç sistem ilk açıldığında kendisini LECS'e kayıt ettirmelidir. Ancak kayıt işlemi gerçeklendikten sonra iletişim için gerekli bağlantı kurulması isteğinde bulunabilir. Aksi durumda o uç sistemin bağlantı istekleri kendisine ait olan LES'e ulaşmaz.

Uç sistem ilk açıldığında kendisini kayıt ettirmek amacıyla LECS ile iletişimde bulunmalıdır. Bu amaçla bir bağlantı kurulmalıdır. Bu bağlantının kurulabilmesi için ya ILMI MIB kullanılır ya da genel olarak VPI/VCI numaraları bilinen (well known) sanal kanal kullanılır. Uç sistemlerde bu bağlantı için hangisinin kullanılacağı belirtilmelidir.

3.2.5.14.3 LES (Lan emulation server)

LES, genel olarak bir vLAN'a üye olan LEC'lerin yönetimi işini kotarır. Bir LEC, ait olduğu LES'e kendini tanıtırken, LES'e MAC ve ATM adres çiftini gönderir. LES, sahip olduğu adres dönüşüm tablosuna her LEC için MAC ve ATM adres çiftlerini ekler. Bu aşamadan sonra, bir LEC iletişim yapmak için bir bağlantı kurmak istediğinde LES'ten adres dönüşüm işlemi için LE-ARP isteğinde bulunur. Bu adres dönüşüm sürecinden sonra karşı taraftaki LEC ile sanal bağlantı kurulur.

3.2.5.14.4 BUS (Broadcast and unknown server)

BUS, aktarılacak veri paketinin alıcı adresinde grup, yayma (group, broadcat) adresleri olduğu zaman devreye girer veya gönderici konumdaki LEC, MAC adresinden ATM adresi çözümleyemediği durumlarda kullanılır. LAN emülasyonunda BUS'ın sahip olduğu fonksiyonlara ihtiyaç vardır. Çünkü, paket

aktarımına dayanan 802.x ailesinden LAN protokolleri yayma ve çoklu alıcısı olan paket aktarımları yapmaktadır. Ancak ATM bağlantıya yönelik bir aktarım protokolü olduğu için, yayma veya çoklu gönderim BUS aracılığıyla gerçeklenir.

3.2.5.14.5 İşaretleşme (Signalling)

İşaretleşme, ATM ağa UNI arayüzü ile bağlı bir uç sistemin karşı bir sistemle anahtarlamalı sanal bağlantı (SVC) kurulması imkanı verir. İki uç düğüm arasında PVC kurulacaksa, bununla ilgili tanımlama cihazların konfigürasyonu düzeyinde yapılır, yani elle girilir. Ancak sanal bağlantı kurulmasında esneklik sağlayan ve isteyen her uç sistemin kendiliğinden bir başka sistemle, dinamik olarak sanal bağlantı kurabilmesi yeteneği işaretleşme standardıyla sağlanmıştır. ATM Forum'un ilk UNI standardı (Versiyon 2.0) uç sistemler arasında yalnızca PVC kurulması için tanımlama içerir. Daha sonraki uyarlamaları (Versiyon 3.0 ve 3.1) SVC kurulması için gerekli işaretleşme standartlarını da içermektedir. Versiyon 3.0 ve 3.1'de işaretleşme için VPI/VCI ikilisi 5/0 olan sanal bağlantı kullanılır. Tüm SVC kurulması süreci bu 5/0 sanal bağlantısı üzerinden gerçeklenir. Bu sanal bağlantının silinmesi durumunda, işaretleşme yapılamayacağı için tüm sistemde SVC kurulması gerçeklenemez. İşaretleşme Q.2931 UNI işaretleşmesi olarak ta anılmaktadır.

3.2.5.14.6 ILMI (Interim local management interface)

ILMI, ATM ağ üzerinde yönetim işinin kotarılması ve ağ durumunun gözlenebilmesi imkanını sağlar. ILMI iki temel işlev için protokol içerir:

- Uç sistemlerin adres kaydı yapması için kullanılan protokol (adres kayıt işlemi için VPI/VCI ikilisi 0/16 olan PVC sanal bağlantı kullanılır).

- SNMP işlevleri için yönetim protokolü (UNI'Ier üzerinden kurulan sanal bağlantılara ait durum, konfigürasyon ve kontrol bilgilerini sağlar).

3.2.5.14.7 vLAN- ELAN ikilisi

Sanal yerel alan ağı, kısa deyimiyle vLAN (virtual LAN), farklı katlarda ve binalarda bulunan aynı çalışma grubuna ait kullanıcıların, dağılmış ağ cihazları üzerinde, sanki aynı ofis içerisindeki bir ağ cihazına bağlıymış gibi bir LAN oluşturulmasıdır. Büyükçe bir LAN üzerinde, eğer ağ cihazları destekliyorsa, yalnızca konfigürasyon yapılarak birden çok vLAN oluşturulabilir. Her vLAN, diğer vLAN'Iarla aynı cihazlar üzerinde tanımlı olmasına karşın, özerk bir LAN gibi davranır. Birbirleriyle iletişimde bulunabilmesi için araya yine bir yönlendirici koyulması gerekir...

ELAN (Emulated LAN), benzetimi yapılmış LAN anlamındadır. ATM teknolojisi ile Ethernet, FDDI gibi diğer teknolojilerin ATM buluta eklenmesi için, bilindiği gibi LANE'ye ihtiyaç duyulur; LANE bu bütünleştirme işinin genel adıdır. ELAN da bir LAN emülasyonudur. Ancak, ELAN, kenar cihazlar veya sistemler üzerinde tanımlanmış olan vLAN'Iarın ATM buluta eklenmesi için gerekli bir LAN emülasyonudur. Tanımlı her vLAN için bir ELAN oluşturulur ve ilgili vLAN'a atanır.

ATM bulut üzerinde, uygulamaya göre gereksinim olduğu kadar vLAN-ELAN ikilisi oluşturulabilir. Böylece istenildiği kadar birbirinden bağımsız çalışma grupları kendi özel ağlarında çalışıyormuş gibi bir davranış modeli ortaya çıkar. Her çalışma grubunun yarattığı aşırı yayın trafikleri diğer çalışma gruplarının trafiğini etkilememiş olur ve kısmi de olsa bir güvenlik sağlanır. Farklı çalışma gruplarındaki üyeler, ancak bir yönlendirici benzeri sistem üzerinden karşılıklı çalışabilirler.

ATM buluta bir ATM ağ kartı ile bağlı uç sistemler, eğer bulut içerisinde birden çok vLAN-ELAN ikilisi varsa, sisteme ikinci, üçüncü ağ kartları takılmadan birden çok çalışma grubuna üye yapılabilir. Bu desteği ATM ağ kartları üzerindeki LANE yazılımı sunmaktadır!

3.2.5.15 ATM üzerinden çoklu protokol (RFC 1483)

Bu tanımlama IETF tarafından yapılmıştır ve temel amacı, üreticileri farklı olan ürünlerin uyumsuzluk oluşturmadan, üst seviye protokollerinden bağımsız karşılıklı

çalışabilmelerini sağlamaktır. Öneri numarası RFC 1483 olan bu tanımlama, AAL5 üzerinden aktarılmak üzere biri yalnızca PVC'yi destekleyen, diğeri SVC'yi destekleyen iki kapsülleme tanımlamasını da içerir.

3.2.5.15.1 ATM üzerinden IP ve ARP (RFC 1577)

ATM ağların omurga uygulamalarında yaygınlaşması, yoğun olarak kullanılan IP protokolünün ATM ağ üzerinden taşınmasını da gündeme getirmiştir. Bu amaçla IETF, ATM üzerinden IP (IP over ATM) trafik aktarımı üzerine standart olabilecek bir öneri yapmıştır. Numarası RFC1577 olan bu öneri, ATM üzerinde IP ve ATM üzerinde ARP (ATMARP) olmak üzere iki parçadan oluşmaktadır.

RFC1577'ye göre, bir ATM ağda birden çok vLAN varsa ve bunlar IP tabanlı ise (Logical IP Subnetworks, LIS olarak adlandırılır), bu IP tabanlı vLANlar, yani LISIer içerisindeki sistemler birbirleriyle doğrudan iletişimde bulunsun (ki zaten bulunabilirler); ancak farklı LIS içerisinde bulunan sistemler, birbirlerine paket aktarımlarını ATM omurga ile tek bir bağlantısı olan bir yönlendirici üzerinden yapabilsin.

Kısaca söylemek gerekirse, RFC 1577, ATM omurgaya bir ATM arayüz ile bağlı bir yönlendiricinin birden çok LIS'e hizmet edebilmesi ve LIS'Ier için gerekli yönlendirme ve sonlandırma işini kotarabilmesini tanımlamaktadır.

Bu durum özellikle çok sayıda LIS (IP tabanlı vLAN) içeren ve aralarında yönlendirme gereksinimi olan uygulamalarda önem kazanır. Diğer bir uygulama alanı, birbirine uzak iki ATM tabanlı LAN'ın üzerinde var olan LIS'Ierin, bir WAN PVC üzerinden iletişimde bulanabilmesi için yönlendiriciler üzerinde sonlandırma yapmasıdır. Dolayısıyla bu tür uygulamalarda kullanılması düşünülen routerların LIS ve ATM üzerinden IP desteğinin olması gerekir.

ATMARP, IP adresi ile ATM adresi arasında adres çözümlemesi işini kotarır. Ağ içindeki her LIS, adres çözümlemesi için ARP servisine ihtiyaç duyar. Bu servis atanmış (dedicated) olarak kurulabildiği gibi genel bir ARP servisi de kullanılabilir.

ARP hizmeti veren sunucunun ATM adresi, LIS'e ait olan bir uç sistem kurulurken verilmelidir.

3.2.5.16 ATM ağ uygulama örnekleri

ATM, teorik olarak uçtan uca çözüm sunan güçlü bir ağ teknolojisidir; LAN omurga uygulamalarında, uç sistemlerin omurgaya bağlanmasında ve WAN bağlantılarının gerçeklenmesinde seçim olabilecek çözümleri vardır. İletişimde hizmet kalitesi (QoS) sunması ve uygulama programlarının farklı türde gereksinim duyduğu hizmet sınıflarını desteklemesi ATM'in uygulamada, özellikle omurga uygulamasında yoğun olarak kullanılmasını sağlamıştır:

- LAN Omurga Kurulması
- Kampüs Omurga Oluşturulması
- WAN Omurga Kurulması
- Uç Sistemlerin Omurga Bağlantısı

ATM teknolojisi, sunduğu hizmet kalitesi ve hizmet sınıflarının yanı sıra port yoğunluğu fazla, hızlı anahtarlama yapabilen switchlerin veya benzeri ATM cihazların kabul edilebilir maliyetlerle üretilmesine de imkan vermektedir.

3.2.5.16.1 LAN omurga kurulması

ATM cihazlarla güçlü bir LAN omurga yapısı kurulabilir. Projelendirmesi bir darboğaz oluşturmadan yapılırsa, başarımı, eklenecek kullanıcı sayısına göre azalmayacak bir omurga kurulumu gerçeklenebilir. Örneğin 4 katlı bir binaya dağılmış, her katta 30-40 kullanıcısı ve merkezi bir yerde 2-3 tane ana sunucuları olan bir LAN uygulamasında ATM iyi bir çözüm sunabilir.

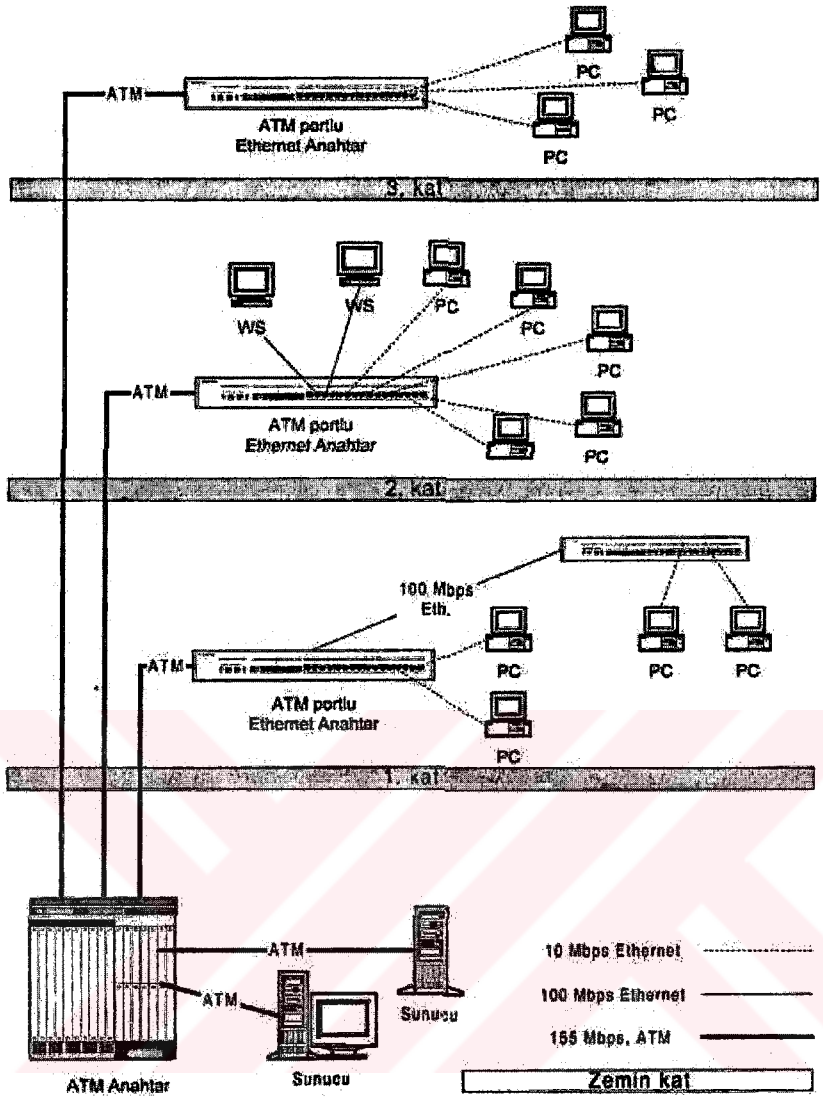
Şekil 3.39'da görüldüğü gibi omurga olarak 1 tane ATM anahtar seçilmiş ve bina katlarda bulunan Ethernet anahtarlara ATM bağlantı (155 Mbps) yapılmıştır. Katlarda bulunan bilgisayar sistemleri, Ethernet kartları üzerinden Ethernet anahtarlara bağlıdır. Ağda bulunan sunucular, yine ATM bağlantı ile omurgaya

bağlıdır. Katlarda bulunan kullanıcı sayısı çok ise 1. katta olduğu 2. Ethernet anahtar veya HUB eklenebilir.

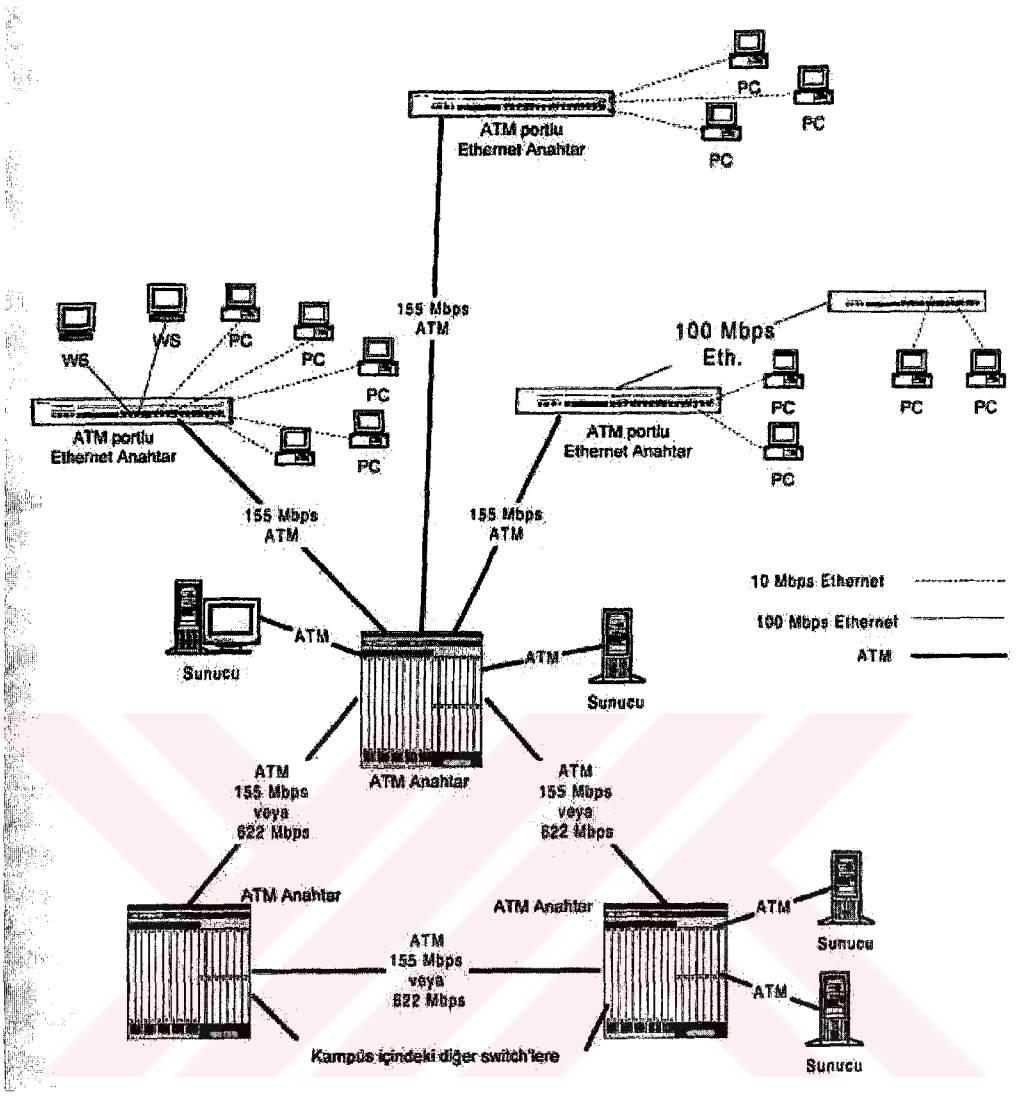
3.2.5.16.2 Kampüs omurga oluşturulması

Kampüs uygulamaları genel olarak LAN uygulamasıyla mesafe açısından farklılık gösterir. Tüm LAN teknolojileri mesafe sorunu olmadığı zaman kampüs uygulamasında kullanılabilir. Kampüs uygulaması daha geniş bir alana yayılmış olup birden çok binayı içerebilir. Kullanıcı sayısı daha fazla olması beklenir ve kullanıcılar arasında gruplama (her bölüm için ayrı bir çalışma grubu) yapılması gerekir.

Kampüs uygulamalarında en iyi çözümü FDDI ve ATM sunar. Ethernet teknolojisi tüm kampüse yayılamayacak kadar mesafe sınırlamasına sahip olduğu için kampüs omurga uygulamasında iyi bir çözüm sunmaz. Ancak kampüs uygulamasında yeri vardır. Bina katlarında bulunan uç sistemlerde Ethernet teknolojisi kullanılabilir (uygulamada oldukça yaygındır).



Şekil 3.39 LAN Omurga çözümünde ATM ömeği



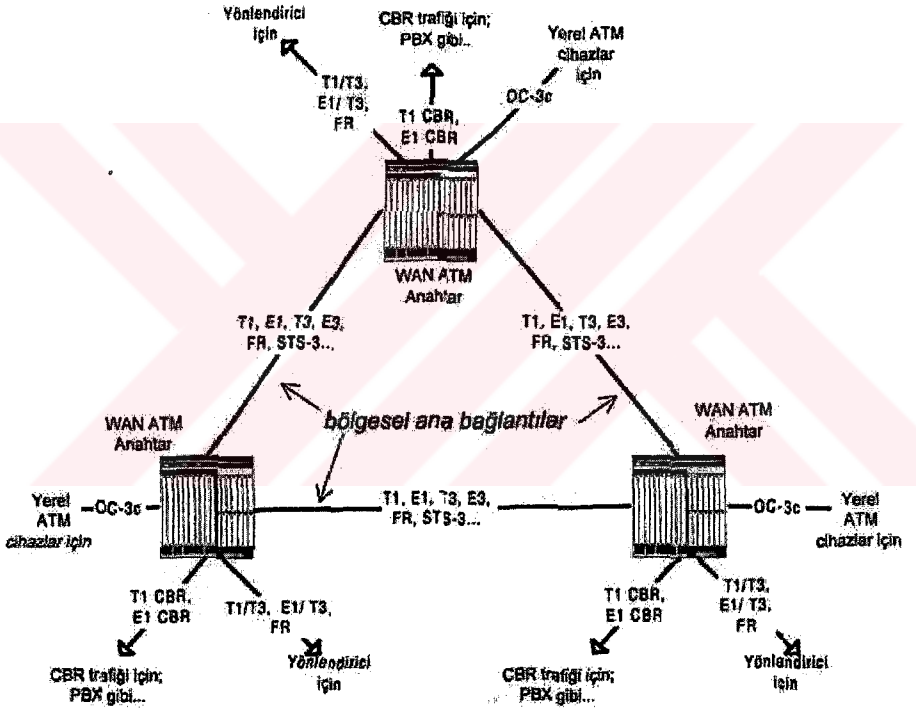
Şekil 3.40 Kampüs Omurga Uygulamasında ATM örneği

3.2.5.16.3 WAN omurga kurulması

WAN birbirinden uzakta olan LAN'ların birbirlerine bağlanması, uzak ofislerin merkezi LAN'a bağlanması veya mesafesi uzak her tür sayısal iletişim yapılabilmesi için aktarım ortamı veya aktarım devresi sunan bir uygulamadır. Bu tür uzak erişimlerin yapılabilmesi, yine anahtarlama cihazlarıyla gerçeklenir. Buralarda kullanılan anahtarlama cihazları ATM tabanlı olabilir. Bu durumda, bu tür cihazlar WAN ATM anahtarlama (switch) cihazı olarak adlandırılır. LAN uygulamasında kullanılan ATM cihazları ise LAN ATM cihazı olarak adlandırılır. Her iki tür cihaz temelde aynı yapıya sahiptir. Ancak cihaz üzerinde olan portların fiziksel arayüzleri

farklı olur. Biri, daha çok LAN bağlantısı için gerekli özellikte portlara sahip iken, diğeri daha çok WAN bağlantısı standartlarda portlara sahiptir.

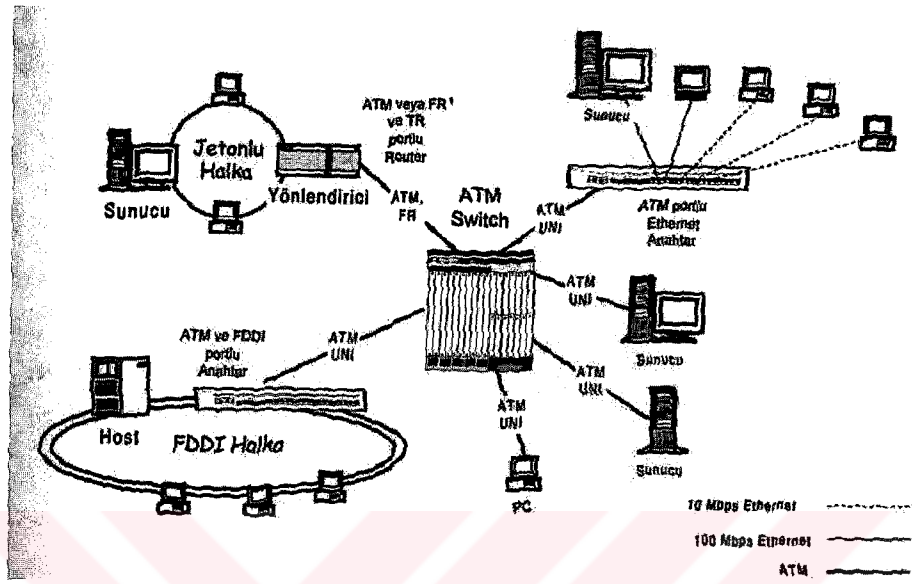
WAN ATM cihazlar, daha uzak mesafelerde bağlantıların yapılabilmesine imkan vermesi nedeniyle, daha çok tek modlu fiber optik (single mode fiber optic; SMF) bağlantı arayüzlerine sahip olurlar. LAN ATM cihazlarının mesafe kısıtlamasının engel olduğu durumlarda WAN ATM anahtarlar kampüs uygulamasında da kullanılabilir.



Şekil 3.41 WAN Omurga Uygulamasında ATM örneği

3.2.5.16.4 Uç sistemlerin omurga bağlantısı

ATM omurgaya sahip bir uygulamada, uç sistemler omurgaya birkaç değişik şekilde bağlanabilir. Uç sisteme bir ATM arayüz kartı (ATM NIC) takılır ve sistem ATM ağa doğrudan ATM standardı ile bağlanmış olur. Uç sistemlerde Ethernet veya token ring kartı vardır. Bu durumda uç sistemler önce kendilerinde var olan arayüze sahip bir anahtar veya HUB'a bağlanır ve oradan da ATM arayüzü ile omurgaya bağlanabilir. Şekil 3.42'de her iki durum için bağlama şekli gösterilmektedir.



Şekil 3.42 ATM omurgaya uç sistemlerin bağlanması

BÖLÜM 4. TCP/IP PROTOKOL GRUBU

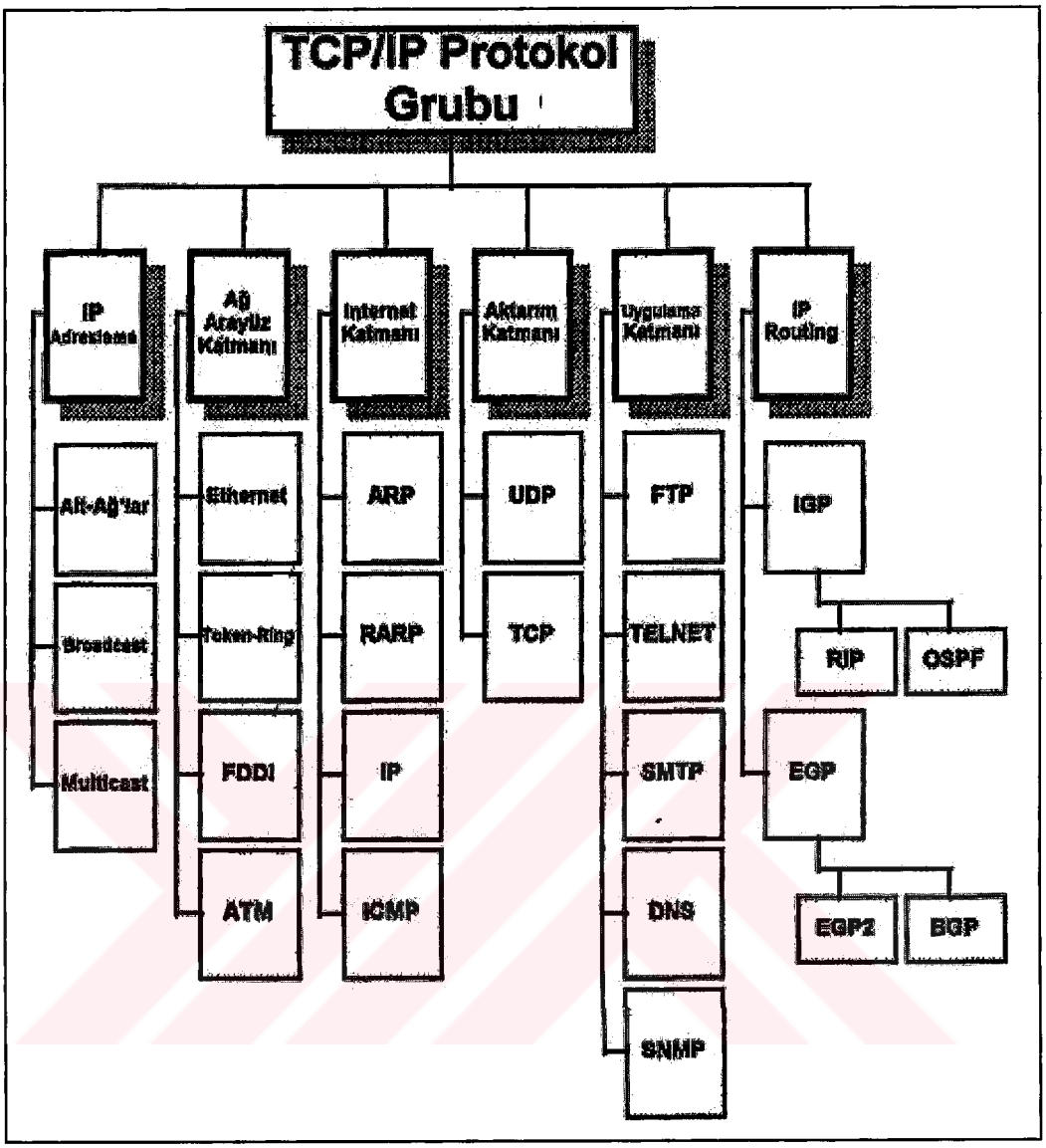
Günümüzde, heterojen (farklı topoloji ve protokollere sahip) bilgisayar ağlarını birbirine bağlamada en popüler protokoller serisi TCP/IP protokolleridir. Bu protokollerden en çok kullanılan protokol çifti ise TCP (Transmission Control Protocol) ve IP (Internet Protocol)'dir. TCP/IP grubu protokoller, internet protocol grubu olarak da isimlendirilir.

TCP/IP protokol grubu, OSI modelinin ağ katmanını ve üstündeki protokolleri tanımlar. TCP/IP protokol grubunun Veri-Bağlantı ve Fiziksel katmandan bağımsız olarak tanımlanması, onun günümüzde bu kadar çok popüler ve başarılı olmasındaki en önemli nedendir.

4.1 Niçin TCP/IP Protokolleri?

TCP/IP protokolleri belirli hedeflerin gerçekleştirilebilmesi için geliştirilmişlerdir. Bu hedefleri oluşturan talepler şunlardır: [5]

- Üreticiden bağımsız tüm üreticilerin ürünlerini içine alan bir kapsam dahilinde, sistemleri birbirleriyle görüştürme (IBM, DEC, Sun, HP vb).
- Tüm ölçekteki bilgisayarları birbirleriyle görüştürme (PC, Midrange systems, Mainframe vb).
- UNIX sistemlerle tam uyumluluk.
- Dinamik router teknolojisinin desteklenmesi.
- Client/Server bilgi işleme teknolojisinin desteklenmesi.
- Birçok OSI 1. ve 2. katman protokollerinin desteklenmesi (Ethernet, Token-ring, FDDI vb).
- Peer-to-Peer yapılanmasına uygun teknolojiye sahip olması.



Şekil 4.1 TCP/IP Protokol Grubu

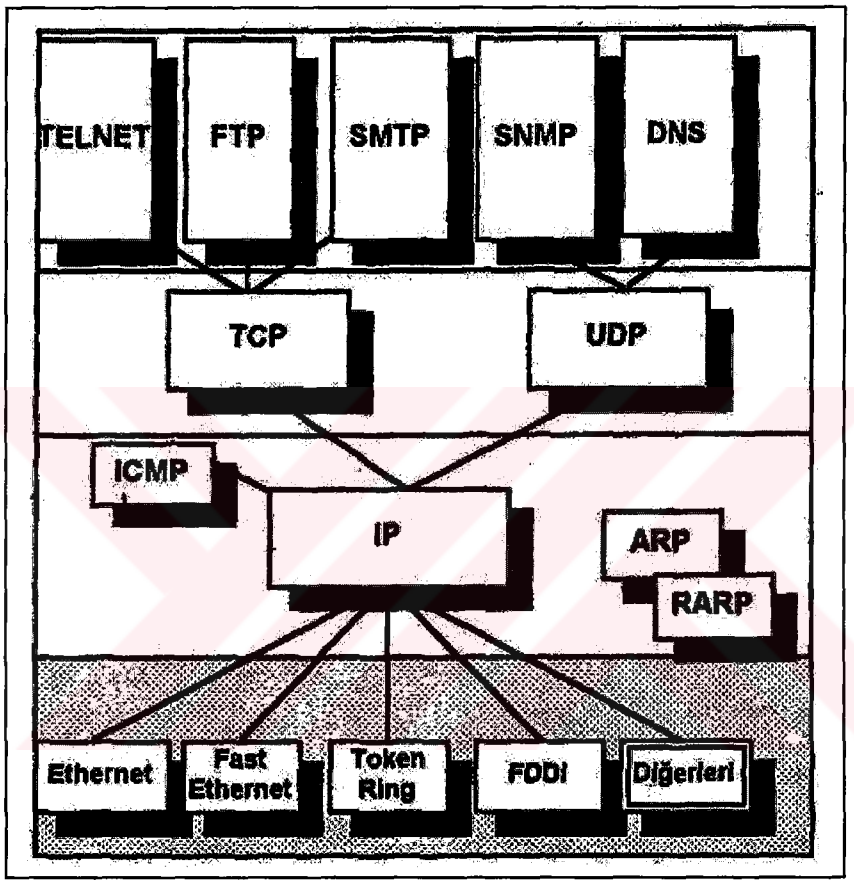
4.2 Ağ Arayüz Katmanı Protokolleri

OSI modelindeki Fiziksel ve Veri-Bağlantı katmanlarına karşılık gelir. Ağ Arayüz Katmanı protokolleri LAN ortamına hangi kurallar dahilinde erişileceğini belirlerler.

Gerek DoD modelinde gerekse OSI modelinde bu katmanların TCP/IP protokol grubunda tanımlamaları yapılmamıştır. Yani TCP/IP bu katmanda diğer standart protokolleri desteklemekte, kendisi yeni bir tanımlama dolayısıyla kısıtlama getirmemektedir. Örneğin bu katmanlarda Ethernet protokolünü, IEEE 802 protokollerini ya da IBM token-ring protokolünü kullanmak mümkündür. Protokol

kullanımındaki bu esneklik ortam (kablo) kullanımına da yansır. İletişim ortamı olarak bu protokollerin desteklediği herhangi bir fiziksel ortam kullanılabilir. [2]

Bu katmanda kullanılabilecek tüm protokoller diğer bölümlerde incelenmiş olup burada inceleme yapılmayacaktır.



Şekil 4.2 Ağ Arayüz Katmanı ile diğer katmanlar arasındaki ilişki

4.3 Internet Katmanı Protokolleri

Bu katman, OSI modelindeki Ağ katmanına karşılık gelir. Ağlar arasında veri transferini sağlayan protokoller bu katmanda yer alır.

4.3.1 ARP (Address resolution protocol) protokolü

Internet adreslerini fiziksel adrese dönüştürmek için kullanılır. Bir paketin bir bilgisayardan çıktığında nereye gideceğini IP numarası değil gideceği bilgisayarın fiziksel adresi belirler. İşte bu adreste paketin gideceği ip numarası kullanılarak elde

edilir. Ve bu işlemden sonra paket hedef ip adresine sahip bilgisayara gitmek için gerekli yönlendirmelerle yolculuğuna başlar. Bilgisayara takılı olan ethernet kartlarının bir ethernet adresi vardır. Ve bu adres IP adresinden farklıdır. Bir paket makineden çıktığı anda gideceği adres diğer bir makinenin ağ kartıdır ve bu ağ kartı ile IP numarası arasında bir bağ yoktur. Paket bu karta gidebilmesi için kartın fiziksel numarasını bilmek durumundadır.

ARP adres çözümlemek istediği zaman tüm ağa bir ARP istek mesajı gönderir ve bu IP adresini gören yada bu IP adresine giden yol üzerinde bulunan makine bu isteğe cevap verir ve kendi fiziksel adresini gönderir. ARP isteğinde bulunan makine bu adresi alarak verileri artık bu makineye gönderir.

4.3.2 RARP (Reverse address resolution protocol)

ARP protokolünün tam tersi şekilde çalışır. Fiziksel adresin bilindiği durumlarda bu adrese atanmış IP adresinin bulunması için kullanılan bir protokoldür.

4.3.3 Internet protokolü (IP)

Temel olarak datagram paketleri için bir iletim yolu belirleme işlevini yerine getirir.

IP'nin sağladığı fonksiyonlar :

- Global adresleme yapısı,
- Servis isteklerini tiplendirme,
- Paketleri iletim için uygun parçalara ayırma,
- Hedef hostta paketleri tekrar birleştirme.

IP'nin sorumluluğu üst katmandan gelen segment ya da datagram'ları birbirine bağlı ağlar üzerinden iletmektir. IP bu segment ve datagram bilgilerini TCP veya UDP den alır.

UDP nin oluşturduğu veri bütününe 'Datagram', TCP'nin oluşturduğu veri bütününe 'Segment' ismi verilir. İkisi arasındaki temel fark, segment'i oluşturan veri grubunun

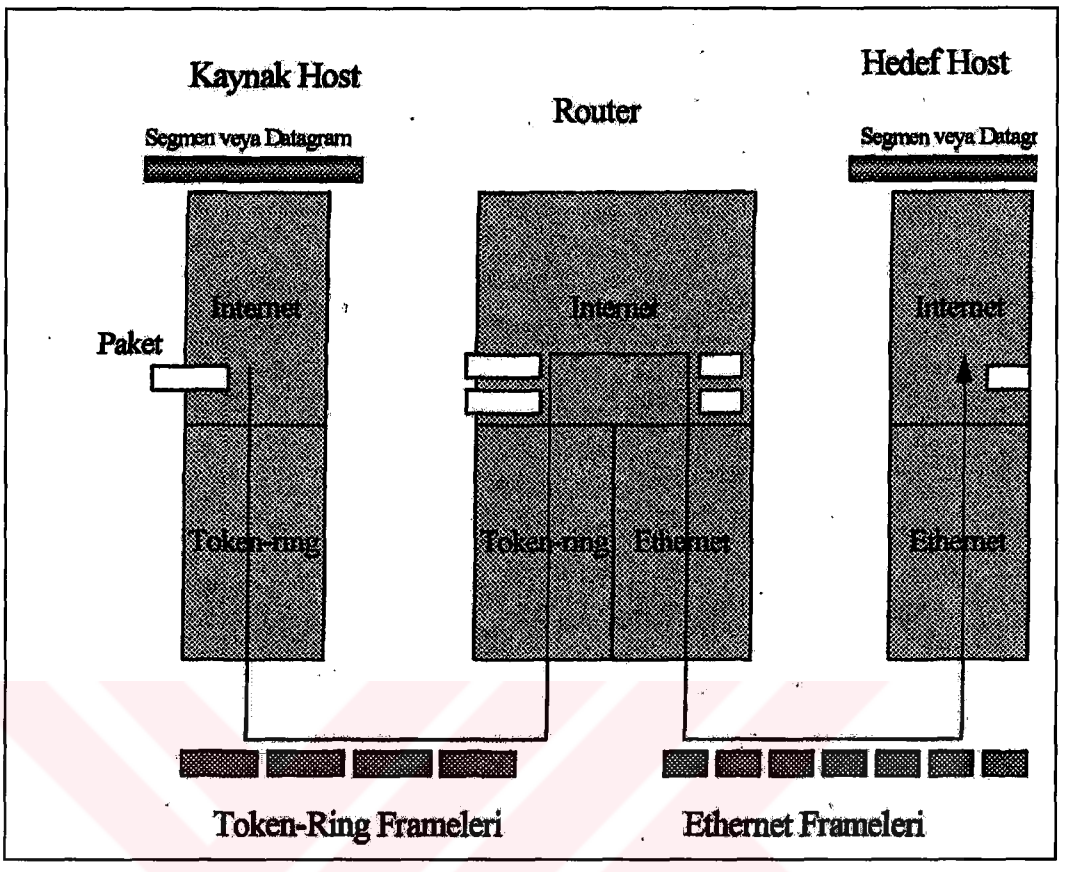
başında sıra numarası bulunmasıdır. Ancak çoğu kez her ikisi yerine 'datagram' kelimesi tercih edilir. Aktarım katmanında oluşturulan veri bütününün TCP tarafından gerçekleştirildiğinin vurgulanmak istendiği yerlerde 'segment' kavramı kullanılır. [3]

Her bir datagram veya segment IP tarafından kendi başlığı eklenerek IP paketi haline getirilir ve her bir IP paketi birbirinden bağımsız olarak hedef host'a gönderilebilir.

IP bir parçalama ve yeniden birleştirme mekanizması kullanır. Bu mekanizma IP protokolünün çalıştığı Host'a özgüdür. Eğer Host üzerinde çalışan alt protokol paket uzunluğu olarak neyi kabul ediyorsa segment IP başlığı ve iletim protokolü başlığı da dahil olmak üzere bu sınırlamayı geçmeyecek şekilde parçalanır. Örneğin Kaynak Host üzerinde Token ring çalışıyor olsun. Token ring'in frame boyu 4096 byte'dır. Segmentler bu sınırlama dahilinde parçalanır. Hedefe iletilen bu framelerin karşılarına bir ethernet protokolü çalıştıran router çıktığında bu paketler uygun şekilde yeniden IP tarafından parçalanacaklardır. Çünkü ethernet frame'nin uzunluğu 1518 byte'tır. En son varılan hedef host'tada bu paketler segment ya da datagram'ı oluşturacak şekilde tekrar IP protokolü tarafından birleştirilir.

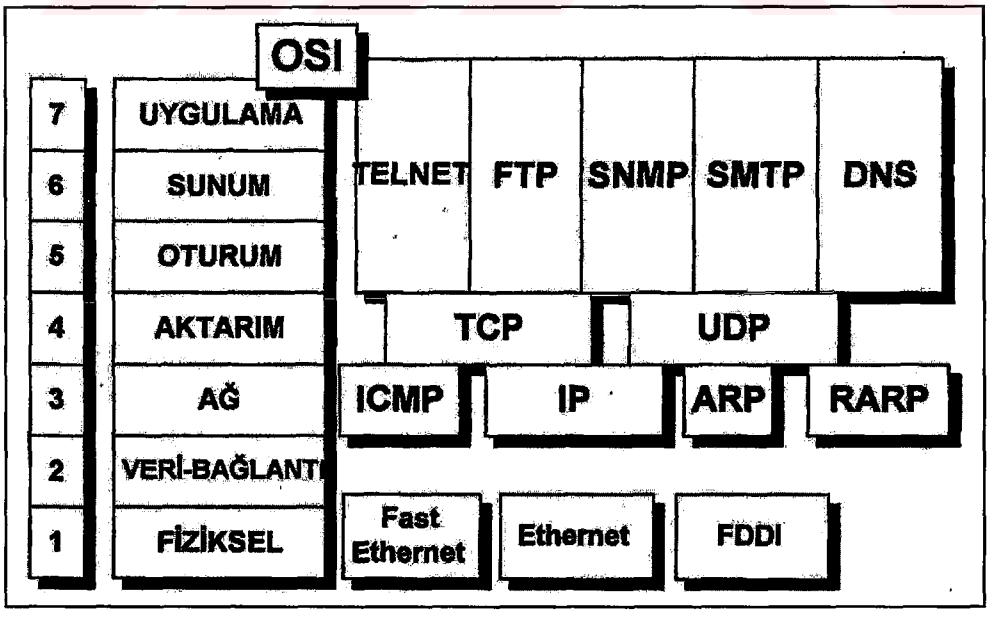
IP'nin temel özellikleri şunlardır: [4]

•Paketler üzerinde çok sınırlı bir hata kontrolü vardır. IP, 16 bitlik başlık hata kontrolü (checksum) sağlar. Bu IP paketini alan hostun IP başlığında bir bozulma oluşup oluşmadığını kontrol etmesini sağlar.
•Onay mekanizması kullanmaz.
•Verinin internet katmanına bozuk ulaştığını değerlendirip yeniden gönderimi sağlıyabilecek mekanizmaya sahip değildir. Bu görev bir üst katmandaki TCP ya da TCP'nin kullanılmadığı durumlarda daha üst katman protokollerince yerine getirilir.
•Akış kontrol ve paket sıralama mekanizmalarına sahip değildir. Yine bu fonksiyonlar gerektikçe, daha üst katmanlar tarafından yerine getirilir.
•IP bağlantısız paket dağıtım servisi sunar.



Şekil 4.3 Paketlerin iletimi

4.3.3.1 IP ve OSI Modeli



Şekil 4.4 OSI modeline TCP/IP protokol grubunun yerleşimi

OSI modeline TCP/IP protokol grubunun yerleşimi gösterilmiştir. IP, görüldüğü gibi ağ katmanı diğer ICMP, ARP ve RARP ile birlikte kullanır. Ancak ICMP paketleri

IP paketleri içerisinde taşınırken, ARP ve RARP ise doğrudan alt katman protokolleri (Veri-bağlantı katmanı protokolleri) içerisinde taşınır. [5]

4.3.4 ICMP (Internet control message protocol)

Hata (Error) mesajlarının ve diğer dahili mesajların iletiminde kullanılır. Bu mesajlar, TCP/IP protokol grubunun çalışmasının birer üyesi olan mesajlarıdır.

4.4 Aktarım Katmanı Protokolleri

OSI modelindeki Aktarım katmanın karşılığıdır. Temel fonksiyonu uygulamalar arasındaki haberleşmeyi sağlamaktadır.

İnternet katmanı sadece bir veri dağıtım servisi sağlar. Aktarım katmanı ise güvenli iletişim,hata düzeltme, gecikme kontrolü vb. fonksiyonlarla ilgilenir. Bu fonksiyonlarla Uygulama katmanına servis sunar. [4]

4.4.1 TCP (Transport control protocol)

Uçtan uca (End-to-end) veri dağıtım (akış) fonksiyonu sağlar. Verinin güvenli iletimi için gerekli mekanizmaları içerir.

Bu mekanizmalar Hata denetimi (checksum), Sıra numarası (sequence number), Onay (acknowledge) ve Yeniden gönderim (retransmit) fonksiyonlarını içerir. TCP güvenli ve sıralı hale getirilmiş veriyi uygulama katmanına sunar. [4]

4.4.2 UDP (User datagram protocol)

Güvenli bir iletişim fonksiyonuna gerek duyulmadığı durumlarda, uygulamalar için TCP den daha iyi bir performans sağlar. Güvenli iletişim bir çok kontrol mekanizmasını işletim sırasında devreye soktuğu için üzerinde çalıştığı host'a yük getirir ve iletişimde de bir miktar gecikmeye neden olur. [4]

4.5 Uygulama Katmanı Protokolleri

OSI referans modelindeki Uygulama, Sunum ve Oturum katmanlarının bütününe karşılık gelir. [3]

4.5.1 Telnet

Bir uzak terminal, erişim protokolüdür. TCP'nin servislerini kullanır. Terminal servisi sunan bir Hosta bağlanmak için kullanılır.

4.5.2 FTP (File transfer protocol)

Bir hosttan diğerine kolay dosya transferi yapmak için kullanılır. TCP'nin servislerini kullanır. Böylelikle dosyaların doğru ve güvenli bir şekilde transferi garantilenmiş olur.

4.5.3 SMTP (Simple mail transfer protocol)

Elektronik posta hizmeti sunar. Posta'ların(mail) güvenli bir şekilde adreslerine ulaşabilmesi için TCP servislerinden yararlanır.

4.5.4 DNS (Domain name system)

Internet üzerindeki hostların isimlerini ve bunlara karşılık gelen IP adreslerini veri tabanı halinde tutmayı sağlayan bir protokoldür. İsim (Name) kullanarak servis almak isteyen protokol veya uygulamalara ilgili host'un IP adresini temin etmek için kullanılır. Genelde UDP'nin servislerini kullanır.

4.5.5 SNMP (Simple network management protocol)

TCP/IP hostlarını standart birtakım ağ yönetim (management) fonksiyonlarını kullanarak yönetme işleminde kullanılır. UDP servislerini kullanır.

BÖLÜM 5. BİLGİSAYAR AĞLARINDA GÜVENLİK

Son yıllarda internetin ve internet üzerinden ticaretin gelişmesiyle birlikte, ağlar oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Ve ağların bu zayıflıkları, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur. Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hala büyük bir tehlike oluşturmaktadır. [12]

Günümüzde internet, gerek kişisel gerekse iş ilişkileri arasındaki bilgi akışını sağlayan, dünyanın en büyük iletişim aracı haline gelmiştir. İnternetin tüm dünyada böylesine yaygın kullanımı, güvenlik tehlikelerini de artırmaktadır. Önemli bir bilgi kaybı olabilir, gizlilik ihlal edilebilir (kredi kartı numarasının bulunması gibi) veya saatler hatta günler süren yükleme zamanları ortaya çıkabilir. İnternetteki bu tür güvenlik açıkları, insanları internete karşı güvensizleştirebilir ve web tabanlı şirketlerin sonunu hazırlayabilir. Bu yüzden şirketler, güvenliklerini her geçen gün arttırmakta ve yeni tehditlere karşı önlem almak amacıyla yatırımlarını sürdürmek zorundadırlar.

5.1 Güvenlik Mimarisinin Kurulması

Bir güvenlik sistemi kurulmadan önce şirketin ihtiyaçlarına göz önünde tutularak güvenlik politikaları oluşturulmalıdır. Güvenlik Politikasının ardında, onun nasıl uygulanacağını anlatan prosedür ve kılavuzlar hazırlanmalı, çalışanlar bu politikaya uymamanın bir karşılığı olacağını ve şirketin konu üzerinde ne kadar titizlikle durduğunu anlamalıdırlar. Tüm bu kılavuz, doküman ve politikalar herkesin anlayabileceği bir dilde ve açık olarak hazırlanmalı, herkesin ulaşabileceği bir yerde bulundurmalıdır. Daha da ötesinden bu belgeler günün koşullarına göre güncellenmeli ve herkes okumakla yükümlü olmalıdır. Kurumun bilgi güvenliği

prosedürleri hazırlanırken "BS7799 (ISO17799)" gibi bir standard yol gösterici olarak kullanılabilir. [9]

Bu prosedürel önlemlerden sonra, sistem mimari anlamda güvenlik hesaba katılarak tasarlanmalı; sadece dışarıya açık sistemler (web sunucular gibi), hem dışarıya hem içeriye açık sistemler (eposta sunucuları gibi), sadece içeriye açık sistemler (bazı veritabanı sunucuları gibi) birbirlerinden ateş duvarları ile ayrılarak konumlandırılmalı ve bu noktalardaki faaliyetler saldırı önleme sistemleri ile monitör edilmeli, farklı bir noktada mümkünse sadece yazılabilir bir medyaya kayıt edilmelidir. [14]

5.2 Güvenlik Politikalarının Belirlenmesi

Kurumların kendi kurmuş oldukları ve İnternet'e uyarladıkları ağlar ve bu ağlar üzerindeki kaynakların kullanılması ile ilgili kuralların genel hatlar içerisinde belirlenerek yazılı hale getirilmesi ile ağ güvenlik politikaları oluşturulur. Güvenlik politikasının en önemli özelliği yazılı olmasıdır ve kullanıcıdan yöneticiye kurum genelinde tüm çalışanların, kurumun sahip olduğu teknoloji ve bilgi değerlerini nasıl kullanacaklarını kesin hatlarıyla anlatmasıdır. Güvenlik politikası olmadan güvenli bir bilgisayar ağı gerçekleştirilemez. [7]

Ağ güvenlik politikaları, kurumların yapılarına ve gereksinimlerine göre değiştiğinden bir şablondan söz etmek mümkün değildir. Güvenlik politikası oluştururken dikkat edilmesi gerekenler belirtilmiştir. Bilgi ve ağ güvenlik politikalarından söz edildiğinde birçok alt politikadan söz etmek mümkündür. Bunun nedeni, politikaların konuya veya teknolojiye özgü olmasıdır. Ağ güvenliğinin sağlanması için gerekli olan temel politikalar aşağıda sıralanmıştır: [15]

1.Kabul edilebilir kullanım (acceptable use) politikası,
2.Erişim politikası,
3.Ağ güvenlik duvarı (firewall) politikası,
4.İnternet politikası,
5.Şifre yönetimi politikası,

6.Fiziksel güvenlik politikası,
7.Sosyal mühendislik politikası,

5.2.1 Kabul edilebilir kullanım (Acceptable use) politikası

Ağ ve bilgisayar olanaklarının kullanımı konusunda kullanıcıların hakları ve sorumlulukları belirtilir. Kullanıcıların ağ ile nasıl etkileşimde oldukları çok önemlidir. Yazılacak politikada temelde aşağıdaki konular belirlenmelidir: [13]

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

5.2.2 Erişim politikaları

Erişim politikaları kullanıcıların ağa bağlanma yetkilerini belirler. Her kullanıcının ağa bağlanma yetkisi farklı olmalıdır. Erişim politikaları kullanıcılar kategorilere ayrıldıktan sonra her kategori için ayrı ayrı belirlenmelidir. [6]

5.2.3 Ağ güvenlik duvarı (Firewall) politikası

Ağ güvenlik duvarı (network firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları çözmek üzere tasarlanan çözümlerdir. Ağın dışından ağın içine erişimin denetimi burada yapılır. Bu nedenle erişim politikaları ile paraleldir. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmektedir: [14]

-Proxy,
-Anti-Virus Çözümleri,
-İçerik Süzme (Content Filtering),

-Saldırı Tespit Sistemleri (Intrusion Detection Systems-IDS)

5.2.4 İnternet politikası

Zararlı kodlar: Virüs veya truva atı (trojan) gibi zararlı yazılımların sisteme girmesine yol açabilir. Virüslerden korunmak için her kullanıcının makinasına bir antivirüs yazılımının kurulmasını sağlamak veya internet (http, email, ftp) trafiğini sunucu(lar)da tarayıp temizledikten sonra kullanıcıya ulaştırmak gibi önlemler alınmakıdır. [8]

Etkin Kodlar: Programların web üzerinde dolaşmalarına olanak sağlayan Java ve ActiveX gibi etkin kodlar saldırı amaçlı olarak da kullanılabilmektedir. [8]

Amaç Dışı Kullanım: İnternet hattı, kurumun amacı dışında da kullanılabilmektedir. Film, müzik gibi büyük verilerin internet'ten çekilmesi hat kapasitesini gereksiz yere dolduracağından kurumun dış kaynaklara erişim hızında yavaşlamalara yol açabilecektir. [8]

Zaman Kaybı: İnternet ortamında gereksiz web sitelerinde zaman geçirmek kurum çalışanlarının iş verimini azaltabilir. Bunu engellemek için kurum politikasında bazı kullanıcılara internet erişimi verilmeyebilir. [8]

5.2.5 Şifre yönetimi politikası

Basit ve kolay tahmin edilebilir şifreler seçmelerini engellemek için kullanıcılar bilinçlendirilmeli ve programlar kullanılarak zayıf şifreler saptanıp kullanıcılar uyarılmalıdır. Her hesap için ayrı bir şifre kullanılmalı ve şifreler sık sık değiştirilmelidir. [17]

5.2.6 Fiziksel güvenlik politikası

Kurumun ağını oluşturan ana cihazlar ve hizmet sunan sunucular için alınabilecek fiziksel güvenlik politikaları kurum için belirlenmelidir. [11]

5.2.7 Sosyal mühendislik politikası

Sosyal mühendislik, kişileri inandırma yoluyla istediğini yaptırma ve kullanıcıya ilişkin bilgileri elde etme eylemidir. [16]

Bu politikalar belirlendikten sonra kurumun hangi cihazların güvenliğini sağlanmasına karar vermelidir.Bu cihazları kime karşı koruyacağı, bilgilerin nasıl yedeklenenip saklanacağını ve yaptırım gücünü belirlenmesi gerekmektedir.

Tüm bu işlemler yapıldaktan sonra risk analizi yapılmalı ve eksiklik görülen noktalarla ilgili politikalar geliştirilmelidir.

5.3 Bilgisayar Ağlarında Güvenlik Nasıl Sağlanabilir?

Network güvenliği mutlaka sağlanmalıdır. Çünkü iç network'te bulunan bilgisayarlara internet üzerinden istenmeyen kişiler tarafından erişilebilir veya sistem açıklarından dolayı bilgi hırsızlıkları yapılabilir.İnternet üzerinden iş yapan kurumlara, kişiler tarafından yeni tehditler oluşturulabilir. [19]

Computer Security Institute (CSI) tarafından yapılan en son ankete göre, saldırıların %70'i kurum çalışanları tarafından yapılmaktadır.

Network güvenlik tehditleri 4 kategoriye ayrılır.Bunlar:

-Yapısal olmayan tehditler: Genellikle kolay ve internetten kolaylıkla bulunan hacker tool'ları ile rastgele yapılan saldırılar.
-Yapısal tehditler: Hacker'ların yapısal olarak biçimlendirdiği ve planlı olarak yapmış olduğu saldırılar.

-Dış tehditler: Dış ağlardan, iç ağa yetkisi olmayan kişiler tarafından iç ağa erişmek için yapılan saldırılar.

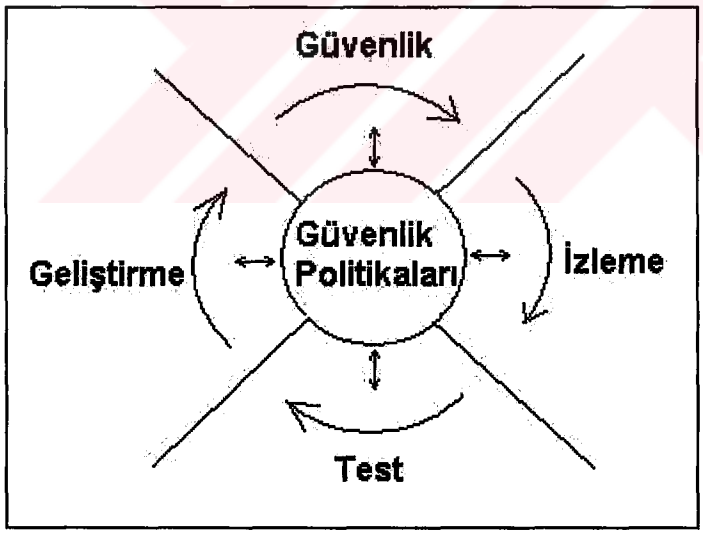
-İç tehditler: Kurumun kendi ağı içerisindeki kişilerin, kurumun önemli bilgilerini ele geçirmek için yapılmış saldırılar.

Network saldırıları 3 çeşittir. Bunlar:

-Keşif Saldırıları: Saldırgan tarafından sistemleri, servisleri ve sistem açıklarını araştırmak ve haritalamak için yapılan saldırılar.

-Erişim Saldırıları: Saldırgan tarafından networkler yada sistemlerin, datalarına erişmek, erişimden kazanç elde etmek yada ayrıcalıklı erişimleri elde etmek için yapılan saldırılar.

-Servisleri Engelleme Saldırıları: Saldırgan tarafından networklere,sistemlere veya servislerin isteklere cevap veremeyeceği duruma getirerek, kişilerin bu servislere ulaşmasını engellemek için yapılan saldırılar.



Şekil 5.1 Güvenlik Çemberi

Bilgisayar Ağlarında güvenliğin sağlıklı bir şekilde işlemesi ve maksimum seviyede güvenliğin sağlanması bu çemberi takip etmekle elde edilebilir. Belirlenmiş olan güvenlik politikalarına bağlı olarak güvenlik,izleme,test ve geliştirme döngüsü içerisinde güvenlik optimum seviyeye çıkarılabilir. [19]

5.3.1 Güvenlik

Yetkilendirilmemiş erişim yada aktivitileri önlemek ve bilgiyi korumak için güvenlik çözümlerine ihtiyaç vardır.Bunlar: [19]

Kimlik Denetimi (Authentication): Sadece yetkilendirilmiş kullanıcılara erişim sağlar.

Şifreleme (Encryption): Yetkilendirilmemiş yada kötü niyetli kişilere, açıklanması istenilmeyen bilgileri şifreleyerek, bilgilerin okunmasını engeller.

Firewall: Sadece geçerli servis ve bilgi tarfiğine izin veren dış dünya ile iç network'u birbirinden ayıran network trafik filtreleyicisidir.

Bulunan Açıkları Yamalamak: Herkes tarafından bilinen açıkların yetkilendirilmemiş yada kötü niyetli kişiler tarafından saldırılarını durdurmak, işletim sistemlerinin yada programların açıklarını kapatmak için yüklenen programlardır.

5.3.2 İzleme

Kurumun güvenlik politikalarına karşı yapılan saldırılar ve ihlaller için network'un izlemesi gerekir. Bunun için gerçek zamanlı saldırı tespiti sistemleri (IDS) kullanılır. Bu sayede çalışan sistemlerin denetlenmesini ve güvenlik uygulamalarının geçerliliğini denetlenmiş olacaktır. [19]

5.3.3 Test

Güvenlik politikalarının etkinliğini geçerli olduğunu denetlemek için, sistemin denetlenmesi ve açıklarının taranması gerekmektedir. [19]

5.3.4 Geliştirme

Güvenlik uygulamaları geliştirmek için, izleme ve test fazındaki bilgiler kullanılır. Bununla güvenlik açıklarını ve riskleri tanımlayarak güvenlik politikaları yeniden

düzeltilebilir.Güvenlik uygulamaları yeniden düzenlenen politikalara göre, güvenlik çemberi döngüsü içerisinde devamlı olarak incelenir. Böylelikle güvenlik optimum seviyede sağlanmış olur. [19]

5.4 Güvenlik Cihazları ve Ürünlerinin Seçimi

5.4.1 Firewall (Güvenlik duvarı)

Güvenlik duvarı özel ağ güvenlik sisteminin önemli bir parçasıdır. Bir güvenlik duvarı kurumun özel ağı ile internet gibi herkesin kullanımına açık ağlar arasında güvenliği sağlar. Bu iki ağ arasındaki tüm trafik güvenlik duvarı tarafından incelenmelidir. Güvenlik duvarından sadece izin verilen trafik geçebileceğinden internet ile kurumun özel ağı arasındaki haberleşmenin serbestlik seviyesini kontrol etmede kullanabilir. Örneğin, hangi servislerin kurumun ağına girişine ve hangilerinin çıkışına izin verileceğine karar verebilir. Ayrıca dahili servislere kimlerin erişebileceği belirlenebilir. [18]

Bir güvenlik duvarı, ağ adresi çevrimi (NAT - Network Address Translation) olarak da bilinen IP adres maskelemesi sağlar. IP adres maskelemesi ile kurumun ağındaki makinelerin adresleri harici kullanıcılar tarafından bilinmez. Bunun yerine harici kullanıcılar haberleşmeleri kurumun ağ geçidini (gateway) IP adresine gönderirler ve oradanda doğru kişiye yönlendirilirler.

IP adres maskeleme sadece güvenlik sağlamakla kalmaz, aynı zamanda IP adreslerinin yetmediği durumlarda çözüm sağlar. Ayrıca başka bir Internet Servis Sağlayıcısına geçildiğinde ağdaki tüm makinelerin IP adreslerinin değiştirilmesi gerekmez.

Güvenlik duvarları sadece intranet ile internet arasındaki haberleşmede kullanılmaz. Aynı zamanda intranet içerisindeki trafiği kontrol etmede ve izlemede de kullanılabilir. Dahili güvenlik duvarları uygulamak kurumun intranetini güvenlik alanları'na ayırır. Eğer kurumda tüm dahili bilgilere erişmemesi gereken kişiler varsa kurumun ağı güvenlik alanlarına bölünebilir.

5.4.2 IDS (Intrusion detection sensor-Saldırı tesbit cihazı)

Ağ güvenliği ile ilgili teknolojilere göz atıldığında, bu alanda en yaygın uygulaması bulunan teknolojinin güvenlik duvarları (firewall) olduğunu öne sürmek mümkün olacaktır. Temel olarak bir güvenlik duvarı, bir ya da daha fazla ağ arasına yerleştirilen ve bu ağlar arasında belirlenen bir politika çerçevesinde izolasyon sağlayarak onları birbirinden yalıtan bir ağ bileşenidir. [10]

Güvenlik duvarları, yaygın kanaatin aksine, tek başlarına eksiksiz bir güvenlik çözümü oluşturamamaktadır. Kişisel olarak sıkça karşılaşılan bir durum, yalnızca kaynak ve hedef bilgilerine bakarak seçici geçirgenlik gösteren "paket filtreleyen güvenlik duvarı" uygulamalarının yanlış kullanımlarıdır. İnternet'e açık web hizmeti veren bir sistemi korumak üzere kurulan bir "paket filtreleyen güvenlik duvarı sistemi" kaçınılmaz olarak bu sisteme doğru gelen tüm web istemlerini geçirmek zorundadır; ancak saldırganların web üzerinden yapabilecekleri saldırılar için herhangi bir koruma sağlanamamaktadır. Örnek sistem için aynı düzeyde koruma, doğrudan sistemin basit ayarları ile de gerçekleştirilebilir durumdadır.

Ağ güvenliğindeki ivme ile özellikle saldırı tespit sistemleri (intrusion detection systems) ve zayıflık inceleme araçları (vulnerability assessment tools) giderek önem kazanan diğer bilişim güvenliği uygulamaları olarak çözüm paketinin oluşturulması esnasında dikkatle değerlendirilmesi gereken bileşenlerdir.
Saldırı tespit sistemleri sunucu ve ağ temelli olarak iki türü vardır. Saldırı tespit sistemleri üzerinde kayıtlı olarak bulunan saldırı imzalarını, gelen paketlerle karşılaştırarak bir saldırı olup olmadığına bakar. Eğer bir saldırı var ise; yöneticinin o atağa karşı vermiş olduğu komut ile atağın bloklanmasına veya sadece bilgi olarak yönetim konsoluna bilgi olarak göstermesi sağlanır. Eğer Cisco güvenlik cihazları kullanılan bir firma ise saldırganın ip adresini IDS tarafından router'a otomatik olarak ekleyetilerek saldırganın iç network'e girmesi engellenir.

5.4.3 SSL (Secure socket layer)

SSL (Secure Socket Layer) protokolü , Netscape tarafından geliştirilmiştir ve şu anda web üzerinden yapılan işlemlerin güvenliği için yaygın olarak kullanılmaktadır. SSL

protokolü, ağ ile uygulama seviyesi arasında çalışarak sunucunun kendisini kullanıcıya, opsiyonel olarak kullanıcının kendisini sunucuya tanıtmasını ve aradaki bağlantının şifrelenmiş bir şekilde kurulmasını sağlar. SSL, uygulama seviyesinin altında çalıştığından uygulama bağımsız bir protokoldür. Herhangi bir uygulama örneğin telnet, ftp, http ssl protokolü ile güvenli hale getirilebilir.

SSL bağlantılarında, sunucu kimliğini kullanıcıya ispat eder. Kullanıcı tarafındaki internet tarayıcı yazılım (Internet Explorer, Netscape Navigator gibi), açık anahtar algoritmalarını (public key cryptography) kullanarak sunucunun sertifikasını kontrol eder. Tarayıcı, beraberinde gelen güvenilen CA (Sertifika otoritesi) listesine bakarak sunucu sertifikasının bunlardan biri tarafından verildiğini doğruladıktan sonra sertifika üzerindeki bilgilerin doğruluğunu sorgular.

Kullanıcının kendisini sunucuya tanıtması opsiyoneldir. Bu sefer kullanıcı kendi sertifikasını sunucuya gönderir ve sunucu güvendiği bir CA tarafından verilen sertifikayı kontrol ederek kullanıcı kimliğini doğrular.

SSL bağlantılarında aradaki bilgi transferi şifrelenmiş bir şekilde gerçekleştirilir. Bu sayede araya girip trafiği analiz eden bir 3. şahıs bu bilgileri okuyamaz. Ayrıca kullanılan bazı mekanizmalarla bilgilerin bütünlüğü de kontrol edilir. Arada bir yerde bilgiler değiştirilmişse karşı taraf bunu anlar ve bu bilgileri yorumlamaz.
Data Digestion (Hashing) algoritmaları:

Bu algoritmalar şifreleme amaçlı değildir. Veriler, bu algoritmalara sokularak 128-160 bit uzunluğunda bir numara elde edilir. Burada önemli olan noktalar; bu işlemin tek yönlü olması ve aynı hash değeri veren ikinci bir verinin bulunmaması gereğidir. Aynı algoritmaya sokulan değer, bir bit bile farklı olsa ortaya çıkan hash değeri çok farklıdır. Ancak daha büyük bir değer matematiksel bir fonksiyonla küçük bir değere eşleştirildigi için birbiri ile aynı hash değerini veren iki farklı input olabilir. Buna "collision" denir. Burada önemli olan böyle iki değerin mevcut donanımla bulunabilmesinin çok zor olmasıdır. Ayrıca, digest değerin ne olduğunu bilen bir kişi bu değerden orijinal veriyi elde edemez. MD5 ve SHA1'in en çok kullanılan digestion algoritmaları olduğunu söyleyebiliriz.

5.4.3.1 Simetrik şifreleme

Mesajın şifrelenmesi ve şifrelenen mesajın tekrar şifresinin çözülmesi aşamalarında tek bir anahtar (key) kullanılır. Asimetrik şifrelemeye göre daha hızlıdır. Her iki tarafta da aynı anahtarın bulunması gereklidir. Burada kritik konu bu anahtarın nasıl birinden diğerine güvenli bir şekilde transfer olacağıdır. SSL protokolünde, önce asimetrik algoritmalar ile bu gizli anahtarların hem sunucuda hem de kullanıcıda bulunması sağlanır. Daha sonraki aşamalarda simetrik şifreleme kullanılır ve mesajlar hep bu ortak anahtar ile şifrelenir. En çok kullanılan simetrik şifreleme algoritmaları 3DES, DES, RC2 ve RC4 olarak sayılabilir.

5.4.3.2 Asimetrik şifreleme

Bu algoritmalarda şifrelemek için bir anahtar, şifreyi çözmek için başka bir anahtar kullanılır. Çiftler halinde üretilen bu anahtarlardan özel olan (private key) sadece o makinede kalır ve başka hiç kimseye aktarılmaz. açık anahtar (public key) ise mesaj alıp verilecek herkese gönderilir. Özelin şifrelediği bir mesajı sadece ilgili açık anahtar ve açık anahtarın şifrelediği bir mesajı sadece ilgili özel anahtar çözebilir.

Asimetrik şifreleme, simetrik şifrelemede ortaya çıkan güvenli bir şekilde anahtar paylaşımı sorununu çözse de, daha yavaş çalışan bir mekanizma olduğundan, ssl bağlantılarında ilk aşama olarak kullanılır. Bu algoritma ile ortak bir gizli anahtar bulunduktan sonra mesajların şifrelenmesi simetrik algoritmalar ile gerçekleştirilir.

Bir e-ticaret sitesine girildiğinde sitenin sunucusu ile ortak bir anahtar belirlerken yukarıda da bahsettiğimiz gibi asimetrik şifreleme kullanılmakyadır. Kullanılan internet tarayıcı yazılımı ile güvenli bir siteye girildiğinde ilk olarak kerkes tarafından güvenilen bir CA tarafından imzalanmış olan sunucu sertifikasını alınır. Bu sertifika CA'in özel anahtarı ile imzalanmıştır. Tarayıcılarda bulunan CA'in açık anahtarı ile bu sertifika çözülür ve sunucu ile ilgili pek çok bilgi ile beraber sunucunun açık anahtarını da elde edilmiş olur. İşlemler neticesinde ortak gizli bir anahtar elde edilir. Diffie-Hellman ve RSA en çok kullanılan asimetrik şifreleme algoritmalarıdır.

5.4.3.3 Dijital imza

Dijital imza, bir tarafın kimliğini diğer tarafa kanıtlamasına ve gönderilen mesajın bütünlüğünün korunduğunun ispatına yarayan mekanizmadır. Sunucu bir input mesaj belirler ve bunu bir hash (digest) algoritmasına sokar. Ortaya çıkan değeri özel anahtarı ile şifreler. Şifrelenmiş hash değer sunucunun dijital imzasıdır. Orijinal mesaj ile beraber dijital imza da karşı tarafa gönderilir. Diğer taraf da aynı hash algoritmasını kullanarak mesajın digest değerini bulur. Daha sonra dijital imzayı sunucunun açık anahtarı ile çözer ve ortaya çıkan iki hash değeri mukayese eder. Eğer iki değer aynıysa imza doğrudur. Bu durumda hem sunucu iddia ettiği kişidir hem de mesajın bütünlüğü bozulmamıştır.

5.4.3.4 Dijital sertifika

Güvenilen bir CA (Certificate Authority) tarafından imzalanan sertifika ile sunucu, açık anahtarını kullanıcıya iletmiş olur bununla beraber kimliğini de ispatlar. Sertifika üzerinde, sunucunun açık anahtarından başka sunucunun alan adı, sertifikanın geçerlilik tarihi, seri numarası, sertifika imzalanırken kullanılan algoritmalar, sertifikayı imzalayan CA'in adı ve CA'in dijital imzası bulunmaktadır.

Internet tarayıcısı olarak kullandığımız Internet Explorer, Netscape Navigator gibi yazılımlarla beraber belli başlı CA'lerin açık anahtarları hazır halde elimize geçer. Bu açık anahtarları kullanarak sunucunun bize gönderdiği sertifikadaki CA'in dijital imzası çözülür ve sertifika üzerindeki bilgilerin doğruluğunu kanıtlanmış olunur. Böylece bize gönderilen sertifikanın, gerçekten bizim bağlanmak istediğimiz sunucunun sertifikası olduğunu öğrenmiş olur ve sunucunun açık anahtarını elde etmiş oluruz.

Sunucular için CA'den sertifika alırken şu aşamalardan geçilir:

1. Sunucu genel ve özel anahtar çiftini oluşturur.

2. Sunucu, açık anahtarı ve alan adı gibi bilgilerle bir istek mesajı oluşturur ve bu mesajı özel anahtarı ile imzalayarak CA'ye gönderir.
3. CA bu talepteki bilgileri yorumlayarak bir mesaj oluşturur. Bu mesajı kendi özel anahtarı ile imzalayarak dijital imzasını oluşturur. Oluşturduğu mesaj ve dijital imzayı birleştirerek bir sertifika oluşturur.
4. CA oluşturduğu bu sertifikayı sunucuya gönderir.Sertifikasını alan sunucu, bundan sonraki bağlantılarında kimliğini ispatlamak için bu sertifikayı karşı tarafa gönderir.

5.4.3.5 SSL bağlantılarında kullanılan şifreleme metodları

Kullanıcı bilgisayarı, ssl sertifikası yüklü sunucuyla TCP bağlantısını kurduktan sonra, ssl protokolünün elsıkışma (handshake) mekanizmalarını kullanarak, hangi cipher suite'in bu bağlantıda kullanılacağı konusunda sunucu ile anlaşır. SSL protokolünün versiyonuna göre farklı şekillerde gerçekleşen bu safha neticesinde, üzerinde anlaşılan cipher suite kullanılarak kullanıcı ile sunucu ortak bir anahtar belirler ve yine üzerinde anlaşılan bir simetrik şifreleme algoritması ile bu anahtar kullanılır.

Kullanıcının bilgisayarı ile sunucu arasında bu konu görüşülürken her iki makinanın desteklediği en güçlü metod seçilir. Bazı firmalar, güvenlik eksikliği nedeniyle zaten web sunucularına 40 bit ve 56 bit bağlantılar kurulmasını istemediğinden bu şifreleme metotlarına destek vermez.

SSL bağlantılarında kullanılan bazı cipher suite'ler şunlardır;

3 DES ve SHA-1: En güçlü metottur. 3 DES kullanarak 168 bit'lik bir şifreleme sağlar. Digest algoritması olarak SHA-1 kullanılır.

RC4 (128 bit) ve MD5: Simetrik şifrelemeyi RC4 ile yapar. 128 bit büyüklüğünde anahtarlar kullanır. 3 DES'ten daha hızlı bir metottur.

RC2 (128 bit) ve MD5: RC2, RC4'e göre daha yavaştır. SSL versiyon 2'de desteklenir fakat SSL versiyon 3'de yoktur.

DES ve SHA-1: 56 bitlik bir şifreleme sağlar.

RC4 (40 bit) ve MD5: Bu metotta kullanılan anahtarlar yine 128 bittir fakat sadece 40 bitlik bölümü şifreleme için kullanılır ve güvenlik konusunda eksiklikleri vardır.

RC2 (40 bit) ve MD5: Aynı şekilde güvenlik konusunda yetersizdir.

MD5: MD5 ile mesajların bütünlüğü kontrol edilir ama herhangi bir şifreleme uygulanmaz. Kesinlikle en güvensiz metottur ve kullandığımız web sunucularımızda bu bağlantılara izin vermemeliyiz.

5.4.3.6 SSL Handshake

SSL bağlantısı kurmak istediğimiz bir sunucuya bağlanıldığında, öncelikle SSL Handshake denilen mesaj alışverişleri gerçekleşir. Sunucunun kimliğini bize ispatlaması, eğer gerekliyse kullanıcı olarak bizim kimliğimizi sunucuya ispatlamamız, bağlantıda kullanılacak simetrik anahtar'ın bulunması ve kullanılacak cipher suite'lerin bulunması hep bu safhada gerçekleşir. Kullanılan SSL versiyonuna göre farklı işlemler gerçekleşir. Daha yeni ve güvenli olan SSL versiyon 3'ü incelendiğinde; TCP bağlantısı kurulduktan sonra SSL görüşmeleri başlar. Kullanıcı bilgisayarı Client Hello mesajını sunucuya gönderir. Bu mesaj içerisinde Session ID, desteklenen cipher suite'lerin listesi, 28 bayt uzunluğunda rastgele bir numara (Client Hello Random), kullanılmak istenen SSL versiyon bilgileri bulunur. Session ID bölümü eğer boş değilse, sunucu kendi üzerindeki bir tabloya bakarak bu değerin karşısındaki simetrik anahtarı kullanma kararını alır ve tekrar bir ssl handshake mekanizması başlamaz. Web sitesi içerisinde gezdiğimizi düşünelim. Her bir sayfa için tekrar bir görüşme yapılarak kullanıcı ile sunucu arasında ortak bir anahtar bulma ve kimliklerini ispatlama gereği yoktur. Session ID bunu sağlar. Eğer bu değer boşsa bu, bağlantının yeni bir bağlantı olduğu anlamına gelir. Kullanıcının internet tarayıcı programı ayrıca 28 bayt uzunluğunda bir rakam üretir. Bu değer simetrik anahtarların hesaplanmasında kullanılır. SSL versiyon bilgisi de kullanıcı tarayıcısının versiyon 2'yi mi yoksa 3'ü mü desteklediğini sunucuya bildirir.

Sunucu, Client Hello mesajını aldıktan sonra eğer hatalı bir durum algılamadıysa Server Hello mesajını oluşturur ve karşı tarafa gönderir. Bu mesajda, SSL versiyonu, 28 bayt uzunluğunda rasgele bir değer (Server Hello Random), bu bağlantı için oluşturduğu Session ID, ve bağlantıda kullanılacak olan cipher suite bilgisi bulunur. Sunucu, kullanıcıdan gelen cipher suite listesini kendi destekledikleri ile karşılaştırarak, her ikisinin de desteklediği en güçlü algoritmayı bulur ve bu mesaj ile karşı tarafa bildirir. Bu bilgilerin dışında, sunucu bu mesaj ile SSL sertifikasını da kullanıcıya gönderir.

Kullanıcı, sunucudan gelen sertifikayı inceleyerek sunucunun kimliğini kontrol eder. Öncelikle sertifika üzerindeki, sertifikanın geçerlilik tarihi bilgisini kontrol eder. Bu tarih geçmişse, sunucunun kimliğini doğrulamaz. Sertifikanın geçerlilik süresi geçmemişse, sertifikanın hangi CA tarafından verildiğini kontrol eder. Sertifikayı imzalayan CA, kullanıcının internet tarayıcısının güvendiği bir CA ise kimlik doğrulama işlemine devam eder, aksi takdirde sunucunun kimliğini doğrulamaz. Bir sonraki aşama olarak CA'in dijital imzasını sorgular. CA'in açık anahtarı ile dijital imzayı çözerek sertifikanın imzalanmasından sonra herhangi biri tarafından içeriğinin değiştirilip değiştirilmediğini kontrol eder. Bir sonraki aşama olarak da sertifika üzerindeki alan adı bilgisini kontrol ederek bu bilgi ile kendi bağlanmak istediği sitenin aynı isimde olup olmadığını doğrular. Internet tarayıcı yazılım, eğer sertifika üzerindeki alan adı, bağlanmak istenilen sitenin alan adı ile aynı değilse bu durumu bir uyarı mesajı ile ekrana getirerek kullanıcıdan bir onay ister. Örneğin ssl sertifikası olan bir web sunucuya alan adı değil de IP adresi ile bağlanırsak bu uyarı ekranını görebiliriz. Tüm bu aşamaların sonunda kullanıcı, sunucunun kimliğini ispatlamış olur.

Kullanıcı bilgisayarı, Client Key Exchange mesajını karşı tarafa gönderir. Bu mesaj içerisinde, kullanıcının yarattığı 48 bayt uzunluğunda bir pre-master secret değer vardır ve bu değer, sunucunun açık anahtarı ile şifrelenerek sunucuya gönderilir. Sunucunun açık anahtarı ile şifrelendiğinden, sadece sunucunun kendisi bu mesajı çözerek bu değer'i açığa çıkarabilir. Aynı paket ile beraber ayrıca 1 bayt uzunluğunda Change Cipher Spec mesajı da gönderilir. Bu mesaj ile bundan sonraki mesajların, üzerinde anlaşılan cipher suite kullanılarak korunacağını karşı tarafa bildirilmiş olur.

Aynı paket içerisinde ayrıca Encrypted Handshake mesajı da iletilir. Bu mesaj karşı tarafa artık SSL Handshake safhasının bittiğini ve veri alış-verişine başlayabileceklerini bildirir.

Sunucu, kullanıcıdan gelen pre-master secret değeri, özel anahtarını kullanarak ortaya çıkarır. Daha sonra bu değeri kullanarak bir master secret değerini hesaplar. Aynı hesapları kullanıcı da yaparak aynı master secret'i bulur. Master secret bulunurken, her iki tarafın yarattığı random değerler (Client HelloRandom ve Server HelloRandom), pre-master secret değer, belirli karakterler ("A","BB","CCC"), hashing algoritmaları (MD5 ve SHA-1) kullanılır.

Daha sonra, Master secret değeri kullanılarak hem sunucu hem de kullanıcı aynı fonksiyonları kullanarak simetrik anahtarları hesaplar. Burada 2 tane anahtar hesaplanır. Bir tanesi kullanıcının mesaj gönderirken kullandığı anahtar (Client Write Key) bir tanesi de sunucunun mesaj gönderirken kullandığı anahtar (Server Write Key). Her iki anahtar da hem sunucuda hem de kullanıcıda bulunur. Örneğin sunucu bir veri göndereceği zaman ServerWriteKey ile bu veriyi şifreler ve kullanıcı da bu veriyi aldığında yine aynı ServerWriteKey ile şifreyi çözer. Simetrik anahtarlar hesaplanırken, master secret değer, ve master secret değer hesaplanırken de pre-master secret değer kullanılıyor. Pre-master değerini zaten kullanıcı yarattığından kullanıcı bu bilgiyi bilir. Fakat kullanıcı bu değeri sunucuya gönderirken bu değeri sunucunun açık anahtarı ile şifrelediğinden pre-master secret değeri ve dolayısıyla simetrik anahtarları sadece sunucu elde edebilir. Bir şekilde sunucu ile kullanıcı arasına kötü niyetli birisi girse bile, şifrelenmiş pre-master değeri bulamayacağından bu anahtarları hesaplayamayacaktır. SSL'in, asimetrik şifreleme kullanarak simetrik anahtarları hesaplamasında temel aldığı güvenlik mantığı da budur. Sunucu, Change Cipher spec ve Encrypted Handshake mesajları göndererek SSL Handshake işlemlerinin artık bittiğini ve bundan sonra veri alışverişinin başlayabileceğini kullanıcıya bildirir. Bu mesajdan sonra artık uygulama düzeyinde haberleşme başlar. Artık bu aşamadan sonra veri alışverişi başlar. Beraberce hesaplanan gizli anahtarlar ve üzerinde anlaşılan şifreleme ve hashing algoritmaları sayesinde veriler şifrelenmiş bir şekilde sunucu ile kullanıcı bilgisayarı arasında gidip gelir. Hiç kimse bu anahtarları bilmediğinden çeşitli araçları kullanarak ağ trafiğini dinleyen kişiler

bilgileri açığa çıkaramaz. SSL protokolü, handshake esnasında her iki tarafın da oluşturduğu bazı diğer anahtarlarla mesajların bütünlüğünü ve tekrar edilip edilmediğini de kontrol eder ve tehlikeleri ortadan kaldırır.

5.5 IPSec (Internet protocol security)

Internet Protocol Security (IPSec) güvenli haberleşmeler sağlamak ve IP ağları üzerinde kişisel gizliliği korumak için standartlar üzerine kurulmuş bir yapıdır. IPSec RFC (Requests for Comments) 2401-2411 de tanımlanmış olan bir IETF (Internet Engineering Task Force) standartıdır. Çoğu ağların güvensiz olduğu ve kablo üzerinde seyahat ederken verileri korumak için ek komponentler gerektirdiği düşüncesinden yola çıkarak IPSec kaynak kimlik tanılama, bütünlük kontrolü ve içerik gizliliği sağlamaktadır.

5.5.1 Kimlik tanımlama

IPSec`in kullandığı protokollerden biri 'Kimlik Tanılaması Başlığı'dır (AH-Authentication Header). AH tüm datagram`ın bir 'sağlama toplamını' (checksum) içermektedir ve IPSec datagram`ındaki orjinal IP başlığından sonraya yerleştirilir.

AH aşağıdakilerden oluşur:

-Sonraki başlığı (Next Header)
-Orjinal IP başlığının protokol numarası.
-Yük boyutu (Payload Length)
-Kimlik tanılaması başlığının uzunluğu.
-Güvenlik Parametre İndeksi (Security Parameter Index - SPI)
-Kimlik tanılama başlığı bağlantılarını diğerlerinden ayırmayı mümkün kılan 32-b-itlik bir seri numara
-Sıra Numarası (Sequence Number)
-Replay koruması için Kimlik Tanılaması datagram`ının seri numarası
-Bütünlük Kontrol Değeri (Integrity Check Value-ICV)

-AH datagram`ının kriptografik bir bütünlük sağlama toplamı (checksum).

5.5.2 AH hangi saldırılardan korur?

1-Replay Saldırıları: Kötü amaçlı bir kişinin bazı paketleri yakalaması, daha sonrası için kaydetmesi ve sonra tekrar yollaması. Bu tip saldırılar saldırganın artık ağda bulunmayan bir makinenin yerine geçebilmesini sağlar. AH pakete anahtarlanmış bir 'hash' ekleyerek, başkalarının paketi tekrar gönderebilmesini engelleyerek replay saldırılarına karşı koruma sağlar.

2-Değişiklik: IPSec`in kullandığı anahtarlanmış hash paketin gönderildikten sonra içeriğinin değiştirilmediğine emin olunmasını sağlar.

3-Spoof: AH protokolü iki-yönlü kimlik tanılama sunar, istemci ve sunucunun her ikisinin de bir diğerinin kimliğinden emin olmasını sağlar.

5.5.3 Gizlilik

Kimlik tanılama başlığı (AH) saldırılara karşı kimlik tanılama sağlar. IPSec ayrıca gizlilik için anlaşılan bir algoritma ile veriyi kriptolamak için ESP (Encapsulating Security Payload) protokolünü de kullanır. ESP protokolü her paketin içindeki tüm içeriği kriptolar fakat IP başlığında bir kriptolama veya checksum sağlamaz.

ESP başlığı aşağıdaki verileri içerir:

1-Güvenlik Parametre İndeksi (SPI): Hedef adres ve güvenlik protokolü (AH veya ESP) ile birlikte kullanıldığında haberleşme için doğru güvenlik ilişkisini (SA-Security Association) tanımlar. Alıcı bu değeri kullanarak bununla hangi güvenlik ilişkisinin kullanılacağını belirler.

2-Sıra Numarası: SA için anti-replay koruması sağlar. 32 bit`tir. 1 den başlayarak ekleyerek haberleşmede güvenlik ilişkisi üzerinde gönderilen paket sayısını

belirleyen sayıyı artırır. Sıra numarasının tekrarlanmasına izin verilmez. Alıcı bu alanı kontrol ederek bu numaraya ait güvenlik ilişkisinin daha önce alınıp alınmadığını kontrol eder. Eğer daha önce alınmış ise paket kabul edilmez.

3-Ekleme/Takviye (Padding): Kullanılan blok şifrelemenin blok ölçüsüne uyacak şekilde verinin uzunluğunu değiştirir. 0 ile 255 byte arasındadır.

4-Pad uzunluğu: Takviye alanının byte olarak uzunluğudur. Bu alan alıcı tarafından takviye alanını atmada kullanılır.

5-Sonraki Başlığı (Next header): Orjinal IP başlığının protokol numarasıdır. Yükü tanımlamak için kullanılır, TCP veya UDP gibi.

ESP IP başlığından sonra ve TCP, UDP veya ICMP gibi üst katman protokolden önce yada zaten yerleştirilmiş olan diğer IPSec başlıklarından önce yerleştirilir. ESP`yi takip eden herşey (üst katman protokolü, veri ve ESP trailer) imzalanır. IP başlığı imzalanmaz ve bu sebeple değişikliklerden korunmaz. Üst katman protokolü bilgisi, veri ve ESP trailer kriptolanır.

5.5.4 IPSec Modları

İki protokol de iki moddan birinde kullanılabilir, nakil (transport) ve tünel (tunnel) modları. AH ve ESP`nin moda dayalı olarak işlemleri farklı değildir, tek fark verinin bütünlük amaçlı imzalanmasıdır. Modların ve protokollerin 4 mümkün kombinasyonu vardır. AH ve ESP tünel veya nakil modlarında kullanılabilir. AH pratikte tünel modunda kullanılmaz çünkü nakil modunun koruduğu aynı veriyi korur.

1-Nakil modu: Nakil modunda, AH ve ESP nakil başlığını korur. Bu modda AH ve ESP nakil katmanından ağ katmanına akan paketleri yakalarlar ve ayarlanan güvenliği sağlarlar. IPSec`in nakil modu sadece güvenlik son noktadan son noktaya arzulanıyorsa yapılabilir.

2-Tünel modu: Tünel modu güvenliğin paketlerin kaynağı olmayan bir cihaz tarafından sağlandığı durumlarda (VPN`lerde olduğu gibi) veya paketin gerçek hedefinden farklı bir yerde güvenli hale getirilmesine ihtiyaç duyulduğunda kullanılır. Kriptografik son-nokta bir ağ için güvenlik sağlayan bir güvenlik ağ-geçididir.

5.5.5 Güvenlik ilişkileri (SA)

İki makine IPSec ile haberleşmeden önce birbirlerinin kimlik tanılamasını yapmalı ve bir kriptolama metodu üzerinde anlaşmalıdırlar. Makineler bunu bir veya daha fazla Güvenlik İlişkisi (SA) kurarak gerçekleştirirler. Güvenlik İlişkisi iki makine arasında kullanılacak olan belirli güvenlik ayarlarına bağlı bir anlaşma gibi düşünülebilir. AH ve ESP aynı SA`yı paylaşamazlar, tipik olarak, iki taraf arasındaki iki-yönlü haberleşmelerde iki SA`ya ihtiyaç vardır. Güvenlik İlişkileri her IPSec bilgisayarda belirli bir veritabanında saklanır. SA`lar veritabanı içerisinde her AH veya ESP başlığında bulunan Güvenlik Parametre İndeksinden (SPI) tanınırlar.

Gerekli SA`ları kurmak için Internet Anahtar Takas (IKE-Internet Key Exchange) protokolünü kullanır. IKE SA`lerin yaratılmasını üstlenir ve bilgiyi güvenli hale getirmede kullanılacak anahtarları yaratır. Bu teknik veriyi kriptolayıp dekriptolamada kullanılacak simetrik anahtarların yaratılmasını sağlar. IKE gerekli olan Diffie-Hellman`ın çalışabilmesi için güvenli bir kanal sağlar.

5.5.6 IPSec sürücüsünün ana sorumlulukları

-Gelen veya giden her IP paketini belirli IP politikası filtrelerine uyup uymadığına bakmak için inceler.
-Yeni bağlantılar için güvenlik ilişkileri istekleri inceler.
-Politika tarafından belirlenen kimlik tanılama metodunun kullanımını inceler.
-Güvenlik ilişkilerini güncel tutmak.

5.6 Özel Sanal Ağ (Virtual Private Networks-VPN)

Özel Sanal Ağ (Virtual Private Networks), kişiye veya kuruma ait özel bilgi ve verinin herkese açık şebekeler veya İnternet gibi global ağlar üzerinden aktarılmasını sağlar. İnternet gibi geniş bir alana yayılmış bir ağın, kurumsal bir işletmenin çok çok uzaktaki ofislerinin veya trafik yoğunluğu çok fazla olmayan şubelerinin güvenli bir iltişim yapılacak biçimde internet üzerinden bağlanması sanal ağ oluşturulması anlamına gelir.

Özel sanal ağ uygulamalarında temelde , biri kullanıcı/geçityolu diğeri geçityolu/geçityolu olarak adlandırılan ikitür bağlantı yapılır . Kullanıcı/geçityolu bağlantısında (ki daha gezici kullanıcılar için geçerlidir) doğrudan kullanıcı bilgisayarı ile geçityolu arasında bir şifrelenmiş tunel kurulur. Kullanıcı tarafından yüklü olan yazılım gönderme işleminden önce veriyi şifreler ve VPN üzerinden alıcı tarafındaki geçityoluna gönderir. Geçityolu önce kullanıcının geçerli biri olup olmadığını sınar ve gönderilen şifrelenmiş paketi çözerek içeride korunmuş alandaki alıcıya gönderir; alıcının verdiği yanıt ta yine önce geçityoluna gider ve orada şifrelenerek kullanıcıya gönderilir. Geçityolu/geçityolu bağlantısında birbiriyle iltişimde bulunacak sistemler, kendi taraflarında bulunan geçityoluna başvururlar; kullanıcı sistemleri verilerini geçityoluna gönderir ve onlar kendi aralarında şifreli olarak iletişimde bulunurlar. Bu durum, farklı yerlerdeki LAN'ların internet gibi herkese açık güvenli bir şekilde bağlanması için kullanılır.

Ağ erişim noktasının görevi, kullanıcılardan gelen paketleri kapsüle ederek verinin güvenli bir şekilde iletilmesini sağlamaktır. Günümüzdeki uygulamalar, bu işlem için PPTP (Point-toPoint Tunneling Protocol) ve L2F (Layer Two Forwarding) protokollerini kullanır. PPTP, internet servis sağlayıcı tarafından akış kontrolü gibi görevlerle kullanılırken, L2F protokolünün kullanımı daha kolaydır ve yönetilebilir ağlara daha uygundur. Bu iki protokolün en iyi yönleri ele alınarak L2TP (Layer Two Tunneling Protocol) adı verilen bir protokol ortaya çıkmıştır. L2TF protokolü, özelleştirilmiş protokoller ile kullanıldığında internet üzerinden güvenli tüneller kurulmasını sağlayacaktır. . En temel şifre doğrulama protokolleri PAP (Password Athentication Protocol), CHAP (Challenge Handshake Athentication Protocol) ve SPAP (Shiva Password Authentication Protocol) protokolleridir. Daha güvenli şifre

doğrulama çözümleri ise, zamanla senkronize edilmiş anahtarları ve dijital sertifika gibi gelişmiş teknolojileridir. Veri güvenliği, IPSec protokolü ile gerçekleştirilir. IPSec, güçlü bir şifreleme sağlarken, veri bütünlüğünü de garanti eder.

5.7 Proxy

Proxy'ler internet'e çıkacak kişilere vekalet eden, onların yerine internete bağlanan ve sonucunuda ilgili kişilere ileten bir yazılımlardır. Proxy'lerin internet kullanacak kişilerin hangi servislerden yararlanacağına eklenecek rollerle karar verir. Bu sayede kullanıcılar yönetim tarafından belirlenen kurallara uymuş olacaklardır.

Günümüzde güvenliğin ön plana çıkması nedeniyle birlikte yeni nesil proxy server'lar çıkmaya başlamıştır. Yani firewall özelliği de bulunan yazılımlar (Örnek olarak Microsoft ISA Server) çıkmaya ve kullanılmaya başlanmıştır.

5.8 Antivirüs Sistemleri

Kurum içerisindeki bütün bilgisayarlara bir antivirüs programı kurulmalıdır ve gerçek zamalı olarak çalıştırılmalıdır. Bu sayede ağ üzerinden bulaşabilecek virüslere karşı önlem alınmış olacaktır.

Gelen ve giden bütün mailler, mail server üzerinde çalışacak antivirüs programı ile taranmalıdır. Bu işlem ile mail yoluyla yayılan virüsler önlenmiş olacaktır.

Bütün bu antivirüs programları kullanım kolaylığı nedeniyle tek bir merkezden yönetilmelidir. Antivirüs programlarının kurulması yeterli değildir. Çünkü yeni çıkan virüslerin tanınabilmesi için bütün bilgisayarlar tek bir merkezden otomatik olarak update edilmelidir.

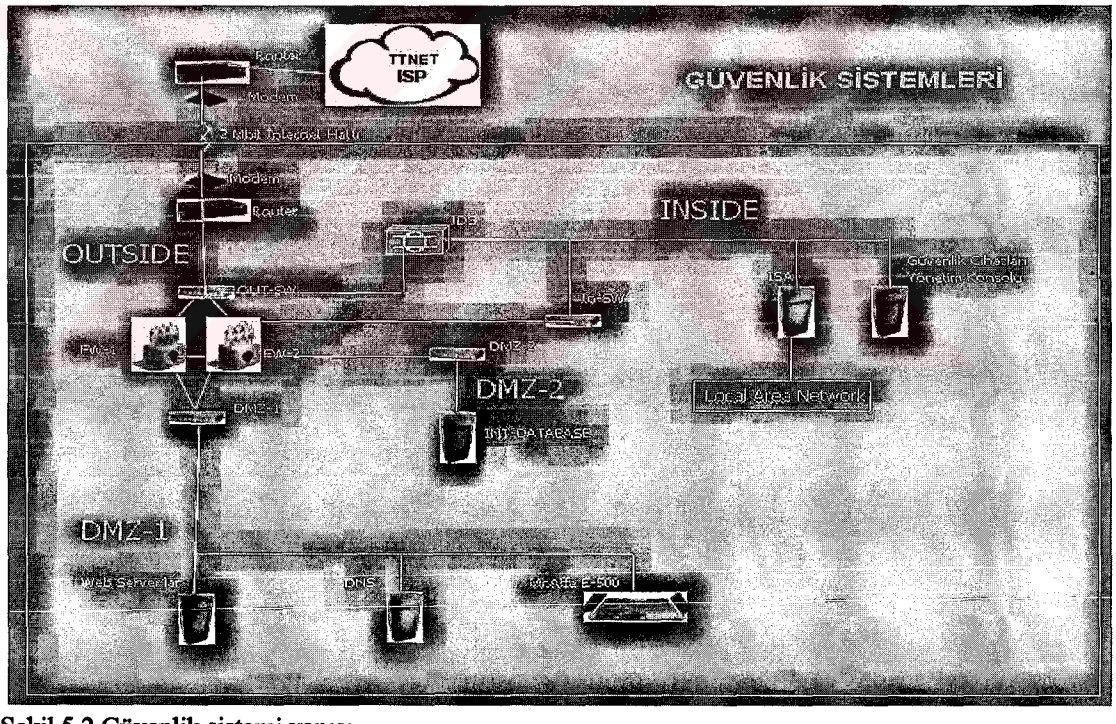
5.9 Web İçerik Kontrolü

Internet üzerinde çalışanların aktiviteleri incelemek, verilen yetkiler dahilinde internete girmelerini sağlayarak hem internet hattının daha verimli kullanılması,

hemde kullanıcıların gereksiz yere zaman kaybetmelerini önlemek için kullanılan bir programdır. [18]

Web içerik kontrol programı bir sirketin mevcut proxy sunucusu, firewall'u, cache motoru veya diger internet araçlari ile entegre bir sekilde çalisabilir ya da yalniz tek basina duran bir proxy sunucusu olarak görev yapabilir. Bir buçuk milyondan fazla site (iki buçuk milyondan fazla Web sayfasi) içeren ana veritabanina bagli çalisarak internet içerigini filtre eder. Bu veritabanı, MP3, kumar, alisveris, yetiskinlere yönelik muhtelif siteler gibi siteleri 65'ten fazla kategori altinda toplar. Kategorilere ait erişim izinleri ve engellemeleri kullanici ve grup bazlarinda veya erişim zamani göz önünde bulundurularak belirlenirler.

5.10 Örnek Bir Güvenlik Sisteminin İncelenmesi



Şekil 5.2 Güvenlik sistemi yapısı

Gelişen teknolojilere ayak uydurmak isteyen bu şirket, kendi web sitesini ve diğer uygulamalarını internet üzerinde hizmet etmek istemektedir. Yapılacak saldırılarla hem şirketin prestijine zarar gelmemesi hemde internet üzerinde yapacağı işlerde zarar etmemesi için güvenlik sistemlerini kurmaya karar vermiştir. Bunun için uzun bir süre güvenlik alt yapısını nasıl şekillendirmesi gerektiğine yapılan araştırmalardan ve testlerden sonra şu kararlar alındı:

1-Güvenlik Politikaları oluşturulacak ve alınan cihazlar bu politikaya uygun olacak şekilde seçilecek,
2-Güvenlik cihazlarının hem donanım, hem de yazılım tabanlı bir ürün olacak,
3-Firewall'un işletim sistemi UNIX temelli olmamalı, kendine has özel bir işletim sistemine sahip olacak,
4-Firewall'un işletim sistemleri tarafındaki açıkları diğer ürünlere göre en az olanlar arasından seçim yapılacak,
5-Güvenlik cihazlarının kurulumu, yönetimi, update ve upgrade'leri kolay olarak yapılacak,
6-Konfigürasyonun kolaylıkla ayarlanabilmesi için kullanıcı arayüzüne sahip olacak,.
7-Firewall ile sorunsuz çalışabilecek IDS cihazı alınacak,
8-IDS Network temelli olacak ve gelen-giden tüm paketleri inceleyecek kapasiteye sahip olacak,
9-Smtp,Pop3,Ftp ve Http trafiğini bir antivirus gateway'i ile taramadan geçirerek iç ağa aktarabilecek bir cihaz alınacak,
10-Bütün PC'lere ve Server'lara antivirus programı kurulacak,
11-Mail server üzerine antivirüs programı kurularak tüm mailler taranacak,
12-Kurum içerisindeki tüm PC'lere antivirüs programı kurulacak ve tek bir yerden update edilebilecek. Aynı zamanda konfigürasyonlarını da yapılabilecek,

Firmanın güvenlik sistemi yukarıdaki gibi şekillendirildi ve konfigürasyonları güvenlik politikalarına göre yapıldı.

Güvenlik Sistemi şu şekilde çalışmaktadır:

Outside da bulunan switch'in tüm portlarındaki trafik IDS'in bulunduğu port'a switch üzerinde mirror özelliği kullanıldı. Böylece tüm portlardan geçen trafik IDS'e de ulaştırılmış oldu.

IDS'in üzerinde tanımlı bulunan saldırı imzaları konfigure edildi. Yani hangi atağa karşı ne tarz bir tepki vereceği IDS üzerinde tanımlandı.Yüksek riskli atakları internet çıkışı üzerinde bulunan router'a ip'si bildirilererek saldırganın iç ağ geçmesi bloklama işlemiyle gerçekleştirilmiş oldu.

Firewall üzerinde tanımlanan kurallara gore trafiği filtereleme görevi yapmaktadır. Aynı zamanda üzerinde tanımlı bulunan ve en çok yapılan 50 'ye yakın atağı firewall engellemektedir ve DoS tarzı ataklardan etkilenmemektedir.

Şu an 2 tane DMZ alanı kullanılmaktadır. DMZ1'de Web Server'lar,DNS ve Antivirüs Gateway cihazı bulunmaktadır. DMZ2 alanında ise uygulama database'i bulunmaktadır.

Firewall üzerinde kurallar tanımlarken; outside'dan inside'a geçiş izin verilmemiştir. Aynı zamanda outside'dan DMZ2 alanına da direk olarak bir erişim izni verilmemiştir. İnternet kullacıları sadece DMZ1 alanında bulunan server'lara erişim sağlamaktadır.

Ayrıca Firewall'un arkasında Microsoft ISA Server bulunmaktadır.MS ISA server hem proxy'lik görevi, hemde firewall özelliğine sahip bir yazılımdır. Firewall özelliğini de iç network'un önüne koyarak ek bir güvenlik sistemi sağlamış oldu.

Kullanıcılar ISA server üzerinde bulunan web içerik kontrolunde verilen yetkiler dahilinde internet sitelerini geziyorlar. Web içerik kontrolu sayesinde kullanıcılar çalışma zamanlarını daha iyi değerlendirilmesine hemde bant genişliğimizi daha verimli kullanmamıza olanak sağlamıştır.

Antivirüs gateway'i gelen ve giden tüm mailler (smtp,pop3), kullanıcıların internette gezerken yaptığı ftp ve http trafiği üzerinden geçirerek virus taramasından geçirir.

Kullanıcılar üzerinde Norton antivirus programı çalışmaktadır. Bu program antivirus server'a bağlıdır. Bir güncelle çıktığı zaman bütün kullanıcılara otomatik olarak dağıtmaktadır. Aynı zamanda mail server üzerinde de mailer virus taramasından geçirilmektedir.

5.11 Güvenlik Tehditlerine Örnekler

Bir kullanıcı veya firma internet güvenliğinin aşıldığı bir durumda çeşitli tehditlerle karşılabilir. Bu tehditlerin sonuçları kullanıcının iş alanına bağlıdır. Örneğin bazı kullanıcılar servislerin tutarlılığı ve hızı konusunda endişelenirken diğerleri bilgisyarlarındaki gizli bilgilerin gizliliği konusunda endişe duyabilirler. [25]

Güvenlik problemlerinin iki ana sınıfı rahatsızlık verici saldırılar ve kötü amaçlı saldırılardır. Rahatsızlık verici saldırılar işinizi yapmanızı engelleyen saldırılardır. Bu tip bir saldırı bilgisayarın yavaşlamasına veya çökmesine yol açabilir. Genelde rahatsızlık verici saldırılarda kalıcı hasar veya kayıp amaçlanmaz.

Eğer bir saldırgan kurumun ağına erişim sağlarsa, dosyaları silebilir, kişisel verileri okuyup değişiklik yapabilir veya makinalara virüs bulaştırabilir.
Kötü amaçlı saldırılar genelde bir firma yada kullanıcıya kayıp yada hasar vermeye yöneliktir. Eğer internet'e doğru güvenlik önlemleri alınmamışsa bilgi sistemlerini risk altına aldığı bilinmelidir. Kurumun ağına bir web sunucusu kurduğunda potansiyel olarak tüm internet'in kurumun yerel ağına erişebileceği bir pencereye açılıyordur. Kurumun sitesinin çoğu ziyaretçisi web sunucuna amaçlandığı şekilde kullanacaktır. Fakat bazıları ağdaki özel bilgilere erişmeye çalışacak hatta dahili ağa erişim için sistemde güvenlik açığı arayacaktır. Sistem güvenlini kimlerin aşmaya çalışabileceğinden her zaman haberdar olunmalıdır. Hacker'lar üniversite ortamındaki öğrencilerden rakiplere veya profesyonel hacker'lar ve endüstriyel casusluk ajanlarına kadar farklılık gösterebilir.[25]

Kaynakları korumada bilmeniz gereken belirli tehditleri bulmak için risk değerlendirmesi yapmak iyi bir fikirdir. Risk değerlendirmesi sadece güvenlik

sistemlerini kurarken değil düzenli olarak gerçekleştirilmelidir. Bu değerlendirmelerde dahili sisteminizin kullanıcıları da içerilmelidir. Muhtemel bir güvenlik ihlalinde risk altında olacak tüm kaynakları bilmek önemlidir. Örneğin, donanım, yazılım ve veri gibi belirli kaynakları tanımlamanın dışında kurumun ağını kullananların da korunması gereken kaynaklar olduğundan haberdar olunmalıdır.

Kurumun bilgisayar sistemini kullanan personel genelde kişisel bilgilerini bilgisayarlarında depolarlar. Bu kişiler bilgisayarları internet'e bağlandığında kişisel bilgilerinin ekstra koruma gerektirdiğini bilmelidirler.

Ağlar bilgisayarlar ve veritabanları gibi değerli kaynakları birbirine bağlar ve firma için gerekli olan servisleri sağlarlar. Bir sunucunun sağladığı özellikler çoğaldıkça güvenlik açıkları içerme riski de o oranda artar. Bunun sebebi internet protokol ve standartlarının dizayn edilirken güvenliğin düşünülmemesidir.

Kullanıcıların genelde işlerini yeterlilikle yapabilmeleri ağ servislerine bağlıdır. Eğer kullanıcıların bu servislere erişimi engellenirse daha az üretken olurlar ve bu da firma için mali kayıp demektir.

Servis kullanımı engelleme (DoS) internet`teki istemci ve sunucular için en ciddi tehditlerden biridir. Aynı zamanda engellenmesi en zor güvenlik tehditidir. Bir servis kullanımı engelleme saldırısı kurbanın normalde erişebildiği bir servise erişebilmesini engelleyen kötü amaçlı bir saldırıdır. Bir saldırganın bunu gerçekleştirebilmesi için pek çok farklı yol vardır.

Bir ağı kullanılmaz hale getirmenin yollarından biri ona bozuk ICMP paketleri göndermektir (bir ICMP pakedi IP paketleri gönderen kişilere ağ problemi olduğunu belirtmekte kullanılır). Örneğin bir ağı işlemez hale devamlı olarak 'Destination Unreachable' (Hedef erişilemez) ICMP mesajları göndererek getirebilir. [25]

Hackerlar ağ parçalarını birbirine bağlayan router gibi kritik bir bileşeni kullanım dışı bırakabilirler veya güvenlik duvarı gibi ağı koruyan cihazları kullanım dışı bırakabilirler.

En kolay servis kullanımı engelleme saldırılarından biri başka bir kullanıcının disk veya hafıza birimini anlamsız mesajlar ile doldurmaktır. Bir saldırgan bunu e-posta ile veya FTP kullanarak bir kaç yüz megabyte işe yaramaz veri göndererek gerçekleştirebilir. Örneğin bir kullanıcının bir dosya için yaptığı isteğe kullanıcının diskinin kapasitesi kadar bir dosya ile cevap verilebilir. [25]

Bir saldırgan web sitesine çok sayıda bağlantı kurarak gerçek kullanıcılarına bu servisin sunulmasını yavaşlatabilir. Gerçekte pek çok sunucu aynı anda yapılabilen bağlantıları sınırlayarak bağlantılar için yeterli kaynak olduğundan emin olurlar. Bu sayede saldırgan mevcut tüm bağlantıları devamlı olarak kullanarak kullanıcıların erişimini tamamen engelleyebilir.

Bir saldırgan kurumun ağına çok sayıda TCP SYN bağlantı istekleri göndererek yavaşlatabilir (SYN yeni bir bağlantı isteği için gönderilen bir sinyaldir). Sunucu her bağlantı isteğini aldığında karşılık verir ve önceden belirlenmiş bir zaman sürecinde, zaman aşımına uğrayana kadar karşı taraftan bir onay bekler. Fakat saldırgan onay mesajlarını göndermez ve SYN`ler göndermeye devam ederse sunucunun tüm kaynakları kullanılacaktır. Buna SYN seli (flood) saldırısı adı verilir. [25]
Ping programı bağlantının kurulup kurulamayacağını görmek için bir makineden diğerine ICMP paketleri göndermede kullanılır. 'Ping of Death' saldırısı karşı tarafın işleyemeyeceği kadar büyük paketlerle pinglenmesi ile gerçekleştirilir. Bazı durumlarda protokol yazılımındaki bu açık yüzünden makinenin çökmesi mümkündür. [25]

Bir sistemi yavaşlatma yada çökertmenin diğer bir yolu da sistemin kaynaklarını tüketen bir virüs kullanımıdır. Robert Morris tarafından geliştirilen meşhur 'Internet Solucanı' (worm), bırakıldıktan sonra bir kaç saat içinde Internet`te 6.000 makineyi etkiledi (Solucanlar bilgisayar ağlarında kendilerini çoğaltarak yayılan virüslerdir). Internet Solucanı 'finger' sunucusuna belirli karakter dizileri göndermede 'finger' kodundaki bir güvenlik açığını kullandı. Bu karakter dizisi programın dahili veri alanlarında süper kullanıcı statüsündeki bölümlerinin üzerine yazarak solucanın yayılabilmesini sağladı.

Bilgi ve haberleşmelerini güvenli hale getirmede kriptografik işlemler kullanan çalışma istasyonları belirli tipte bir servis kullanımı engelleme saldırısına açıktırlar. Bu saldırı makineye çok sayıda bozuk 'imzalanmış' mesajlar göndererek gerçekleştirilir. Kriptografik imzaları onaylamak zaman alıcı bir işlem olduğundan makine tüm zamanını bu mesajları onaylamada kullandığından kullanılamaz hale gelecektir.

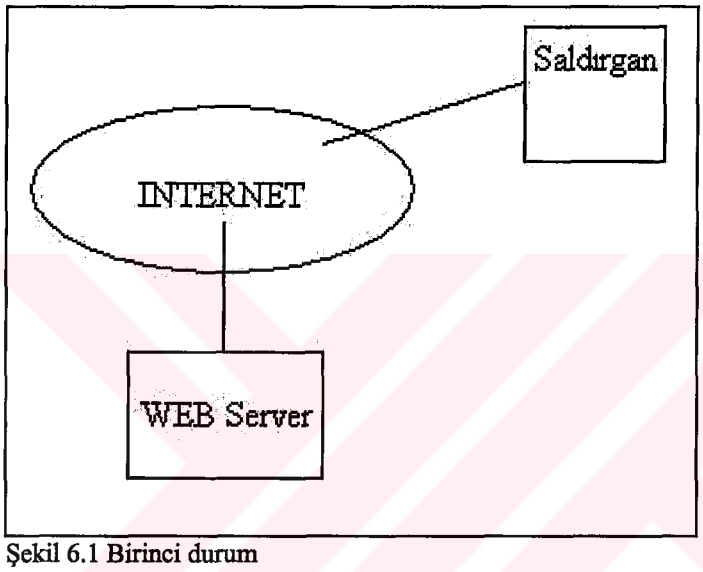
Java ve JavaScript`de de güvenlik problemleri keşfedildi. Java veya JavaScript ile yazılmış programlar çok CPU veya hafiza kaynakları kullanarak makineyi kullanılamaz hale getirebilirler (Java ve JavaScript web sayfalarına etkileşim eklemede kullanılan dillerdir). Örneğin, basit bir Java programı Java runtime sistemlerini dondurabilir. Ve çoğu program çalışırken kesmenize izin vermez. Bu sebeple sistemi reboot (tekrar başlatma) etmeniz gerekir. [25]

Her firmayı endişelendiren güvenlik tehditlerinden biri de sistemlere yetkisiz erişimdir (Önceden belirlenmiş bir izin olmadan herhangi bir ağ kaynağının kullanımı yetkisiz erişim olarak adlandırılır). Kurumun sistemine veya ağına yetkisiz erişimin ciddiyeti yapılan işin doğasına bağlıdır. Bazı siteler için en büyük kayıp değerli verilerin yokedilmesi olabilir. Bazıları için anahtar ticari bilgilerin görüntülenmesi önemli olabilir.

Doğru güvenlik önlemleri olmadan Internete bağlanmanın sonucunda oluşacak potansiyel riskler hafife alınmamalıdır. Örneğin, doğru olarak gönderilmeyen şifreler kolayca ele geçirilebilir. Saldırganlar sisteminize erişebildiğinde önemli verileri silebilir yada kopyalayabilirler. Fakat verileri yokedenlerin sadece harici hacker'lar olmadığı unutulmamalı.

BÖLÜM 6. GÜVENLİK LABORATUAR ÇALIŞMASI

Laboratuar ortamında 1 adet server (internette hizmet veren server) ve 1 adette client (saldırı yapacak pc) kullanılmıştır.



Şekil 6.1 Birinci durum

Labaratuar ortamı şu şekilde oluşturuldu:

İnternet bağlantıları:

-Web server'ın internet bağlantısı frame relay hat üzerinden 2 Mbit olarak sağlandı.

-Saldırgan ise 56 Kbit'lik modem ile bir internet servis sağlayıcı aracılığı ile internet'e bağlantısı sağlandı.

Hizmet edecek servisler:

Web server üzerinde Microsoft IIS servisi kuruldu. Aynı zamanda http ve smtp server servisi çalıştırıldı.

6.1 Birinci Durum

Bu durumda işletim sisteminin hiçbir yaması yüklenmemiştir.

Saldırgan PC tarafından port tarama programı ile bu webserver'ın açık bulunan portları, paylaşımları, üzerinde tanımlı kullanıcıları tarandı.

Tarama sonucunda şu veriler elde edildi:
Açık bulunan portlar:25, 80, 135, 139, 445
Ağa paylaştırılmış klasörler: incoming, C$
Üzerinde tanımlı bulunan kullanıcılar: Administrator, ATM, Guest

Bu tarama işlemi ile saldırgan 25. portun açık olmasından SMTP Server (Mail Server) servisinin açık olduğunu anladı ve Relay'e açık olup olmadığını anlamak için webserver'a aşağıdaki gibi bağlantı kurdu. ("→ " işaretli satırlar saldırgan tarafından yazılmıştır.)

→ telnet webserver 25

220 webbe Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at Thu, 18 Mar 2004 12:02:35 -0800
→ helo webbe
250 webbe Hello [212.133.33.233]
→ mail from:yilmazerdogan@mynet.com
250 2.1.0 yilmazerdogan@mynet.com....Sender OK
→ Rcpt to:ozcelik@sakarya.edu.tr
250 2.1.0 ozcelik@sakarya.edu.tr....Sender OK
→ data
354 Start mail input; end with <CRLF>.<CRLF>
→ SMTP Server'ınız RELAY'e açık..
→ .
250 2.6.0 <WEBBEQool1Ng5PoNXOQ00000001@webbe> Queued mail for delivery

Burada webserver'ın 25 portuna telnet ile bağlanıldı. Helo,mail from, rcpt to ve data SMTP komutları ile sanki Yılmaz Erdogan mail gönderiyormuş gibi ozcelik@sakarya.edu.tr" email adresine mail gönderildi.

Saldırgan 80. portun açık olmasından, web server'ın http servisinin çalıştığını anlamış oldu. Sonra saldırgan bu servis'in açıklarını kullanarak webserver'a ulaşmaya çalışacak.

Saldırgan İnternet gezginin adres satırına aşağıdaki komutu yazdı. Microsoft IIS'deki açıklar, yamalarla kapatılmadı ise webserver'ın "C" sürücününü içeriğini saldırgana listeyecektir.
"http:\\www.webserver.com/scripts/winnt/system32/cmd.exe /c+dir"

Bu işlemin sonucu:
Documents and Settings
I386
My Documents
Program Files
WINNT
Autoexec
Config.sys

Saldırgan 139. ve 445. portların açık olmasıyla, webserver'ın dosya paylaşımına da açık olduğunu anladı. Paylaşımda bulunan incoming klasörünün herkese açık ve yazma hakkı olup olmadığını görmek için webserver'a bağlandı (\\webserver). Saldırgan paylaştırılmış klasörlere erişmek için "Kullanıcı adı ve Paralo" sorduğunu gördü. Daha evvel tesbit edilen kullanıcılardan Guest'in kapatılıp kapatılmadığı kontrol etti ve kapalı olduğu gördü. Sonra Administrator kullanıcısıyla dosya paylaşımına ulaşılmaya çalışıldı. Bunun için de basit, kolay ve tahmin edilebilir şifreleri denemeye başladı.

Denenen şifreler:
abc
root
test
temp
qwerty

password
pass
passwd
newpass
notused
internet
asshole
12345678
123456
12345
1234
123
12
1
x
xx
xxx
xxxx
0246
a1b2c3

Saldırgan şifrenin a1b2c3 olduğunu deneme sonucunda anlar ve klasöre tam yetki ile giriş yapar. Aynı zamanda ağdan \\webserver\c$ paylaşımına administrator kullanıcısı ile giriş yapar. Böylece "C" sürücüsündeki tüm dosyalara tam erişim sağlamış olur.

6.2 İkinci Durum

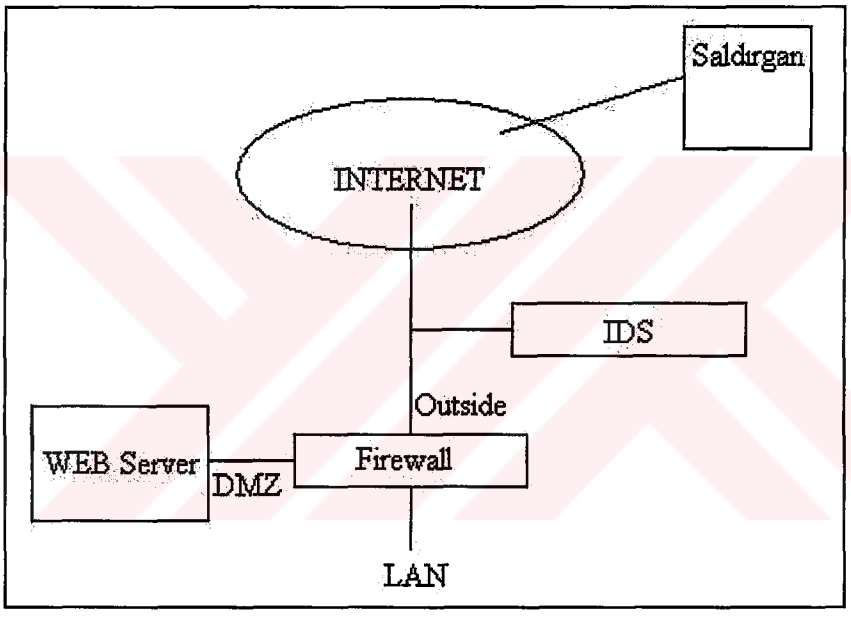
Bu durumda gerekli güvenlik önlemleri alınmaya başlanacaktır.

Webserver'ın güvenliğini sağlayacak önlemler alınmaya başlandı. İlk önce Microsoft'un sitesine girilerek tüm güvenlik açıklarını kapatacak yamalar yüklendi.

Kullanıcı şifreleri tahmin edilemesi çok zor şifreler ile değiştirildi. SMTP servis'inin "Relay" özelliği kapatıldı.

Sonra saldırganın yaptığı işlemleri yeniden denedi ve hiçbir sonuç alamadı.

Webserver'ın güvenliği sağlanmış oldu. Ancak webserver'ın portlarının taramasını engellemek, dosya paylaşımlarına erişimi engellemek için ve yapılan saldırıları tesbit edebilmek için Firewall ve IDS şekildeki gibi yerleştirildi ve gerekli konfigürasyon ayarları yapıldı.



Şekil 6.2 İkinci durum

Webserver Firewall'ın DMZ alanına yerleştirildi. Firewall önüne de tüm trafiği dinlemesi için IDS konuldu.

IDS üzerinde şu işlem ve tanımlar yapıldı:

-Bütün saldırıları tanıması için en son saldırı imzaları IDS'e yüklendi.
-Yüksek seviyeli saldırıları 1 saat boyunca blokla.
-Orta seviyeli saldırıların bağlantısını kes.
-Düşük seviyeli saldırıları sadece görüntüle.

Firewall üzerinde yapılan tanımlar:

-İntenet'ten 80. port ile gelen istekleri DMZ'te bulunan webserver'a ilet.
-İnternet'ten diğer portlardan gelen bütün istekleri DMZ'te bulunan webserver'a iletme
-192.92.92.1 iç IP'sini dışarıya 212.133.33.233 olarak internet'e çıkar.

Yapılan bu ayarlamalar ile saldırgan ile yeniden çeşitli açıkları yakalamaya çalışıldı.

Port tarama programı ile bulunanlar:80. port'un açık olduğu
Ağa paylaştırılmış klasörler: bulunamadı
Üzerinde tanımlı bulunan kullanıcılar:bulunamadı

IDS portların tarandığını anladı ve yöneticiye düşük seviyeli Net-Sweep Echo saldırının olduğunu bildirdi. IDS saldırgan'a bir kural uygulamdı.

Sonra Internet gezginin adres satırına aşağıdaki komut yazıldı.. Sonuçta bir değer geri dönmedi. http:\\www.webserver.com/scripts/winnt/system32/cmd.exe /c+dir

IDS saldırganın webserver üzerinde cmd.exe komutunun çalıştırılacağını anladı ve yöneticiye yüksek seviyeli "IIS execute attack" saldırısının olduğunu bildirdi ve saldırganı 1 saat boyunca bloklamaya başladı. Saldırgan bundan sonra 1 saat boyunca webserver'a erişime kapatılmış oldu.
Sonra tekrar port tarama programı çalıştırıldı. Bu sefer hiç bir sonuç alınamadı. Böylelikle güvenlik optimum seviyede sağlanmış oldu.

BÖLÜM 7. SONUÇLAR

Bilgisayar ağlarının ve dolayısıyla Internet'in yaygınlaşması, şirketlerin web sitelerinin yayınlanmasına, online alış-veriş hizmetlerinin verilmesine hatta bankacılık hizmetlerinin bile internet üzerinden yapılması, günümüzün vazgeçilemez araçları olmuştur. İş dünyasının yüksek hızda veri iletimi ihtiyacı mevcut teknolojilerin geliştirilmesine ve yeni teknolojilerin araştırılmasına yol açmaktadır. Bahsedilen bu nedenlerden dolayı haberleşmenin önemi bir kat daha artmış olmaktadır.

İnternet'in yaygınlaşması ile güvenlik problemleri de gün yüzüne çıkmaya başlamıştır. Bu nedenle ağlar oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Ağların bu zayıflıkları, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur. Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hala büyük bir tehlike oluşturmaktadır.

Bilgisayar ağları kullanıcılardan kaynaklanan veya kullandıkları işletim sistemlerinden kaynaklanan yada network protokollerinden kaynaklanan açıklar olabilir. Bu nedenle şirketler güvenlik sistemlerini mutlaka kurmalıdırlar.

Eğer güvenli bir bilgisayar ağı isteniyorsa güvenlik politikaları oluşturmalı, alınacak güvenlik cihazlarını ona göre tercih etmeli ve ona göre konfigürasyon edilmelidir. Bunun yanında kullanıcılara gerektiği kadar erişim sağlanmalı ve kullanıcıları bu konular hakkında bilinçlendirilmelidir. Sadece firewall alınarak bir güvenlik sistemi oluşturulamaz. Mutlaka yardımcı cihazlarında (IDS vs.) yanında alınması gerekir. Güvenlik cihazlarını yönetecek sistem yöneticilerinin gerekli güvenlik eğitimleri almalıdırlar.

KAYNAKLAR

[1]Andrev S. Tanenbaum, "Computer Networks" (3. Edition), Prentice-Hall, 1996.

[2]Wiliam Stalling, "Data And Computer Communications", Prentice-Hall, 1997

[3]Rıfat Çölkesen, "Bilgisayar Haberleşmesi Ve Ağ Teknolojileri", Papatya Yayıncılık, Ekim 2000, 2. Baskı

[4]Frank J. Derfler, "Network Sistemleri Ve Bilgisayar Bağlantı Klavuzu", Sistem Yayıncılık, Şubat 1998, 2.Basım

[5]Murat Şen, "Internetworking & TCP/IP", Armada Eğitim Merkezi , Haziran 2000

[6]Scott Barman, "Writing Information Security Policies", New Riders Publishing, 2001

[7]Lütfi Yelkenci, "Güvenlik Politikasız Güvenlik Nereye Kadar?", http://www.guvenlikhaber.com/koseyazisi.asp?ID=8

[8]The SANS Security Policy Project, "Security Policies", http://www.sans.org/resources/policies, 2003

[9]Türker Cambazoglu, "Bilişimde Güçlü Güvenlik Politikalarından Ne Anlıyorsunuz? (I-II) ", http://www.bilisimrehber.com.tr

[10]Sun System, "How to Develop a Network Security Policy , An Overview of Internetworking Site Security, Sun Microsystems", http://wwws.sun.com/software/whitepapers/wp-security-devsecpolicy/

[11]J.P. Holbrook, J.K. Reynolds, "The Site Security Handbook", Jul-01-1991, http://rfc.net/rfc1244.html

[12]SANS Enstitute, "Acceptable Use Policy Template", http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

[13]Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM), "Kabul Edilebilir Kullanım Politikası Sözleşmesi", http://www.ulakbim.gov.tr/ulaknet/AUP.uhtml

[14]Enis Karaaslan, "Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar", Akademik Bilişim, 2003

[15]Internet Software Marketing Ltd, "Tips for Creating a Network Security Policy", http://secinf.net

[16]Burç Yıldırım, Burak Dayıoğlu, "Kurumsal Güvenlik", http://www.dikey8.com/

[17]Ege Üniversitesi Network Güvenlik Grubu, "Şifre Seçimi", http://security.ege.edu.tr/dokumanlar.php

[18]Enis Karaaslan, "Network Cihazlarının ve Sistemlerinin Güvenliği", inet-tr, 2002 Konferansı

[19]Cisco System, "Network Security Policy Best Practices Whitepaper", http://www.cisco.com/warp/public/126/secpol.pdf

[20]Simet İletişim Bilgisayar Ltd. Şti., "ISDN", http://www.isdnturk.com

[21]Türk Telekomünikasyon A.Ş., "ISDN Hakkında", http://212.175.64.11/h-isdn.html

[22]Türk Telekomünikasyon A.Ş., "Frame Relay Hakkında",
http://www.telekom.gov.tr/h-frame.html

[23]Veritim Veri iletisimi, Telekomünikasyon ve Bilgi Teknolojileri San. ve Tic. Ltd., "ADSL", http://www.adslkur.com/

[24]Türk Telekomünikasyon A.Ş., "ADSL Hakkında",
http://www.telekom.gov.tr/adsl/adsl-sss.html

[25]Olympos Security, "İnternet Güvenliği",
http://www.olympos.org/article/articleview/128/1/2/

ÖZGEÇMİŞ

Cüneyt BERGEL, 01.02.1977'de Gaziantep'de doğdu. İlkokul öğrenimini 1988 yılında Gaziantep Bahattin Kayalı İlkokulu'nda, ortaokul öğrenimini 1992 yılında İstanbul Vedide Baha Pars ortaokulu'nda, Lise eğitimini de 1995 yılında İstanbul Fatih Şehremini Lisesi'nde tamamladı. 1996 yılında Sakarya Üniversitesi, Elektronik ve Elektrik Mühendisliği Bölümü'nü kazandı ve 2000 yılında mezun oldu.