T.C.

BEYKENT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME YÖNETİMİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ BİLİM DALI

BİLGİSAYAR AĞLARI VE BEYKENT ÜNİVERSİTESİ ÖRNEĞİ

YÜKSEK LİSANS TEZİ

İsmail Erkan ÇELİK

İSTANBUL 2005

T.C.

BEYKENT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME YÖNETİMİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ BİLİM DALI

BİLGİSAYAR AĞLARI VE BEYKENT ÜNİVERSİTESİ ÖRNEĞİ

YÜKSEK LİSANS TEZİ

İsmail Erkan ÇELİK

DANIŞMAN: YRD.DOÇ.DR.GÖKHAN SİLAHTAROĞLU

İSTANBUL 2005

T.C.
BEYKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ
YÜKSEK LİSANS TEZ SINAV TUTANAĞI

8/12/2005

Enstitümüz ***İşletme Yönetimi Anabilim Dalı Yönetim Bilişim Sistemleri Bilim Dalı*** yüksek lisans öğrencilerinden YB2251-102 numaralı ***İsmail Erkan Çelik'in*** *"Beykent Üniversitesi Lisansüstü Eğitim - Öğretim ve Sınav Yönetmeliği"*nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği **"*BİLGİSAYAR AĞLARI - BEYKENT ÜNİVERSİTESİ ÖRNEĞİ*"** adlı Tezini, Yönetim Kurulumuzun 14.11.2005 tarih ve 2005/18-2 sayılı toplantısında seçilen ve Fakülte binasında toplanan biz jüri üyeleri huzurunda, ilgili yönetmeliğin *(c) bendi gereğince* (80) dakika süre ile aday tarafından savunulmuş ve sonuçta adayın tezi hakkında ***oybirliği*** ile ***Kabul*** kararı verilmiştir.

İşbu tutanak, 5 nüsha olarak hazırlanmış ve Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

DANIŞMAN
YRD.DOÇ.DR.GÖKHAN SİLAHTAROĞLU

ÜYE
YRD.DOÇ.DR.RIZA HALUK KUL

ÜYE
YRD.DOÇ.DR.BAHADDİN SİNSOYSAL

İsmail Erkan Çelik

Home: (212) 880 3515, **GSM:** (532) 273 7767

E-mail: erkancelik@beykent.edu.tr

Adress: Cumhuriyet Mahallesi, Beylikdüzü, Beykent Sitesi, Adem Çelik Şirketler Grubu
34500 Büyükçekmece/İSTANBUL

INDIVIDUAL INFORMATION

Nationality	T.C.
Birth Place	İstanbul
Birth Date	11/03/1979
Military Status	Postponed
Marriage Status	Single

EDUCATION STATUS

	Beykent University, Management Information Systems, Master Programs, İstanbul/TURKEY
	Lectures that I attended and achieved;
2003-2004	- Decision Taking Techniques - Organizaitonal Behaviour - Managerial Economics - Business Administration - Computer Networks and Communications - Human Resource Management - Management Information System - Strategic Management
2001-2003	Beykent University, Faculty of Architecture- Engineering, Department of Architecture, İstanbul/TURKEY
1999-2001	University of John Moores, Faculty of Architecure, Department of Architecture, Liverpol/ENGLAND
1997-1999	Beykent University, Faculty of Architecture, Department of Architecture, İstanbul/TURKEY
1990-1997	Beykent College- Mathematics-Turkish Department
1985-1990	Bahçelievler High School

EXPERIENCES

01/11/2003-24/08/2005	Beykent University	General Secretary
15/01/2001-…/…/…	Doğa Turism and Construction Commercial Company	Member of Board of Directory
03/04/2000-06/10/2003	Beykent University	Member of Board of Trustee
26/07/1999-…/…/…	Beykent Private Education and Sports Institution Commercial Company	Assistant of Board of Directory

FOREIGN LANGUAGE

English (advanced)
Italian (beginner)
Germa (beginner)

COMPUTER

AutoCAD, Allplan, Photoshop, Freehand, 3D Studio viz/max, Dreamweaver, SPSS, Microsoft Office Applications, Excel, Word, Powerpoint

SEMINARS AND ATTENDANCE CERTIFICATES

2004-05 September	Symposium of Private School Association; Consultant Education, Details
2003- January, February	Symposium of Private School Association;Foreign Language and Quality Research, Pre School Education during the process of entering to European Union- Problems and Recomendations
2003	Dialog, Expression and Communication; Seminar of Right, good human relation
2003	Brand
2002	TÜSSİDE, Continuous Quality Development in Education
2001	Pronto, Italian Education Centre

SOCIAL ACTIVITIES AND MEMBERSHIP

2004	Membership of Association of Turkey Young Businessman
2003	Aviation School of Onur Air
2002	Membership of Trabzonspor Club
2000	Liverpool John Moores University, Membership of Turkish students Association
2005	Captain of Amateur Sailing
2004	Membership of Büyükçekmece Human Right Commitee
2000	Liverpool John Moores University, Membership and player of Basketball Club

INTERESTS

Flying (planes that has one motor), motor sports, voyage, squash, basketball, swimming, fighting sports, reading book, listening to music, piano, playing drumbs.

ÖNSÖZ

Bilgisayar ağı, elektronik tabanlı haberleşmenin ve bilgisayarlı uygulamaların kan damarı; ağ üzerinde oluşan bir tıkanma tüm sistemin performansını düşürebilmektedir. Dolayısıyla, ağ projelendirilmesi ve konfigürasyonu bilinçli bir şekilde yapılmalıdır.

Günümüzde bilgisayar ağlarından beklentiler artarak şekil değiştirmeye başlamıştır; daha düne kadar yalnızca bilgisayar ve benzeri sayısal cihazların veri iletişimi için düşünülen ve ona göre protokol, standart belirlenen, ona göre optimize edilen bilgisayar ağları, bugün ses, veri ve hareketli görüntü bilgilerini de aktarma görevini üstlenmiş durumdadır; aynı zamanda gerçek zaman uygulamalarına da olanak sağlaması beklenmektedir. Dolayısıyla, komple ağın ana parametreleri olan LAN, Kampüs, WAN ve uzak bağlantı gibi kısımlarının performans kaybına neden olmadan bütünleştirilmesi gereksinimi ortaya çıkmıştır.

Komple bir ağ kurulmasında en önemli unsurlar teknoloji seçimi, iletim altyapısı (kablolu/kablosuz), cihazların seçimi ve bilinçli konfigürasyon yapılmasıdır. Bilinçli konfigürasyon, belki de, ağ kurulmasında en önemli parametredir denilebilir. Çünkü, teknoloji ve cihazlar ne olursa olsun, bilinçli konfigürasyon yapılarak, olası en yüksek performansa ulaşılmaya çalışılır.

Bu projede bir ağ nelerden oluştuğunu, komple ağın parametreleri olan LAN (Local Area Network- Yerel Alan Ağı), WAN (Wide Area Network-Uzak Alan Ağı) ve Şehirlerarası Bağlantıdan, bilgisayar ağlarının amaçlarından, bir ağ ortamı ile sağlanan tipik yararlarından, bir ağın bileşenlerinden, ağ yapılarından (topolojisinden), iletişi protokollerinden, mimariden, ağların birbirine nasıl bağlandığından (repeater, bridge, router, gateway, hub, switch), ağ cihazlarının yönetimi ve güvenliğinden, Internetten, TCP/ IP Protokolünden, Beykent Üniversitesi Network yapısından ve üniversitenin Network planlarını bir yüksek lisans tezi için danışmanca uygun bulunan hacim ve içerikde açıkladım.

Bu tezin oluşum aşamasında bana teknik anlamda destek olan Bilgi İşlem Bölümüne ve danışmanlığımı üstlenen Sayın Yrd.Doç.Dr.Gökhan Silahtaroğlu'na teşekkür ederim.

Ağustos, 2005 **İsmail Erkan Çelik**

İÇİNDEKİLER

İKİNCİ BÖLÜM

2. OSI(OPEN SYSTEM INTERCONNECTION), İLETİŞİM BİÇİMLERİ, AĞ BAĞLANTILARI, AĞ CİHAZLARI

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

Üniversitesi : **Beykent Üniversitesi**
Enstitüsü : **Sosyal Bilimler Enstütüsü**
Programı : **Yönetim Bilişim Sistemleri**
Tez Danışmanı : **Yrd.Doç.Dr.Gökhan SİLAHTAROĞLU**
Tez Türü ve Tarihi : **Yüksek Lisans – Ağustos 2005**

ÖZET

BİLGİSAYAR AĞLARI, BEYKENT ÜNİVERSİTESİ NETWORK YAPISI

İsmail Erkan ÇELİK

Bu çalışmada, bir ağın nelerden oluştuğundan, komple ağın parametreleri olan LAN (Local Area Network- Yerel Alan Ağı), WAN (Wide Area Network-Uzak Alan Ağı) ve Şehirlerarası Bağlantıdan, bilgisayar ağlarının amaçlarından, bir ağ ortamı ile sağlanan tipik yararlarından, bir ağın bileşenlerinden, ağ yapılarından (topolojisinden), mimariden, ağların birbirine nasıl bağlandığından (repeater, bridge, router, gateway, hub, switch), ağ cihazlarının yönetimi ve güvenliğinden, Internetten, TCP/ IP Protokolünden, Kablosuz ağdan, Beykent Üniversitesi Network yapısından ve üniversitenin Network planlarından söz edilmiştir. Komple bir ağ kurulmasında en önemli unsurlar teknoloji seçimi, iletim altyapısı (kablolu/kablosuz), cihazların seçimi ve bilinçli konfigürasyon yapılmasıdır. Beykent Üniversitesinin ağ yapısı incelendiğinde alt yapı bakımından karmaşık gibi görünse de standart bir ağ yapısına rastlamaktayız ve daha verimli sonuçlar alınması için bilinçli bir alt yapı ve konfigürasyonun yapılmasının kaçınılmaz olduğu gözlenmiştir.

University : **Beykent University**
Institute : **Institutiton of Social Sciences**
Programme : **Management Information System**
Supervisor : **Dep.Doç.Dr.Gökhan SİLAHTAROĞLU**
Degree Awarded and Date : **Master – August 2005**

ABSTRACT

NETWORK

NETWORK STRUCTURE OF BEYKENT UNIVERSITY

İsmail Erkan ÇELİK

In this study, Local Area Network, Wide Area Network and Metropolitian Area Network whose are the parameters of a whole network, the main benefits of network environment, network structure, OSI model, how a network can be constructed and connected with each other (repeater, bridge, router, gateway, hub, switch), the management and security of network devices, TCP/IP Protocol, Wireless Network, and the Network structure of Beykent University and its Network Plans. The fundamental determinators of construction of a whole network are selection of devices and conscious configuration. When we look at the network structure of Beykent University, even we can encounter a complex network structure, the existing structure meet the requirement, and when the university develop its structure, they can get more productive results.

1. Giriş

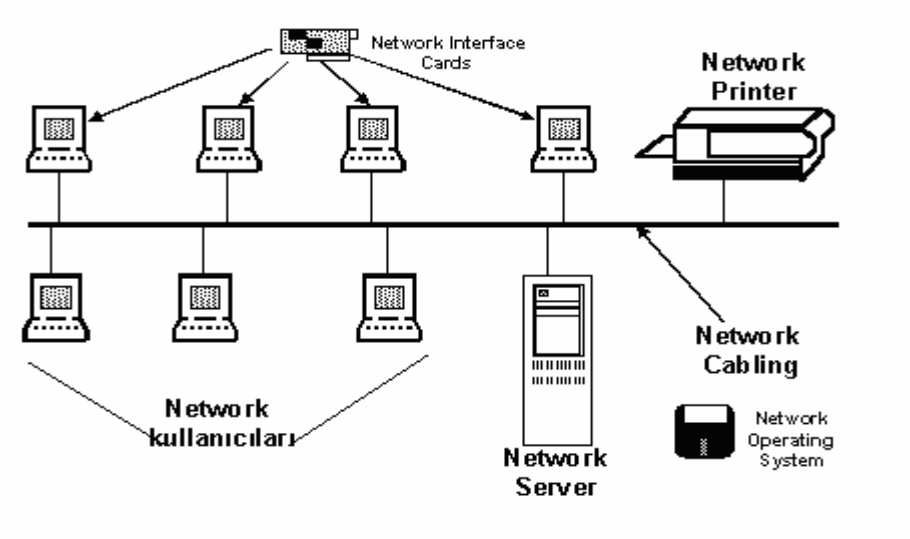
Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan çalışma biçimine bilgisayar ağı (computer network) denir. Bir bilgisayar ağında çok sayıda bilgisayar yer alır. Bu bilgisayarlar yan yana duran iki bilgisayar olabileceği gibi tüm dünyaya yayılmış binlerce bilgisayar olabilir. Ağ içindeki bilgisayarlar belli bir biçimde dizilirler. Bilgisayarlar arasında genellikle kablo ile bağlantı sağlanır. Kablo bağlantısının mümkün olmadığı durumlarda mikro dalgalar ve uydular aracılığıyla da ağ içindeki iletişim kurulur. Bilgisayar ağlarının ilk uygulamaları 1960'lı yılların sonlarında başlamıştır. Ancak yerel bilgisayar ağlarının yaygınlaşması 1980'li yıllarda başlamış ve gelişmiştir. 1980'li yıllarda, kişisel bilgisayarların çoğalması, bilgisayar teknolojisindeki ve iletişim teknolojilerindeki gelişmeler bilgisayar ağlarının daha yararlı olmasını sağlamıştır.

Bilgisayar ağı, birbirine bağlı (interconnected) bir çok bağımsız bilgisayar anlamına gelir. İki bilgisayarın birbirinin kaynaklarını (diskini ya da diskinde yer alan bilgilerini) paylaşabilmesi ve konuşabilmesi onların birbirine bağlı olduğunu gösterir.

İşletmecilik açısından ağlar, yönetime ve denetime yardımcı olurlar. Bir bankanın ya da üniversitenin çok sayıda bilgisayarı birbirine bağlı olarak kullanılması,onları bağımsız olarak kullanmasından daha anlamlı ve verimli olur. Böylece birimler arası iletişim daha kolay sağlanmakta ve bütünleşik (integrated) uygulamalar daha kolay gerçekleştirilmektedir.

Bilgisayar ağına bağlı olan bir bilgisayar diğer bilgisayarlarla bağlantı içindedir. Diğer bilgisayarlarla iletişim kurar, onların sabit diskinde yer alan verilere erişir, onların programlarından yararlanır. En basit biçimi ile ağ, genellikle modemlerle birbirine seri bağlantılı olan iki makinedir. Daha karışık ağ yapılarında ise,TCP/IP (Transmissions Control Protocol/Internet Protocol), protokolü kullanılmaktadır. Bu , yüz binlerce bilgisayarın birbirine bağlı olduğu Internet üzerinde diğer bilgisayarlar ile bağlantı kurmamızı sağlayan protokol ailesidir.

BİRİNCİ BÖLÜM



Şekil 1: Basit Bir Network

1. AĞ, PARAMETRELERİ, AMAÇLARI, BİLEŞENLER ve YAPILARI

1.1 Bir Ağ Nelerden Oluşur?

1.1.1 Sunucu (Server)

Bir sunucu üzerinde bulunan kaynakları diğer bilgisayar ve terminallerin kullanılmasına izin veren ana sistemdir. Çoğu ağ sisteminde merkezi sistem kullanılır. Bunun anlamı ana sunucunun tüm kaynakları kendi üzerinde barındırması ve ağa bağlı bilgisayarlardan çok daha üstü olmasıdır. Sunucu ne kadar iyi ise sistem o derecede rahat çalışabilir. Bir sunucu disk ve yazıcı paylaşımı yapabilir. Bir sunucu tek başına pek çok servisi verebilir veya bu servislere ayrı ayrı sunucular atanabilir. Örneğin;

- Dosya Sunucusu (File Server): Diğer bilgisayarlar genelde sabit diske sahip değildir. Sadece bir disket veya Ethernet kartı üzerinde programlanmış bir bootrom sayesinde açılışta bu bilgisayarlara bağlanarak gerekli işletim sistemini ve uygulama programlarını yüklerler.

- Veritabanı Sunucusu (Database Server): Bir ağ üzerinde herkesin aynı anda güncelleştirilmiş aynı veriye erişebilmesi için kullanılır.

- Web Sunucusu (Web Server): Üzerinde güncel Web sayfalarını saklayan ve bunları diğer insanların kullanımına sunulması için kullanılan sunucu.

- Yazıcı Sunucusu (Print Server): Kendisine bağlı yazıcının kontrolünü üstlenir ve bu yazıcıyı ağdaki diğer bilgisayarların kullanımına izin verir.

1.1.2 Kaynaklar (Resources)

Kaynaklar, paylaşılabilen her şeydir. Yazıcı, yazılım, fax/modem kartı, CD-ROM sürücü, sabit disk alanı, işlemci gücü vs. olabilir. Özellikle akademik alanda birden çok ağların hızlı bir ağ yardımıyla bağlanıp işlemci güçlerini birleştirmeleri sayesinde yapılan çalışmalar gözle görülür bir şekilde artmaktadır.

1.1.3 Terminal

Sadece sunucunun kaynaklarını kullanan "aptal sistemlerdir". Bunlara bu ismin verilmesinin nedeni sadece klavye ve monitörden oluşmaları ve tüm işlemleri sunucunun kaynaklarını kullanarak yapmalarıdır. Sunucu/istemci (client/server) modelinde kullanılabilir.

1.1.4 Bilgisayarlar (Node, Host)

Bilgisayarlar terimini kullanırken ağa bağlı bilgisayarlardan bahsetmekteyiz. Terminallerin aksine sunucuya yük olmadan kendi işlerini yapabilecek kapasitedirler. Genellikle sunucunun disk, CD-ROM, yazıcı, fax/modem kartı gibi kaynaklarından yararlanırlar. Hem sunucu/istemci hem de türdeş ağ çeşitlerinde kullanılabilirler. Genellikle sunucu makineye nazaran daha düşük güç ve kapasitede olurlar.

1.1.5 Yazıcı (Printer)

Ağlarda iki çeşit yazdırma yöntemi kullanılmaktadır. Bu yöntemlerin birinde ağ yazıcısı kendi ağ kartına ve diğer birimlere sahiptir ve bu sayede başka hiçbir donanıma gerek duymaksızın ağ üzerindeki bilgisayarların gönderdiği bilgiyi yazar. Diğer bir yöntem de ağ yazısının bir bilgisayar veya ana sunucuya bağlı olduğu sistemdir. Yazıcıdan alınmak istenen çıktılar bu bilgisayarın denetiminde yazıcıya gönderilir ve böylece çıktı alınabilir.[1] **Çelik, Kaan Güneş, Çetin, Görkem,** Bilgisayar Ağları ve Linux Ağ Yönetimi El Kitabı, 1998, Sistem Yayıncılık

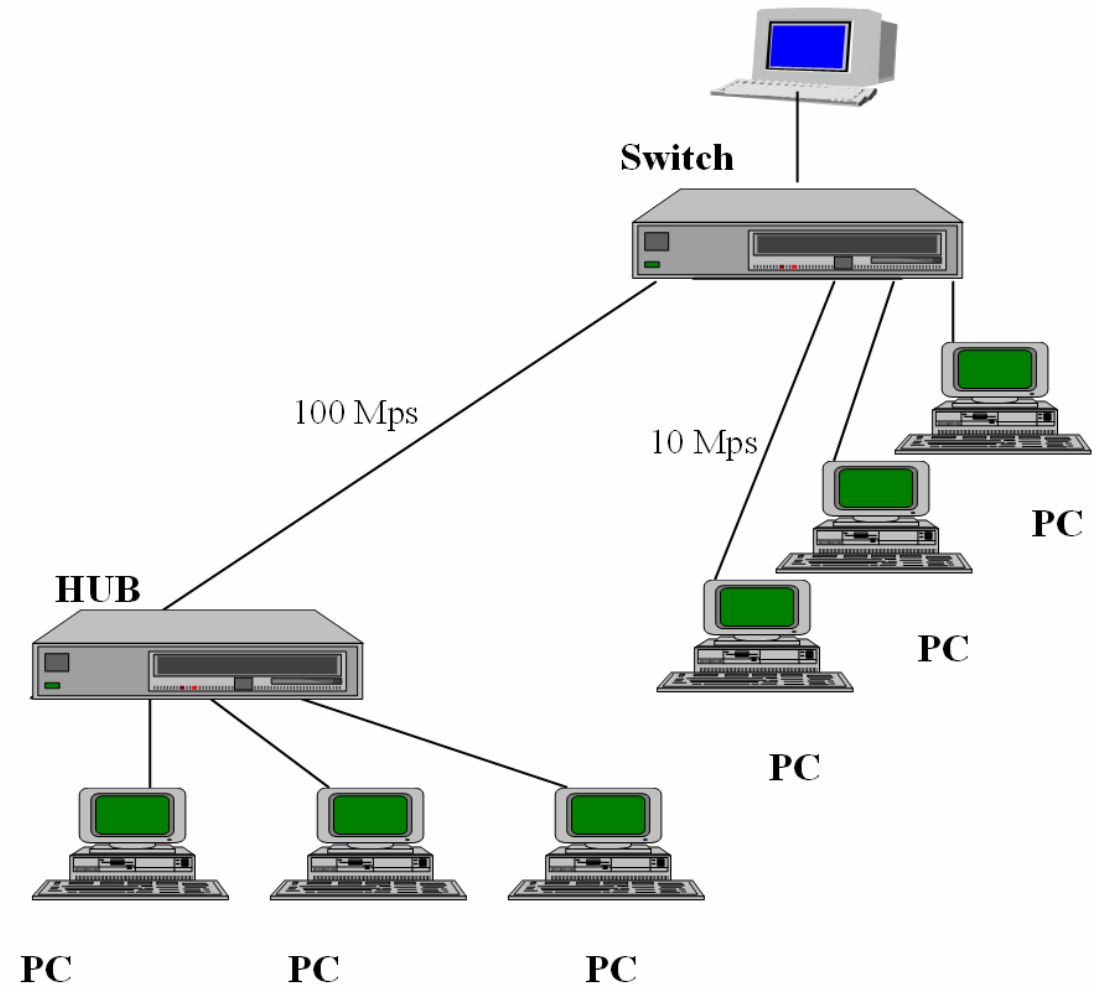
1.2 Komple Ağın Parametreleri:

1.2.1 LAN (Local Area Network- Yerel Alan Ağ):

LAN'larda temel özellik, sistemlerin aynı ortamda veya birbirlerine yakın mesafede olmalarıdır. Bu nedenle sistemler arasında kullanılacak kabloların seçiminde büyük bir esneklik vardır ve kablolama altyapısı bir kez kurulduktan sonra maliyetsiz büyük bir ileti ortamı sağlar. En basitinden 1 HUB ile LAN kurulabilir. LAN uygulamasında yüksek hızlara çıkılabilir; kullanılan teknolojiye göre 10, 16, 100, 155, 622 Mbps ve 1 Gbps hızında band genişliğine sahip olunabilir. Bir yerel ağın en büyük özelliklerini sayacak olursak,

- Ucuz iletişimi sağlayacak kablolama ihtiyacı
- Benzer şekilde nispeten daha az masraf gerektiren donanım ihtiyacı (modemler, yineleyiciler ve yönlendiriciler)
- Yüksek hızda veri iletişimini sağlayan ağ teknolojileri
- Bilgisayarların ve genel olarak tüm ağ birimlerinin birbirleriyle kolaylıkla bağlanabilmesi, yeniden yapılanmanın düşük maliyeti ve yüksek hızda gerçekleştirilebilmesi

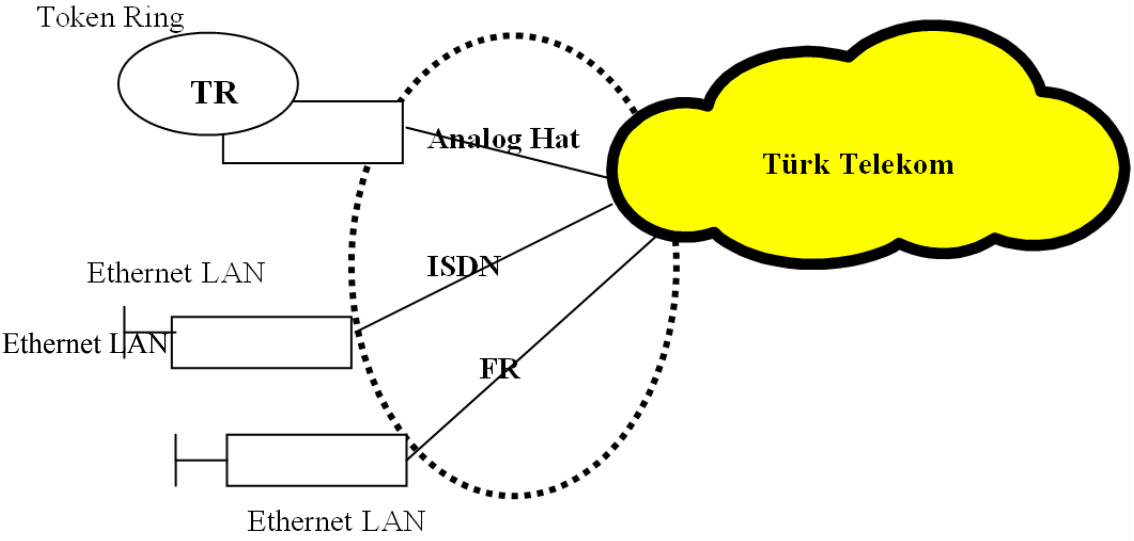
Intranet ve LAN, birbirlerinden ayrı tutulamayan iki kavramdır. Eğer bir LAN, şirket içinde kurulmuşsa ve şirket personeli tarafından kullanılıyorsa intranet adını alır. Bu ağ üzerinde WWW sunucu, FTP dosya sunucusu, veritabanı sunucuları ve haber öbekleri bulunur.[2] **Çölkesen, Rifat**, Network, TCP/IP, UNIX El Kitabı, 2001, Papatya Yayıncılık



Şekil 2: LAN Uygulaması

1.2.2 Geniş Alan Bilgisayar Ağları *(*WAN, Wide Area Network)

Bir ülke ya da dünya çapında yüzlerce veya binlerce kilometre mesafeler arasında iletişimi sağlayan ağlardır. Coğrafi olarak birbirinden uzak yerlerdeki (şehirlerarası/ülkelerarası) bilgisayar sistemlerinin veya yerel bilgisayar ağlarının (LAN) birbirleri ile bağlanmasıyla oluşturulur. Genellikle kablo ya da uydular aracılığı ile uzak yerleşimlerle iletişimin kurulduğu bu ağlarda çok sayıda iş istasyonu kullanılır. WAN' lar üzerinde on binlerce kullanıcı ve bilgisayar çalışabilir. Şirketinizin Ankara, İzmir ve İstanbul şubelerini bir WAN bağlantısı ile birleştirdiğinizde, Ankara'da bulunsanız bile İstanbul'daki bir makineyi tıpkı önündeymiş gibi yönetebilirsiniz.[2] **Çölkesen, Rifat**, a.g.e



Şekil 3: WAN Uygulaması

1.2.3 Şehirsel Bilgisayar Ağları (MAN, Metropolitan Area Network*)*

LAN' ın kapsadığı alandan daha geniş, fakat WAN' ın kapsadığından daha dar mesafeler arası iletişimi sağlayan ağlardır. Genellikle şehir içi bilgisayar sistemlerinin birbirleriyle bağlanmasıyla oluşturulur.[2] **Çölkesen, R.,** a.g.e.

1.3 Bilgisayar Ağlarının Amaçları

Bilgisayar ağları; özel amaçlı, eğitim amaçlı, ulusal olarak ve halka açık olarak kurulabilir. Yerel bilgisayar ağları (LAN) ise çok katlı bir bina, okul, hastane gibi sınırlı bir alanda kurulan ve genellikle kişisel bilgisayarların yer aldığı ağlardır. Yerel Bilgisayar Ağları, çokluk ofis otomasyonu için kurulur ve firmanın organizasyonuna göre yerleşimi biçimlendirilir.

Bilgisayar ağlarının bir diğer amacıda ölümcül donanım sorunlarının önlenmesidir. Örneğin muhasebe uygulanmasının yürütüldüğü bilgisayarda bir arızanın oluşması onun tümüyle kullanılamaması ve muhasebe uygulamasının kesilmesi anlamına gelir. Oysa, Yerel Bilgisayar Ağı (LAN) üzerinde bir terminalin (ucun) yerine başka bir uç yada iş istasyonu kullanılabilir.

Bilgisayar Ağlarının temel amacı, ağ içindeki kullanıcıları iletişir, konuşur hale getirmek ve özgün uygulamalarına destek olmaktır. Yerel Bilgisayar Ağı (LAN) olarak gerçekleştirilen ağlar, çok katlı belli bir alan içinde çalışırlar;ofis, bina, kampus içinde kullanıcıları ve iş istasyonlarını birbirine bağlayan ağ, bağımsız çalışmaları, iletişimi ve aynı zamanda merkezcil yöntemi de destekler.

Bilgisayar ağları kullanıcılarına birçok olanağı da sunarlar; kullanıcılar bilgisayar ağlarına başvurarak (girerek) yeni yazılımlar elde edebilirler. Yine bilgisayar destekli eğitimde ya da üniversiteler arası bilgi alışverişlerinde bilgisayar ağları çok yararlı bir eğitim ortamı sağlarlar. Diğer bir olanak da uzak veri tabanlarına (data base) erişimdir. Bir bilgisayar kullanıcısı kendi bilgisayarından uzak veri tabanlarına girerek kendisine bir uçak bileti alabileceği gibi sermaye piyasası hakkında da bilgi sahibi olabilir.

Sonuç olarak, ağlarla sağlanan iletişim olanakları onların en büyük amaçlarını oluşturur.

1.4 Bir Ağ Ortamı ile Sağlanan Tipik Yararlar

Bir ağ işletim sistemi, tek bir kişisel bilgisayarın işletimini sağlayan işletim sistemine göre çok daha üstün özelliklere ve yeteneklere sahiptir.

- Programların ve dosyaların paylaşımı
- Ağ kaynaklarının paylaşımı
- Hata Toleransı
- Disk Önbelleği
- Elektronik posta
- Bir çalışma grubunun yaratılması
- Merkezi yönetim
- Kayıt Koruma
- Güvenlik
- Uzak Erişim
- Kişisel bilgisayar kullanımının ekonomik olarak artırımının sağlanması

1.5 Bir Ağın Bileşenleri

Bir ağ (network) belli yazılım ve donanım parçalarından (bileşenlerinden) oluşur.

Bu temel parçalar şunlardır:

- Ağ işletim sistemi yazılımı
- Hizmet birimi (Ana makine)
- İş istasyonu
- Ağ ara birim kartı
- Kablolama sistemi
- Paylaşılan kaynaklar ve çevre birimleri

Ağ işletim sistemi yazılımı, ağın işletimini sağlayan özel bir yazılımdır. Ağın yönetimini, iletişimi, kaynakların kullanımını sağlayan bu yazılım genellikle büyük firmaların ürünü olan gelişmiş ürünlerdir. Novell Netware, yaygın kabul görmüş bir ağ işletim sistemi yazılımıdır. Bunun dışında başka ağ yazılımları da vardır:

Ağ işletim sisteminin temel görevi ağ kaynaklarının kullanımının sağlanmasıdır. Ağ kaynaklarının yanı sıra ağın güvenliği ve denetimini de sağlayan ağ işletim sistemlerinin çok sayıda özellikleri vardır. Çünkü, ağ ile birlikte kullanıcıların yapabildikleri artar ve sistemin denetimi güçleşir.

Hizmet birimi (ana makine/server), ağ işletim sistemini işleten bilgisayardır. İş istasyonları hizmet birimine bağlanarak ağa dahil olurlar. Ağın denetimini, yazdırma vs. temel işlemleri hizmet birimi sağlar.

İş istasyonu (workstation),hizmet birimine ve dolayısıyla ağa bağlı olan bir bilgisayar, iş istasyonu (workstation) yada düğüm (node) olarak adlandırılır. İş istasyonları genellikle DOS işletim sistemi ile çalışan bilgisayarlardır. İş istasyonlarının kendi sabit diski olabileceği gibi disksiz de olabilir. Disksiz iş

istasyonları, ağ birimi kartlarında yer alan özel bir öz-yükleme (boat) programı ile hizmet birimine bağlanırlar.

Ağ ara birim kartı (Network interface card), ağa bağlı olan her bilgisayarı bir karta gereksimi vardır. Bu kart sayesinde iş istasyonu ağa dahil olur. Kablolama sistemi üzeriden hizmet birimine erişilir. Ağ kartları genellikle sonradan eklenirler. Kartlar ağ tipine uyum sağlamak zorundadırlar.

Kablolama sistemi, ağ içinde ana makine ile iş istasyonlarını birbirine bağlar. Kablo çeşitleri şunlardır:

- Eş eksenli kablo (coaxial)
- Burgulu çift kablo
- Fiber optik kablo

Fiber kablolar ışığı iletme özelliğine sahip cam liflerden oluşurlar. Çok hafif, ince ve hızlı olmaları onların üstünlüğüdür.[3] **Kaplan, Yasin,** Veri Haberleşmesi Kavramları, 2000, Papatya Yayıncılık

1.6 Ağ Yapıları (Topolojiler)

1.6.1 Ortak Yol Ağ Yapısı :

Ortak yol topolojisinde ağdaki tüm bilgisayarlar v.s. gibi düğümler aynı anda bir ortak iletim ortamı üzerinden haberleşirler. Veri ve denetim işaretleri aynı anda tüm düğümlere birden gönderilir. Her düğümün bir adresi vardır. Düğümler yol üzerindeki her mesajı okurlar ve yalnızca kendilerini adresleyeni işlerler. Ortak yola yeni düğüm ekleme kolay olur. Ancak, her yeni eklenen düğüm ; düğüm başına düşen yol kapasitesini azaltır.

Şekil 4: Ortak Yol Topolojisi

1.6.2 Halka Ağ Yapısı :

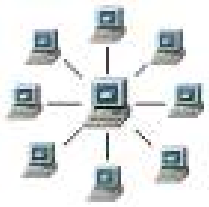
Halka topolojisinde her düğüm , komşu iki düğüme bağlıdır ; iletim yolu halka biçimindedir. Yolun ele geçirilmesi için en yaygın kullanılan yöntem : Jetonu halka üzerinde dolaştırmaktır. Jeton (Token) bir kayıt mesajdır. Her bilgisayar bir paket göndermek istediğinde bu jetonu bekler. Yolu kimin kullanacağını , yolda dolaşan bir jeton belirler; onu yoldan alıp yola verisini koyar. Göndereceği verisi bittikten sonra jetonu yeniden yola koyar. Aynı düğüm tekrar veri göndermek isterse jetonu ele geçirene kadar beklemelidir.

Halka topolojisinin olumlu yanı yoğun iletişim anında bile başarımını fazla düşürmemesidir. Ancak, ağa yeni kullanıcı eklenmesi biraz daha zahmetli olur. Halka üzeinde veri alışverişi uygulamaya göre tek veya iki yönlü olabilir.

Şekil 5: Halka Topolojisi

1.6.3 Yıldız Ağ Yapısı :

Yıldız topolojisinde düğümlerin tamamı merkezi noktadan bir cihaza bağlıdır. Ağ üzerindeki tüm trafik , bu merkez noktadan geçer. Günümüzdeki ağ uygulamalarında yoğun olarak yıldız topolojisi kullanılmaktadır. Ortak yol ve halka uygulamaları bile , mantıksal olarak yol ve halka biçiminde olsa dahi fiziksel bağlantıları yıldız şeklinde olabilmektedir. Yıldız topolojinde de ağa yeni düğüm kolayca eklenebilir. Ancak, her düğüme ayrı ayrı kablo çekilmesi gerekliliği maliyeti yükselten bir unsurdur. Merkezdeki düğüm bozulduğunda tüm iletişim kopar.



Şekil 6: Yıldız Topolojisi

Ağaç ve Örgü topolojileri WAN uygulamalarında kullanılır.

1.6.4 Ağaç Ağ Yapısı :

Ağaç topolojisi hiyerarşik topoloji olarak da adlandırılır. Bu topolojide veri yönetim ve işleme sorumluluğu farklı farklı olan sistemler sorumluluk düzeyine göre sıralanarak bir ağaç yapısında bağlanırlar. Ağacın kökünde sorumluluğu en yüksek olan sistem vardır. Aşağılara doğru sistemlerin sorumlulukları azalır. Ağaç topolojisi daha çok büyükçe firmaların omurga WAN yapısını kurmak için kullanılır.

Şekil 7: Ağaç Topolojisi

1.6.5 Örgü Ağ Yapısı :

Örgü topolojisinde sistemlerin birbine bağlanması için çoğunlukla bir organizasyon veya geometrik desen gözükmez. Yeni bir sistem , genellikle , kendisine en yakın mesafede olan bir yerden bağlanarak eklenir. Internet ve çoğu genel amaçlı WAN ; örgü topolojisi yapısındadır.[4] İşletmeler İçin Çözümler - Bilgisayar Ağları, Alan Neibauer, Çeviren : D.Kaya, A.Pamukçu, A.Ulutaş, M.Tan, Ü.Türkoğulları web: http://kemalgok.virtualave.net/ag/network.htm

Şekil 8: Örgü Topolojisi

İKİNCİ BÖLÜM

2. OSI, İLETİŞİM BİÇİMLERİ, AĞ BAĞLANTILARI, AĞ CİHAZLARI YÖNETİMİ VE GÜVENLİĞİ

2.1 OSI (Open System Interconnection) Başvuru Modeli

- Uygulama Katmanı (Aplication Layer)

Kullanıcının çalıştırdığı uygulama programları doğrudan bu katmanda tanımlıdır. Dosya aktarımı (FTP), elektronik mektuplaşma (e-mail), ağ yönetimi (SNMP), Internet hizmetlerine erişim programları.

- Sunuş Katmanı (Presentation Layer)

Bilginin iletimde kullanılacak biçiminin düzenlemesini sağlar: sıkıştırma/açma, şifreleme/çözme, EBCDIC-ASCII dönüşümü ve ters dönüşümü gibi işlevlerin yerine getirilmesini kapsar.

- Oturum Katmanı Session Layer

Uç düğümler arasında gerekli oturumun kurulması, yönetilmesi ve sonlandırılması işlerini kapsar. İletişimin mantıksal sürekliliğinin sağlanması için, iletişimin mantıksal sürekliliğini sağlanması için, iletişimin kopması durumunda bir senkronizasyon noktasında başlayarak iletimin kaldığı yerden devam etmesini sağlar.

- Ulaşım Katmanı (Transport Layer)

Bilginin son alıcıda her tür hatadan arındırılmış olarak elde edilebilmesini sağlar. Ulaşım katmanının oluşturduğu bilgi bloklarına bölüm denir.

- Ağ Katmanı (Network Layer)

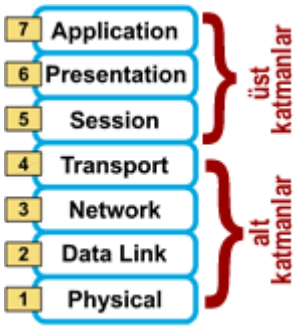
Veri Paketlerinin bir uçtan diğer uca ağdaki çeşitli düğümler (Yönlendirici, geçityolu vs.) üzerinden geçirilip yönlendirilerek alıcısına ulaşmasını sağlayan işlevlere sahiptir. Buradaki bilgi bloklarına paket adı verilir. Internet'in protokol kümesi olan TCP/IP'de IP protokolü bu katmana ait bir protokoldür.

- Veri Bağı Katmanı (Data Link Layer)

Gönderilecek bilginin hatalara bağışık bir yapıda lojik işaretlere dönüştürülmesi, alıcıda hataların sezilmesi, düzeltilemiyorsa doğrusunun elde edilmesi için göndericinin uyarılması gibi işlevleri vardır.

- Fiziksel Katman (Physical Layer)

Verinin fiziksel olarak hat üzerinden aktarılması için gerekli işlevleri kapsar. Bu katman için tanımlanan standartlar taşıyıcı işaretin şekli, verici ve alıcı konumundaki uç noktaların elektriksel ve mekanik özelliklerini belirler. Kablo, konnektör standartları bu katmanda yapılır. [5] **Çölkesen, Rifat,** a.g.e.



Şekil 9: OSI Başvuru Modeli

2.2 Mimari (İletişim Biçimleri)

Geniş anlamda bilgisayarların birbirleri ile iletimin hangi hiyerarşik yapıda yapıldığını tanımlar; Uçtan-uca *(Peer-to-peer)* veya Sunucu-istemci *(Client-server)*.

2.2.1 Sunucu-İstemci (client-server)

Sunucu-İstemci çalışma biçiminde ağın hizmet birimi bütün işlemleri yüklenir. Paylaşılan bütün kaynaklar hizmet birimine de yer alır. İşlemleri hızlı bir şekilde yaparak iş istasyonuna sonuçları yollar. Böylece hızlı bir işletimi sağlar. Bunun aksi durum ise iş istasyonlarının işlemlerini kendi veri programlarını kendi belleğine

yükleyerek kendi işlemcisiyle işlemesidir. Bu nedenle işlemlerin hızı iş istasyonunun performansına bağlı olacaktır.

2.2.2 Eş düzeyli (peer-to-peer)

İki yada daha çok bilgisayarın, bir hizmet birimi (server) kavramı olmadan en basit biçimde birbirine bağlandığı ve bütün makinelerin kaynaklarının her iş istasyonu tarafından kullanılabildiği ağlardır.

Bu çalışma biçiminde ağ içindeki bütün bilgisayarlar eşit düzeydedir. Yani aynı özellikte ve önceliktedir. Bir hizmet birimi (ana makine) ve iş istasyonu kavramı yoktur. Ağdaki her kullanıcı diğer bir kullanıcının kaynaklarına kolaylıkla erişebilmekte ve iletişimde bulunabilmektedir.

Yukarıdaki iki biçimden hangisinin seçileceğine karar vermeden önce yapılacak işlerin ne olduğu saptanmalıdır. Bir hizmet birimi ve müşteriler olarak tasarlanan ağ daha geniş bir ağdır. Büyük bir firma ve denetime gerek duyar. Eş düzeyli ağların ise kullanımı daha kolaydır. Bu ağlarla iki yada üç gibi az sayıda kullanıcının birbirine herhangi bir üstünlük kurmadan bağlanması söz konusudur.[6] **Karaaslan, Enis,** 2001, Ege Üniversitesi Cisco Network Akademisi Ders Notları, web: http://cnap.ege.edu.tr

2.3 Ağları Birbirine Bağlamak

Bir yerel bilgisayar ağı genellikle bir bina yada yerleşim birimi içinde yer alır. Ağın genişletilmesi ise genellikle ağa yeni iş istasyonlarının eklenmesi ve diğer yerleşim birimlerine taşması durumunda karşılaşılan bir durumdur.

Bir bilgisayar ağı diğer bir bilgisayar ağına da bağlana bilir. Böylece daha geniş bir ağ kaynağı kullanıcıların hizmetine sunulmuş olur.

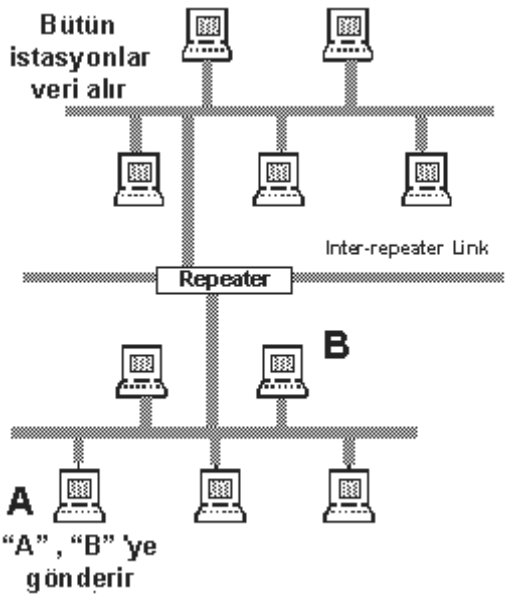
Ağların birbirlerine bağlanmaları için belli aygıtlar kullanılır. Bu aygıtlar iki ağın iletişim biçimlerini uyumlu hale getirirler. Bu aygıtlar:

- Repeater (yineleyici)
- Bridge (Köprü)
- Yönlendiriciler (Yönlendirici)

- Geçitler (Gecit)
- Hub
- Switch

2.3.1 Repeater (Yineleyici)

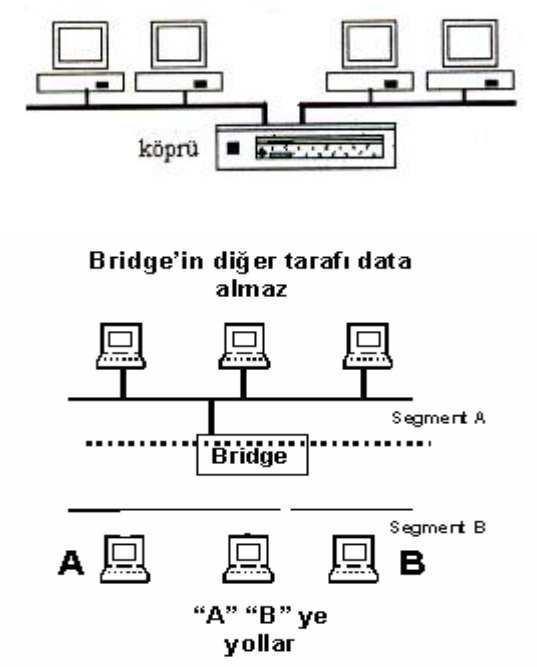
İki yada daha fazla bilgisayar ağını birbirine bağlamak için kullanılan en kolay yol yineleyicilerdir. Bu aygıtlar ağın uzak yerleşimlere erişmesini sağlarlar. Bu aygıtların işlevi ağ içindeki sinyalleri kuvvetlendirip diğer ağa taşımaktır. Kablo üzerinde bir bilginin etkisini kaybetmeden nasıl gider? Örneğin, kalın koaks kablolarda 500 metre ve ince koakslarda iki segment arasındaki uzaklık 185 metredir. Daha fazla uzaklığa kablolama gerekiyor ise bu limitlerde zayıflayan sinyallerin güçlendirilmesi lazımdır. Yineleyiciler sayesinde daha uzak ağları birbirine bağlaya biliriz. Genellikle ince ve kalın koaks kablolarda kullanılırlar, UTP tipi kablolarda zaten hub'lar birer yineleyici görevini görmektedir. Token Ring sistemlerinde ağa bağlı her iş istasyonu kendisine gelen paketi güçlendirdiği için yineleyicilere gerek duymazlar.Ethernet ağlarında en fazla 3 adet yineleyici kullanılabilir.[7] **Danielyan, E.,** 2002, Cisco Internet Protocol Journal - Mar.



Şekil 10: Repeater

2.3.2 Bridge (köprü)

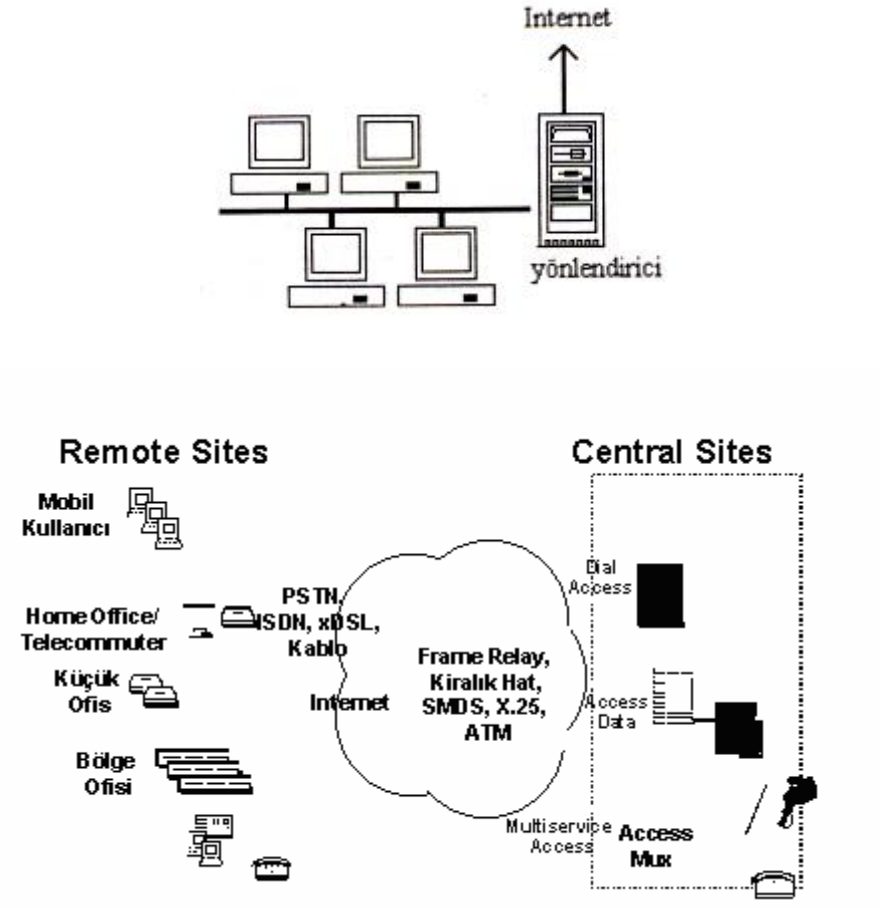
İki ağı birleştirirler ve bilgi paketlerinin geçişini sağlarlar. Köprüler genel anlamda yineleyicilerin yaptığı işi yaparlar. Fakat temel farkları, bir yineleyici kendisine gelen mesajı güçlendirir ve hedefe bakmadan doğrudan yollar. Köprüler eğer paket hedefine ulaşamayacaksa bu paketi göndermezler. Ayrıca köprüler birbirlerinden farklı ağları birleştirir ve bunların ararlarında iletişim kurmalarını sağlarlar.[8] **Danielyan, E.,** a.g.e.



Şekil 11: Köprü (Bridge)

2.3.3 Yönlendiriciler

Büyük ve değişik protokollere sahip bilgisayar ağlarını birleştirirler. Yönlendiriciler bir ağ üzerindeki tüm bilgisayarların adreslerini bilir ve buna göre kendilerine gelen paketi en uygun şekilde hedefe yollar. Yönlendiriciler genellikle dinamik yönlendirmeyi kullanır.Bunun anlamı kendisine gelen bir paketin tüm ağ taranarak en güvenli ve hızlı yolun denenmesidir. Verinin içeriğini inceler ve iletilmesi gerekmiyorsa iletmez. Eğer herhangi bir sorun çıkarsa, alternatif bir yol arayarak mutlaka paketi hedefine ulaştırmaya çalışırlar. Yönlendiriciler ağa bağlı özel bir araç veya ağa bağlı bir bilgisayar olabilirler.[9] **Danielyan, E.,** a.g.e.



Şekil 12: Yönlendiriciler (Yönlendirici)

2.3.4 Geçitler

Genellikle bir bilgisayarın başka bir ağa bağlanmasını sağlarlar. Geçitler ağların farklı iletişim protokollerine sahip ağlarla bağlanmasını sağlarlar. Örneğin bir geçit, Netware ağının IBM sistemine bağlanabilmesini sağlar. Kullanıcı geçit üzerinden o sisteme bağlanır ve kaynaklarını kullanır.

Birçok ağın birleşmesinden oluşan büyük ağlarda, her bir ağ kendine özgü protokoller ve sistemler kullanmaktadır. Bu ağların birbirleri ile sorunsuz olarak anlaşabilmeleri için geçitler kullanılmaktadır. Geçitler, birbirlerinden tamamıyla farklı ağları birleştirirler. Halen daha pek çok farklı ağ sistemleri kullanılmakta olduğundan geçitlere büyük ihtiyaç duyulmaktadır.[10] **Danielyan, E.,** 2002, Cisco Internet Protocol Journal - Mar.

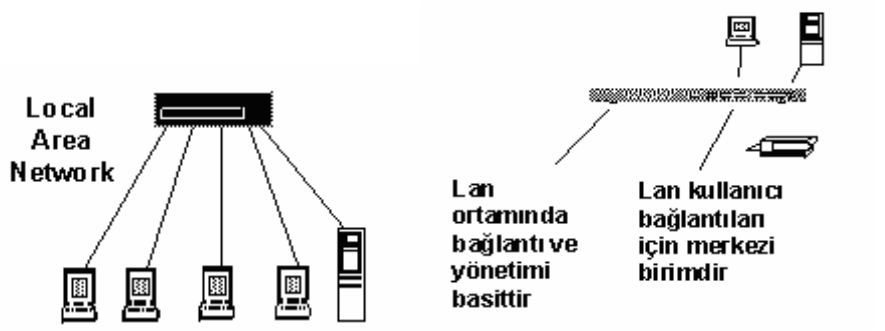
2.3.5 Hub

Hub'lar star ağ yapılarında merkezi bağlantı üniteleridir. Hub kendisine bağlanılan tüm node'ların birbirleri ile iletişim kurmasını sağlar. Node; bir network ekipmanı (hub veya switch gibi) ile haberleşebilen, server, printer, fax makinası vb. aygıtlardır. Hub'a bağlanılan her ekipmanın kendi güç kaynağı olduğu gibi hub'ında kendi güç kaynağı vardır. Hub üzerinde bulunan durum ışıkları ağ durumunu izlememizi ve arıza tespit işlemlerini kolaylaştırır. İkiden fazla hub birbirine bağlanabilir fakat Ethernet standartlarında bazı sınırlar vardır. Hub-Hub bağlantıları yerine switchlerden hub'lara gidilebilir, ve bu durum ağ performansını arttırır. 10 Mbps veya 100 Mbps ağlar için hub'lar bulunmaktadır.

Yıldız topolojiye uygun olarak kendisine bağlanan cihazlar arasında iletişimi sağlarlar. Üzerinde genellikle 5 ila 32 bilgisayarın bağlanabileceği kadar iskele (port) bulunur. Ağ üzerindeki bilgisayarlar UTP türü kablo kullanarak hub'a bağlanırlar. Kullanılan kabloların uzunluğu 100 metreden fazla olamaz. Birden çok hub birbirine bağlanarak (en fazla üç adet) ağınızı daha da genişletebilirsiniz.

Hub'lar tüm bilgisayarların bağlandığı bir merkezi sistem gibi çalıştıklarından açık kalmaları ağın sağlığı için çok önemlidir. Genellikle bir ağdaki hub, yönlendirici,köprü gibi birimler insanlardan uzak yerlere konur.

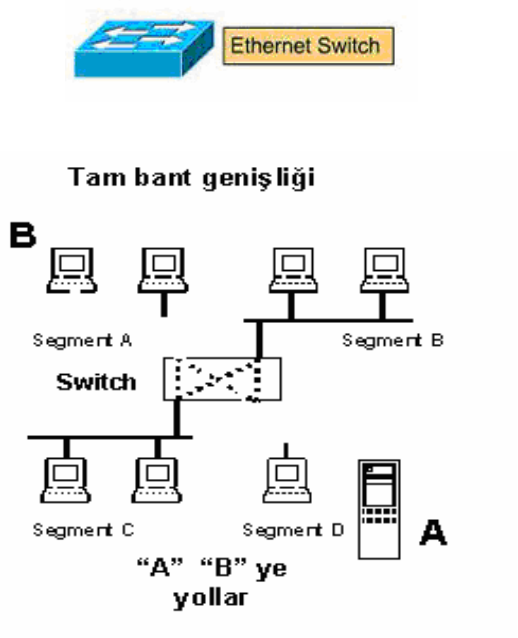
Hub'ın görevi kendisine ulaşan sinyalleri alıp yine kendisine bağlı olan ağ ekipmanlarına dağıtmaktır. Hub bu işlem sırasında bir tekrarlayıcı görevi görür ve sinyali güçlendirir.[11] **Danielyan, E.,** a.g.e.



Şekil 13: Hub

2.3.6 Switch

Switchler daha kompleks ve daha verimli hub' lardır. Büyük bir ağı segmentlere (parçalara) bölerek ağ performansını arttırır. Herhangi bir node'tan gelen verinin tüm ağa dağıtılması yerine istenilen node'a dağıtılmasını sağlar. Ağ durumunu izler, veriyi gönderip, iletim işleminin yapılıp yapılmadığını test eder. Bu özelliğe "store and forward" (depola ve ilet) denir.[12] **Danielyan, E.,** a.g.e



Şekil 14: Switch

2.4 Ağ Cihazlarının Yönetimi ve Güvenliği

Ağ cihazları yönetim açısından, yönetilebilir (*managable*) veya yönetilemez (*unmanagable*) cihazlar olarak ikiye ayrılmaktadır. Yönetilebilir cihazların kendilerine özgü bir işletim sistemi ve konfigürasyonu bulunmaktadır. Cisco cihazlarda IOS ve CatOS, Alcatel XEON'larda XOS, Avaya cihazlarında Unixware, Juniper'de Free BSD örnek olarak verilebilir. Diğer cihazlarda da genelde UNIX tabanlı işletim sistemleri bulunmaktadır. Ağ cihazlarının ayarlanması, yönetimi ve kontrolü aşağıdaki şekillerde sağlanabilmektedir:

- HTTP protokolü ile,
- Telnet veya SSH ile,
- SNMP protokolü ile,
- TFTP veya FTP ile,
- Konsol portuyla.

Konsol portu aracılığıyla erişimde fiziksel güvenlik ön plana çıkmaktadır. Diğer erişim türlerinde ise TCP/IP protokolü kullanılacağından bu protokolün zayıflıklarına karşı önlem alınması gerekecektir.

Cihazların ayarları menüler aracılığıyla, komut (*command*) yazarak veya grafik arayüzlerle yapılabilmektedir. Cihazlarda kurulum sırasında oluşan varsayılan (default) ayarların, kullanıcı tarafından aktif edilen bazı ayarların iptal edilmesi veya düzgün olarak tekrar ayarlanması gerekebilmektedir.[13] Increasing security on IP Networks web: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

2.4.1 Fiziksel Güvenlik

Cihaza fiziksel olarak erişebilen saldırganın konsol portu aracılığıyla cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya tap (özel ekipmanla kabloya erişim) ederek hattı dinleyebilir veya hatta trafik gönderebilir . Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal yöntemlerin hiç bir kıymeti bulunmamaktadır. Bazı fiziksel güvenlik önlemleri aşağıda verilmiştir:

- Cihazlar sadece ağ yöneticisinin veya onun yardımcısının açabileceği kilitli odalarda tutulmalıdır. Oda ayırmanın mümkün olmadığı yerlerde özel kilitli dolaplar (kabinetler) içine konmalıdır.
- Cihazlara fiziksel olarak kimin ve ne zaman eriştiğini belirten erişim listeleri tutulmalı (*access auditing*) ve bu listeler sık sık güncellenmelidir.
- Kablolar tek tek etiketlenmeli ve kayıtları tutulmalıdır. Kullanılmayan kablolar devre dışı bırakılmalıdır.

- Cihazların yakınına güvenlik bilgileri (şifre, IP adresi) gibi bilgiler yapıştırılmamalı ve gizli tutulmalıdır.

- Cihazlara fiziksel erişim mümkün ise kullanılmayan portlar disable edilmelidir.

- Aktif cihazların elektriği aldığı güç kaynaklarının yeri belirlenmeli ve saldırganın bu güç kaynaklarını kesmesi engellenmelidir. Devamlı güç kaynaklarına (ups) yatırım yapılmalıdır.

- Aktif cihazların fiziksel erişime açık olduğu yerlerde saldırganın güç kablosunu çıkartmasını engellemek için cihazın üstünde çeşitli aparatlar kullanmalı, güç kablosunu gözden ırak tutmalı, mümkünse uzakta ve fiziksel güvenliği sağlanan bir prize bağlanmalıdır.

Her ne kadar aktif cihazların çalınması pek olası olmasa da bu tür olayları engellemek için mümkünse çeşitli kilit ve alarm mekanizmaları kullanılmalıdır.[14] web: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm (Increasing security on IP Networks)

2.4.2 Şifre Yönetimi

Şifreler cihazlara her türlü izinsiz erişim de hesaba katılarak iyi seçilmelidir. İyi şifrelerin özellikleri aşağıdaki gibidir:

- Büyük ve küçük harf içerirler,

- Noktalama işaretleri ve rakamlar içerirler,

- Bazı kontrol karakterleri ve/veya boşluklar içerirler,

- Kolaylıkla hatırlanabilirler ve bu nedenle bir yere not edilme ihtiyacı duymazlar,

- En az yedi veya sekiz karakter uzunluğundadırlar,

- Kolay ve hızlı yazılırlar; ve böylece etraftan bakan birisi ne yazdığını anlayamaz.

Şifre yönetmenin en iyi yolu LDAP, TACACS+ veya RADIUS doğrulama (*authentication*) sunucuları aracılığıyla onay mekanizmasını kullanmaktır. Bu sistem kullanılsa bile yetkili (*privileged*) haklar için o cihaza yerel (*local*) tanımlı bir şifre, konfigürasyon dosyasında bulunmalıdır . Birçok yönetilebilir cihaz, kullanıcı (user) modu ve yetkili (enable) mod gibi iki ayrı login mekanizmasına sahiptir. Kullanıcı modunda sadece arayüzler (interface) incelenebilirken yetkili modda ek olarak cihaz konfigürasyonu da yapılabilmektedir. Cisco cihazlarında girilen kullanıcı ve parolaların konfigürasyon dosyasında gözükmemesi için "*service password-encryption*" komutu girilmiş olmalıdır. Zayıf şifreleme algoritması kullanan "*enable password*" komutu yerine MD5-tabanlı algoritmayla şifreyi koruyan "*enable secret*" komutu kullanılmalıdır. "*no enable pass*word" komutu kullanılarak enable password'ler silinmeli yerine "*enable secret yeni_şifreniz* " ile yeniden şifreler girilmelidir. [15]SAFE: A *Security* Blueprint for *Enterprise* Networks, Sean Convery , Bernie Trudel, 2000 web: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

2.4.3 Cihaz Erişim Protokollerine Dair Ayarlar

Ağ cihazlarının ayarlanması, yönetimi ve kontrolünde kullanılan HTTP, Telnet, SSH, SNMP, TFTP ve FTP; TCP/IP protokolünün alt elemanları olduklarından, bu protokolün zayıflıklarına karşı önlem alınması gerekmektedir. Bu türden erişimlerde denetim, bu cihazların ve dolayısıyla ağ trafiğinin güvenliği için çok gereklidir.

2.4.4 Belirli IP'lerin Cihaza Erişimine İzin Vermek

Cihazlara sadece belirli IP adreslerinin ulaşmasına izin verilmelidir. Bu da access-list yazılarak sağlanır. Örneğin Cisco IOS'de sadece 200.100.17.2 ve 200.100.17.3 IP'lerin erişimine izin verilmesi ve diğer ip'lerin engellenmesi aşağıdaki access-list ile sağlanmaktadır.

access-list 7 permit 200.100.17.2

access-list 7 permit 200.100.17.3

access-list 7 deny any log

Örnekte verilen 7 numaralı access-list belirtilen IP'lere izin vermekte (permit), diğer IP'leri kabul etmemektedir (deny). Bu access-list'in devreye girmesi için herhangi

bir ara yüzde etkin hale getirilmesi gerekmektedir. Telnet (veya ssh) için uygulanması da aşağıdaki gibi olmaktadır:

line vty 0 4

access-class 7 in

Http erişimi için kısıtlanması da aşağıdaki gibi olmaktadır:

ip http access-class 7

SNMP erişimine belirtilen IP'lerin izin verilmesi ise aşağıdaki gibi olmaktadır: [16]

[16] SAFE a.g.k.

snmp-server host 200.100.17.2 snmp_şifresi

snmp-server host 200.100.17.3 snmp_şifresi

2.4.5 HTTP Erişimi

HTTP protokolü ile web arayüzünden erişim, cihaza interaktif bağlantı demektir. Yönetilebilir cihazlarının birçoğunun üzerinde web sunucusu çalışır. Bu da 80 nolu portta bir web sunucunun kurulu beklediğini gösterir. Daha önceden de belirtildiği gibi HTTP servisi verilecekse bu ağ yönetimini sağlayan belirli IP'lere kısıtlı olarak verilmelidir. Cihaz güvenliği nedeniyle mümkün olduğunca bu tür web üzerinden yönetimin kullanılmaması gerektiği önerilmektedir. Ama web üzerinden yönetim gerekiyorsa web sunucusu sadece sistem yöneticisinin bileceği başka bir port üzerinden, örneğin 500 nolu portta çalıştırılabilecek şekilde ayarlanmalıdır.

HTTP protokolünde doğrulama mekanizması ağda şifrenin düz metin şeklinde gönderimi ile sağlandığı için efektif değildir ama farklı üreticilerin değişik çözümleri bulunmaktadır. Doğrulama mekanizması, onay sunucuları (Tacacs+, Radius …vb) kullanılarak yapılabilir. Cisco IOS'de doğrulama mekanizması "*ip http authentication*" komutuyla sağlanmaktadır.[17]

[17] web:http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

2.4.6 Telnet ve Secure Shell (SSH) Erişimi

Telnet ile erişimlerde saldırganın ağ üzerinden dinlenme (sniff) yoluyla iletilen bilgiyi elde etmesi mümkün olduğundan, iletilen veriyi şifreleyen SSH protokolü mümkün olduğunca kullanılmalıdır. SSH şu anda bütün cihazlar ve cihaz işletim sistemleri tarafından desteklenmemektedir. Bu konuda üretici firmanın cihaz dokümantasyonu incelenmelidir.[18] SAFE

2.4.7 SNMP Erişimi

Simple Network Management Protokol (SNMP), cihaz ve ağ yönetimi için vazgeçilmez bir protokoldür. Trafik istatistiklerinden bellek ve CPU kullanımına kadar bir cihaz hakkında çok detaylı bilgiler edinilebilmektedir. Bir veya daha fazla Ağ Yönetim İstasyonu, üzerlerinde çalışan yazılımlarla belirli aralıklarla ağ cihazları ve sunuculardan (server) bu istatistikleri toparlayacak (poll) şekilde ayarlanmalıdır. Cihazda gözlenen CPU, bellek veya hat kullanımının fazla olması bir saldırı tespiti olabilmektedir. Toplanan verileri grafiksel olarak görüntüleyen Multi Yönlendiriciler Traffic Grapher (MRTG) gibi programlar bulunmaktadır.

SNMP protokolünün, özellikle SNMP Version 1'in birçok uygulamasında zayıflık (vulnerability) olduğu CERT 'in raporlarında belirtilmiştir. Birçok cihaz üreticisi bu konuda yama (patch) çıkartmış ve önerilerde bulunmuştur. SNMP Version 1, düz metin (clear text) doğrulama dizileri (string) kullandığından bu doğrulama dizilerinin spoof edilmesi söz konusu olabilmektedir. Bu yüzden MD5'a dayanan öz (*digest*) doğrulama şeması kullanan ve çeşitli yönetim verilerine kısıtlı erişim sağlayan SNMP Version 2'nin kullanılması gerekmektedir. Mümkünse her cihaz için ayrı bir MD5 gizli (*secret*) değeri kullanılmalıdır.

Öneriler:

- Sadece Oku (*Read only*) ve Oku-Yaz (*Read-Write*) erişimleri için kullanılan varsayılan SNMP şifre (*community*) adları değiştirilmeli ve bu iki parametre birbirinden farklı olmalıdır.

- SNMP şifrelerine kritik bir UNIX makinesindeki root şifresi gibi davranılmalıdır.

- SNMP erişimi hakkı sadece belirli güvenilir (*trusted*) IP'lere (Ağ Yönetim istasyonlarına) sağlanmalıdır.

- Ağ Yönetim İstasyonu tarafından SNMP erişimi yapılırken "Sadece Oku" parametresi kullanılmalıdır. Mümkünse cihazlarda "Oku-Yaz" parametresi iptal edilmelidir.

Ağ Yönetimi için ayrı bir subnet, mümkünse VLAN yaratılmalıdır. Access-list ve Ateş Duvarı (*firewall*) kullanılarak bu ağa dış ağlardan gelen trafik kısıtlanmalıdır. [19] SAFE

2.4.8 VLAN Uygulamaları

Virtual Lan (VLAN - sanal ağlar) kullanılarak kullanıcıları fiziksel lokasyonundan bağımsız olarak gruplamak, farklı subnetlerde toplamak mümkündür. VLAN'a almak tek başına bir güvenlik önlemi sayılmamakla beraber bir güvenlik artışı olmaktadır. Ağ Yönetimi için ayrı bir VLAN yaratılmalıdır. Bölgeler VLAN trafiklerine göre prunning yapılarak ayrılmalı, sadece o bölgede kullanılan VLAN'lar iletilmelidir.

VLAN bilgilerini ve bütün ağ trafiğini aktif cihazlar arasında taşımak için kullanılan cihaz port'ları "trunk" olarak tanımlanmaktadır. Trunk olmayacak port'ların trunk olarak tanımlanması o port'a bağlı cihazın bütün ağ trafiğini almasını sağlayacağından bu tür yanlış tanımlamalar mutlaka düzeltilmelidir.

Cihazların kullanılmayan portlarını L3 (OSI 3.katman) bağlantısı verilmemiş bir VLAN'a atamalı veya portlar "disable" edilmelidir. Böylece saldırganın cihazın boş portuna girip ağa ulaşması engellenmiş olmaktadır.

Switch'in port numarasına, cihazın MAC adresine veya kullanılan protokole göre dinamik VLAN ataması uygulanarak cihazların VLAN ve IP bilgileri tek noktadan kontrol edilebilmekte ve daha güvenilir ağ yapısı oluşturulmaktadır. Böylelikle sadece kayıtlı MAC adreslerine sahip cihazlar izin verilen ağlara ulaşabilmektedir.

Ağ güvenliği sadece bir güvenlik duvarı (*firewall*) alınarak sağlanamaz. Ağ Güvenliği Yönetimi'nin her zaman devam eden bir süreç olduğu unutulmamalıdır.

Ağa bağlı her elemanın güvenliği belirli seviyelerde sağlanmalı ve sistem devamlı kontrol altında tutulmalıdır. Bu bildiride ağ trafiğinin üzerinden aktığı ağ cihazlarında alınması gereken temel güvenlik önlemleri ele alınmış ve ipuçları verilmiştir.[20] Are there Vulnerabilites in VLAN Implementations?, VLAN Security Test Report, David Taylor, 2000

web: http://www.sans.org/newlook/resources/IDFAQ/vlan.htm

ÜÇÜNCÜ BÖLÜM

3. INTERNET, TCP/IP PROTOKOLLER VE KABLOSUZ KİŞİSEL ALAN AĞLARI

3.1 Internet Nedir?

Internet tam anlamıyla ağlar arası ağdır. Internet, büyük küçük binlerce ağın birleşmesinden oluşmuş en büyük ağdır. Internet'e belli bir protokole sahip olan her türlü bilgisayar bağlanabilir.

Internet kavramı aslında bir savaş sırasında düşünülen basit bir projeden ibaretti. İlk başlarda şimdiki amacından uzaktı ve ülkeler arası bilgiyi paylaşım ortamı olabileceğini kimse aklına getirmiyordu. DARPA'nın (Defence Advanced Research Project Agency) 1969 yılında başlattığı bir projeye dayanmaktadır. Bu proje büyük bilgisayarları birbirine bağlamayı ve olası bir savaşta, ne olursa olsun bu ağın kopmamasını, bilgisayarlara arası haberleşmenin bir şekilde sağlanmasını amaçlıyordu. İlk bağlantı dört bilgisayar arasında gerçekleştirildi. Bunlardan üç tanesi Kaliforniya, bir tanesi de Utah'da idi. Yavaş yavaş bu ağa üniversitedeki bilgisayarlar da bağlandı ve ağ giderek büyümeye başladı. Gelecekte sorun çıkmaması için ortak bir protokol geliştirme çalışmalarına başlandı.

Bu proje aha sonra ARPANET(Advanced Research Projects Agency NETwork) adını aldı. Ağa akademik kuruluşların yanı sıra sivil kişi ve kuruluşlar da bağlandı. Silahlı kuvvetler, eğitim kurumları ve özel kişi ve kuruluşların yararlandığı bu dev ağ Amerika'yı kapsamaya başladı. Beklenenden fazla büyüme sonucunda askeri bölümün ayrılması kararlaştırıldı ve MILNET denilen bölüm ayrıldı. Tüm bu bölünmelerin sonucunda birbirinden ayrı fakat aralarında bilgi alış verişi süren bir sistem düşünüldü ve böylece 1983 yılında IP (Internet Protocol) kavramı kabul edildi. Internet'e bağlanan her bilgisayar bu protokolü kabul etmek zorundaydı.

ARPANET'e giderek küçük ağların ve diğer kullanıcıların da bağlanması sonucu istekler artıyordu. Bunun üzerine NSFNet(National Science Foundation) duruma el attı ve beş süperbilgisayarı devreye soktu. Bu bilgisayarlar kullanıcılardan isteklerini alıyor, bu bilgileri kullanıcılar için araştırıyor ve bulduğu bilgileri tekrar kullanıcılara geri aktarıyordu. Bir süre sonra bunlar da yetersiz kalınca ARPANET resmen

kullanımdan kaldırıldı ve ARPANET'te geliştirilen TCP/IP(İletim Kontrol Protokolü/Internet Protokolü) geliştirildi ve Internet'te halen kullanılmaktadır.

3.2. TCP/IP ve PROTOKOLLER

3.2.1 TCP/IP Protokolü

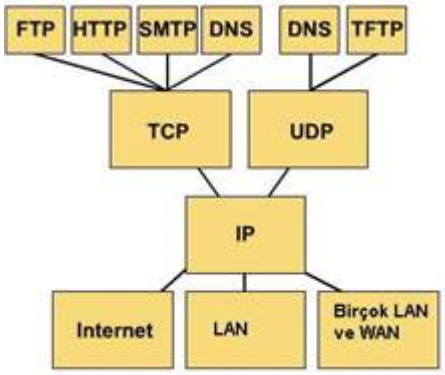
TCP/IP, her geçen gün değişen, gelişen ve içinde birçok ağlararası iletişim (internetworking) protokolleri barındıran bir protokol yığınıdır. Amerikan Savunma Bakanlığı tarafından nükleer savaş durumunda bile çalışabilecek bir sistem olarak tasarlanmıştır. Daha çok akademik ortamlarda geliştirilen bu protokol, firmalardan bağımsız olduğu için dünya çapında farklı sistemler arasında iletişim için (yani Internet'te) en yaygın kullanılan protokoldür. TCP/IP, Internet'i yaratan protokoldür dersek yanlış olmaz. TCP/IP Protokol yığıtı, OSI modelin 7 katmanına karşılık gelen 4 katmandan oluşmaktadır:

- Uygulama: OSI'nin son üç katmanlarına (5-6-7) karşılık gelir.
- Transport: Güvenilirlik, akış (flow) kontrolü ve hata düzeltme gibi servis kalitesini belirleyen parametrelerle uğraşır. Bağlantılı (TCP) ve bağlantısız (UDP) servisleri içerir.
- Internet: Amaç izlenen yollardan ve ağlardan bağımsız olarak hedef cihaza veri iletiminin sağlanmasıdır. Yol (path) belirleme ve veriyi o yola yönlendirmek (routing) için paket anahtarlama bu seviyede yapılır. IP protokolü kullanılır.
- Network Access: OSI'nin ilk iki katmanına (1-2) karşılık gelir.

TCP/IP'de yaygın olarak kullanılan protokoller yandaki protokol grafiğinde verilmiştir. Uygulama seviyesinde bir ağ ortamında sıkça rastlayacağımız protokoller belirtilmiştir:

- FTP - File Transfer Protocol (Dosya Transfer Protokolü)
- HTTP - Hypertext Transfer Protocol (Çoklu Metin Transfer protokolü)
- SMTP - Simple Mail Transfer Protocol (İleti Transfer Protokolü)

- DNS - Domain Name System (Alan Adı Sistemi)



Şekil 15: TCP/IP Protokolü

TCP/IP modelinin Internet'i yaratan bir standart olması ve bir çok protokolü bünyesinde bulundurması onu daha popüler yapmaktadır. OSI modelin özellikle ağ temellerinin eğitiminde bir rehber olduğu unutulmamalıdır.[21] CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP),

web: http://www.cert.org/advisories/CA-2002-03.html

3.2.2 IP Protokolü ve IP Adresleme

Internet Protokolü (IP) bir ağda uçtan uca (end-to-end) veri yönlendirmesi için kullanılır. IP tanımlamaları 1982 yılında RFC 791'de yapılmıştır. Bu tanımlamalar IP adreslerinin yapısını da içerir. Şu an dünyada yaygın olarak IPv4 (IP version - sürüm 4) kullanılmaktadır. Bu yapı Internet üzerindeki herhangi bir cihaza (makine veya yönlendirici arayüzüne) 32 bit mantıksal adres sağlar. IPv6'nın tanımlamaları da tamamlanmak üzeredir. IPv6, daha büyük bir adres uzayı (128 bit adres) ve verilerin şifrelenerek gönderilebilmesi gibi daha gelişmiş özelliklere sahiptir.

Bir IP adresi aralarında nokta bulunan 0-255 arasında değerler alabilen 4 adet ondalık değerden oluşur. Her ondalık değer 8 bittir ve bir "octet" denir. Örneğin: 131.108.122.204

IP adresleri ağ adresi ve cihaz (host) adresi olmak üzere iki kısımdan oluşur. Örneğin ev adresimiz gerçek hayatta "Bağdat Caddesi 54 numara" olsun. Ağ adresini sokak adresimize (Bağdat Caddesi), cihaz adresini de ev numaramıza (54 numara) benzetebiliriz.

IP adresleme standardının ilk tanımlamalarında IP adres sınıfları bulunmamaktaydı ama yönetim kolaylığı açısından bu sınıflara ayırma sonradan eklenmiştir. Adres sınıfları aşağıdaki gibidir:

- **A Sınıfı:** Sınırlı sayıda bulunmaktadır, çok büyük ağlar için ayrılmıştır. A sınıfı IP adresi kullanılan bir ağda, 2^{24} -2 yani 16,777,214 adet IP addresi cihazlara tanımlanabilir.

- **B Sınıfı:** Daha fazla sayıda bulunmaktadır, orta büyüklükte (intermediate-sized) ağlar için ayrılmıştır. B sınıfı IP adresi kullanılan bir ağda, 2^{16} -2 yani 65,534 adet IP addresi cihazlara tanımlanabilir.

- **C sınıfı**: Çok fazla sayıda bulunmaktadır, küçük ağlar için ayrılmıştır. C sınıfı IP adresi kullanılan bir ağda, 2^{8} -2 yani 254 adet IP addresi cihazlara tanımlanabilir.

- **D sınıfı:** Çoğa gönderim - Multicasting (Tek veri gönderimi ile birden fazla cihazın verilen iletileri alması) için ayrılmıştır.

- **E sınıfı:** Deneyler ve araştırmalar için ayrılmıştır.

A sınıfı adresler artık kalmamıştır. B sınıfı da bulmak çok zordur. C sınıfı adresler günümüzde RIPE'den veya Internet Servis Sağlayıcılar (ISP) gibi aracı kuruluşlar tarafından temin edilebilir.

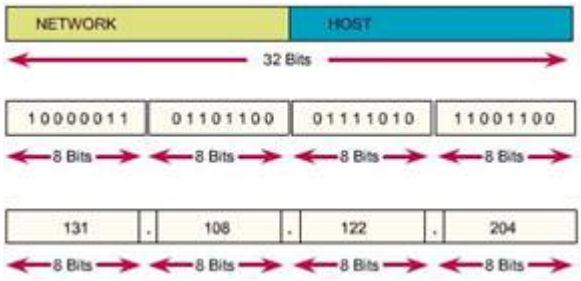
Özel adresler, Internet'e bağlanmayan, NAT (Network Address Translation) veya proxy sunucusu aracılığı ile Internet'e bağlanan cihazlarda kullanım için ayrılmıştır. Bu adresler aşağıda belirtilmiştir:

- 10.0.0.0 – 10.255.255.255

- 172.16.0.0 – 172.31.255.255

- 192.168.0.0 – 192.168.255.255

Bir IP sınıfı ağı daha iyi yönetmek için IP adresini satın alan kuruluş tarafından küçük parçalara ayrılabilir. Buna da "IP subnetting" denmektedir. [22]**Çelik, Kaan Güneş, Çetin, Görkem,** a.g.e.



Şekil 16: IP Adresi

3.2.3 World Wide Web (WWW)

Web'i Internet'in kimliğini bulamasını sağlayan başlıca olgulardan birisi olarak düşünebiliriz. Web yardımıyla diğer tüm protokollere bağlanabilir, bir arayüz yardımıyla tüm Internet servislerine ulaşabiliriz.

Internet'te yer alan bilginin sınırı yok. Bu bilgi deposuna HTTP protokolü yardımıyla erişebilir ve faydalanmak istediğimiz bilgileri kendi amaç doğrultusunda kullanabiliriz.

Web sistemi bir istemci (client) ve bu istemcinin bağlandığı bir sunucudan ibarettir. İstemcilere örnek olarak Netscape ve Internet Explorer'ı örnek gösterebiliriz. Evinden veya iş yerinden Web tarayıcı yardımıyla bir Web sayfasına bağlanarak sayfanın içeriğini görebiliriz. Sunucu ise istenen Web sayfasını tarayıcıya göndermekle yükümlüdür.

Web'de kullanılan dokümanlar büyük oranda .html veya .htm uzantılıdır. Bu tür dokumanlar HTML dilinde yazılmış kod satırları içerirler. İstemci dokumanı alır, işler, belli bir yapıda kullanıcının önüne getirir.

HTML belgelerinin diğer özelliği de hypertext yani doküman içinde ses, görüntü, veya başlı başına bir program Java, Java Script gibi, bulunabilme özelliğidir. Java Web tarayıcı makine üzerinde çalışır. Yani siz Web sayfasına bağlandığınız zaman Netscape, Internet Explorer kullanıyorsanız Internet Explorer Java programını yükler ve bilgisayarınız bunu otomatik olarak çalıştırmaya başlar. PHP bir script dilidir ve PHP ile yazılan kodlar bir editörde yazılıp PHP uzantılı dosya olarak kaydedilir. PHP ile yazılan dosyalar derlenmezler (compile edilmezler). Sadece Web Server'da bu

dilde yazılmış scriptleri yorumlayabilecek bir PHP yorumlayıcı program mevcuttur. İstemci(Client) tarafından PHP dosyası bir tarayıcı (browser) ile çağrılır. ASP'nin açılımı Active Server Pages şeklindedir. ASP bir programdır ve IIS içinde çalışır. IIS'in açılımı Internet Information Services'dır. ASP dosyası server üzerinde çalıştırılır.[23] **Çölkesen, R., a.g.e.**

3.3 Kablosuz Kişisel Alan Ağları

Kablosuz Kişisel Alan ağları, Bluetooh ve HomeRF gibi standartların son yıllarda duyurulması ile popülerlik kazanmış ve uygulama alanı bulmuşlardır. Genel olarak bu teknolojiler, küçük bilgi cihazları veya elektronik ev aletlerinin birbirleri ile kablo olmadan haberleşebilmelerine olanak tanımaktadırlar.

3.3.1 Bluetooth

Onuncu yüzyılda ayrı krallıkları birleştirmeye çalışmış olan Danimarka krallarından birinin adı ile anılan Bluetooth, taşınabilir bilgisayarlar, modemler, kameralar, LAN erişim cihazları, telefonlar ve PDA'lar gibi elektronik cihazlar arasında veri iletimi için kısa mesafeli radyo bağlantısının sağlanması için teşkil edilen endüstri konsorsiyumunun adıdır. Bluetooth ayrıca ses iletimini de desteklemektedir.

HomeRF'in aksine Bluetooth yukarıda sıralanan bilgi cihazları arasında kablo yerine kullanılacak noktadan noktaya *(Kim durumlarda noktadan çok noktaya)* bir arayüz oalrak düşünülebilir. Bluetooh bir "Piconet" *(Bluetooh cihazlarının oluşturduğu mini ağ)* içinde sekize kadar cihazı desteklemektedir. Bluetooth güncel birçok kablosuz ağ teknolojisi gibi 2.4 GHz ISM bandını kullanmaktadır.[24] **Kaplan, Y.,** a.g.e.

Frekans Aralığı	2402 - 2480 MHz
Veri Oranı	1 Mbps
Kanal Bandgenişliği	1 MHz
Mesafe	10 metreye kadar ancak genişletilebilir
RF atlama	1600 kez/s
Kriptolama	GSM gibi, cihaz ID ve 0/40/64 bitlik anahtar uzunlukları
TX Çıkış Gücü	Azami 20 dBm *(0.1W)*

Tablo 1: **Bluetooth Genel Özellikleri**

3.3.2 HomeRF

Mart 1998'de Home Radio Frequency Working Group *(HRFWG)*, evde kullanılan tüketici elektronik cihazların kablosuz bir ortamda haberleşebilmesini sağlayacak Shared Wireless Access Protocol *(SWAP)*'ü duyurdu. Bu standart yine 2.4 GHz ISM bandında çalışmaktadır. Yine Bluetooth gibi kablo yerine kullanılabilecek bir arayüz gibi düşünülebilir. HomeRF, Bluetooth gibi kaliteli ses iletimini desteklemektedir.[25]

Kaplan, Y., a.g.e.

Frekans Aralığı	2402 - 2480 MHz
Veri Oranı	2 Mbps *(4FSK)*
Kanal Bandgenişliği	1 MHz
Mesafe	100 metreye kadar
RF atlama	50 kez/s
Kriptolama	Blowfish
TX Çıkış Gücü	Azami 20 dBm *(0.1W)*

Tablo 2: **HomeRF Genel Özellikleri**

3.3.3 Güvenlik

Kablosuz ağlarda güvenlik üzerinde en çok durulması gereken konulardan biridir. Genel olarak radyo işaretlerinin havadan iletilmesi bu işaretlerin izlenebilmesini ve takip edilebilmesine olanak sağlamaktadır. Noktadan noktaya mikro dalga iletim sistemleri izlenmesi çok zor bir haberleşme yöntemidir ancak noktadan çok noktaya iletimler teknik açıdan izlenmesi daha kolay bir haberleşme türüdür. Bu tür sistemlerde dahili kriptolama özellikleri mevcut olmasında rağmen son yıllarda yapılan çalışmalar bu tür sistemlerin saldırıya sanıldığından daha zayıf olduğunu göstermiştir. Güvenliği artırmak için en basit yaklaşım VPN teknolojilerinin *(IPSec veya TLS)*, kablosuz haberleşme sistemleri ile birlikte kullanılmasıdır ancak bu yaklaşım maliyetlerin artmasına neden olmaktadır.

Her ne kadar dağıtık spektrum kullanan kablosuz sistemler teoride güveli gibi görünseler de, dağıtma desenleri çok sınırlı olduğundan bunları tahmin etmek ve izlemek kolaydır. Öte yandan HomeRF'de dağıtma deseni frekans atlamalarında uçbirimlere iletildiğinden, bu işareti yakalayarak trafiği izlemek mümkündür.

Kablosuz LAN'lerle ilgili başka bir sorunda ISM bandlarında işletilen farklı teknolojilerin aynı anda işletilmesinde ortaya çıkmaktadır. Aynı frekans bandında *(Çoğunlukla ISM)* işletilen radyo iletim sistemleri birbirlerinin performanslarını

olumsuz bir şekilde etkilemektedirler *(Bluetooth ve 802.11 gibi)*. Bu yüzden kablosuz ağlar tasarlanırken istasyon yerleşimlerine çok dikkat edilmelidir.

Kablosuz erişim teknolojileri kuşkusuz önümüzdeki yıllarda özellikle veri iletimi konusunda daha yaygın olarak kullanılacaklardır. Ayrıca, daha yüksek veri iletim oranları sağlayacak yeni nesil hücresel telefon sistemleri de bu ortamlardaki uygulamaların sayısı ve çeşidi hızla artacaktır.

Şu anda kablosuz veri iletim sistemlerinin en büyük rakibinin DSL sistemleri olduğu görülmektedir. Ancak, çoğu yerde altyapının yetersiz olması ve genel olarak Telekom firmalarının bakır altyapılarına yatırım yapmada isteksizlikleri kablosuz iletim sistemlerinin pazarda yükselmesini sağlayacaktır.

Altyapıda kullanılacak kablosuz iletim teknolojisi seçilirken, ölçeklenebilirlik ve güvenlik göz önünde bulundurulmalıdır.[26] **Kaplan, Y.,** a.g.e.

DÖRDÜNCÜ BÖLÜM

4. BEYKENT ÜNİVERSİTESİ NETWORK YAPISI VE PLANLARI

4.1 Beykent Üniversitesi Network Yapısı

4.1.1 Altyapı Teknolojisi

Geniş bir alana yayılmış olan Beykent Üniversitesi kampusu, eğitim ortamında en verimli ve hızlı veri haberleşme ortamını sağlayabilmek amacıyla, güçlü bir altyapı ile donatılmaya çalışmaktadır. Altyapıyı oluşturan, kablolama, aktif cihazlar ve kampus Internet bağlantısı, kullanıcı sayısı ve yükün artması durumlarında da gereksinimleri karşılayabilecek şekilde tasarlanmayı amaçlamaktadır.

4.1.2 Kablolama

Ağ oluşturmada birinci aşama olan kablolamada önce CAT5 sistemi kullanıldı daha sonra ise CAT6'ya geçildi. En son olarak CAT7 kablosu kullanıldı. Kabloların kategorilere ayrılması gönderdikleri veriyle ilgilidir. CAT5'le saniyede 100 Mps data, CAT6'yla 1000 Mps, CAT7 ile 2000 Mps data gönderilir. Kablo şekilleri de birbirinden farklıdır. En ucuzu CAT5, en pahalı sistem Fiber'dir. Beykent'te CAT5, Maslak'ta CAT6 kullanıldı.

Kampus aktif ağ birimleri (Yönlendiriciler, swicth....vb) arası haberleşme olanağını sunan CAT6 kablolarla gerçekleştirilmiştir. Aktif cihazlar arası bağlantılarda bakır kablolar kullanılmamıştır. Kampus içerisinde üç merkezi nokta yerel ağ omurgasını oluşturmak amacıyla tüm kampus binalarından gelen kabloların kesişim noktaları durumundadırlar. Her bir kampus binası, bu merkezi noktalara olan uzaklığına bağlı olarak CAT6 kablo ile her üç merkeze birden bağlıdır.

Kullanıcı bilgisayarları CAT-5 standardındaki bakır kablolar ile kablo hızında haberleşme olanağı sunan aktif cihazlara bağlanmaktadır. CAT-5 standardı bakır kablolar üzerinden 100 Mbps kapasitelere destek verebilmektedir.

4.1.3 Yerel Ağ

Kampus yerel ağı 2 Mbit'lik bir omurga üzerinden, hızlı yönlendirici cihazlar ile, tüm kullanıcılara hızlı ve sürekli haberleşme ortamı sağlamaktadır.

Haberleşmede sürekliliği ve hatlar üzerinde yük dağılımını gerçekleştirebilmek için, kampus binaları 2Mbit'lik CAT5 hatlarla yerel ağ omurgasına ve oradan da Internete bağlanmıştır. Yerel ağ üzerinde oluşturulan sanal ağlar (VLAN) ile kampus binaları arası trafikler birbirlerinden ayrılmış ve gerçek hat değerleri üzerinden haberleşme ortamı sağlanmıştır.

Kampus yerel ağı 2Mbps kapasite ile Taksim'de bulunan iletişim merkezine bağlıdır.

Beykent Üniversitesi'nde 7 Switch bulunmaktadır. Switch'ler merkezde olmalı. Çünkü 80 metreden sonra veri kaybolabilir. Ondan sonra sorunlar oluşur. Merkezdeki Switch'e (Backbone) gelir.

Beykent'te öğrenci ve personel birbirinden tamamen ayrılır.Ama sanal olarak aynı Switch'e takılır. Ayazağa Kampüsü 5 kattan oluşmaktadır. Ayazağa'da her katta Switch dolabı bulunmaktadır. Sistem odası 2. kattadır. Beş kattaki Switch'ler Sistem odasındaki Patch Panel'e gelmektedir. Buradan da Omurgaya (Backbone) gelmektedir.

Laboratuarlarda Switchler var. Personel Switchleri var. Hepsi sistem odasına gelir. Bunlar sanal olarak Omurga'da (Backbone) ayrılır. Bu sayede öğrenciler ve akademi birbirlerine ulaşamıyor.

4.1.4 Sunucular:

- Mail- Örenci ve personel mailleri bu sunucuda tutulmaktadır. İşletim sistemi olarak Linux kullanılmaktadır.
- WEB- Okulun Web'i ve Öğrencilerin Web'i var. Öğrencilere 10 Mb hak verilmiş. İşletim Sistemi Linux'tur.
- DNS- Ağ üzerindeki veri alış verişi tamamen 193.140.183.4 gibi sayısal adreslerle gerçekleştirilir. Ancak kullanıcı düzeyinde, sayısal IP adresleriyle uğraşmak, onları akılda tutmak, hatırlamak güç olur.

Bu nedenle kullanıcı düzeyinde simgesel adresler kullanılmıştır. Örneğin 193.140.183.4 beykent.edu.tr'ye tekabül etmektedir. DNS (Domain Name Server) kullanıcı düzeyinde verilen simgesel adreslerin sayısal karşılığını bulmak için kullanılan bir sistemdir. DNS'in bir tablosu vardır ve burada sayısal adres/simgesel adres çiftleri tutulur. Beykent Üniversitesinde işletim sistemi olarak Windows Server kullanılmaktadır.

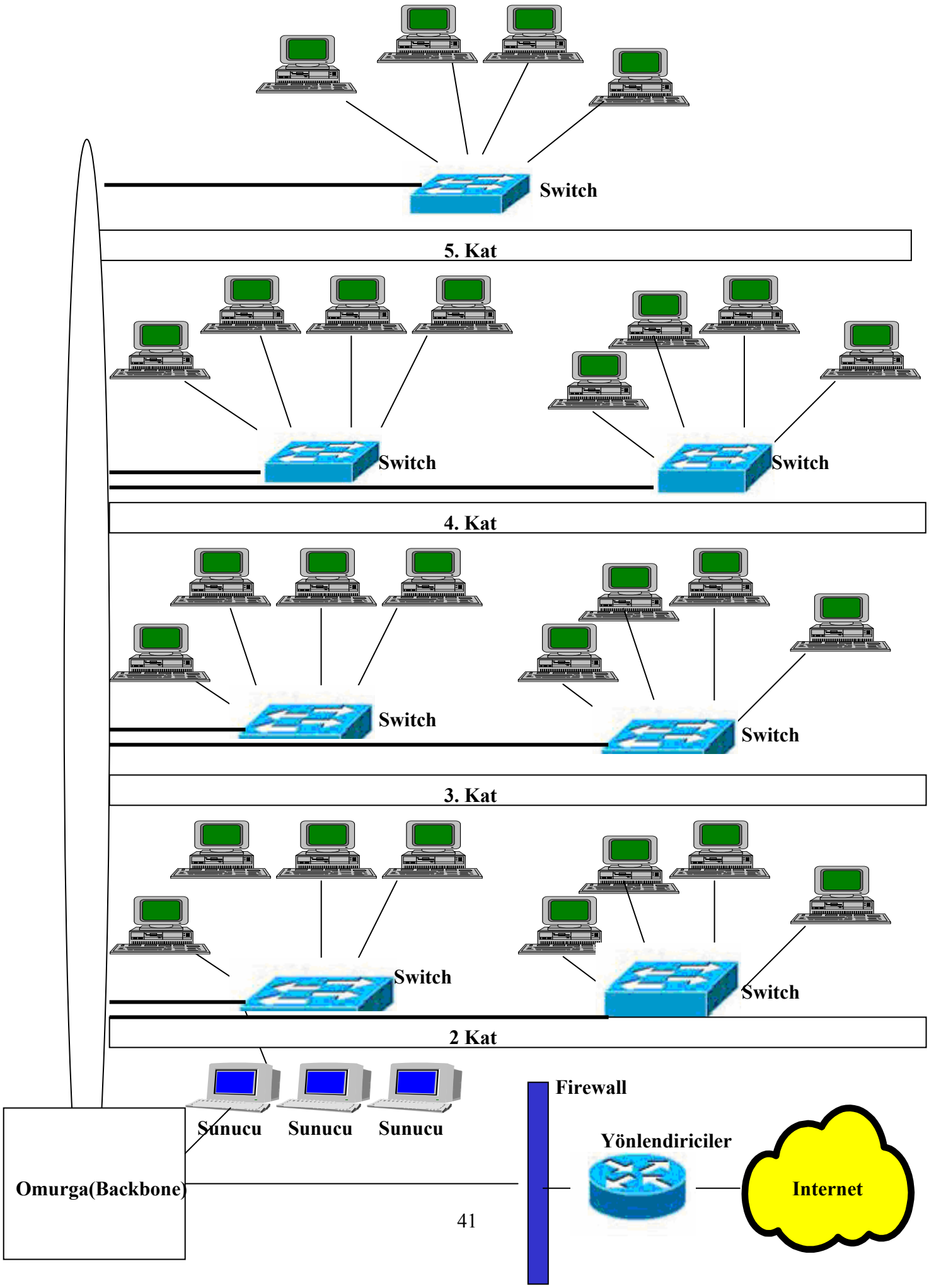
- Kütüphane- Kütüphane programının kurulu olduğu sunucudur. Şu an YORDAM adında program kullanılıyor. İşletim sistemi 2003 Server'dır.

- Öğrenci İşleri için application Server bunda Linux kurulu ve Database Server fakat bu aktif değil bunda da Linux kurulu.

- Active Directory- 2003 Server. Kullanıcıların şifreyle login olmalarını sağlıyor ve makine sistemine dokunmaması için kullanıcılara bazı kısıtlamalar getiriyor.

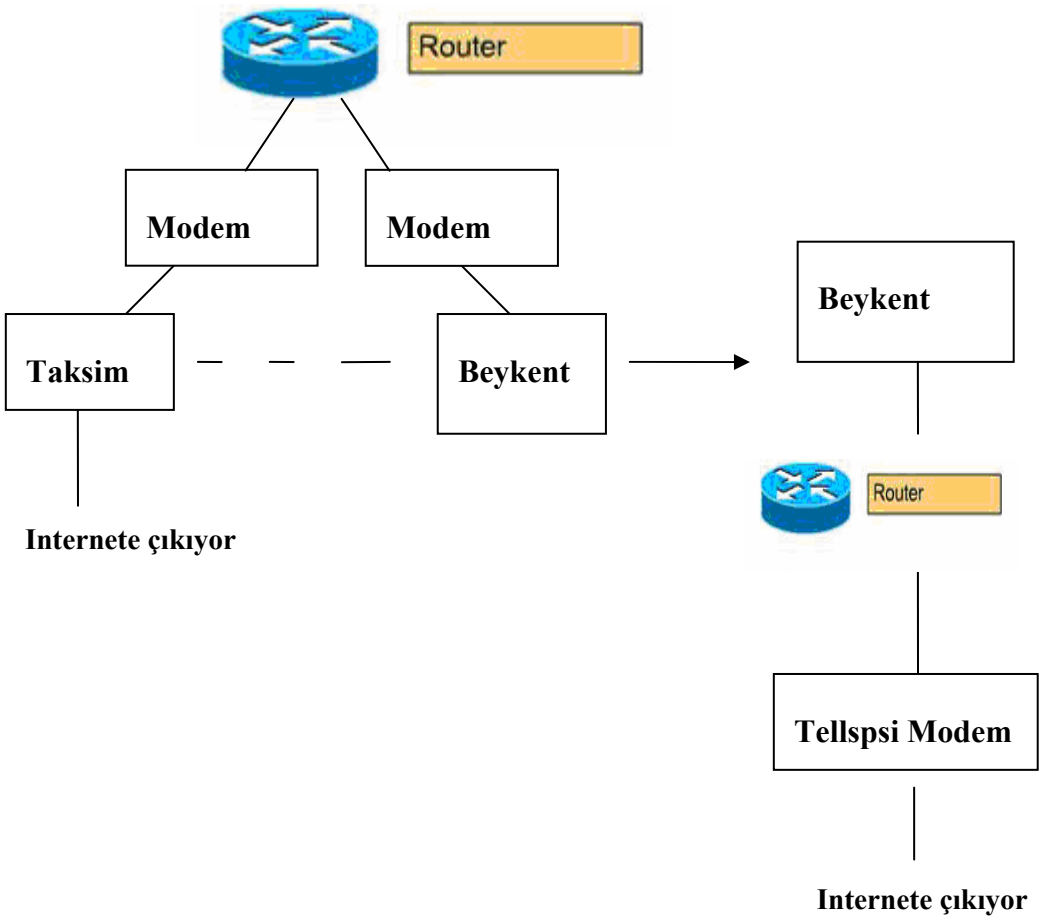
- Backup- Personelin yedeklerinin tutulduğu sunucudur. İşletim sistemi 2003Server'dır.

4.1.5 Şekil 17: BEYKENT ÜNİVERİSTESİ NETWORK YAPISI



4.1.6 Internet'e Nasıl Çıkılıyor?

ISP olarak Ulaknet kullanılmaktadır. Ulaknet üniversiteye 2 Mbit leaseline kullanım hakkı tanımıştır. 3600 serisinden Cisco Yönlendiriciler bulunmaktadır. 2 tane de Tellaps markalı Modemler vardır.

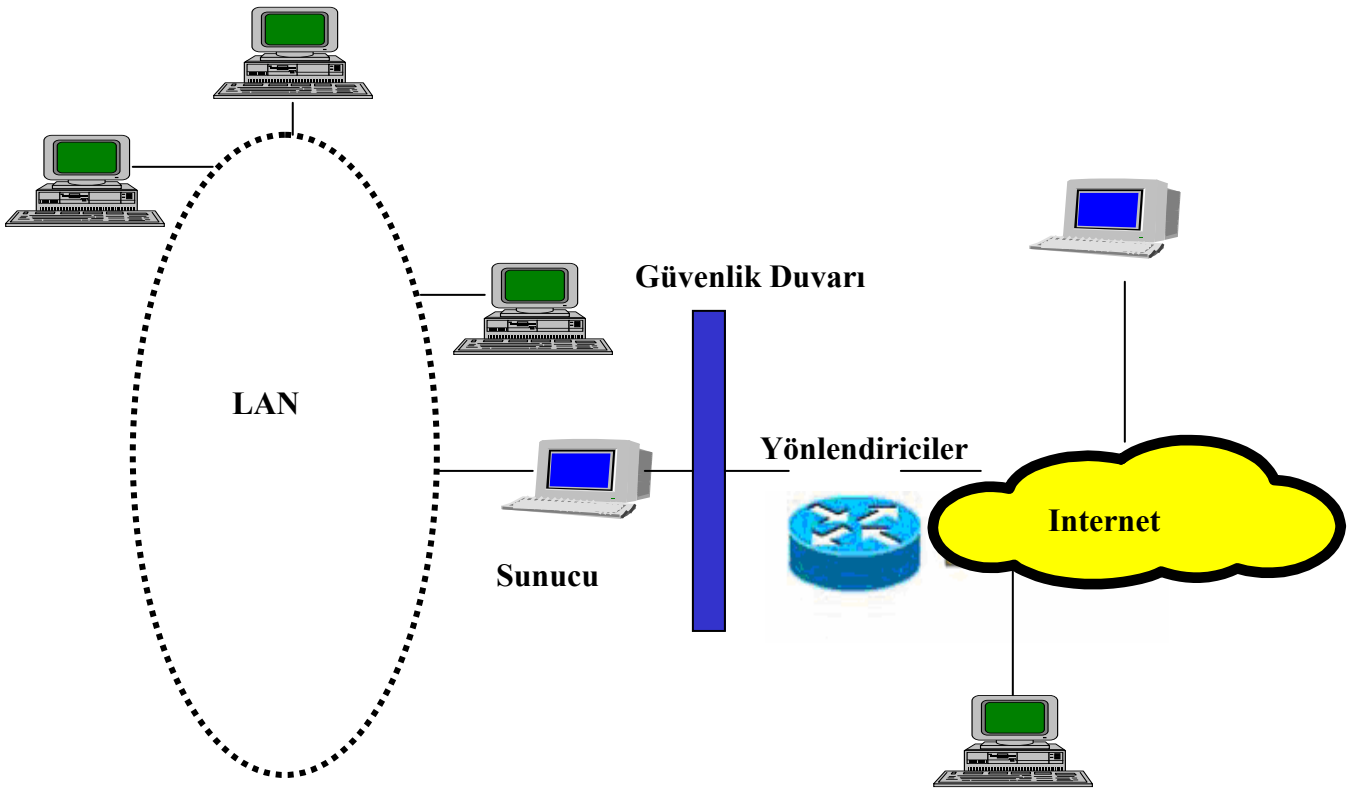


Şekil 18: Internet'e Çıkış

4.1.7 Güvenlik:

Beykent Üniversitesinin güvenliği Firewall(Güvenlik Duvarı) ile sağlanmaktadır. Tellapsi Modem'den gelen hat Firewall'a geliyor. Firewall'dan backbone Switch'e geliyor. Diğer sunucular da Backbone'a bağlı bulunmaktadır. Firewall ve sunucularda Anti-virus programları kurulmuştur. Güvenlik Duvarı özel ağ ile Internet arasına konan ve istenmeyen erişimleri engelleyen bir sistemdir.; bununla ağ güvenliği sağlanmaya çalışılır ve erişim hakları düzenlenir. Güvenlik duvarının sistem üzerinde tam olarak etkili olabilmesi için, ağ ortamı ile Internet arasındaki tüm trafiğin güvenlik duvarı üzerinden geçirilmesi gerekir.

Güvenlik duvarının tercih edilmesi için en büyük nedenlerden biri de adres dönüşüm (NAT, Network Adress Translation) özelliğidir. Sadece tek bir IP adresi ile tüm ağ kullanıcıları Internet'e çıkabilir ve yerel ağ ortamındaki IP adresleri tamamen Internet ortamından yalıtılmış şekilde kullanılabilir.



Şekil 19: Güvenlik

4.1.8 Servisler

4.1.8.1 Ağ Erişim Servisleri

4.1.8.1.1 IP (Internet Protocol) Ataması ve Yönetimi: Kullanıcı bilgisayarları bağlandıklarında IP numaraları otomatik olarak DHCP (Dynamic Host Configuration Protocol) sunucusundan sağlanmaktadır. Yaklaşık 15 farklı altağı olan yerel ağda gezici kullanıcılar bilgisayarlarında hiç bir ayarlama yapmadan dolaşabilmektedirler.

4.8.1.1.2 Alan Adı Servisleri (DNS): Alan adı servisi, Üniversite sunucularına ve kullanıcı PC'lerine alan adı tahsisini yapmanın yanında kullanıcıların Internet erişimlerinde alan adı-IP dönüşümlerinin gerçekleştirilmesini sağlar. DNS servisi iç ve dış olmak üzere iki tanedir.

İç DNS servisi kampus içerisinden yapılan bağlantılarda iç IP numaraları ile alan adlarını eşleştirir. Hizmet veren sunucuların yanında, SU-Net'e bağlanan her kullanıcı bilgisayarı için de DNS kaydı otomatik olarak gerçekleştirilmektedir. DHCP sunucusundan IP alan her bilgisayar için kullanıcı adı ile başlayan bir DNS kaydı yapılmaktadır. (kullanıcıadı.beykent.edu.tr gibi)

Dış DNS servisi ise Üniversite'nin Internete açık sunucularının IP adreslerine isim tahsisi yapmaktadır.

4.1.8.2 Vekil (Proxy) Sunucu Servisi: Vekil sunucu kullanıcıların ziyaret ettikleri Web sitelerini geçici olarak depolayarak, daha sonraki erişimleri hızlandırmaktadır.

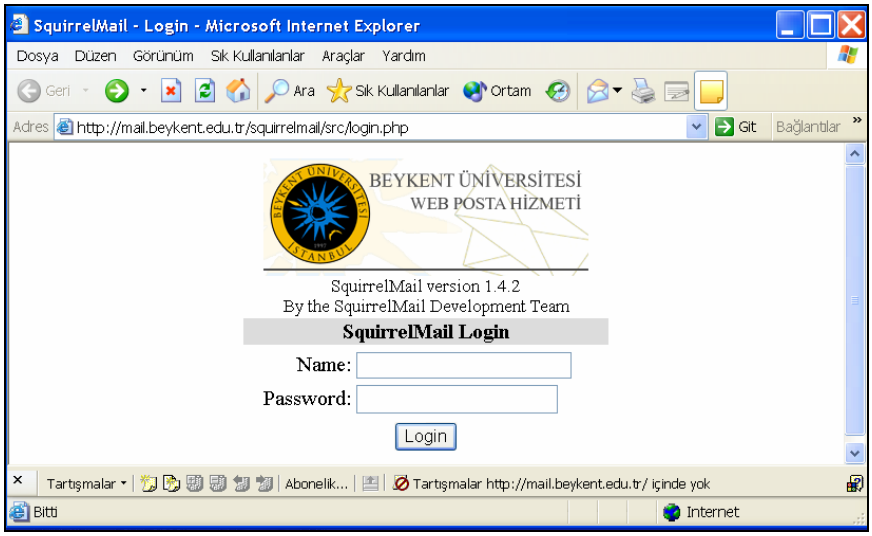
4.1.8.3 E-Posta (E-Mail)

E-Posta Servisi, bir bilgisayar ağında kullanılabilecek pratik ve hızlı bir haberleşme şeklidir. Bir ağdan diğerine e-posta yardımıyla haberleşmek için elektronik postayı gönderecek ve alacak bir yazılıma ihtiyacınız var. Bir e-posta mesajında gönderenin kimliği, adresi, mesajın konusu, içeriği gibi bilgiler bulunur. Doğaldır ki bu mesajın içinde yollanması gereken adres de olmalıdır.

E-postalar sadece metin tabanlı mesajları göndermek üzere programlanmamışlardır. Kullanıcı kendine ait bir fotoğrafı, bir ses kaydını, hatta hareketli görüntyü dünyanın herhangi bir köşesindeki arkadaşına ulaştırabilir. Bu işlemleri MIME standartları yardımıyla gerçekleştirir.

E-posta göndermek için en çok kullanılan yazılımlar Netscape, Internet Explorer gibi Web tarayıcılarıdır.

Tüm akademik, idari personel ve öğrencilerin bir e-posta adresi bulunmaktadır. Elektronik haberleşme sistemlerinin yoğun olarak kullanıldığı kampus eğitim ortamında e-posta adeta kampus yaşamının ayrılmaz bir parçası haline gelmiştir. Ayrıca kullanıcıların her zaman, her yerden mesajlarına erişebilmeleri amacıyla Web üzerinden e-posta okuma ve gönderme (webmail) olanakları sağlanmaktadır.



Şekil 20: Beykent Üniversitesi Webmail

Sunucular için yoğun iş yükünü kaldıracak güçlü donanımlar üzerindeki LINUX platformları tercih edilmiş ve kurulduğu günden beri e-posta haberleşmesinin kesintisiz işlemesi sağlanmıştır.

4.1.8.4 Web Servisleri

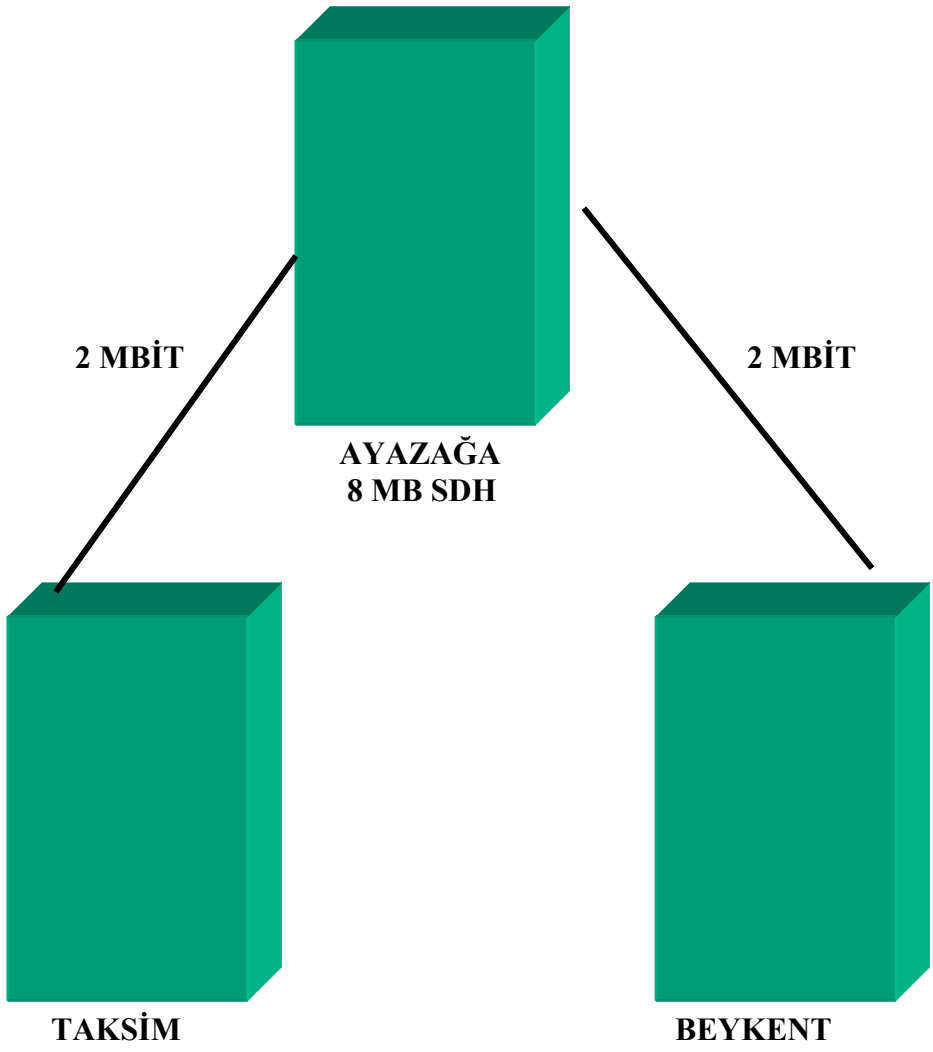
İç ve dış kullanıma hizmet eden iki adet ana web sitesi bulunmaktadır.

4.1.8.4.1 Dış Web Sitesi: (www.beykent.edu.tr) Üniversite'nin Internetten görünen sayfalarını barındırır ve ziyaretçilere birimler, fakülteler ve faaliyetler hakkında güncel bilgileri sunar.

Şekil 21: Beykent Üniversitesi Web Sayfası

4.1.8.4.2 Kişisel Web Sayfaları: Tüm kullanıcıların kişisel Web sayfalarını hazırlama olanağı bulunmaktadır. Bu olanak sayesinde kullanıcılar kendilerine ayrılan alanlara yükledikleri sayfalar ile kendilerini tanıtabilecek web sitelerini hazırlayabilirler.

4.2 Beykent Üniversitesi'nde Network Planları:



Şekil 22: Network Planları

Network merkezi Ayazağa olacak. Cisco Yönlendiriciler yerine SDH Yönlendiriciler kullanılacak.

Ulaknet'ten 8 Mbit kullanma hakkı alınacak. Fiber Kablo kullanılacak. 4 Mbit Ayazağa kullanacak, 2 Mbit Taksim ve 2 Mbit Beykent Kampüsü kullanacak. Merkezde Yönlendiriciler 3600 ve 2 Modem olacak. Her kampüste Yönlendiriciler ve Modem olacak.

- CAT7 Kablolama sistemi kullanılacak,
- Switchler alınacak,
- Sistem Odası Beykent'ten Ayazağa'na gidecek,
- Bina tamamen kablosuz ağ (Wireless) olacak.

4.2.1 Niçin Kablosuz ?

Kablosuz yerel ağ yardımıyla kullanıcılar kolayca kaynaklara ulaşabilecek, ağ yöneticileri ise kablo döşemeden ya da yer değiştirmeden ağ kurabilecek veya mevcut ağda değişiklik yapabileceklerdir.

Kablosuz yerel ağların, geleneksel yerel ağlara karşı üstünlükleri şunlardır:

- **Mobilite :** Kablosuz yerel ağlar ağ kullanıcılarına şirketlerinin hangi noktasında olursa olsunlar, hareket halinde dahi gerçek zamanlı bilgi erişimi sağlar.
- **Kurulum Hızı ve Basitliği :** Kablosuz yerel ağ sistemleri kurulumu hızlı ve kolaydır, ayrıca duvar ve tavanlardan kablo çekme zorunluluğu da ortadan kaldırır.
- **Kurulum Esnekliği :** Kablosuz ağ teknolojisi kablolu ağın erişemeyeceği yerlere ulaşımı sağlar.
- **İleriye Yönelik Maliyet Kazancı :** Kablosuz ağ kurabilmek için ilk olarak harcanması gereken miktar kablolu bir ağdan daha fazla olmakla birlikte hayat evresi sarfiyatı çok azdır. Uzun vadeli kazançları, çok yer değiştirme gerektiren dinamik ortamlarda kendini belli eder.

Genişletilebilirlik : Yapılar kolaylıkla değiştirilebilir ve az miktarda kullanıcının oluşturacağı "peer to peer" ağ yapısından, binlerce kullanıcıya geniş bir yelpazeyi kapsar.[27] **Arbaugh, W. A., Narendar S., Y.C.** web: http://www.cs.umd.edu/~waa/wireless.pdf Justin War, 2001, "Your 802.11 Wireless Network Has No Clothes"

4.2.2 Diğer Planlar

- Santral yerine IP Telephoning Sistemi kurulacak. Bir santral kurmanın maliyeti 20-30 milyar arasında değişmektedir. Her telefon için telefon kablosu, ahize maliyeti bulunmaktadır. IP Telephoning'te ise kablolama masrafı bulunmaktadır. Network kablosu üzerinden olabiliyor. Her lokasyona bir numara atanacak. Örneğin Ayazağa 5, Beykent 6 ve Taksim 7 numarasını alacak.Beykent'ten Ayazağa aranmak istenirse 5102'yi çevirmek yeterli olacak. Yurt dışından herhangi biri Notebook'la ücret ödemeden kulaklık ve mikrofonla Internet bağlantısıyla Taksim, Beykent veya Ayazağa'yla görüşme yapabilecek. Görüldüğü gibi IP Telephoning'te sadece yatırım maliyeti bulunmkatadır.

- Diğer bir projede akıllı sınıfların oluşturulması. Laboratuarlarda iki tane kamera bulundurulacak. Biri Hoca ve biri de tahtayı görüntülemek için. Bütün bilgisayarlarda mikrofon ve kulaklık bulunacak. Diğer iki kampüstede de aynı sistem kurulacak. Konferans Sisteminde olduğu gibi diğer kampüslerden hatta farklı şehirlerden öğrenciler derse katılabilecek, gerektiğinde hocaya sorular sorabilecektir. Sınıfta anlatılan dersi görsel ve işitsel anlamda yedeklenmesini yapacak bir Backup ünitesine ihtiyaç bulunmaktadır.

- Kamera, Giriş Çıkış Sistemi: Bina girişlerinde minimum 4 tane olmak üzere turnikeler oluşturulacak. Bina içerisinde minimum 32 olmak üzere kamera sistemi ile Online olarak gözetilecek. Bunların maliyeti keşiften sonra ortaya çıkacaktır.

Belli noktaların giriş çıkış sistemleri dijital kart okuyucuları ile sağlanacaktır. Örneğin; Bilgi İşlem, Öğrenci İşleri, Genel Sekreterlik, Rektörlük, Yazı İşleri gibi.

Bu planları gerçekleştirmek için yaklaşık maliyetler şu şekilde hesaplanmıştır:

- Fiber Maliyeti: 8 Mbit Internet hattının Ayazağa Kampüsüne çekilmesi mesafeye göre fiber maliyeti değişmektedir. 4-5 Km mesafede maliyet

80.000 YTL'yi bulmaktadır. Bu yatırım bir sefere mahsus yapılacak bundan sonraki hız artırımlarında üret ödenmeyecektir.

- SDH Maliyeti: Hem Telekom hem de Ayazağa Kampüsü tarafına alınması gereken cihaz çift satılmakta ve maliyet 10.000-15.000$ arasında değişmektedir.

- Kampüslere yapılacak yatırım: Şu anda elde bulunan cihazlar yapılacak işlemler için yetersiz kalacağından değiştirilmesi gerekmektedir. 2 adet Cisco Yönlendiriciler 3700 serisinden maliyet 15.000$ seviyesindedir.

  Bunlar yapıldıktan sonra Telekom'a düzenli ödeme 8 Mb için 4500 YTL, 2 Mb hatlar içinse aylık (1500*2=3000 YTL) arasında bir ücrettir.

SONUÇ

Özellikle son yıllarda artan bilgisayar kullanımı ve karşılaşılan iletişim zorunluluğu bilgisayar ağlarının gelişimini doğurmuştur. Bilgisayar ağları, kullanıcıların başka bilgisayarlara veya diğer donanımlara kolaylıkla ulaşmasını sağlarlar, ekonomik olarak kazanç getirirler kişisel bilgisayarlar arasındaki bağlantıyı ve iletişimi sağlarlar. Globalleşmenin kaçınılmaz olduğu ve bireysel çalışmalar yerine takım çalışmasının ve iletişimin ön plana çıktığı günümüzde bilgisayar ağlarının önemi ve kullanımı her geçen gün artmaktadır.

Bu çalışmada, bir ağın nelerden oluştuğundan, komple ağın parametreleri olan LAN (Local Area Network- Yerel Alan Ağı), WAN (Wide Area Network-Uzak Alan Ağı) ve Şehirlerarası Bağlantıdan, bilgisayar ağlarının amaçlarından, bir ağ ortamı ile sağlanan tipik yararlarından, bir ağın bileşenlerinden, ağ yapılarından (topolojisinden), mimariden, ağların birbirine nasıl bağlandığından (repeater, bridge, Yönlendiriciler, Geçitler, hub, switch), ağ cihazlarının yönetimi ve güvenliğinden, Internetten, TCP/ IP Protokolünden, Kablosuz ağdan, Beykent Üniversitesi Network yapısından ve üniversitenin Network planlarından söz edilmiştir.

Beykent Üniversitesi'nde Ağ yapısı sayesinde maliyetler azalmıştır. Yönetim açısından yatırım maliyeti – kablolama, sunucuların alımı, bilgisayar ve ağ cihazlarının alımı -dışında ek bir maliyet oluşmamaktadır. Öğrenci ve personeller ağ yapısı sayesinde birbirleriyle haberleşmekte, bu sayede bütün veri akımları bilgisayar ortamında gerçekleşmektedir. Bu hem kırtasiye masraflarını ortadan kaldırmakta hem de kullanıcı memnuniyetini arttırmaktadır. Ayrıca bilgisayar ağları Beykent Üniversitesi'nde bilgisayar destekli eğitim ve üniversiteler arası bilgi alışverişlerinde çok yararlı bir eğitim ortamı sağlarlar. Diğer bir olanak da uzak veri tabanlarına (data base) erişimdir. Bir bilgisayar kullanıcısı kendi bilgisayarından uzak veri tabanlarına girerek on-line kütüphanelere ve akademik kaynaklara ulaşabilirler.

KAYNAKÇA

Alan N., İşletmeler İçin Çözümler - Bilgisayar Ağları, Çeviren :D.Kaya, A.Pamukçu,A.Ulutaş,M.Tan,Ü.Türkoğulları
web:http://kemalgok.virtualave.net/ag/network.htm

Arbaugh, W. A., Narendar S., Y.C. Justin War, 2001, "Your Wireless Network Has No Clothes", http://www.cs.umd.edu/~waa/wireless.pdf

Aron, H., Why Is Physical Security Important?, 2001, http://www.informit.com

Avaya Security Advisories on SNMP Vunerability,

http://support.avaya.com/security/2002-1/index.jhtml

Alcatel's response to SNMP Security Vulnerability,

http://www.ind.alcatel.com/service_support/CERT_Bulletin_031101_00.pdf

CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP), web:
http://www.cert.org/advisories/CA-2002-03.html

Cisco Advisory on SNMP Vulnerability,

http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml

Çelik, K. G., Çetin, G., Bilgisayar Ağları ve Linux Ağ Yönetimi El Kitabı, 1998, Sistem Yayıncılık

Çölkesen, R., Network, TCP/IP, UNIX El Kitabı, 2001, Papatya Yayıncılık

Danielyan, E., 2002, Cisco Internet Protocol Journal - Mar.

David, T., Are there Vulnerabilites in VLAN Implementations?, VLAN Security Test Report, 2000, http://www.hiperlan2.com/default.asp/16.07.2005

Improving Security on Cisco Yönlendiriciler,

http://www.cisco.com/warp/public/707/21.html

Increasing security on IP Networks

web:http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

Johnson, M., 1999, HiperLAN/2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band, HiperLAN/2 Global Forum

Kaplan, Y., Veri Haberleşmesi Kavramları, 2000, Papatya Yayıncılık

Karaaslan, E., 2001, Ege Üniversitesi Cisco Network Akademisi Ders Notları, web: http://cnap.ege.edu.tr

Multi Yönlendiriciler Traffic Grapher,

http://people.ee.ethz.ch/~oetiker/webtools/mrtg

SAFE: A *Security* Blueprint for *Enterprise* Networks, Sean Convery , Bernie Trudel, 2000 web:
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

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

Talisker's Intrusion Detection List,

www.networkintrusion.co.uk/Cisco.htm

Wireless Networking Standards and Organizations, 2002, Wireless LAN Association

http://www.bluetooth.com/ 20.07.2005

http://www.umtsworld.com/ 22.07.2005

http://www.hiperlan2.com/default.asp/19.07.2005

http://www.bluetooth.com/17.07.2005

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm/22.07.2005