

İÇİNDEKİLER

Bölüm 1: İnternete Genel Bakış.

1. İnternet Nedir?.....	1
1.1. Tarihçe.....	1
1.2. Standartlar.....	1
1.3 İşletmen ve Servis Sağlayıcı Kuruluşlar.....	1
1.4.İnternet Kaynakları.....	1
1.4.1.Haberler.....	1
1.4.2 Elektronik Posta.....	1
1.4.3.Gerçek Zaman Uygulamaları(real time application).....	2
1.4.4 Kütüphane Katalogları.....	2
1.5.İnternete Erişim Yöntemleri.....	2
1.5.1 Terminal Erişimi.....	3
1.5.2 Ağ Erişimi.....	3
1.6 İnternet Olanakları.....	3
1.6.1 Dosya Transfer Protokolü (FTP).....	3
1.6.2 Telnet.....	3
1.6.3 İnternet relay Chat.....	4
1.6.4 Geniş Bölge Bilgi Serveri(WAIS).....	4
1.7 Yönetim.....	4
1.8 Kullanıcı Gereksinimlerinin Belirlenmesi.....	4
1.9 Güncel İnternet Konuları.....	5
1.9.1 Güvenlik.....	5
1.9.2 Adres Yayılımı.....	5
1.9.3 Yönetmelik.....	5
1.9.4 Diğer Konular.....	6
2. Bilgisayar Ağları Temelleri.....	6
2.1 İletişim Ağları Yapısal Modeli.....	7
2.1.1 OSI Referans Modeli.....	7
2.1.2 Bağlantı Aygıtları.....	7
2.1.2.1 Tekrarlayıcı(repeater).....	7
2.1.2.2 Köprü(bridge).....	8
2.1.2.3 Yönlendirici (router).....	9
2.1.2.4 Geçityolları(gateway).....	10
3. TCP/IP VE Bileşenleri.....	11
3.1 Genel Tanımlar.....	11
3.1.1 TCP Katmanı.....	12
3.1.2 IP Katmanı.....	13
3.1.3 Fiziksel Katman.....	13
3.1.3.1 Ethernet Encapsulation (ARP).....	14
3.1.4 TCP Dışındali Diğer Protokoller :UDP ve ICMP.....	14
3.1.5 İnternet Adresleri.....	15
3.1.6 Alt Ağlar.....	16
3.1.7 Özel Adresler.....	17
4. Yönlendirme.....	17
4.1 Yönlendirme Protokolleri.....	18
4.2 Sabit Yönlendirme Tablosu.....	18
4.3 Diğer Yönlendirme Protokolleri.....	19

5.İsimler ve Adresler.....	20
5.1 Adresleme Stratejileri.....	20
5.2 TCP/IP ve DNS.....	21
6. Arayüz Kuruluşu.....	23
6.1 –ifconfig Komutu.....	23
6.2 Arayüzler ve Netstat Komutu.....	23
6.3 Arayüzün ifconfig Komutu ile Kontrolü.....	24
6.4 Seri Hatlar Üzerinde TCP/IP Konfigürasyonu.....	24
6.4.1 Slip Kuruluşu.....	25
6.4.2 PPP Kuruluşu.....	25
7. İnternet Bağlantısı İçin Alternatif Çözümler.....	26
7.1 Kişisel veya tek kullanıcı Bilgisayar ile Terminal Türü Bağlantı.....	26
7.1.1 Gerekli Yazılım ve Donanım.....	27
7.2 Bir Yerel Ağ yada Çok Kullanıcı Bilgisayar İle Yapılacak Bağlantı.....	27
7.3 Fiziksel Bağlantı Sonrası.....	29
Bölüm 2: İnternet Uygulama Programları	
1. Windows 2000 Web Server Kurulumu.....	30
2. Front Page Server Kurulum.....	38

1. İnternet Nedir?

. İnternet genel bilgiye erişimi destekler ve elektronik posta (elektronik mail), konferans, bildiriler gibi konularda iletişim hizmetleri sağlar. Bütün bilgi ve servisler, İnternet'i oluşturan çeşitli ağlara dağıtılmıştır ve geçerli bir İnternet adresi ve fiziksel bağlantısı olan herhangi bir yerden ulaşılabilir durumdadırlar. Kuruluşlar İnternet'e iki ana nedenden dolayı bağlanmaktadır. Birincisi, İnternet yararlı bilgilere dünya çapında bir bağlanabilirlik ve erişim sağlar. İkincisi, İnternet'e bağlanmak, kuruluşlara özel bir geniş bölge ağı kurmaktan daha ucuza mal olmaktadır. Amerika Birleşik Devletleri'nde İnternet'in işletimi federal yönetimlerce vergi mükelleflerinin vergilerinden karşılanmaktadır. İnternet'in kullanımı bir zamanlar araştırma, eğitim ve devlet kuruluşlarının etkinlikleriyle sınırlandırıldıysa da, son zamanlarda ticari kullanımı büyük oranda artmıştır. Bu gelişmeler, bazı gözlemcileri İnternet'in yakın gelecekte tamamıyla özelleştirileceği yolunda spekülasyonlara itmektedir. Böyle bir durumda İnternet kaynaklarına ulaşım kullanım fiyatlarına göre belirlenebilecektir.

1.1 Tarihçe

İnternet'in ortaya çıkışı Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan 'Savunma İleri Düzey Araştırma Projeleri Kurumu'na (DARPA- Defence Advanced Research Project Agency) dayanır. 1969'da çeşitli bilgisayar bilimleri ve askeri araştırma projelerini desteklemek için Savunma Bakanlığı ARPANET adında Paket Anahtarlamalı Ağ'ı oluşturmaya başladı. Bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki bilgisayarlarını da içererek büyüdü. 1973 yılında, ağ için bir protokol seti geliştirmek amacıyla Stanford Üniversitesi'nde - daha sonra BBN'in ve University college, London'in da dahil olduğu - bir internetworking projesi başlatıldı. 1978'e kadar İletim Kontrol Protokolü'nün (TCP - Transmission Control Protocol) dört uyarlaması geliştirildi ve denendi. 1980'de bu küme sabitleşti ve ARPANET'e bağlı bilgisayarlar arasındaki iletişimi kolaylastırdı. 1983'te tüm ARPANET kullanıcıları İletim Kontrol Protokolü/İnternet Protokolü (TCP/IP Transmission Control Protocol/İnternet Protocol) olarak bilinen yeni protokole geçiş yaptılar. O yıl TCP/IP, ARPANET'i de içeren Savunma Bakanlığı İnternet'inde kullanılmak üzere standartlaştırıldı. ARPANET 1990 Haziranı'nda kullanımdan kaldırıldı. Yerini ABD, Avrupa, Japonya ve Pasifik ülkelerinde ticari ve hükümet işletimindeki omurgalar (backbone) aldı. ARPANET'in kaldırılmasına rağmen, TCP/IP protokolü kullanılmaya devam etti ve gelişti.

1.2 Standartlar

TCP/IP protokol kümesinde yaklaşık 100 protokol bulunur. Bir çoğu, IP datagramlarının alt katman protokollarına nasıl taşınacağını gösterir. Setteki anahtar protokoller İletim Kontrol Protokolü (TCP), İnternet Protokolü (IP) ve Kullanıcı Datagram Protokolü'dür (UDP- User Datagram Protocol). Uygulama servisleri içinde uç temel protokol bulunmaktadır: Bunlar virtual terminal hizmeti veren TELNET Protokolü, Dosya Aktarma Protokolü (FTP File Transfer Protocol) ve Basit Posta Aktarma Protokolü'dür (SMTP-Simple Mail Transfer Protocol). Ağ yönetimi ise Basit Ağ Yönetim Protokolü'nce (SNMP-Simple Network Management Protocol) sağlanmaktadır.

TCP/IP başından beri Yerel Ağ bağlantısı (LAN-Local Area Network), Yerel ve geniş bölge Ağları (LAN-WAN) bağlantısı, bilgisayar ağı yönetimi, ve bilgi servisi sağlanması gibi yeni ortaya çıkan konulara da hitap etmektedir. Protokol kümesi akla gelebilecek her tip bilgisayara destek vermektedir. TCP/IP'nin kaynak kodu genel ortamda bulunup, kullanımı teşvik edilmiştir. Ağ yönetimi açısından SNMP, İnternet'i oluşturan TCP/IP tabanlı ağların yönetiminde de-facto standart durumundadır. SNMP istemci/sunucu (client/server) mimarisini kullanarak çeşitli ağ aygıtlarını işletmekte ve denetlemektedir. 1988'de kullanılmaya başladığından beri SNMP öylesine basar ili olmuştur ki bir çok ticarî ağ işletmeni kendi özel İnternet'leri üzerindeki çeşitli Yerel bölge Ağ elemanları için SNMP'yi kullanmaya başlamışlardır. Pek çok endüstri çözümleyicisi ise SNMP'nin yaygın kullanımını, OSI-tabanlı Ağ Yönetim sistemlerinin yavaş ilerleme nedeni olarak görmektedir.

1.3 İşletmen ve Servis Sağlayıcı Kuruluşlar

İnternet'in ağırlığının araştırma ve devlet projelerinden daha geniş ilgi alanlarına kaymasıyla beraber ağ işletmenleri ve servis sağlayıcıları da ticarî erişim de dahil olmak üzere İnternet servislerini sunmaya başladılar. Örneğin, IBM, MCI Communications Corp. ve Merit Network Inc.'in oluşturduğu Gelişmiş Ağlar ve Servisler (ANS, Advanced Network and Services) adındaki bir konsorsiyum, NSFNET omurgası aracılığı ile İnternet'e bağlanmayı da içeren çeşitli hizmetler sunmaktadır. ABD'deki İnternet üzerindeki ana omurga olan NSFNET, Ulusal Bilim Vakfı (National Science Foundation) tarafından kurulmuştur. NSFNET'e bir geçityoluyla (gateway) bağlanmak isteyen bölgesel ve devlet Ağları, üniversitelerin veri tabanlarına erişmek isteyen bilgi sağlayıcıları ve firmalar ANS'nin müşterileri arasında yer alır.

1.4 İnternet Kaynakları

1.4.1 Haberler

İnternet üzerindeki en yararlı kaynaklardan biri, çok sayıda konu içeren ilan tahtası sistemlerinin (BBS-Bulletin Board Systems) bir toplamı olan ağ haberleri'dir (Netnews). Haber grupları, bir ağaç yapısında düzenlenmiştir. Bu yapıdaki her bir kok bilim, sanat gibi ana bir konuya ayrılmıştır. Kökler de, her biri bir konu alanı belirleyen dallardan oluşur. Ağ haberleri UNIX tabanlı sistemlerde ortaya çıkmıştır. Rn, nn, trn ve xrn gibi UNIX programları ağ haberlerini okumak için kullanılmaktadır. UNIX kullanıcısı olmayanlar, ağ haberlerini IBM PC ve uyumlularıyla, Machintosh ve VAX/VMS sistemlerinde okuyabilecek yazılım paketlerini kullanmaktadırlar. Pek çok yerel ilan tahtası da ağ haberlerine erişimi sağlamaktadır.

İnternet kullanıcıları bir listeye üye olarak istedikleri konuda bilgi alabilirler. Liste yöneticileri periyodik olarak listelerindeki üyelere toplanılan bilgi paketlerini yollarlar. Bu elektronik posta (e-mail) listelerinin çoğuna Usenet aracılığıyla ulaşılabilir. Usenet 3500'den fazla konuyu içeren haber gruplarının sunulduğu genel bir BBS yapısıdır.

1.4.2 Elektronik Posta

İnternet dünyanın en büyük elektronik posta (e-mail) ağıdır. Bugün yaygın olarak kullanılan elektronik posta sistemleri arasında büyük farklar vardır. Buna rağmen, İnternet, kullanıcılarına mesajları okuma, saklama, gönderme, sıraya sokma ve yanıtlama gibi çeşitli hizmetler vererek kullanıcılarının dünyanın dört bir tarafı ile haberleşmesini sağlamaktadır. İnternet'in anı popülerliğinin nedeni aslında elektronik posta servislerinde sunduğu artan etkileşimli bağlantıdır. İnternet'te kullanıcı kodu bulunan bir kişi diğer İnternet kullanıcılarıyla olduğu gibi, compuserve, BITNET, MCI, Applelink ve benzer posta sistemleri kullanıcılarıyla da elektronik posta iletişimi kurabilir. Benzer şekilde bu sistemlerin kullanıcıları da İnternet'i kendi aralarında bir iletişim yolu olarak kullanabilirler.

Aynı zamanda, çeşitli yazılım şirketleri kişisel bilgisayarlardan oluşmuş Yerel Ağlar ve UNIX ortamları arasında da mesaj değişimi için geçiyolu (Gateway) sağlamaktadırlar. Örneğin, Bilgisayar Posta Servisleri şirketi (Computer Mail Services, CMS), S-bridge adında, mesaj servisi veren posta ofislerini, SMTP tabanlı elektronik posta sistemlerine bağlayan bir geçiyolu ürünü sunmaktadır. Bu ürün, Mesaj Kontrol Servisleri'ni (Message Handling Service, MHS) destekleyen kişisel bilgisayar tabanlı elektronik posta programlarıyla, UNIX işletim sistemindeki SMTP tabanlı elektronik posta programı arasında mesaj değişimini sağlamaktadır. MHS, kişisel bilgisayarlardan oluşmuş Yerel Ağlarda kurulu olan en popüler elektronik posta sistemlerinin kullandığı sakla-ve-ilet (Store-and-Forward) teknolojisini kullanmaktadır. CMS'in bir diğer geçiyolu ürünü ise UNIX tabanlı makinalar için M-bridge'tir. Bu ürün MCI Mail'i faks ve teleks servisleri ile birlikte SMTP tabanlı elektronik posta sistemlerine bağlamaktadır.

1.4.3 Gerçek Zaman Uygulamaları (Real Time Applications)

Elektronik postaya ek olarak, İnternet çeşitli gerçek zaman işlemlerini de desteklemektedir. Örneğin, Amerika'daki belli başlı üniversitelerdeki öğrenciler birbirleri ya da çevrim-içi programlarla 'etkileşimli oyunculuk benzetimleri' ve diğer etkinlikleri gerçekleştirmektedirler. Bu benzetimler gerçek ya da hayal ürünü olan politik veya tarihsel olaylardan oluşabilmektedir. Öğrencilerden varolan karakterlerden kendi rollerini seçmeleri istenir. öğrenciler bu rolleri oynarken aynı zamanda derslerini de öğrenirler.

Karar verme benzetimlerinde, öğrenciler çevreye en az etkisi olan çeşitli çevre ve inşaat problemleriyle karşı karşıya bırakılırlar. Buna örnek olarak verilebilecek bir program, Michigan Üniversitesi Eğitim Okulu'nda etkileşimli İletişim ve Benzetimler Projesi dahilinde dokuz yıldır çalışmaktadır. Bu zaman içerisinde yirmi ülkedeki dörtüzyük okuldan onikibinden fazla öğrenci programın çeşitli öğrenim benzetimlerine katılmıştır.

1.4.4 Kütüphane Katalogları

Bugün, İnternet üzerinde 300'e yakın Kütüphane katalogu bulunmaktadır. Bunlar arasında 100'den fazla koleksiyon, arşiv ve araştırma kütüphanesinin kataloglarını gösteren ve 40 milyondan fazla kaydı bulunan bir veritabanına sahip Araştırma Kütüphaneleri Bilgi Ağı (RLIN) anılmaya değer bir örnektir. İnternet, Amerikan Kongresi Kütüphanesi'ne, Colorado Üniversitesindeki 220,000 konu başlığına, Boston, Maine ve Harvard Üniversitesindeki Kütüphane kataloglarına erişimi sağlamaktadır. ABD içinde istediği kitabın yerini belirleyen bir İnternet kullanıcısı kendi yerel kütüphanesinden Kütüphanelerarası Ödünç Alma Programını kullanarak bu kitabı Ödünç alabilir. 1992 başlarında, Carneige Mellon Camp Üniversitesi, Amerika'da Dağıtık İşleme dayalı ilk elektronik Kütüphane sistemlerinden birini kurdu. Sistem, bilgiyi tek bir ana bilgisayar yerine yerleskeye dağılmış olan serverlarda saklamaktadır. Sistem, fakülte ve öğrencilere, odalarından dışarı bile çıkmadan, üniversite kütüphanesinde bulunan dökümanları edinme olanağı sağlamaktadır. üniversite İnternet'e bağlanarak bazı koleksiyonlarının tüm dünyadaki kullanıcılara ulaşmasını olanaklı kılmaktadır.

1.5 İnternet'e erişim Yöntemleri İnternet'e, modemi ve kişisel bilgisayarı olan biri çok az bir ücret karşılığında bağlanabilir. Bir çok durumda istenilen servisin türüne göre BBS üzerinden dahi bir bağlantı temin edilebilir. Aynı şekilde, E-mail olanaklarını kullanan bir geçiyolu sayesinde de İnternet'e bağlanılabilir. Örneğin, MCI Mail ve AT&T's Easy Link kullanıcıları elektronik posta mesajlarını İnternet üzerindeki herhangi bir adrese gönderebilirler. Fakat, bu dolaylı bağlantı yöntemleri, İnternet'in gerçek zaman uygulamalarını desteklemez. Kullanıcılar, İnternet'e çeşitli yollarla bağlanabilirler. bağlantı seklini, kullanıcının İnternet'e ne kadar sıklıkla bağlanacağı belirler. İnternet'e arada sırada bağlanan kullanıcılar dial-up hat kullanabilirler, ancak bu tip bağlantı sıklıkla bağlananlar için verimli değildir. Bu kullanıcılar, İnternet'e kiralık hatlar yada paket anahtarlamalı ağlar yoluyla bağlanmalıdırlar.

Bağlantıların nasıl yapılabileceğine ilişkin ayrıntılı teknik bilgi ilerideki bölümlerde verilecektir.

1.5.1 Terminal Erişimi

Terminal erişimi, kullanıcının istediğinde İnternet'e dial-up tipi bağlantı yapmasını sağlar. ABD'de herkese açık, NETCOM (San Francisco), World (Brooklyn, MA) gibi kamu bilgisayarlarına, modem yoluyla dial-up terminal bağlantısı yapılabilir. Bütün İnternet servisleri ve kaynakları, bu bilgisayarlar vasıtasıyla kullanıcı ve erişim kısıtlamaları dahilinde, kullanıcıya açıktır. Bazı servislere erişmek için ise özel şifreler gerekmektedir.

1.5.2 Ağ Erişimi

TCP/IP'nin çalıştığı bir bilgisayar veya LAN server'la İnternet'in tüm fonksiyonlarına ulaşabilecek bir bağlantı gerçekleştirilebilir. İnternet'le bir ağ katmanı bağlantısı kurarak, bir bilgisayar veya server İnternet üzerindeki diğer bilgisayar ve server'larla iletişim kurabilir. TCP/IP yazılımı, çoğu UNIX tabanlı bilgisayarlarda işletim sistemi ile birlikte gelmektedir. MS-DOS tabanlı diğer sistemler için ise bu yazılımı paylaşılabilir ve ücretsiz yazılım olarak elde etmek mümkündür.

Bilgisayarlarında TCP/IP çalıştıran kullanıcılar TELNET, FTP, IRC (İnternet Relay Chat) ve diğer IP uygulamalarını doğrudan kullanabilirler. Böylelikle İnternet'le, bir terminal olarak dial-up bağlantı kurmak zorunda kalmazlar. Bu yöntem kullanıcılara tam bir IP bağlantısı sağladığı için, bir çok uygulamayı aynı anda çalıştırmak mümkündür. Örneğin, ayrı ayrı pencerelerde, iki FTP, iki TELNET ve bir IRC aynı anda çalıştırılabilir.

Genel dial-up bağlantı hizmeti sunan bir servis sağlayıcı kuruluş aracılığı ile de IP bağlantısı kurmak mümkündür. Bilgisayar, TCP/IP'yi desteklemenin yanı sıra telefon hattı üzerinden haberleşmeyi sağlayacak geçerli bir protokolu de desteklemelidir. Çoğu durumda, TCP/IP yazılımı dial-up bağlantı biçiminde ya Point-to-Point Protokolü (PPP)'nu ya da Serial Line IP Protokolü (SLIP)'nu kullanır.

Herhangi bir kuruluş, Yerel Ağ'ından kiralık hat bağlantısı yoluyla İnternet'e tam zamanlı, tam fonksiyonlu bir erişim isterse, İnternet servis sağlayıcı kuruluşa (Türkiye de TR-NET) başvurmalıdır.

1.6 İnternet Olanakları

Genelde kullanılmakta olan İnternet olanakları IP bağlantısı gerektirmektedir. Bu olanaklardan bazıları FTP, TELNET, GÖPHER, WWW, IRC ve WAIS'dir.

1.6.1 Dosya Transfer Protokolü (FTP)

Dosya Transfer Protokolü (FTP) bir veri yığınının -ASCII, EBCDIC, ve binary- bir uç aygıttan diğerine iletimi için kullanılmaktadır. Bir dosyayı FTP kullanarak başka bir TCP/IP ağı üzerindeki kullanıcıya yollamak için o ağıdaki bilgisayarda geçerli bir kullanıcı ismi ve şifresi gerekmektedir. İnternet 'anonim FTP' ye (anonymous FTP) destek vermekle birlikte bunu dosyayı yollamak için değil sadece okumak için verir. Bu durum, ağ üzerindeki her kullanıcıya postanın yollanmasını sağlayan SMTP yoluyla asılabilir. Fakat SMTP sadece metin iletebildiği için diğer tip dosyalar gönderilmeden önce metin dosyasına çevrilmelidir. Daha sonra da alıcı tarafından tekrar eski haline çevrilir. Diğer taraftan elektronik postada kullanılan OSI X.400 standardı, kullanıcıya metin, grafik, telex, fax, video, ve hatta ses yollamasına izin verir. Elektronik döküman değişimini (EDI-Eleçtroniç Document Interchange) de destekler. Ancak, bu uygulamalar diğer OSI uygulamaları gibi yeterli yaygınlığa ulaşmamıştır.

OSI FTAM (dosya transfer, erişim ve yönetim) protokolü TCP/IP'nin FTP'sinden daha işlevseldir. Görüntü (Virtual) dosya saklama yeteneği sağlmasına ek olarak, FTAM kullanıcısı, tüm dosya yerine dosyanın bir kısmını da gönderebilir. TCP/IP ortamında da aynı düzeyde işlevsellik sağlamak için dosyaları parçalar halinde taşıyabilen Sun Microsystems'in Ağ Dosya Sistemi (NFS-Network File System) FTP yerine kullanılabilir. Bu özelliğinden dolayı NFS'in popülaritesi artmış ve firmalar NFS'i pek çok TCP/IP türüyle entegre etmişlerdir.

1.6.2 TELNET

TELNET aslında ARPANET için geliştirilmiş basit bir terminal emulasyon aracıdır. TELNET ağ-bağımsız bir virtual terminal aracılığıyla kullanıcı koduna sahip olduğu uzak bir TCP/IP yetenekli bilgisayara bağlanabilmeyi sağlar. Kullanıcı uzak TCP/IP bilgisayarındaki standart bağlanma işlemlerini izler ve o bilgisayara ait komutları kullanabilmek için uzak işletim sisteminin karakteristiklerini bilmek zorundadır. TELNET uzak terminalerin bir ana bilgisayara bağlanmasını, bağlanılan bilgisayarın işletim sistemine sanki yerel bir terminal bağlanıyormuş gibi göstererek sağlar. Çoğu zaman TELNET full-duplex mod'da çalışır, yani aynı anda yollama ve alma yeteneği sağlar.

TELNET protokolünün kullanıcı ve server işlemleri kendi aralarında mantıksal bir sıra izlerler. Kullanıcı TELNET programı, kullanıcı ile server arasında bir passthrough gibi çalışarak veri iletimini sağlar. Makinanın rolüne ve gücüne göre, TELNET'in hem kullanıcı hem de server olarak kullanılması sağlanabilir. Tek- görevliliğinden dolayı DOS işletim sistemini kullanan mikrobilgisayarlar genellikle TELNET'in kullanıcı tarafını kullanırlar. Diğer yandan, UNIX ve OS/2 işletim sistemini kullanan bilgisayarlar TELNET'i iki yonlu olarak kullanabilirler. Çünkü bunlar çok-görevli işletim sistemidirler.

1.6.3 İnternet Relay Chat (IRC)

İnternet Relay Chat (IRC) iletişim tahtası sistemlerinin gerçek zaman uygulamasıdır. Her çevrim içi kullanıcının girdisini konuya ilgisi olan ve konu başlığına ya da listesine üye olan diğer kullanıcılara yayınlayan bir konferans sistemidir. Liste güncel politik olaylar, profesyonel uğraşlar ya da haber paylaşımı gibi konularda odaklanabilir.

1.6.4 Geniş Bölge Bilgi Server'i (WAIS)

WAIS (Wide Area Information Server), belli baslı konular için ayrılmış 80'den fazla server'dan metin, görüntü, ses ve düzenlenmiş veri olarak kodlanmış bilginin bulunması, saklanması ve alınması için kullanılan istemci/sunucu sistemidir. Kullanıcı arama işlemi için gerekli olan anahtar sözcükleri girer ve aramanın hangi kaynaklarda yapılacağını belirtir. WAIS platform gözetmeden doğal dildeki soruları kullanarak ilgili dökümanları arar. Arama başarılı olupta kullanıcının istediği bilgi getirildiği zaman, arama otomatik olarak yeni bilgiler elde etmek üzere yeniden başlatılabilir. Thinking Machines CORP. tarafından geliştirilen WAIS bir tek arayüzle

kullanıcıların çeşitli tipteki veritabanlarına ulaşmasını sağlar ve Amerikan Kongre Kütüphanesi'nce kullanılan Z39.50 standart protokolunu kullanır.

1.7 Yönetim

İnternet teknik açıdan olduğu gibi yönetim yapısı açısından da merkezi değildir. Her otonom sistemin yönetim otoritesi, genellikle, kendini finanse etmeye ve kendi kural ve yöntemlerini belirlemekle yükümlüdür. Merkezi olmayan yönetimin iki önemli avantajı vardır. Birincisi, İnternet'in işlerliği bir tek kuruluşun bütçesine bağımlı değildir; büyüme ve güncel tutma giderleri bir çok kuruluşa dağılmıştır. İkincisi, İnternet'e bağlanmak isteyen kuruluş varolan ağ yapısında koklu değişiklikler yapmak veya İnternet'le olan ilişkilerindeki yönetsel kontrollerinin herhangi birinden vazgeçmek zorunda değildir. Buna rağmen, bazı yönetim fonksiyonları merkezidir. Örneğin, IP adreslerinin ve İnternet üzerinde kullanılan protokolların standardizasyonunun belirlenmesi, İnternet'in, tüm kullanıcıların çıkarları doğrultusunda işlemlerini sağlar. Bunu sağlayan iki önemli yönetim organizasyonu Gövernment Systems Inc.(GSI) ve İnternet Activities Board(IAB) dir. GSI, IP adreslerini ve adreslemeyle ilgili servisleri sunarken, IAB İnternet protokollarının standardizasyonunu koordine etmektedir. IAB, kendi işyerlerinden sağladıkları kaynakları İnternet'e yardım da kullanan 12 gönüllü iletişim uzmanından oluşan gayriresmi bir gruptur. Diğer yandan, 1991 sonlarında 'İnternet Society' İnternet' e resmi bir yapı sağlamak üzere kurulmuştur.

IAB, iki görev kuvvetinin etkinliklerini yönetir: İnternet Engineering Task Force (IETF) ve İnternet Research Task Force(IRTF). IETF açıl problemlerle uğraşırken IRTF ileride gerekebilecek İnternet protokollarını ve teknolojisini geliştirmeye çalışır.

IETF İnternet'in işletimini denetler ve İnternet'in işletimi, protokolu ve mimarisıyla ilgili problemlerde öncelik belirler ve uygular. IETF problem alanlarına ve çözümlerine yönelik iş grupları oluşturur. Önerilen bir İnternet standardi Öneri Standart (Proposed Standard) olarak başlar. IETF'nin onayıyla Taslak Standart'a (Draft Standard) yükselir ve numaralandırılır. Daha sonra İnternet'te Görüş İsteği (RFC-Request for Comment) başlığıyla ilan edilir. RFC herhangi bir kişiden gelebilir. Sadece IETF değil, İnternet ile ilgilenen tüm kullanıcıların standard oluşturma işlemine katılımı için şans tanınır.

İnternet kullanıcıları topluluğunun görüşlerini bildirmesi için gerekli bir süreden sonra ve IETF onayıyla taslak standart 'İnternet Engineering Steering Group'(IESG)a sunulur. 1992 sonlarında, İnternet Society, IESG 'ye İnternet standartlarının onaylanmasında gözetileceği ölçüleri belirlemiştir. Daha önceden IESG, IAB'ye son onay için standartlar önerirdi. İnternet Society tarafından belirlenen bir diğer ölçü de IAB ve IESG üyelerinin iki yıllık dönem için seçilmeleridir.

1.8 Kullanıcı Gereksinimlerinin Belirlenmesi

İnternet servisi sağlayan kurumlarla bağlantıya geçmeden önce, kullanıcılar kurumsal gereksinimlerini belirleyerek, giderlerini karşılayabilecekleri doğru düzey ve tipteki İnternet erişimine karar vermelidirler. Göz önüne ilk alınması gereken konu, İnternet kullanımının amacıdır. Bu, ticari, araştırma, eğitim amaçlı olabileceği gibi sadece elektronik posta hizmetinden yararlanmak içinde olabilir.

Kullanım amacına ek olarak kullanım sıklığı da belirlenmelidir. Eğer kullanıcılar İnternet'e çok sık bağlanmayı düşünmüyorsa, klasik çevirmeli telefon hatları (dial- up) kullanmak en ekonomik yol olabilir. Eğer İnternet kullanımının çok yoğun olacağı hesaplanmışsa kiralık hat yada paket anahtarlamalı ağ kullanarak ağa bağlanmak düşünülmelidir. Kiralık hat kullanmaya karar verilmişse, bir sonraki karar verilmesi gereken konu hattın kapasitesinin ne olacağıdır. Hat kapasitesini bir kaç etken etkiler. Bunlar, herhangi bir zamanda İnternet'e kaç kişinin ulaşacağı, hat üzerinde gitmesi gereken trafiğin yoğunluğu ve hatta taşınması düşünülen dosyaların büyüklüğü gibi unsurlardır. Bunlara göre belirlenecek uygun bir hat kapasitesi gecikmeleri onlayacak ve İnternet'e hızlı bir erişim sağlayacaktır.

Bağlantı şekli ve hat kapasitesinin belirlenmesiyle birlikte düşünülecek diğer bir nokta da, bilgisayarların İnternet'e bağlanmasında gerekçe arabirimleridir. Bu durumda da kullanım yoğunluğuna göre çeşitli alternatifler değerlendirilmelidir. Bütün ana bilgisayarları ve PC'leri bu arabirimlerle donatmak, trafik yoğunluğu masrafları kaşılamadığı sürece oldukça pahalı olabilir. Çoğu durumda gerekli arabirimleri takarak, (eğer varsa) bir LAN server'ini İnternet'e geçiyolu yapmak en ekonomik çözüm olmaktadır.

Birbirinden uzak ve çeşitli bölgelere yayılmış olan kurumlarda hesaplar her bölge için ayrı ayrı yapılmalıdır. Yoğun trafik hacmi olan bölgelerde İnternet'e kiralık bir hatla bağlanılabilir. Zaman zaman İnternet kullanımı için dial-up erişimi de kullanılabilir.

İnternet servislerinin ve kullanıcılarının gereksinimleri de göz önüne alınmalıdır. Bazı etkileşimli uygulamalar bütün TCP/IP protokol kümesini gerektirdiği halde, e- mail gibi uygulamalar için, buna gerek yoktur. eğer tüm TCP/IP protokol kümesi gerekiyorsa, kullanıcılar özellikle çoklu ortamların (multi-session) desteklenmesi için UNIX tabanlı olmayan bilgisayarlarını uygun yazılımlarla donatmak zorunda kalabilirler. UNIX sistemlerinin çoğunda ise TCP/IP yazılımı işletim sistemiyle birlikte bulunmaktadır. Kullanıcılar, İnternet'e tam gün Bağlantı için hangi yönlendirici ve köprülerin gerektiğininde belirlemelidirler. Köprü ve yönlendirici satan firmaların çoğu TCP/IP yi desteklese de kullanıcılar, kullanım yükü çoğaldığında bununla başa çıkıp çıkamayacaklarını ve İnternet'e yeni bağlantılar gerektiğinde boş portları olup olmayacağını belirlemek zorundadırlar. Bu olmadığında, ilave Bağlantı aletlerinin (ya da yenileme) giderlerini iletişim bütçelerine eklemek zorundadırlar. Son olarak kurum içindeki iletişim elemanlarının uzmanlık düzeyine göre dışarıdan almaları gereken servisler de önem kazanabilir. Pek çok kitap ve referanslar yeni kullanıcılara gereken ipuçları ve öneriler vermektedir.

1.9 Güncel İnternet Konuları

IAB pek çok konuyu gündeme getirmektedir. Bunlardan ağırlıkta olan ikisi güvenlik ve İnternet adreslerinin yetersizliğidir.

1.9.1 Güvenlik

İnternet'teki güvenliğin olmaması SNMP standartları sürecinin çabuk ve basit felsefesinin bir sonucudur. 1988'de ilk orijinal SNMP tanımlamaları geliştirildiğinde standartlar topluluğunda bunun nasıl güvenli yapılabileceği konusunda bir uzlaşma sağlanamadı ve SNMP, güvenlik özellikleri olmaksızın kullanıma sunuldu. IAB'çe göz önüne alınmakta olan tanımlamalar aşağıdaki güvenlik özelliklerini sağlamaktadır:

* SNMP ve kullanıcının birbirine gönderdiği mesajlar için veri şifrelemesi : Bu bir SNMP istasyonunun hangi yönetim işlevlerine erişeceğini belirleyen veya istasyon içerişindeki yetki düzeyini tanımlayan anahtarların gönderilmesinde büyük fayda sağlar.

* Köken doğrulama (origin authentication): Yetkili olmayan kullanıcıların bir SNMP iş istasyonunun erişim kodunu alarak yetkili bir kullanıcıymış gibi yanıltmalarını engeller.

* Replay koruması (Replay protection): Kullanıcıların SNMP iletişimini geciktirmelerini engeller. Örneğin, bir komut bir iş istasyonunu çevrim dışı (off-line) bırakarak bir SNMP iletişiminin gecikmesine yol açabilir.

* Mesaj bütünlüğü (Message Integrity): Yetkisiz kullanıcıların SNMP mesajlarının içeriğini değiştirmesini engeller.

1.9.2 Adres Yayılımı

1992 ortalarında IAB, İnternet'in yönlendirilmesi için kullanılan İnternet protokolunu OSI' nin Bağlantısız Ağ Protokolüyle (CLNP-Connectionless Network Protocol), mümkün olan en iyi çözüm diyerek değiştirmek istedi. IAB' nin ÇLNP' nin oturtulması için olan kararı İnternet topluluğunun önemli gruplarınca diğer çözüm önerilerini engelleyen bir duvar olarak algılandı. Bu direnişin artmasıyla IAB diğer alternatif önerilerin ileride tartışılabilmesi için CLNP'yi geri çekti. Alternatifler "'P" İnternet Protokolü (PIP) ve 'Yeni İnternet Yönlendirme ve Adres Mimarısı'nden (NIMROD-New İnternet Routing and Address Architecture) oluşmaktadır. Dikkat çeken eski düşüncelerden bazıları ise IP adres Encapsulation'ini ve Adres Çevrimi'dir. CLNP'nin istediği IP protokolu gibi bir temeli değiştirmenin ağlar üzerinde belirgin bir etkisi olacak ve yeni adreslerle uğraşmak için, yönlendirme bilgisini kullanan alet ve uygulamaların güncelleştirilmesi gerekecektir. Geçiş planı yeni sistemlere uygulanırken güncelleştirilmemiş eski sistemler için de bir yol içermesi gerekir. Geçiş, kullanıcılar için zaman ve para maliyeti çıkartacaktır ve bunun firmalar üzerinde de büyük etkisi olacaktır.

1. 9.3Yönetmelik

İnternet akademisyenler tarafından kullanılan global bir araştırma ağından, işletim, yönetim, ücretlendirme ve güvenlik konularında kullanıcılarının düşük tolerans gösterdiği global bir ticari servise dönüşmektedir. İnternet'e ücret ödeyen Kuruluşlar ihtiyaçlarıyla ilgilenilmesi ve karşılanmasının verimli bir şekilde ve zamanında yapılmasını beklemektedirler. FCC'nin izlemesi mümkün olmadığı halde, Amerikan devleti tarafından İnternet'e müdahale edilerek sınırları içinde akan verinin düzenlenmesine ve ücret toplanmasına yönelik bir girişim olmuştur.

İnternet'te ticari kurumların sayısı arttıkça bu tip girişimlerin tekrarlanacağı düşünülmektedir. Yanıtlanması gereken ilk soru İnternet'in sahibinin kim olduğudur. Ticarileşmeyle birlikte, İnternet, kamu ve özel kuruluşların oluşturduğu karma bir kimliğe bürünmektedir. İnternet'in büyük BÖLÜMu devletce finanse edilse de İnternet servislerinin geliştirilmesi ve ağıın yayılması için finansman sağlayan kamu ve özel kuruluşlarının da olmasıyla, İnternet için uygun bir başlık bulmak oldukça zorlaşmaktadır.

İnternet'in devlet tarafından finanse edilmesi birtakım sorulara maruz kalmaktadır. Örnek olarak, NASA ve Enerji Bakanlığı gibi Kuruluşlar tarafından belirlenen bölge ağlarında istenilen yeniliklerin yapılması isteğini verebiliriz.

Diğer birtakım kişiler ise devlet kaynaklarının amacına ulaşmış bölge ağlarından çok iyi yönetilmeyen bölge ağlarına kaydırılması gerektiğini tartışmaktadırlar. İnternet'in ticari yönü arttıkça her miktardaki finansman tartışma konusu olmaktadır.

1.9.4 Diğer Konular

İnternet, sadece on yıl içerisinde gevşek yapıdaki bir akademik ortamdan, dünyanın en büyük iletişim ağı durumuna gelmiştir. Ağ yönlendirme tabloları yöneticilerin geliştirebileceğinden çok daha hızlı büyümektedir. Bu kadar büyük bir topluluğu yönetmek de güçleşmektedir. Ticari amaçlarla kullanımı arttığı için eski kullanım için hazırlanmış kurallar, ticari gerçekler de gözönüne alınarak yeniden düzenlenmelidir.

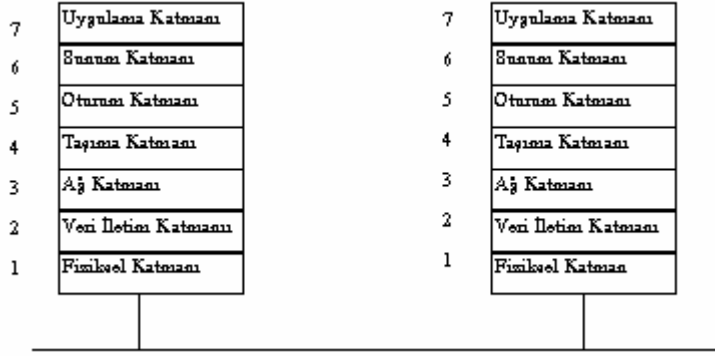
2.Bilgisayar Ağları Temelleri

2.1 İletişim Ağları Yapısal Modeli

Bu BÖLÜMde bilgisayar ağlarının birbirleri ile olan iletişimi (internetworking) konusunda bazı temel kavramlar hakkında bilgi verilecektir.

2.1.1 OSI Referans modeli

Bilgisayarlar arası iletişimin başladığı günden itibaren farklı bilgisayar sistemlerinin birbirleri arasındaki iletişim daima en büyük problemlerden birisi olmuş ve bu sorunun üstesinden gelebilmek için uzun yıllar boyunca çeşitli çalışmalar yapılmıştır. 1980'li yılların başında Uluslararası Standartlar Organizasyonu (International Standards Organization-ISO) bilgisayar sistemlerinin birbirleri ile olan iletişimde ortak bir yapıya ulaşmak yönünde çabaları sonuca bağlamak için bir çalışma başlatmıştır. Bu çalışmalar sonucunda 1984 yılında Açık Sistem Bağlantıları (Open Systems Interconnection-OSI) referans modeli ortaya çıkarılmıştır. Bu model sayesinde değişik bilgisayar firmalarının ürettikleri bilgisayarlar arasındaki iletişimi bir standarda oturtmak ve farklı standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak hedeflenmiştir. OSI referans modelinde, iki bilgisayar sistemi arasında yapılacak olan iletişim problemini çözmek için 7 katmanlı bir ağ sistemi önerilmiştir. Bir başka deyişle bu temel problem 7 adet küçük probleme parçalanmış ve her bir problem için ayrı ayrı bir çözüm yaratılmaya çalışılmıştır. Bu 7 katmanın en altında yer alan iki katman yazılım ve donanım, üstteki beş katman ise genelde yazılım yolu ile çözülmüştür. OSI modeli, bir bilgisayarda çalışan uygulama programının, iletişim ortamı üzerinden başka bir bilgisayarda çalışan diğer bir uygulama programı ile olan iletişiminin tüm adımlarını tanımlar. En üst katmanda görüntü ya da yazı şeklinde yola çıkan bilgi, alt katmanlara indikçe makine diline dönüşür ve sonuç olarak 1 ve 0 lardan ibaret elektrik sinyalleri halini alır. Aşağıdaki şekilde OSI referans modeli katmanları ve bir yerel ağ üzerindeki durumu gösterilmektedir:



Çizim-1 OSI Referans modeli

OSI katmanlarının tanımlanan temel görevleri:

7- Uygulama

Kullanıcıya en yakın olan katmandır. Spreadsheet, kelime işlemci, banka terminali programları vs. bu katmanın parçalarıdır.

6- Sunum

Bu katmanda gelen paketler bilgi haline dönüştürülür. Bilginin karakter set çevrimi veya değiştirilmesi, şifreleme vs. görevlerini bu katman üstlenir.

5- Oturma

İki bilgisayar üzerindeki uygulamaların birbirini farketmediği katmandır.

4- Taşıma

Bu katman gelen bilginin doğruluğunu kontrol eder. Bilginin taşınması esnasında oluşan hataları yakalar ve bunları düzeltmek için çalışır.

3- Ağ

Bağlantıyı sağlayan ve ulaşılmak istenen bilgisayara giden yolu bulan katmandır. Yönlendirme protokolları bu katmanda çalışır.

2- Veri iletim

Bu katman fiziksel katmana ulaşım stratejisini belirler. Fiziksel adresleme, ağ topolojisi, akış kontrolü vs. bu katmanın görevlerindedir. Köprü cihazları bu katmanda çalışır.

1- Fiziksel

Bu katman ağın elektriksel ve mekanik karakteristiklerini belirler. Modülasyon teknikleri, çalışma voltajı, frekansı vs. bu katmanın temel özelliklerindedir. OSI referans modeli bir ağ uygulaması değildir. OSI sadece her katmanın görevini tüm detayları ile tanımlar. Bu modeli bir gemi ya da ev projesine benzetebiliriz. Nasıl aynı gemi planını alıp farklı firmalar gemi yapabilirse OSI modeli de böyledir. Nasıl aynı gemi planından iki farklı firma gemi ürettiğinde en azından kullanılan çiviler farklı yerlere çakılırsa, OSI modeli de gerçekleştiren firmadan firmaya farklılık gösterebilir.

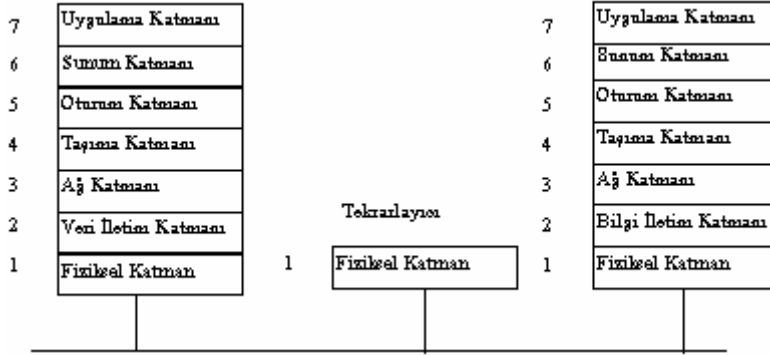
2.1.2 Bağlantı Aygıtları

Bilgisayar ağı erişiminde genel olarak dört tip bağlantı aygıtı kullanılır: tekrarlayıcı (repeater), köprü (bridge), yönlendirici (router) ve geçityolu (gateway). Tekrarlayıcılar tamamen protokol bağımsız olarak fiziksel katmanda çalışır ve fiziksel genişleme amaçlı kullanılırlar. Geleneksel köprüler aynı protokol kullanan Yerel Ağlar arasında temel veri düzeyinde bağlantı sağlar. Buna karşılık, geleneksel yönlendiriciler değişik tipteki ağ protokollarını idare edebilecek şekilde programlanabilirler ve böylelikle aynı geniş ağ alanı üzerinde farklı tipteki Yerel Ağları ve bilgisayar sistemlerini

destekleyebilirler. Geçit yolları daha karmaşık olup, işlem yoğunluklu protokol çevrimi yaparak uygulamalar arasında işletilebilirliği (interoperability) sağlarlar.

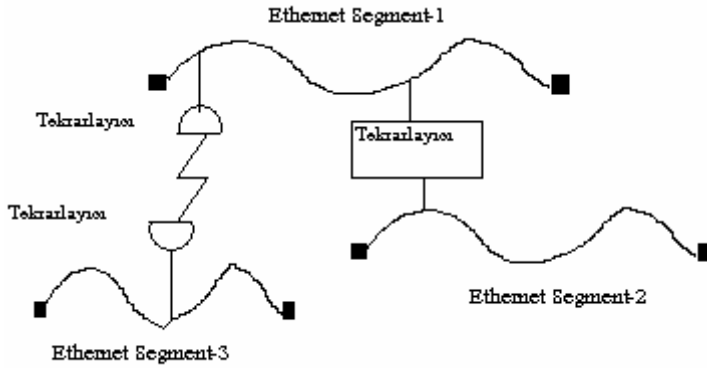
2.1.2.1 Tekrarlayıcı (Repeater)

Tekrarlayıcılar Çizim-3'deki şekilden de görüleceği gibi fiziksel katmanda çalışan cihazlardır.



Çizim-2 Tekrarlayıcı ve OSI modeli

Tekrarlayıcının temel görevi bir fiziksel ortamdaki (kablo, fiber-optik, radyo dalgası vs.) sinyali alıp kuvvetlendirip bir diğer fiziksel ortama vermektir. Ağların fiziksel büyüklük sınırlarını daha da genişletmek amacı ile kullanılan bu cihazlar ile kuramsal olarak bir bilgisayar ağı sonsuza kadar genişletilebilir. Ancak çeşitli bilgisayar ağlarındaki tasarım sınırlamaları nedeni ile gerçekte bu genişleme belli sınırlar içinde kalmaktadır. Çizim-4 tekrarlayıcıların bir



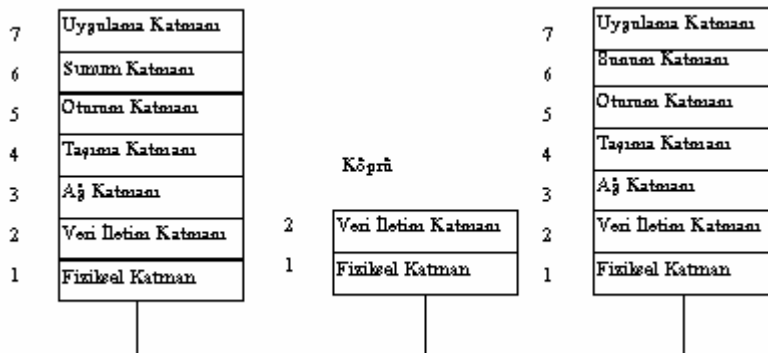
ağ üzerinde nasıl kullanıldıklarını göstermektedir.

Çizim-3 Bir tekrarlayıcı uygulaması

Temelde bir ağı genişletilmesi amacı ile kullanılan tekrarlayıcılar çok kolay kurulumları, çok az bakım gerektirmeleri ve fiyatlarının ucuz olması sebepleri ile çok popüler cihazlardır.

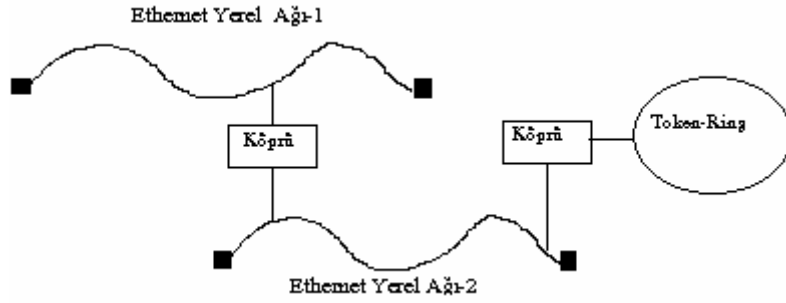
2.1.2.2 Köprü (Bridge)

Modern, protokol-şeffaf köprüler aşağıdaki şekilde görüldüğü gibi OSI referans modelinin veri iletim (data link) katmanında çalışırlar



Çizim 4 köprü ve OSI modeli

Köprü cihazları temelde bağımsız iki ağın (farklı ağ teknolojilerini kullanabilirler- Ethernet ve Token-Ring gibi) birbirine bağlantısı için kullanılırlar. Aşağıdaki şekilde iki Ethernet ve bir Token-Ring ağının birbirlerine köprüler vasıtasıyla yapılan bağlantısı gösterilmektedir. Bir köprü bağladığı alt ağlar üstündeki tüm trafiği yürütür. Her paketi okur, paketin nereden geldiğini ve nereye gittiğini görmek için MAC (Media Access Control)-katman kaynağını ve yerleşim (destination) adresini inceler. Bu süzme yeteneği mesajları yayınlamak ya da yerel veri trafiğinin diğer ağ üzerine geçmesini engellemek için etkili bir yol sağlar. Bazı köprüler adres süzmenin ve protokol tipine bağlı süzgecin de ötesine gider.

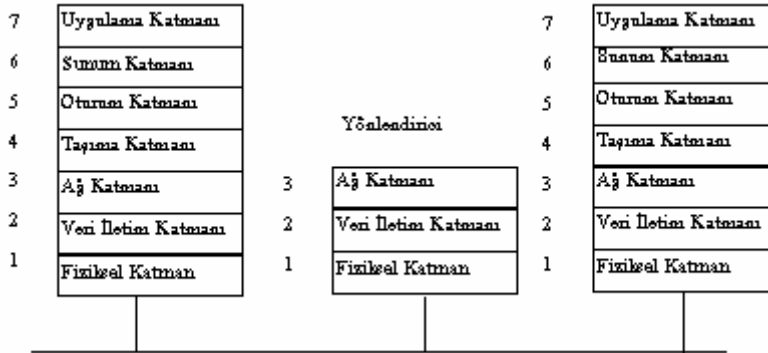


Çizim-5 Bir Köprü uygulaması

Bir köprü, DEÇnet, TCP/IP, XNS gibi farklı iletişim protokollarını kullanarak, protokol uyumluluğunu gözönüne almadan ağlar arasında fiziksel bağlantı sağlayabilse de, bu uygulamalar arasında işletilebilirliğini garanti etmemektedir. Bu, OSI referans modelinin yüksek katmanlarında işleyen ve farklı işlem ortamları arasında çevrim yapabilen standalone protokol çeviricilerini gerektirmektedir. Köprülü ağlar, protokol çevrimlerinin olmadığı, güvenlik gereksinimlerinin en az olduğu ve gereken tek şeyin basit yönlendirme olduğu durumlarda başarılıdır.

2.1.2.3 Yönlendirici (Router)

Yönlendiriciler aşağıdaki şekilde görüldüğü gibi OSI referans modelinin ağ (network) katmanında çalışırlar

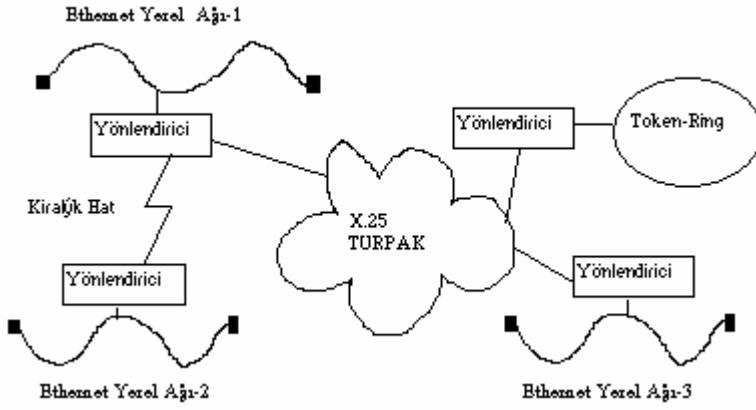


Çizim-6 Yönlendirici ve OSI modeli

Bir köprü sadece paketlerin kaynağını ve gittiği yerin adresini kontrol ederken bir yönlendirici çok daha fazlasını yapar. Bir yönlendirici ağın tüm haritasını tutar ve paketin gittiği yere en iyi yolu belirleyebilmek için tüm yolların durumunu inceler.

Yönlendirici farklı fiziksel yapıda olan ve farklı protokolları çalıştıran yerel ya da geniş alan ağlarının birbirleri ile olan bağlantısında başarı ile kullanılabilir.

Bir yönlendirici, OSI referans modelinin ağ katmanında genel olarak tanımlanan protokollerle, yerel bölge ağlarını geniş bölge ağlarına bağlar. Bu özellikleri sayesinde örneğin yönlendirici TCP/IP kullanarak bir Ethernet ağının X.25 paket ağına bağlanmasını sağlar. Eski yönlendiriciler protokol bağımlı olduklarından, kuruluşların ağ işletim ihtiyaçlarını karşılamak için birden fazla yönlendirici gerekebilir. Yeni yönlendiriciler ise, birden fazla ve değişik protokolu aynı anda idare edebilmektedirler.

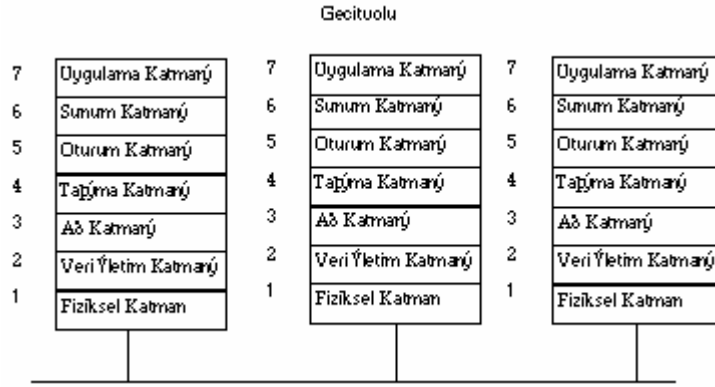


Çizim-7 Bir yönlendirici uygulaması

Yönlendiriciler paketleri iki istasyon arasındaki en iyi yolu gösteren yönlendirme tablosuna göre ilerleterek ağ üzerindeki yolları en iyi şekilde kullanırlar. Yönlendiriciler kendi yönlendirme tablolarını oluşturduklarından, ağ trafiğindeki değişikliklere hemen ayak uydururlar ve böylelikle veri yükünü dengelerler. Aynı zamanda, yönlendiriciler ağdaki değişiklikleri tespit ederler ve aşırı yüklü ve işlemeyen bağlantıları önerler.

2.1.2.4 Geçityolları (Gateway)

Geçityolları köprü ve yönlendiricilerin yeteneklerinin de ötesine geçerler. Aşağıdaki şekilden de görülebileceği gibi OSI referans modelinin üst katmanlarında işlerler.



Çizim 8 geçit yolu ve OSI modeli

Geçityolları sadece farklı noktadaki ağları bağlamakla kalmaz aynı zamanda bir ağdan taşınan verinin diğer ağlarla uyumlu olmasını da garanti ederler. Bu bir server'da, minibilgisayarda ya da ana bilgisayarda bulunan protokol çevirim yazılımıyla yapılır. İnternet protokolları farklı ağlar arasındaki veri iletimini, geçityollarıyla bağlı altağlardan oluşmuş otonom sistem (Autonomous System, AS) gruplarını birbirine bağlayarak yapar. Yani İnternet, her biri merkezi olarak yönetilen ağ ya da altağlar serisi olan AS serisinden oluşmaktadır. Her AS diğer AS'lere bağlantı sağlayan geçityolu sunar. Geçityolları tüm farklı ağları birlikte tutan bir yapıştırıcıdır. İnternet protokolları altağların nasıl birbirine bağlı olduğunu ve bağlantı araçlarının nasıl çalıştığını tanımlar.

3.TCP/IP ve Bileşenleri

Şu ana kadar bilgisayar ağı kavramları ve ağ yapısının fiziksel katmanları hakkında genel bir fikir edindik. Bu noktada bilgisayarlar arası iletişimi sağlayan temel protokol katmanlarına gelmiş bulunuyoruz. Burada alt yapı protokolları ile ilgili detaylı ancak çok teknik olmayan bilgiler verilecek ve sistemin temel çalışma prensipleri açıklanmaya çalışılacaktır.

3.1 Genel tanımlar

TCP/IP katmanlardan oluşan bir protokoller kümesidir. Her katman değişik görevlere sahip olup altındaki ve üstündeki katmanlar ile gerekli bilgi alışverişini sağlamakla yükümlüdür. Aşağıdaki şekilde bu katmanlar bir blok sema halinde gösterilmektedir.

	SMTP	RLOGIN	FTP	TELNET	DOMAIN	TFTP
Uygulama	TCP			UDP		
Taşıma	IP			ICMP		
Yönlendirme	IEEE 802.2 / LAPB/ HDLC					
Fiziksel	Ethernet, X.25, Token-Ring, Dial-up, vs.					

Cizim-9 TCP/IP katmanları

TCP/IP katmanlarının tam olarak ne olduğu, nasıl çalıştığı konusunda bir fikir sahibi olabilmek için bir örnek üzerinde inceleyelim:

TCP/IP nin kullanıldığı en önemli servislerden birisi elektronik postadır (e-posta). E- posta servisi için bir uygulama protokolu belirlenmiştir (SMTP). Bu protokol e- posta'nın bir bilgisayardan bir başka bilgisayara nasıl iletileceğini belirler. Yani e- postayı gönderen ve alan kişinin adreslerinin belirlenmesi, mektup içeriğinin hazırlanması vs. gibi. Ancak e-posta servisi bu mektubun bilgisayarlar arasında nasıl iletileceği ile ilgilenmez, iki bilgisayar arasında bir iletişimin olduğunu varsayarak mektubun yollanması görevini TCP ve IP katmanlarına bırakır. TCP katmanı komutların karşı tarafa ulaştırılmasından sorumludur. Karşı tarafa ne yollandığı ve hatalı yollanan mesajların tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar. Eğer gönderilecek mesaj bir kerede gönderilemeyecek kadar büyük ise (Örneğin uzunca bir e-posta gönderiliyorsa) TCP onu uygun boydaki segment'lere (TCP katmanlarının iletişim için kullandıkları birim bilgi miktarı) böler ve bu segment'lerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar. İnternet üzerindeki tek servis e-posta olmadığı için ve segment'lerin karşı tarafa hatasız ulaştırılmasını sağlayan iletişim yöntemine tüm diğer servisler de ihtiyaç duyduğu için TCP ayrı bir katman olarak çalışmakta ve tüm diğer servisler onun üzerinde yer almaktadır. Böylece yeni bir takım uygulamalar da daha kolay geliştirilebilmektedir. Üst seviye uygulama protokollerinin TCP katmanını çağırması gibi benzer şekilde TCP de IP katmanını çağırılmaktadır. Ayrıca bazı servisler TCP katmanına ihtiyaç duymamakta ve bunlar direk olarak IP katmanı ile görüşmektedirler. Böyle belirli görevler için belirli hazır yordamlar oluşturulması ve protokol seviyeleri inşa edilmesi stratejisine 'katmanlaşma' adı verilir. Yukarıda verilen örnekteki e- posta servisi (SMTP), TCP ve IP ayrı katmanlardır ve her katman altındaki diğer katman ile konuşmakta diğer bir deyişle onu çağırmakta ya da onun sunduğu servisleri kullanılmaktadır. En genel haliyle TCP/IP uygulamaları 4 ayrı katman kullanır. Bunlar:

- Bir uygulama protokolu, mesela e-posta
- Üst seviye uygulama protokollarının gereksinim duyduğu TCP gibi bir protokol katmanı
- IP katmanı. Gönderilen bilginin istenilen adrese yollanmasını sağlar.
- Belirli bir fiziksel ortamı sağlayan protokol katmanı. Örneğin Ethernet, seri hat, X.25 vs.

İnternet birbirine geçiş yolları (gateway) ile bağlanmış çok sayıda bağımsız bilgisayar ağlarından oluşur ve buna 'çatenet model' adı verilir. Kullanıcı bu ağlar üzerinde yer alan herhangi bir bilgisayara ulaşmak isteyebilir. Bu işlem esnasında kullanıcı farkına varmadan bilgiler, düzinelere ağ üzerinden geçiş yapıp varış yerine ulaşırlar. Bu kadar işlem esnasında kullanıcının bilmesi gereken tek şey ulaşmak istediği noktadaki bilgisayarın 'İnternet adresi' dir. Bu adres toplam 32 bit uzunluğunda bir sayıdır. Fakat bu sayı 8 bitlik 4 ayrı ondalık sayı şeklinde kullanılır (144.122.199.20 gibi). Bu 8 bitlik gruplara 'octet' ismi de verilir. Bu adres yapısı genelde karşıdaki sistem hakkında bilgi de verir. Mesela 144.122 ODTU için verilmiş bir numaradır. ODTU üçüncü octet'i kampus içindeki birimlere dağıtmıştır. Örneğin, 144.122.199 bilgisayar merkezinde bulunan bir Ethernet ağda kullanılan bir adrestir. Son octet ise bu Ethernete 254 tane bilgisayar bağlanmasına izin verir (0 ve 255 bilgisayar adreslemesinde kullanılmayan özel amaçlı adresler olduğu için 254 bilgisayar adreslenebilir).

IP bağlantısız "connectionless" ağ teknolojisini kullanılmaktadır ve bilgi "datagramlar" (TCP/IP temel bilgi birim miktarı) dizisi halinde bir noktadan diğerine iletilir. Büyük bir bilgi grubunun (büyük bir dosya veya e-posta gibi) parçaları olan "datagram" ağ üzerinde tek basına yol alır. Mesela 15000 octet'lik bir kütük pek çok ağ tarafından bir kere de iletilemeyecek kadar büyük olduğu için protokoller bunu 30 adet 500 octetlik datagramlara böler. Her datagram ağ üzerinden tek tek yollanır ve bunlar karşı tarafta yine 15000 octet lik bir kütük olarak birleştirilir. Doğal olarak önce yola çıkan bir datagram kendisinden sonra yola çıkan bir datagramdan sonra karşıya varabilir veya ağ üzerinde oluşan bir hatadan dolayı bazı datagramlar yolda kaybolabilir. Kaybolan veya yanlış sırada ulaşan datagramların sıralanması veya hatalı gelenlerin yeniden alınması hep üst seviye protokollerce yapılır. Bu arada "paket" ve "datagram" kavramlarına bir açıklama getirmek yararlı olabilir. TCP/IP ile ilgili kavramlarda "datagram" daha doğru bir terimdir. Zira datagram TCP/IP de iletişim için kullanılan birim bilgi miktarıdır. Paket ise fiziksel ortamdan (Ethernet, X.25 vs.) ortama değişen bir büyüklüktür. Mesela X.25 ortamında datagramlar 128 byte lik paketlere dönüştürülüp fiziksel ortamda böyle taşınırlar

ve bu işlemle IP seviyesi hiç ilgilenmez. Dolayısıyla bir IP datagramı X.25 ortamında birden çok paketler halinde taşınmış olur.

3.1.1 TCP katmanı

TCP'nin ("transmission control protocol-iletişim kontrol protokolü") temel işlevi, üst katmandan (uygulama katmanı) gelen bilginin segmentler haline dönüştürülmesi, iletişim ortamında kaybolan bilginin tekrar yollanması ve ayrı sıralar halinde gelebilen bilginin doğru sırada sıralanmasıdır. IP ("internet protocol") ise tek tek datagramların yönlendirilmesinden sorumludur. Bu açıdan bakıldığında TCP katmanının hemen hemen tüm işi üstlendiği görülmekle beraber (küçük ağlar için bu doğrudur) büyük ve karmaşık ağlarda IP katmanı en önemli görevi üstlenmektedir. Bu gibi durumlarda değişik fiziksel katmanlardan geçmek, doğru yolu bulmak çok karmaşık bir iş halini almaktadır.

Şu ana kadar sadece İnternet adresleri ile bir noktadan diğer noktaya ulaşılması konusundan bahsettik ancak birden fazla kişinin aynı sisteme ulaşmak istemesi durumunda neler olacağı konusuna henüz bir açıklık getirmediğimiz. Doğal olarak bir segment'i doğru varış noktasına ulaştırmak tek başına yeterli değildir. TCP bu segment'in kime ait olduğunu da bilmek zorundadır. "Demultiplexing" bu soruna çare bulan yöntemdir. TCP/IP 'de değişik seviyelerde "demultiplexing" yapılır. Bu işlem için gerekli bilgi bir seri "başlık" (header) içinde bulunmaktadır. Başlık, datagram'a eklenen basit bir kaç octet'den oluşan bir bilgiden ibarettir. Yollanmak istenen mesajı bir mektuba benzetecek olursak başlık o mektubun zarfı ve zarf üzerindeki adres bilgisidir. Her katman kendi zarfını ve adres bilgisini yazıp bir alt katmana iletmekte ve o alt katmanda onu daha büyük bir zarfın içine koyup üzerine adres yazıp diğer katmana iletmektedir. Benzer işlem varış noktasında bir sefer ters sırada takip edilmektedir.

Bir örnek vererek açıklamaya çalışırsak: Aşağıdaki noktalar ile gösterilen satır bir noktadan diğer bir noktaya gidecek olan bir dosyayı temsil etsin,

.....
TCP katmanı bu dosyayı taşınabilecek büyüklükteki parçalara ayırır:

Her segment'in başına TCP bir başlık koyar. Bu başlık bilgisinin en önemlileri 'port numarası' ve 'sıra numarası' dir. Port numarası, örneğin birden fazla kişinin aynı anda dosya yollaması veya karşıdaki bilgisayara bağlanması durumunda TCP'nin herkese verdiği farklı bir numaradır. Uç kişi aynı anda dosya transferine başlamışsa TCP, 1000, 1001 ve 1002 "kaynak" port numaralarını bu uç kişiye verir böylece herkesin paketi birbirinden ayrılmış olur. Aynı zamanda varış noktasındaki TCP de ayrıca bir "varış" port numarası verir. Kaynak noktasındaki TCP nin varış port numarasını bilmesi gereklidir ve bunu iletişim kurulduğu anda TCP karşı taraftan öğrenir. Bu bilgiler başlıktaki "kaynak" ve "varış" port numaraları olarak belirlenmiş olur. Ayrıca her segment bir "sıra" numarasına sahiptir. Bu numara ile karşı taraf doğru sayıdaki segmenti eksiksiz alıp almadığını anlayabilir. Aslında TCP segmentleri değil octetleri numaralar. Diyelim ki her datagram içinde 500 octet bilgi varsa ilk datagram numarası 0, ikinci datagram numarası 500, üçüncüsü 1000 şeklinde verilir. Başlık içinde bulunan üçüncü önemli bilgi ise "kontrol toplamı" (Checksum) sayısıdır. Bu sayı segment içindeki tüm octetler toplanarak hesaplanır ve sonuç başlığın içine konur. Karşı noktadaki TCP kontrol toplamı hesabını tekrar yapar. Eğer bilgi yolda bozulmamışsa kaynak noktasındaki hesaplanan sayı ile varış noktasındaki hesaplanan sayı aynı çıkar. Aksi takdirde segment yolda bozulmuştur bu durumda bu datagram kaynak noktasından tekrar istenir. Aşağıda bir TCP segmenti örneği verilmektedir.

Kaynak Portu	Varış Portu									
Sıra numarası										
Onay (Acknowledgement)										
Data Offset	Reserve	0	1	0	1	0	1	0	1	Pencere (Window)
Kontrol Toplamı	Acil işaret (Urgent Pointer)									
Bilgi diğer 500 octet										

Çizim-10 TCP Segmenti

Eğer TCP başlığını "T" ile gösterecek olursak yukarıda noktalarla gösterdiğimiz dosya aşağıdaki duruma gelir:

T... T... T... T... T...

Başlık içinde bulunan diğer bilgiler genelde iki bilgisayar arasında kurulan bağlantının kontrolüne yöneliktir. Segment'in varışında alıcı gönderici noktaya bir "onay" (acknowledgement) yollar. Örneğin kaynak noktasına yollanan "onay numarası" (Acknowledgement number) 1500 ise octet numarası 1500 e kadar tüm bilginin alındığını gösterir. Eğer kaynak noktası belli bir zaman içinde bu bilgiyi varış noktasından alamazsa o bilgiyi tekrar yollar. "Pencere" bilgisi bir anda ne kadar bilginin gönderileceğini kontrol etmek için kullanılır. Burada amaç her segment'in gönderilmesinden sonra karşıya ulaşmış olup olmadığı ile ilgili onay (ack) beklenmesi yerine segment'leri onay beklemeksizin pencere bilgisine göre yollamaktır. Zira yavaş hatlar kullanılarak yapılan iletişimde onay beklenmesi iletişimi çok daha yavaşlatır. Diğer taraftan

çok hızlı bir şekilde sürekli segment yollanması karşı tarafın bir anda alabileceğinden fazla bir trafik yaratacağından yine problemler ortaya çıkabilir. Dolayısıyla her iki taraf o anda ne kadar bilgiyi alabileceğini “pencere” bilgisi içinde belirtir. Bilgisayar bilgiyi aldıkaça pencere alanındaki bos yer azalır ve sıfır olduğunda yollayıcı bilgi yollamayı durdurur. Alıcı nokta bilgiyi işledikçe pencere artar ve bu da yeni bilgiyi karşıdan kabul edebileceğini gösterir. “Açıl işareti” ise bir kontrol karakteri veya diğeri bir komut ile transferi kesmek vs. amaçlarla kullanılan bir alandır. Bunlar dışında ki alanlar TCP protokolunun detayları ile ilgili olduğu için burada anlatılmayacaktır.

3.1.2 IP katmanı

TCP katmanına gelen bilgi segmentlere ayrıldıktan sonra IP katmanına yollanır. IP katmanı, kendisine gelen TCP segmenti içinde ne olduğu ile ilgilenmez. Sadece kendisine verilen bu bilgiyi ilgili IP adresine yollamak amacıdadır. IP katmanının görevi bu segment için ulaşılmak istenen noktaya gidecek bir “yol” (route) bulmaktır. Arada geçilecek sistemler ve geçiş yollarının bu paketi doğru yere geçirmesi için kendi başlık bilgisini TCP katmanından gelen segment’e ekler. TCP katmanından gelen segmentlere IP başlığının eklenmesi ile oluşturulan IP paket birimlerine datagram adı verilir. IP başlığı eklenmiş bir datagram aşağıdaki çizimde gösterilmektedir:

Version	IHL	Service tipi	Toplam usulak	
Tanımlama			Bayrak	Fragment offset
Yaşam süresi (TTL)		Protokol	Başlık kontrol toplamı	
Kaynak Adresi				
Varış Adresi				
TCP başlığı ve iletilen bilgi				

Çizim 11 IP datagram

Bu başlıktaki temel bilgi kaynak ve varış İnternet adresi (32-bitlik adres, 144.122.199.20 gibi), protokol numarası ve kontrol toplamıdır. Kaynak İnternet adresi tabii ki sizin bilgisayarınızın İnternet adresidir. Bu sayede varış noktasındaki bilgisayar bu paketin nereden geldiğini anlar. Varış İnternet adresi ulaşmak istediğiniz bilgisayarın adresidir. Bu bilgi sayesinde aradaki yönlendiriciler veya geçiş yolları (gateway) bu datagram’i nereye yollayabileceklerini bilirler. Protokol numarası IP’ye karşı tarafta bu datagram’i TCP’ye vermesi gerektiğini söyler. Her ne kadar IP trafiğinin çoğunu TCP kullansa da TCP dışında bazı protokollerde kullanılmaktadır dolayısıyla protokoller arası bu ayırım protokol numarası ile belirlenir. Son olarak kontrol toplamı IP başlığının yolda bozulup bozulmadığını kontrol etmek için kullanılır. Dikkat edilirse TCP ve IP ayrı ayrı kontrol toplamı kullanılmaktadır. IP kontrol toplamı başlık bilgisinin bozulup bozulmadığı veya mesajın yanlış yere gidip gitmediğini kontrol için kullanılır. Bu protokollerin tasarımı sırasında TCP’nin ayrıca bir kontrol toplamı hesaplaması ve kullanması daha verimli ve güvenli bulunduğu için iki ayrı kontrol toplamı alınması yoluna gidilmiştir.

IP başlığını “I” ile gösterecek olursak IP katmanından çıkan ve TCP verisi taşıyan bir datagram şu hale gelir:

IT...IT...IT...IT...IT...

Başlıktaki “Yaşam süresi” (Time to Live) alanı IP paketinin yolculuğu esnasında geçilen her sistemde bir azaltılır ve sıfır olduğunda bu paket yok edilir. Bu sayede oluşması muhtemel sonsuz döngüler ortadan kaldırılmış olur. IP katmanında artık başka başlık eklenmez ve iletilecek bilgi fiziksel iletişim ortamı üzerinden yollanmak üzere alt katmana (bu Ethernet, X.25, telefon hattı vs. olabilir) yollanır.

3.1.3 Fiziksel katman

Fiziksel katman gerçekte Data Link Connection (DLC) ve Fiziksel ortamı içermektedir. Ancak biz burada bu ara katmanları genelleyip tümüne Fiziksel katman adını vereceğiz. Günümüzde pek çok bilgisayar ağının Etherneti temel iletişim ortamı olarak kullanmasından dolayı da Ethernet teknolojisini örnek olarak anlatacağız. Dolayısıyla burada Ethernet ortamının TCP/IP ile olan iletişimini açıklayacağız. Ethernet kendine has bir adresleme kullanır. Ethernet tasarlanırken dünya üzerinde herhangi bir yerde kullanılan bir Ethernet kartının tüm diğeri kartlardan ayrılmasını sağlayan bir mantık izlenmiştir. Ayrıca, kullanıcının Ethernet adresinin ne olduğunu düşünmemesi için her Ethernet kartı fabrika çıkışında kendisine has bir adresle piyasaya verilmektedir. Her Ethernet kartının kendine has numarası olmasını sağlayan tasarım 48 bitlik fiziksel adres yapısıdır. Ethernet kart üreticisi firmalar merkezi bir otoriteden üretecekleri kartlar için belirli büyüklükte numara blokları alır ve üretimlerinde bu numaraları kullanırlar. Böylece başka bir üreticinin kartı ile bir çakışma meydana gelmez. Ethernet teknoloji olarak yayın teknolojisini (broadcast medium) kullanır. Yani bir istasyondan

Ethernet ortamına yollanan bir paketi o Ethernet ağındaki tüm istasyonlar görür. Ancak doğru varış noktasının kim olduğunu, o ağa bağlı makinalar Ethernet başlığından anlarlar. Her Ethernet paketi 14 octet'lik bir başlığa sahiptir. Bu başlıkta kaynak ve varış Ethernet adresi ve bir tip kodu vardır. Dolayısıyla ağ üzerindeki her makina bir paketin kendine ait olup olmadığını bu başlıktaki varış noktası bilgisine bakarak anlar (Bu Ethernet teknolojisindeki en önemli güvenlik boşluklarından birisidir). Bu noktada Ethernet adresleri ile İnternet adresleri arasında bir bağlantı olmadığını belirtmekte yarar var. Her makina hangi Ethernet adresinin hangi İnternet adresine karşılık geldiğini tutan bir tablo tutmak durumundadır (Bu tablonun nasıl yaratıldığı ilerde açıklanacaktır). Tip kodu alanı aynı ağ üzerinde farklı protokolların kullanılmasını sağlar. Dolayısıyla aynı anda TCP/IP, DECnet, IPX/SPX gibi protokoller aynı ağ üzerinde çalışabilir. Her protokol başlıktaki tip alanına kendine has numarasını koyar. Kontrol toplamı (Checksum) alanındaki değer ile komple paket kontrol edilir. Alıcı ve vericinin hesapladığı değerler birbirine uymuyorsa paket yok edilir. Ancak burada kontrol toplamı başlığın içine değilde paketin sonuna konulur. Ethernet katmanında işlenip gönderilen mesaj ya da bilginin (Bu bilgi paketlerine frame adı verilir) son halı aşağıdaki duruma gelir:

Ethernet varış adresi (ilk 32 bit)	
Ethernet varış (ilk 16 bit)	Ethernet kaynak (ilk16 bit)
Ethernet kaynak adresi (son 32 bit)	
Tip Kodu	
IP başlık, TCP başlık, iletilen bilgi	
..... bilginin sonu	
Ethernet kontrol toplamı (checksum)	

Çizim-12 Ethernet Paketi

Ethernet başlığını "E" ile ve Kontrol toplamını "C" ile gösterirsek yolladığımız dosya şu şekli alır:

EIT...C

EIT...C EIT...C EIT...C EIT...C

Bu paketler (frame) varış noktasında alındığında bütün başlıklar uygun katmanlarca atılır. Ethernet arayüzü Ethernet başlık ve kontrol toplamını atar. Tip koduna bakarak protokol tipini belirler ve Ethernet cihaz sürücüsü (device driver) bu datagram'ı IP katmanına geçirir. IP katmanı kendisi ile ilgili katmanı atar ve protokol alanına bakar, protokol alanında TCP olduğu için segmenti TCP katmanına geçirir. TCP sıra numarasına bakar, bu bilgiyi ve diğer bilgileri iletilen dosyayı orijinal durumuna getirmek için kullanır. Sonuçta bir bilgisayar diğer bir bilgisayar ile iletişimi tamamlar.

3.1.3.1 Ethernet encapsulation: ARP

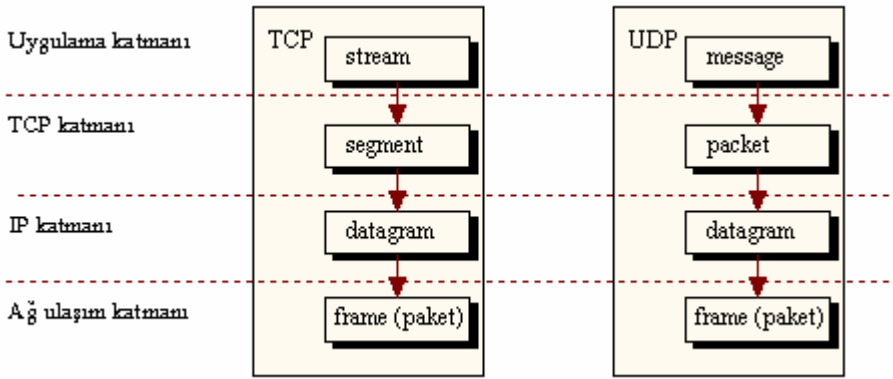
Yukarıda Ethernet üzerinde IP datagramların nasıl yer aldığından bahsettik. Fakat açıklanmadan kalan bir nokta bir İnternet adresi ile iletişime geçmek için hangi Ethernet adresine ulaşmamız gerektiği idi. Bu amaçla kullanılan protokol ARP'dir ("Address Resolution Protocol"). ARP aslında bir IP protokolu değildir ve dolayısıyla ARP datagramları IP başlığına sahip değildir. Varsayalımki bilgisayarınız 128.6.4.194 IP adresine sahip ve siz de 128.6.4.7 ile iletişime geçmek istiyorsunuz. Sizin sisteminizin ilk kontrol edeceği nokta 128.6.4.7 ile aynı ağ üzerinde olup olmadığınızdır. Aynı ağ üzerinde yer alıyorsanız, bu Ethernet üzerinden direk olarak haberleşebileceksiniz anlamına gelir. Ardından 128.6.4.7 adresinin ARP tablosunda olup olmadığı ve Ethernet adresini bilip bilmediği kontrol edilir. Eğer tabloda bu adresler varsa Ethernet başlığına eklenir ve paket yollanır. Fakat tabloda adres yoksa paketi yollamak için bir yol yoktur. Dolayısıyla burada ARP devreye girer. Bir ARP istek paketi ağ üzerine yollanır ve bu paket içinde "128.6.4.7" adresinin Ethernet adresi nedir sorgusu vardır. Ağ üzerindeki tüm sistemler ARP isteğini dinlerler bu isteği cevaplandırması gereken istasyona bu istek ulaştığında cevap ağ üzerine yollanır. 128.6.4.7 isteği görür ve bir ARP cevabı ile "128.6.4.7 nin Ethernet adresi 8:0:20:1:56:34" bilgisini istek yapan istasyona yollar. Bu bilgi, alıcı noktada ARP tablosuna işlenir ve daha sonra benzer sorgulama yapılmaksızın iletişim mümkün kılınır. Ağ üzerindeki bazı istasyonlar sürekli ağı dinleyerek ARP sorgularını alıp kendi tablolarını da güncelleyebilirler.

3.1.4 TCP dışındaki diğer protokoller: UDP ve ICMP

Yukarıda sadece TCP katmanını kullanan bir iletişim turunu açıkladık. TCP gördüğümüz gibi mesajı segment'lere bölen ve bunları birleştiren bir katmandı. Fakat bazı uygulamalarda yollanan mesajlar tek bir datagram'ın içine girebilecek büyüklüktedirler. Bu cins mesajlara en güzel örnek adres kontrolüdür (name lookup). İnternet üzerindeki bir bilgisayara ulaşmak için kullanıcılar İnternet adresi yerine o bilgisayarın adını kullanırlar. Bilgisayar sistemi bağlantı kurmak için çalışmaya başlamadan önce bu ismi İnternet adresine çevirmek durumundadır. İnternet adreslerinin isimlerle karşılık tabloları belirli bilgisayarlar üzerinde tutulduğu için kullanıcının sistemi bu bilgisayardan bu adresi sorgulayıp öğrenmek durumundadır. Bu sorgulama çok kısa bir işlemdir ve tek bir segment içine sığar. Dolayısıyla bu iş için TCP katmanının kullanılması gereksizdir. Cevap paketinin yolda kaybolması durumunda en kötü ihtimalle bu sorgulama tekrar yapılır. Bu cins kullanımlar için TCP nin alternatifi protokoller vardır. Böyle amaçlar için en çok kullanılan protokol ise UDP'dir(User Datagram Protocol).

UDP datagramlarının belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere dizayn edilmiştir. TCP’de olduğu gibi UDP’de de bir başlık vardır. Ağ yazılımı bu UDP başlığını iletilecek bilginin başına koyar. Ardından UDP bu bilgiyi IP katmanına yollar. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir (bu sefer protokol numarası alanına UDP’ye ait değer yazılır). Fakat UDP TCP’nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kaydı tutulmaz. UDP’nin tek sağladığı port numarasıdır. Böylece pek çok program UDP’yi kullanabilir. Daha az bilgi içerdiği için doğal olarak UDP başlığı TCP başlığına göre daha kısadır. Başlık, kaynak ve varış port numaraları ile kontrol toplamını içeren tüm bilgidir.

Diğer bir protokol ise ICMP’dir (“İnternet Control Message Protocol”). ICMP, hata mesajları ve TCP/IP yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır. Mesela bir bilgisayara bağlanmak istediğinizde sisteminiz size “host unreachable” ICMP mesajı ile geri dönebilir. ICMP ağ hakkında bazı bilgileri toplamak amacı ile de kullanılır. ICMP yapı olarak UDP’ye benzer bir protokoldür. ICMP de mesajlarını sadece bir datagram içine koyar. Bununla beraber UDP’ye göre daha basit bir yapıdadır. Başlık bilgisinde port numarası bulundurmaz. Bütün ICMP mesajları ağ yazılımının kendisince yorumlanır, ICMP mesajının nereye gideceği ile ilgili bir port numarasına gerek yoktur. ICMP ‘yi kullanan en popüler İnternet uygulaması PING komutudur. Bu komut yardımı ile İnternet kullanıcıları ulaşmak istedikleri herhangi bir bilgisayarın açık olup olmadığını, hatlardaki sorunları anında test etmek imkanına sahiptirler Şu ana kadar gördüğümüz katmanları ve bilgi akışının nasıl olduğunu aşağıdaki şekilde daha açık izleyebiliriz.



Cizim-13 Katmanlar arası bilgi akış

3.1.5 İnternet Adresleri

Daha önce de gördüğümüz gibi İnternet adresleri 32-bitlik sayılardır ve noktalarla ayrılmış 4 octet (ondalık sayı olarak) olarak gösterilirler. Örnek vermek gerekirse, 128.10.2.30 İnternet adresi 10000000 00001010 00000010 00011110 şeklinde 32-bit olarak gösterilir. Temel problem bu bilgisayar ağı adresinin hem bilgisayar ağını ve hem de belli bir bilgisayarı tek başına gösterebilmesidir.

İnternet’te değişik büyüklükte bilgisayar ağlarının bulunmasından dolayı İnternet adres yapısının tüm bu ağların adres sorununu çözmesi gerekmektedir. Tüm bu ihtiyaçları karşılayabilmek amacı ile İnternet tasarlanırken 32bitlik adres yapısı seçilmiş ve bilgisayar ağlarının çoğunun küçük ağlar olacağı varsayımı ile yola çıkılmıştır.

32-bit İnternet adresleri, 'Ağ Bilgi Merkezi (NIC) İnternet Kayıt Kabul' tarafından yönetilmektedir. Yerel yönetilen bir ağ uluslararası platformda daha büyük bir ağa bağlanmadığında adres rastgele olabilir. Fakat, bu tip adresler ileride İnternet’e bağlanması durumunda sorun çıkartabileceği için önerilmemektedir. Ağ yöneticisi bir diğer IP-tabanlı sisteme, örneğin NSFNET’e bağlanmak istediğinde tüm yerel adreslerin 'Uluslararası İnternet Kayıt Kabul' tarafından belirlenmesi zorunludur.

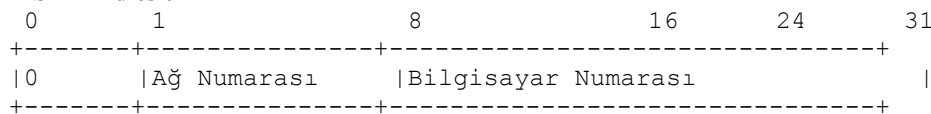
Değişik büyüklükteki ağları adreslemek amacı ile 3 sınıf adres kullanılmaktadır:

A Sınıfı adresler: İlk byte 0 'la 126 arasında değişir. İlk byte ağ numarasıdır. Gerişi bilgisayarların adresini belirler. Bu tip adresleme, herbiri 16,777,216 bilgisayardan oluşan 126 ağın adreslenmesine izin verir.

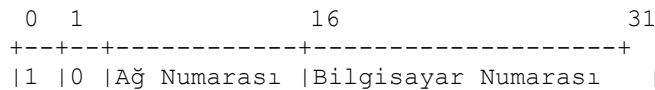
B Sınıfı adresler: İlk byte 128 'le 191 arasında değişir. İlk iki byte ağ numarasıdır. Gerişi bilgisayar adresini belirler. Bu tip adresleme, herbiri 65,536 bilgisayardan oluşan 16,384 ağın adreslenmesine izin verir.

Ç Sınıfı adresler: ilk byte 192 ile 223 arasında değişir. ilk üç byte ağ numarasıdır. Gerişi bilgisayarların adresini belirler. Bu tip adresleme, herbiri 254 bilgisayardan oluşan 2,000,000 ağın adreslenmesine izin verir.

A Sınıfı Adresler



B Sınıfı Adresler



```

+---+---+-----+-----+
C Sınıfı Adresler
 0 1 2          24          31
+---+---+-----+-----+
|1 |1 |0 |Ağ Numarası   |Bilgisayar Numarası   |
+---+---+-----+-----+

```

127 ile başlayan adresler İnternet tarafından özel amaçlarla (localhost tanımı için) kullanılmaktadır. 223'un üzerindeki adresler gelecekte kullanılmak üzere D-sınıfı ve E-sınıfı adresler olarak reserve edilmiş olarak tutulmaktadır.

A sınıfı adresler, NSFNET, MILNET gibi büyük ağlarda kullanılır. C sınıfı adresler, genellikle üniversite yerleşkelerinde kurulu yerel ağlarla, ufak devlet kuruluşlarında kullanılır. NIC sadece ağ numaralarını yönetir. Bölgede olması beklenen bilgisayar sayısına göre A, B veya Ç sınıfı adresleme seçilir. Bir bölgeye ağ numarası verildikten sonra bilgisayarların nasıl adresleneceğini bölge yönetimi belirler. IP adres alanı özellikle son yıllarda artan kullanım talebi sonucunda hızla tükenmeye başlamıştır. Bu nedenle yapılan IP adres taleplerinin gerçekçi olmasının sağlanması için gerekli kontroller yapılmaktadır.

3.1.6 Alt Ağlar (subnet)

subnet ya da alt ağ kavramı, kurumların ellerindeki İnternet adres yapısından daha verimli yararlanmaları için geliştirilen bir adresleme yöntemidir. Pek çok büyük organizasyon kendilerine verilen İnternet numaralarını "subnet" lere bölerek kullanmayı daha uygun bulmaktadırlar. Subnet kavramı aslında 'Bilgisayar numarası' alanındaki bazı bitlerin 'Ağ numarası' olarak kullanılmasından ortaya çıkmıştır. Böylece, elimizdeki bir adres ile tanımlanabilecek bilgisayar sayısı düşürülerek, tanımlanabilecek ağ sayısını yükseltmek mümkün olmaktadır.

Nasıl bir alt ağ yapısının kullanılacağı kurumların ağ alt yapılarına ve topolojilerine bağımlı olarak değişmektedir. Subnet kullanılması durumunda bilgisayarların adreslenmesi kontrolü merkezi olmaktan çıkmakta ve yetki dağıtımı yapılmaktadır. Subnet yapısının kullanılması yalnızca o adresi kullanan kurumun kendisini ilgilendirmekte ve bunun kurum dışına hiçbir etkisi de bulunmamaktadır. Herhangi bir dış kullanıcı subnet kullanılan bir ağa ulaşmak istediğinde o ağda kullanılan subnet yönteminden haberdar olmadan istediği noktaya ulaşabilir. Kurum sadece kendi içinde kullandığı geçiş yolları ya da yönlendiriciler üzerinde hangi subnet'e nasıl gidilebileceği tanımlamalarını yapmak durumundadır. Bir İnternet ağını subnet'lere bölmek, subnet maskesi denilen bir IP adresi kullanılarak yapılmaktadır. Eğer maske adresteki adres bit'i 1 ise o alan ağ adresini göstermektedir, adres bit'i 0 ise o alan adresin bilgisayar numarası alanını göstermektedir. Konuyu daha anlaşılır kılmak için bir örnek üzerinde inceleyelim:

ODTU kampüsü için bir B-sınıfı adres olan 144.122.0.0 kayıtlı olarak kullanılmaktadır. Bu adres ile ODTU 65.536 adet bilgisayarı adresleyebilme yeteneğine sahiptir. Standart B- sınıfı bir adresin maske adresi 255.255.0.0 olmaktadır. Ancak bu adres alındıktan sonra ODTU'nun teknik ve idari yapısı göz önünde tutularak farklı subnet yapısı uygulanmasına karar verilmiştir. Adres içindeki üçüncü octet'inde ağ alanı adreslemesinde kullanılması ile ODTU'de 254 adede kadar farklı bilgisayar ağının tanımlanabilmesi mümkün olmuştur. Maske adres olarak 255.255.255.0 kullanılmaktadır. İlk iki octet (255.255) B-sınıfı adresi, üçüncü octet (255) subnet adresini tanımlamakta, dördüncü octet (0) ise o subnet üzerindeki bilgisayarı tanımlamaktadır.

144.122.0.0 ODTU için kayıtlı adres

```

255.255.0.0 Standart B-Sınıfı adres maskesi      Bir ağ, 65536 bilgisayar
255.255.255.0 Yeni maske                        254 ağ, her ağda 254 bilgisayar

```

ODTU de uygulanan adres maskesi ile subnetlere bölünmüş olan ağ adresleri merkezi olarak BÖLÜMLere dağıtılmakta ve her bir subnet kendi yerel ağı üzerindeki ağ parçasında 254 taneye kadar bilgisayarını adresleyebilmektedir. Böylece tek bir merkezden tüm üniversitedeki makinelerin IP adreslerinin tanımlanması gibi bir sorun ortadan kaldırılmış ve adresleme yetkisi ayrı birimlere verilerek onlara kendi içlerinde esnek hareket etme kabiliyeti tanınmıştır. Bir örnek verecek olursak: Bilgisayar Mühendisliği BÖLÜMu için 71 subneti ayrılmış ve 144.122.71.0 ağ adresi kullanımlarına ayrılmıştır. Böylece, BÖLÜM içinde 144.122.71.1 den 144.122.71.254 'e kadar olan adreslerin dağıtım yetkisi BÖLÜMun kendisine bırakılmıştır. Aynı şekilde Matematik BÖLÜMu için 144.122.36.0, Fizik BÖLÜMu için 144.122.30.0 ağ adresi ayrılmıştır.

Ç-sınıfı bir adres üzerinde yapılan bir subnetlemeye örnek verecek olursak:

Elinde Ç-sınıfı 193.140.65.0 adres olan bir kurum subnet adresi olarak 255.255.255.192 kullandığında

```

193.140.65.0      11000001 10001100 01000001 00000000
255.255.255.192  11111111 11111111 11111111 11000000
<----->|<---->

```

```

|
Ağ numarası alanı   |Bilgisayar Numarası

```

elindeki bu adresi dört farklı parçaya bölebilir. Değişik subnet maskeleri ile nasıl sonuçlar edinilebileceği ile ilgili örnek bir tablo verecek olursak :

IP adres	Subnet	Açıklama
128.66.12.1	255.25.255.0	128.66.12 subneti üzerindeki 1. bilgisayar

130.97.16.132	255.255.255.192	130.97.16.128 subneti üzerindeki 4. bilgisayar.
192.178.16.66	255.255.255.192	192.178.16.64 subneti üzerindeki 2. bilgisayar
132.90.132.5	255.255.240.0	132.90.128 subnetindeki 4.5 inçi bilgisayar.
18.20.16.91	255.255.0.0	18.20.0.0 subnetindeki 16.91 inçi bilgisayar

3.1.6.1 Özel adresler

İnternet adreslemesinde 0 ve 255'in özel bir kullanımı vardır. 0 adresi, İnternet üzerinde kendi adresini bilmeyen bilgisayarlar için (Belirli bazı durumlarda bir makinanın kendisinin bilgisayar numarasını bilip hangi ağ üzerinde olduğunu bilmemesi gibi bir durum olabilmektedir) veya bir ağın kendisini tanımlamak için kullanılmaktadır (144.122.0.0 gibi). 255 adresi genel duyuru "broadcast" amacı ile kullanılmaktadır. Bir ağ üzerindeki tüm istasyonların duymasını istediğiniz bir mesaj genel duyuru "broadcast" mesajıdır. Duyuru mesajı genelde bir istasyon hangi istasyon ile konuşacağını bilemediği bir durumda kullanılan bir mesajlaşma yöntemidir. Örneğin ulaşmak istediğiniz bir bilgisayarın adı elinizde bulunabilir ama onun IP adresine ihtiyaç duyduunuz, bu çevirme işini yapan en yakın "name server" makinasının adresini de bilmiyorsunuz. Böyle bir durumda bu isteğinizi yayın mesajı yolu ile yollayabilirsiniz. Bazı durumlarda birden fazla sisteme bir bilginin gönderilmesi gerekebilir böyle bir durumda her bilgisayara ayrı ayrı mesaj gönderilmesi yerine tek bir yayın mesajı yollanması çok daha kullanışlı bir yoldur. Yayın mesajı yollamak için gidecek olan mesajın IP numarasının bilgisayar adresi alanına 255 verilir. Örneğin 144.122.99 ağı üzerinde yer alan bir bilgisayar yayın mesajı yollamak için 144.122.99.255 adresini kullanır. Yayın mesajı yollanması birazda kullanılan ağın fiziksel katmanının özelliklerine bağlıdır. Mesela bir Ethernet ağında yayın mümkün iken noktadan noktaya (point-to-point) hatlarda bu mümkün olmamaktadır.

Bazı eski şurum TCP/IP protokolüne sahip bilgisayarlarda yayın adresi olarak 255 yerine 0 kullanılabilir. Ayrıca yine bazı eski sürümler subnet kavramına hiç sahip olmayabilmektedir.

Yukarıda da belirttiğimiz gibi 0 ve 255'in özel kullanım alanları olduğu için ağa bağlı bilgisayarlara bu adresler kesinlikle verilmemelidir. Ayrıca adresler asla 0 ve 127 ile ve 223'un üzerindeki bir sayı ile başlamamalıdır.

4.Yönlendirme

Bu BÖLÜMde farklı coğrafi noktalarda yer alan TCP/IP ağlarının birbirleri ile olan iletişiminin sağlanması için en önemli anahtar olan, yol bulma yanı yönlendirme konusu açıklanacaktır.

Daha önceki açıklamalarımızda IP (İnternet Protokol) katmanının datagram'lerin (TCP/IP'de iletişim için kullanılan bilgi birim miktarı) varış noktasına ulaşmasını sağlamakla yükümlü olduğundan bahsettik. Fakat bu işlemin nasıl yapılacağına detaylarını incelemedik. Bir datagram'ın varış noktasına ulaştırılmasına 'yönlendirme' (routing) adı verilmektedir. Yönlendirmenin nasıl yapıldığını kavrayabilmek için IP'nin dayandığı modeli anlamak gereklidir. IP katmanı daima, bir sistemin bir ağa bağlı olduğunu varsayar. Ethernet tabanlı bir ağ üzerinde sadece karşı istasyonun Ethernet adresini bilmek yeterli olduğu için herşey çok kolaydır. Fakat datagram'lar farklı ağlar üzerindeki noktalara gönderilmek istendiğinde sorunlar başlar.

Bir ağ üzerinden diğer ağ üzerine geçecek bilgi trafiğini kontrol etmek, onu yönlendirmek görevi genel olarak 'geçiş noktası aygıtlarına' (gateway) aittir. İnternet üzerinde IP protokolu kullanan ağlarda bu işleri yerine getiren aygıtlara yönlendirici (router) adı verilir. Böyle bir görev üstlenen makina üzerinde birden fazla bilgisayar ağı bağlantısı yer alıp, farklı ağların bilgi trafikleri bu yolla birbirlerine iletilir. IP ağlarındaki yönlendirme tamamen varış noktası adresi temeline oturmaktadır. Örneğin ODTU'nun uluslararası İnternet bağlantısını yapan yönlendirici 144.122.1.2 adresinde bulunmaktadır. Dolayısıyla 144.122.1 ağı üzerinde yer alan diğer sistemler 144.122.1.2 adresini yurt dışı adreslere ulaşmak için geçiş noktası olarak tanımak zorundadırlar. Benzer bir şekilde Bilgisayar Mühendisliği BÖLÜMünün kampus omurga ağına geçiş noktası olarak kullandığı bilgisayarın adresi de 144.122.71.1'dir. 144.122.71 ağı üzerinde bulunan bir bilgisayar, kampus içindeki başka bir bilgisayara ulaşmak için bu geçiş noktasından geçmek zorundadır. Bu ağ üzerinde bulunan bir bilgisayar datagram yollamak istediğinde öncelikle ulaşmak istediği adresin aynı ağ üzerinde olup olmadığına bakar, eğer varış noktası aynı ağ üzerinde ise bilgi doğrudan varış adresine yollanır. Eğer değilse, sistem varış noktasına ulaşmak için gerekli bilgileri araştırmaya başlar.

4.1 Yönlendirme protokolları

Yukarıda da açıklandığı gibi yönlendirme, bir bilgisayar ağı üzerinde yer alan bir bilgisayarın aynı ya da farklı bir ağ üzerinde yer alan başka bir bilgisayara nasıl ulaşacağına karar verirken kullanılan yöntemdir. Bu sayede herhangi iki farklı noktada yer alan kullanıcılar birbirleri ile bilgisayar kullanarak haberleşebilmektedir. Dolayısıyla yönlendirmeyi bir nevi yapıştırıcı gibi düşünebiliriz.

İletişimin en önemli noktası olmasından dolayı yeni bilgisayar ağı kuruluşlarında en önemli sorunlardan birisi yanlış yapılan yönlendirme olmaktadır. Bu noktada yönlendirme ve yönlendirme protokolu arasındaki farkı açıklamak ileride oluşabilecek yanlış anlamaları önlemek açısından yararlı olacaktır. Bir bilgisayar ağına bağlı her sistem bilgiyi bir

noktadan bir diğerine yönlendirebilir ama her sistem üzerinde yönlendirme protokolu çalışmaz. Yönlendirme, bir yönlendirme tablosundaki bilgiye göre bilgi paketlerinin geçirilmesidir. Yönlendirme protokolu ise bu tabloların oluşturulmasında bilgi değişimini sağlayan programlardır. Basit bir bilgisayar ağında bir yönlendirme protokolu çalışmadan, sabit tablolar kullanarak iletişim sağlanabilir.

Temel olarak 3 yönlendirme yöntemi vardır (Aşağıda verilecek olan komutlar UNIX işletim sistemlerinde bulunmakta olup diğer sistemlerde farklı komutlar kullanılabilir):

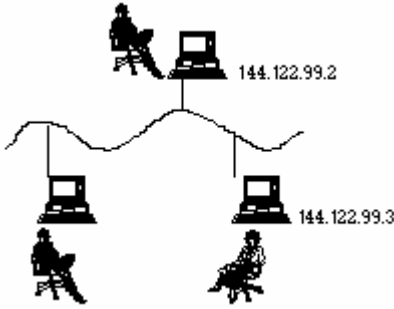
- Minimum yönlendirme: Bir bilgisayar ağı başka bir bilgisayar ağına bağlı olmaksızın tek başına çalışıyorsa minimum yönlendirme ile ağ üzerindeki iletişimi sağlayabiliriz. (Bu yönlendirme genelde sadece ifconfig komutu ile yapılır)

- Sabit yönlendirme: Kurulu bir bilgisayar ağının dış dünyaya bir ya da birkaç çıkışı varsa sabit yönlendirmeyi kullanabilir. (Bu yönlendirme genelde route komutu ile yapılır). Gerekli komut kullanılarak ağın dış dünyaya çıkan trafiği çıkış noktasına yönlendirilmiş olur.

- Dinamik yönlendirme: Ağın dış dünya ile olan iletişimi birden fazla noktadan yapıyorsa, yönlendirme protokolu ile dinamik olarak bir yönlendirme tablosu tutulur ve yönlendirme protokolları birbirleri ile gerekli bilgi alışverişini yaparak en uygun çıkışı kullanırlar. Böylece ağ yöneticisinin elle müdahalesi gerekmez en uygun yolu bu protokoller bulurlar. Dolayısıyla bir çıkış noktasında meydana gelen bir sorunda tüm trafik otomatik olarak diğerine yönlendirilebilir. Bu yönlendirme yöntemlerini biraz daha detayları ile örnekler vererek inceleyelim.

Minimum Yönlendirme Tablosu

Aşağıdaki şekilde görülen ağ üzerinde



Çizim-14 Minimum yönlendirme

```
# ifconfig le0 144.122.99.2 netmask 255.255.255.0 broadcast 144.122.99.255
```

komutu kullanılarak arayüzünün ağ bağlantısı yapılmış olan bir bilgisayarın yönlendirme tablosunun içeriğine bakarsak

```
% netstat -rn
gTables
127.0.0.1          127.0.0.1          UH      1          132         1o0
144.122.99.0      144.122.99.2      U       26         49041       1e0
```

İlk satırdaki 127.0.0.1 loopback adres olarak bilinen lokal bilgisayarın kendisini tanımlayan ve İnternet protokolunu çalıştıran her bilgisayarda bulunan standart bir adrestir. İkinci satırda ise 144.122.99.0 ağına, ethernet le0 arayüzü üzerinden gidileceğini belirtiyor. 144.122.99.2 ise uzaktaki (remote) bir geçiş noktası (gateway) adresi değil le0 arayüzünün kendi adresidir. Flağs alanlarına bakacak olursak her iki satırda da bulunan U (up), her ikisinin de kullanıma hazır olduğunu gösterir. Her iki satırda da Flağs alanında Ğ (Gateway) işareti yoktur zira her iki arayüze aradaki bir geçiş kapısı (gateway) üzerinden ulaşılmamaktadır. Loopback yönlendirme tanımının bulunduğu satırdaki H (Host) işareti bu yönlendirme ile sadece bir bilgisayara (yani kendisine) ulaşılabileceğini tanımlamaktadır. Bu satır bilindiği gibi her yönlendirme tablosunda bulunmaktadır. Bu yönlendirme tablosu görüldüğü gibi sadece 144.122.99.0 ağı ile ilgili yönlendirme bilgisine sahiptir. Dolayısıyla sadece bu ağ üzerinde yer alan bilgisayarlar birbirleri ile iletişime geçebilmektedirler. Bu yönlendirme tablosu oluşturduktan sonra herhangi bir problem olup olmadığının testi ping komutu ile kolayca yapılabilir. Önce bu ağ üzerinde yer alan bir bilgisayarı ping komutu ile kontrol edelim:

```
% ping 144.122.99.3
PING 144.122.99.3: 56 data bytes
64 bytes from 144.122.99.3: icmp_seq=0, time=11, ms
64 bytes from 144.122.99.3: icmp_seq=1, time=11, ms
^Ç
----144.122.99.3 PING statistics----
2 packets transmitted, 2 packets received, 0% packet loss
round-trip (ms) min/avg/max =10/10/11
```

Görüldüğü gibi 144.122.99.3 ile olan iletişimin başarılı olduğu test edilmiş oldu. Bunun yanında aynı ağ üzerinde bulunmayan bir adrese ulaşmak istediğimizde nasıl bir sonuçla karşılaşacağımızı test etmek istersek :

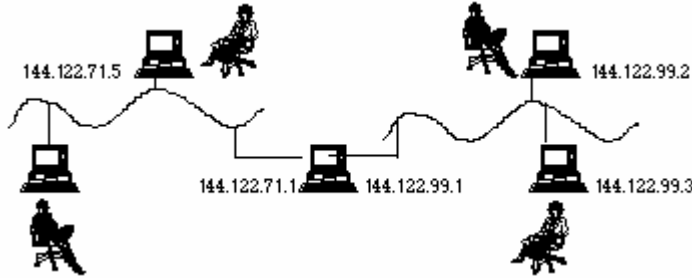
```
% ping 26.40.0.17
```

```
sendto: Network iş unreachable
```

Gelen cevaptan da anlaşılaçağı gibi, ulaşmak istediğimiz bilgisayara ait yönlendirme bilgisine sahip olmadığı için, bilgisayarımız datagram leri varış noktasına iletemediğini ve o noktaya ulaşamaz olduğı mesajını veriyor. Eğer bilgisayar ağıımızın dış dünya ile irtibatı yoksa ifconfig ile yaratılan tablo tüm ihtiyaçlarımızı karşılamaya yeterlidir. Ancak eğer bir dış bağlantı varsa o zaman yönlendirme tablosunun daha fazla bilgiye ihtiyacı vardır.

4.2 Sabit Yönlendirme Tablosu

Yukarıda da gördüğümüz gibi minimum yönlendirme tablosu ile aynı ağ içindeki bilgisayarlara ulaşmak mümkündür. Başka ağlar üzerindeki bilgisayarlara ulaşmak için bunlarla ilgili bilgiler yönlendirme tablolarına girilmelidir. Yönlendirme tablosunu yaratmak için kullanılan yolların en popüler route komutudur. route komutu ile yönlendirme tablosuna elle yeni yönlendirme bilgileri eklenip çıkartılabilir.



Çizim-15 Sabit yönlendirme

Örnek verecek olursak, yukarıdaki şekilde görülen 144.122.99.0 ağındaki bir bilgisayardan 144.122.71.0 ağına ulaşmak için şöyle bir tanım yeterlidir:

```
# route add 144.122.71.0 144.122.99.1 1
add net 144.122.71.0: gateway 144.122.99.1
```

route komutundan sonraki 'add' argümanı yönlendirme tablosuna bir ek yapılacağını söylemektedir. Tablodan bir bilgi silineceğı zaman 'add' yerine 'delete' kullanılarak bu silme işlemi yapılır. Aynı satırdaki üçüncü bilgi bu yönlendirme bilgisi ile ulaşmak istenen adresi belirtmektedir. Ulaşılaacak adres 4 farklı şekilde tanımlanabilir:

a- bir IP adresi ,

b- /etc/networks dosyasındaki bir ağ ismi,

ç- /etc/hosts dosyasındaki bir bilgisayar ismi,

d- default. Eğer ulaşmak istenen adres olarak default kullanılırsa aynı ağ üzerinde yer almayan her adrese burada tanımlanan geçiş yolu üzerinden ulaşmaya çalışılır. Eğer bir ağın dış dünyaya çıkışı tek bir noktadan ise default olarak bu çıkış adresi tanımlanmalıdır.

Komut satırındaki dördüncü bilgi geçiş yolu adresidir. Bu adres ağın dış dünya ile iletişimini sağlayan geçiş kapısıdır. Son argüman ise yönlendirme metrik bilgisidir. Bu bilgi, sadece ROUTE bilgisinin eklenmesi durumunda kullanılır. Metrik bilgisi değerinin 0 olması durumunda yönlendirme bilgisinin lokal ağa ait olduğu şeklinde yorumlanır ve daha önce netstat komutunda gördüğümüz Flağs alanındaki G (Gateway) işareti gözükmez. Ama eğer Metrik 0 değerinden büyükse bu o zaman bu yönlendirme bilgisinin dış dünyaya açılan geçiş yolunu tarif ettiği anlaşılır ve Flağs alanına G işareti konulur. Sabit yönlendirme 0 ve 1 dışında bir Metrik değeri kullanmaz.

4.3 Diğer Yönlendirme Protokolleri

Bütün yönlendirme protokolları temelde en iyi yönü ve yolu bulma işlevini yerine getirirler ve bu yönlendirme bilgisini ağ üzerinde dağıtırlar. Yönlendirme protokolları iki temel gruba bölünebilirler: Interior (iç) ve Exterior (dış).

i-Interior (iç) protokoller: Bu protokoller bağımsız bir bilgisayar ağı içinde kullanılırlar. TCP/IP terminolojisinde böyle bilgisayar ağı sistemlerine Otonom sistemler (AS) adı verilir. Otonom sistem içinde yönlendirme bilgisi, o ağın yöneticisi tarafından belirlenen bir iç yönlendirme protokolu ile dağıtılır. Bu amaçla kullanılabilecek değişik Interior (iç) protokoller mevcuttur.

HELLO en iyi yönü seçerken gecikme faktörünü kullanan bir protokoldur. Gecikme olarak çıkış noktasından varış noktasına gönderilen bir paketin çıkış noktasına ulaşana kadar geçen zaman süresi kabul edilir. Bu protokol çok yaygın olarak kullanılmamaktadır. NSFNET omurgası 56 Kbps ızında iken kullanılmış ve zaman içinde başka protokoller ile değiştirilmiştir.

Son zamanlarda yaygınlaşmaya başlayan bir diğer iç protokol de OSPF'dir (Open Shortest Path First). OSPF 'equal cost multipath routing (esit maliyetli çok yollu yönlendirme) mantığı ile çalışmakta ve çok büyük ağlarda kullanılmaktadır. OSPF aynı varış noktasına birden fazla yönlendirme bilgisini tutmaktadır. Ancak OSPF'in bugün için sadece özel yönlendirme cihazları üzerinde var olması ve henüz UNIX sistemlerin bir parçası haline gelmemesinden dolayı yaygın kullanıma geçilememektedir.

RIP (Routing Information Protocol) bu protokoller içinde en çok kullanılanıdır. RIP'i popüler yapan sebeplerin basında bu protokolün UNIX sistemlerin bir parçası olması gelmektedir. RIP protokolu yönünü en düşük sıçrama sayısı-hop count (metrik) ile seçer. RIP 'hop count', bilginin varış noktasına ulaşana kadar geçeceği geçiş yolları sayısını gösterir. Dolayısıyla RIP en az geçiş yoluyla ulaşılabilir yol en iyi yol olarak seçer. Bu yaklaşımla yol seçme işlemine

'distance- vector algoritması' adı verilir. RIP protokolunun kabul edebileceği maksimum geçiş yolu (gateway) sayısı 15 ile sınırlıdır. Ulaşılmak istenen yön ile ilgili metrik 15'den büyükse, RIP o noktaya ulaşamaz olduğunu varsayar ve ilgili yönlendirme bilgisini atar. Dolayısıyla RIP çok büyük Otonom Sistemler için uygun bir protokol değildir. Bunun yanında en kısa yol en iyi yoldur yöntemi de yavaş ve yüklü hatlar kullanılması durumunda doğru olmamaktadır.

Çok kullanılan bir yönlendirme protokolu olmasından dolayı RIP protokolunun biraz daha detaylarına girelim. Daha önce de belirttiğimiz gibi RIP pek çok UNIX sisteminin bir parçası olarak gelmektedir. RIP bu işletim sisteminde bir yönlendirme deamon'u olarak çalışır. UNIX'deki bu deamon routed'dir. routed çalıştırıldığında yönlendirme tablosunu güncellemek (update) için hemen bir istek paketi yollar ve ardından gelecek olan cevapları dinlemeye başlar. RIP çalıştıran başka bir sistem bu isteği aldığı anda kendi yönlendirme tablosu ile ilgili güncel bilgileri cevap olarak yollar. Bu paket adresler ve bu adreslerle ilgili metrik bilgilerini içerir. Bunun yanında güncelleme paketleri sadece istek üzerine değil periyodik olarak yollanmaya başlanır.

routed bir güncelleme bilgisini aldığı anda gelen paket içindeki bilgiyi alır ve kendi tablolarını günceller. Gelen bilginin içinde yeni bir yönlendirme bilgisi varsa bunu da hemen tablolara ekler. Gelen paket içindeki yönlendirme bilgileri arasında lokal tabloda bulunan bir adres için ikinci bir yol belirtiliyorsa bu durumda lokal tablodaki ve gelen güncelleme tablosundaki metrik bilgileri karşılaştırılır. RIP protokolu Metrik bilgisi düşük olan noktaya daha kolay ulaşılacağı varsayımı ile çalıştığı için tabloya bu değere sahip yöne ilişkin adres yerleştirilir.

RIP tabloları tabii ki belli bir yerden sonra çok fazla büyüyeceği için bir şekilde kontrol altında tutulmalıdır. Bunun için iki yol mevcuttur. Birincisi, bir noktaya ulaşmak için gereken metrik 15'in üzerindeyse bu nokta ulaşamaz kabul edilir ve tablodan çıkarılır. İkincisi, eğer bir geçiş noktası belli bir süre güncelleme bilgisi yollamazsa RIP o noktanın olu olduğunu ve ulaşamadığını varsayar. Genel olarak güncelleme cevabi bekleme süresi 30 saniye civarındadır. Bir UNIX sisteminde RIP protokolunu çalıştırmak için

```
# routed
```

komutunun girilmesi yeterlidir. Genellikle komut hiç bir argüman verilmeden çalıştırılır. Fakat kullanılan sistem bir geçiş noktası değilse ve elindeki yönlendirme bilgisini sürekli yayınlaması gerekmiyorsa bu durumda komut -q opsiyonu ile çalıştırılabilir. Böylece sistem sadece yeni duyurulan yönlendirme bilgilerini dinleyip tablolarını güncelleyecek ancak kendisi bir duyuru yapmayacak dolayısıyla gereksiz trafik yaratılmayacaktır.

ii-Exterior (dış) protokoller: Otonom Sistemler arasında yönlendirme bilgisinin birbirleri arasında değiştirilmesi amacı ile kullanılır. Bu belli bir Otonom Sistem üzerinden hangi ağlara ulaşılabilirliği bilgisini içerir. Bu protokoller içinde en popüler olanları EĞP (Exterior Gateway Protocol) ve BĞP'dir (Border Gateway Protocol). Bu döküman içinde EGP ve BGP protokollerin detaylarına girilmeyecektir.

5.İsimler ve Adresler

5.1 Adresleme stratejileri

İlk bilgisayar sistemleri, kullanıcıların sayısal adresleri anlamaları ve kullanmaları temelinde tasarlanmışlardı (sistem tabloları, yazıcı ve teyp üniteleri gibi cihazlar vs.). Daha sonra ortaya çıkan sistemlerde harici cihazlar (yazıcı vs.) ve dosyalar daha anlaşılır sembolik isimler ile gösterilmeye başladı. Benzer bir değişiklikte ağ bağlantılarında yasadı. Önce bilgisayarlar arası noktadan noktaya bağlı ağ teknolojisi ortaya çıktı ve alt seviye donanım isimleri makinaları tanımlamada kullanıldı. Ancak pek çok bilgisayarın birbiri ile bağlantısı gündeme geldiğinde üst seviye adresleme yapısına gereksinim doğdu. Kullanıcılar pek çok makineden oluşan hesaplama ortamlarında makinaları tanımlamak için anlaşılır sembolik isimlere sahip bir adresleme yapısını talep ettiler. Bilgisayar sayılarının günümüze göre çok az olması sebebi ile başlangıçta sadece makinenin kullanım amacına yönelik bir adlandırma yöntemi kullanıldı (personel, araştırma, muhasebe, geliştirme vs.). Ancak makina sayısının artması ile sembolik yeni isimlerin bulunması ve tüm bu birbirine bağlı sistemlerin adlarının bir merkezden kontrolü zorlaşmaya başladı.

Adresleme problemlerini en aza indirmek için, merkezi olarak bilgisayar isimlerinin kontrolü ve kaydı yerine daha uygun bir sistem olarak sıradüzensel (hijerarşik) ve otoritenin dağıtıldığı merkeziyetçi olmayan bir adresleme sistemi getirildi. Bu sistemde adresleme en genelden özele doğru yapılmakta ve her adres seviyesinin kontrolü yetkisi de dağıtılmaktadır. Bu yapıya 'Alan İsimlendirme Sistemi-Domain Name Sistem' veya kısaca DNS ismi verilmektedir. Hijerarşik yapıdaki Alan (Domain) isimleri kavramını biraz daha detaylı inceleyelim.

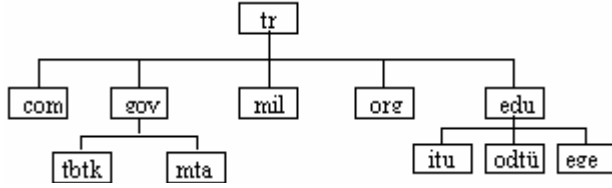
Alan (Domain) ismi birbirinden bir nokta (.) ile ayrılan, sıradüzensel seviyedeki alt isimler (subnames) dizisidir. Mesela ODTU Bilgisayar Merkezi Alan ismi olan

```
cc.metu.edu.tr
```

dört seviye ile gösterilir ve her bir seviyeye de Domain adı verilir. Orneğimizde en alt seviye olan 'cc' (Computer Çenter) Bilgisayar Merkezini göstermektedir. Üçüncü seviye 'metu', ODTU'nun Domain ismidir. Bir üst seviye 'edu' (Education) ise bu domain'in bir eğitim kurumuna ait olduğunu gösterir. En üst seviye 'tr' ise ISO (İnternational Standards Organization) tarafından belirlenen Türkiyenin ülke kodudur. En üst seviyede kullanılan bazı domain isimleri aşağıda listelenmiştir:

.com	ticari kuruluşlar (commercial)
.edu	eğitim kuruluşları (education)
.gov	devlet kuruluşları (government)
.mil	askeri kuruluşlar (military)
.net	ağ organizasyonları (network)

.ülke kodu ISO standart ülke kodu
Kısaltması isimler aşağıdaki domain ve alt domain sıradüzensel yapıya göre verilir:
Makine.altorganizasyon.organizasyon.domain



Çizim 16

5.2 TCP/IP ve DNS

Bilindiği gibi TCP/IP ağlarına bağlı olan her bilgisayarın ağ arayüzü 32-bitlik IP adresi ile tanımlanmaktadır. Ancak IP adreslerinin gündelik hayatta kullanımı ve hatırlanması pek pratik olmadığı için domain isimlendirme sistemi kullanılır. Aslında TCP/IP yazılımlerinin ağ üzerindeki iletişimi sağlamak için isimlere ihtiyacı yoktur, isim yapısı ağ kullanıcılarının hayatlarını kolaylaştırmak için ortaya çıkarılan bir yöntemdir. Kullanıcının tercihine göre IP numaraları veya isimler kullanılabilir. Mesela:

```
% telnet 144.122.199.20
```

```
% telnet knidos.cc.metu.edu.tr
```

komutlarının her ikisinde aynı işlevselliktedir. Her ikisinde de ODTU'de bulunan bir bilgisayara uzaktan bağlanmak için gerekli komut girilmektedir. Her iki durumda da bağlantı IP numarası kullanılarak yapılır. İsim ile bağlantı durumunda sistem önce bilgisayar ismini (knidos.cc.metu.edu.tr) IP numarasına çevirir ve daha sonra bu numaraya bağlantıyı sağlar. Dikkat edilirse bu sistem sayesinde makinanın IP adres değişiklikleri kullanıcıyı hiç etkilememektedir.

İsimler ve adresler arasındaki ilişkiyi sağlayan sistemleri ve programları kurup çalıştırmak sistem sorumlularının görevidir. İsimlerin IP adreslerine çevrilmesi işlemi aslında çok basit bir işlem de değildir. Zira lokal çalışan bir bilgisayar ağında hiç dikkat edilmeyen pek çok konu bilgisayar ağını İnternete bağladığınızda çok ciddi problemlere yol açabilir. Ağ üzerinde yer alan bilgisayarlarınızın isminin IP adresine çevrilmesi artık dünyanın her yerinden sorunsuz olarak yapılmak zorundadır.

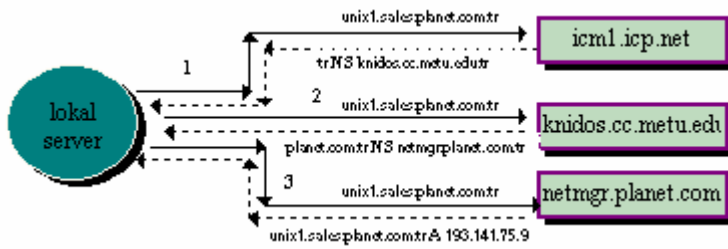
DNS in nasıl çalıştığını ticari bir şirketin İnternete bağlandığını varsayarak bu örnek üzerinde açıklamaya çalışalım. Bu hayali şirketimizin adı PLANET AS. olsun. Şirketimiz şu anda Türkiye de çalıştığı için tabii ki üst seviye domain adı .tr olacak. Alt seviyede ise şirket olmasından dolayı .com domaini altında bulunmaktadır. Bir alt domain ise şirketimizin adını göstermektedir, planet.com.tr. Büyük bir şirket olduğumuz için farklı birimlere sahibiz ve her birimizde ayrı bir domain altındadır. Araştırma geliştirme BÖLÜMu arge.planet.com.tr, satış BÖLÜMu sales.planet.com.tr, destek BÖLÜMu support.planet.com.tr gibi.

Birimlerimiz oldukça büyük olduğu için her birim kendi Domain Name Servisini kendisi kontrol etmektedir. Şirketimizin ayrıca tüm bu alt seviye domainleri tanıyan bir "root name server" makinası bulunmaktadır. Alt domainler sadece kendi domainleri ile ilgili bilgiyi ellerinde tutarlar ve bilemedikleri her türlü domain için sorgusorgu sorgulamayı "root name server" üzerinden yaparlar. Ayrıca eğer istenirse alt seviye domainler (.sales, .arge gibi) kendi içlerinde başka alt seviye domainler de (sub domain) yaratabilirler. Aslında tüm seviyelerdeki domainleri kontrol eden "name server" makinaları kendi sorumlulukları altındaki bilgisayarların isimlerini ve IP adreslerini tablolarda tutan birer Bilgi Bankasından (Database) başka bir şey değildir.

Şirketimiz bu yapıyı kurduktan sonra doğal olarak İnternet üzerindeki başka merkezlerle alfanumerik adresler kullanarak haberleşmek isteyecek ya da dışardan kullanıcılar şirketimizin sunduğu bazı servislerimizi alabilmek için bize ulaşmak isteyeceklerdir. Bu noktada şirketimizin "root name server" makinasını ülke içindeki root name server makinasına tanıtmamız gerekmektedir. Şu anda Türkiye içindeki .com dahil tüm domainler için bu görevi knidos.cc.metu.edu.tr adresinde bulunan bir UNIX makina yapmaktadır. Bu "name server" üzerinde PLANET şirketinin root name server kaydı yapıldıktan sonra artık dünyanın dört bir yanına alfanumerik isimler kullanarak ulaşmak için hazırız demektir. (Name server tanımının yapılmaması IP adresleri kullanarak İnternet üzerindeki adreslere ulaşmamıza engel değildir. Name server bize sadece alfanumerik isimler kullanma imkanını verir.)

Şimdi Amerikadaki bir kullanıcının şirketimizin satış BÖLÜMündeki unix1.sales.planet.com.tr isimli bilgisayara İnternet üzerinden ulaşmak istediğini varsayalım.

Şekilde de görüldüğü gibi unix1.sales.planet.com.tr adresine ulaşmak için lokal server önce ABD'de icml.icp.net adresindeki name server'a soruyu yolluyor. icml.icp.net Türkiye ile ilgili bütün kayıtların knidos.cc.metu.edu.tr adresinden alınacağını bildiği için sorgulamanın bu adresten yapılmasını istiyor. Aynı sorgu bu sefer knidos.cc.metu.edu.tr adresine yollandığında sorgulanan adresin netmgr.planet.com.tr tarafından bilindiği cevabi yollanıyor. Ve sonuçta ulaşılmak istenen adres



Çizim 17

(193.141.75.9) netmgr.planet.com.tr adresinden elde ediliyor.

Bu sorgulama sonucu Amerikadaki kullanıcının makinası unix1.sales.planet.com.tr makinasının IP adresini öğrenmiş oldu ve bu adres ile yapmak istediği iletişimi sağladı. Bu sorgulamanın sonucu ayrıca istekte bulunan bilgisayarın çache belleğine yerleştirildi. Bu bilgi cache bellekte durduğu sürece bir daha aynı adrese bağlanmak isteyen bir kişi tekrar aynı sorgulamayı yapmaksızın o IP adresine doğrudan ulaşabilecektir.

6. Arayüz Kuruluşu

Bilgisayarlar arasında kullanılan iletişim altyapısının sabit olması ve daima aynı fiziksel alt yapının kullanılması durumunda bilgisayar ağı arayüzünün (interface) ağ yazılımına tanıtılmasına gerek kalmaksızın ağ kuruluşu yapılabilir. Ancak günümüz bilgisayar ağlarında kullanılan fiziksel ağ alt yapısı kullanım çeşitliliğine göre çok değişik özelliklere sahiptirler. Bina içlerinde kurulu yerel ağlar farklı bir fiziksel yapı kullanırken kıtalar arası ağ bağlantıları için tamamen farklı bir yapı kullanılmaktadır. Tüm bu çeşitlilik sebebi ile iletişim ağı yazılımına her arayüz ayrı ayrı tanıtılmak ve karakteristiklerine göre konfigürasyonu yapılmak zorundadır.

TCP/IP fiziksel alt yapıdan tamamen bağımsız bir şekilde dizayn edildiği için, adresleme ağ donanımı seviyesinde değil de ağ yazılımı seviyesinde kontrol edilmektedir.

Bu BÖLÜMde TCP/IP kullanılan ağlardaki ara yüz kuruluşunun nasıl yapıldığı standart UNIX komutu olan ifconfig komutu kullanılarak ve örnekler verilerek anlatılacaktır.

6.1 - ifconfig komutu

ifconfig ağ arayüzlerinin (bir bilgisayarın birden fazla ağ arayüzü olabilir) kuruluş ve kontrollerinde kullanılan bir komuttur. Her arayüze İnternet adresinin, subnet maskesinin ve broadcast adresinin verilmesinde kullanılır. Bir örnek üzerinden inceleyecek olursak:

```
# ifconfig le0 144.122.199.20 netmask 255.255.255.0 broadcast
144.122.199.255
```

ifconfig komutu ile kullanılan temel argümanlar :

* arayüz: ifconfig komutu ile konfigüre edeceğimiz arayüzün adı. Yukarıdaki örnekte Ethernet arayüzün ismi 'le0'.

* adres: Bu arayüze verilen İnternet adresi. Bu adres noktalı ondalık formda (dotted decimal form) veya bilgisayar adı olarak girilebilir. Ancak ad olarak girilmesi durumunda bilgisayar adına karşılık gelen İnternet adresinin /etc/hosts dosyasında bulunması gereklidir. Genelde ifconfig komutu DNS'den (DNS detaylarına ileride girilecektir) önce çalıştırıldığı için özellikle bu dosyada bulunması problemlerin önlenmesi açısından önemlidir. Yukarıdaki örnekte 144.122.199.20 bu arayüze verilen adrestir.

* netmask: mask Bu arayüzün subnet maskesi. Eğer kullanılan ağ daha küçük çaptaki subnet lere bölünecekse bu alanda kullanılan değerler önem kazanır. Örnekteki adres için 255.255.255.0 seklindeki subnet maskesi kullanılmış ve ağ subnetlere bölünmüştür.

* broadcast address: Ağın yayın adresi. Bu adres subnet yapısına bağlı olarak belirlenir ve aynı ağ üzerindeki her bilgisayarda aynı değerin kullanılması gerekmektedir. örneğimizde bu adres 144.122.199.255 olarak belirlenmiştir. Burada kullanılan tüm adresler vs. o ağın yöneticisince belirlenir ve bilgisayarlara verilir. Arayüzün ismi genelde sistemden sisteme geçebileceği için kuruluş işlemlerine başlamadan önce sistem dökümanlarının incelenmesinde büyük yarar vardır. Ayrıca şimdi inceleyeceğimiz netstat komutu ile hangi arayüzlerin, nasıl konfigüre edildikleri ile ilgili bilgi de edinilebilir.

6.2 Arayüzler ve netstat komutu

İletişim protokolu olarak TCP/IP kullanılan sistemlerde bilgisayar ağı arayüzlerinin hangilerinin var olduğunu anlamamanın en kolay yollarından birisi netstat komutunun kullanılmasıdır. Örneğin bir sistem üzerindeki tüm ağ arayüzlerinin durumunu kontrol etmek için şu komut kullanılabilir:

```
% netstat -ain
```

-i opsiyonu, netstat'ın konfigüre edilmiş ara yüzlerin durumunu göstermesini

-a opsiyonu, tüm arayüzlerin durumunu göstermesini

-n opsiyonu, gelen bilginin numerik olarak gösterilmesini sağlar.

Gelen cevap :

Name	Mtu	Net/Dest Address	Ipkts	Ierrs	Opkts	Oerrs	Çollis
1e0	1500	144.122.199.0	144.122.199.20	1547	1	1127	0
	135	0					
1o0	1536	127.0.0.0	127.0.0.1	133	0	133	0
	0						

Name: Arayüzün ismi. Bu alanda eğer (*) bulunursa bu o arayüzün o anda çalışmadığını gösterir.

Mtu: Maximum Transmision Unit. Bu arayüz üzerinden bölünmeden gönderilebilecek en uzun paketin boyu (byte olarak).

Net/Dest: Bu arayüzün ulaşım sağladığı ağ veya varış bilgisayarı. Bu alan, varış bilgisayarı adresini sadece PPP (point-to-point) tanımlaması yapıldığında içerir. Diğer zamanlarda bu alanda ağ adresi bulunur.

Address: Bu ara yüze verilmiş olan İnternet adresi.

Ipkts: Input Packets. Bu ara yüz üzerinden alınan paket sayısı.

Ierrs: Input Errors. Bu arayüz üzerinden alınan hatalı paket sayısı.

Opkts: Output Packets. Bu ara yüz üzerinden yollanan paket sayısı.

Oerrs: Output Errors. Hataya yol acan paket sayısı.

Collis: Bu arayüz üzerinde tespit edilen çarpışma sayısı. Ethernet dışındaki arayüzlerde bu alan olmaz.

Queue: Bu arayüz üzerinde kuyrukta bekleyen paket sayısı. Normalde bu değer 0'dir.

Yukarıdaki değerler bu sorgulamanın yapıldığı istasyonun iki ağ ara yüzüne sahip olduğunu göstermektedir. '1o0' arayüzü loopback arayüzü olup standart olarak her TCP/IP sisteminde bulunur ve normalde herhangi bir konfigürasyona da ihtiyaç duymaz. '1e0' bir Ethernet arayüzüdür. Bir makina üzerinde eğer birden fazla Ethernet arayüzü varsa bunlar '1e0', '1e1' ... şeklinde numaralanırlar.

6.3 Arayüzün ifconfig komutu ile kontrolü

Bir arayüzün konfigürasyonu 'ifconfig' komutu ile kontrol edilir.

```
% ifconfig 1e0
1e0: flağs=63 UP,BROADCAST,NOTRAILERS,RUNNING
inet 144.122.199.20 netmask ffffffff0 broadcast 144.122.199.255
```

Gelen cevaptaki ilk satır arayüzün adını ve karakteristiklerini verir. Örnekteki arayüzün adı '1e0' dir. Arayüzün karakteristikleri:

UP: Arayüz kullanıma hazır

BROADCAST: Bu arayüz broadcast'i destekliyor. (Zira arayüz bir Ethernet ortamına bağlı)

NOTRAILERS: Arayüz 'trailer encapsulation' desteklemiyor (Ethernete has bir karakteristik).

RUNNING: Arayüz şu anda çalışıyor.

Gelen cevaptaki ikinci satır direkt olarak bu arayüzün TCP/IP konfigürasyonu ile ilgili bilgi verir. Bu arayüze İnternet, maske ve yayın adreslerinin olarak ne verildiği buradan görülmektedir. Bu adreslerde yapılmak istenen değişiklikler ve düzenlemeleri yine 'ifconfig' komutunu kullanarak gerçekleştirmek mümkündür. Mesela yukarıdaki örnekteki subnet maskesi ve yayın adresini aşağıdaki komutu kullanarak değiştirebiliriz:

```
# ifconfig 1e0 144.122.199.20 netmask 144.122.255.255 broadcast
255.255.0.0
```

Genelde 'netmask' değeri doğrudan komutun içinde belirtilir. Ancak eğer istenirse bu değeri komutun gidip bir dosyadan alması da mümkündür. Kullanılmasına karar verilen 'netmask' değeri /etc/networks dosyasına eklenirse 'ifconfig' komutu bu değeri o dosyadan alır. Örneğin ağ yöneticisi aşağıdaki satırı /etc/networks dosyasına eklesin:

```
odtu-mask 255.255.255.0
```

Bundan sonra 'ifconfig' komutu kullanılırken:

```
# ifconfig 1e0 144.122.199.20 netmask odtu-mask
```

şeklinde verilen komut netmask değerini /etc/networks dosyasından alır. Yukarıdakine benzer şekilde arayüzün İnternet adresini de 'ifconfig' komutu ile değiştirmek mümkündür. Örnek verecek olursak:

```
# ifconfig 1e0 144.122.199.50
```

komutu ile yukarıdaki örneklerde adresi 144.122.199.20 olan bilgisayarın yeni adresi artık 144.122.199.50 olarak değişmiş oldu. Her seferinde numerik adres yazılması istenmiyorsa /etc/hosts dosyasında bu İnternet adresine karşılık gelen isim girilebilir. 144.122.199.50 için /etc/hosts dosyasına eklenecek olan

```
144.122.199.50 artemis.metu.edu.tr artemis
```

satırı ile 144.122.199.50 adresine artemis.metu.edu.tr veya kısaca artemis adı verilmiş olur. Bundan sonra konfigürasyon yaparken

```
# ifconfig le0 artemis
```

olarak girilen komut bu Ethernet arayüzüne 144.122.199.50 adresini /etc/hosts dosyasından alarak verir.

Sistemin yeni açılışı esnasında doğru adresin ve konfigürasyonun yüklenmesi için yukarıda açıkladığımız komutlar her seferinde girilmek durumundadır. Bu işlemin otomatik yapılabilmesi için 'ifconfig' komutu doğru parametreler ile sistem yukleme dosyasında bulunmalıdır. BSD UNIX sistemlerinde bu komut genelde /etc/rc.boot veya /etc/rc.loçal, System V UNIX sistemlerinde ise /etc/tcp veya /etc/init.d/tcp dosyalarına konulur. Böylece sistem her açılışında 'ifconfig' komutunun elle girilmesine gerek kalmaksızın uygun konfigürasyon otomatik gerçekleştirilir.

Arayüzün kontrolüne yönelik olarak 'ifconfig' komutu ile kullanılan başka parametreler de vardır. Arayüzün bir şure kapatılması ve açılması için 'up' ve 'down' parametreleri kullanılır. Arayüz üzerinde yapılacak değişikliklerde (örneğin adres değişikliği) trafik akışının durması için arayüz önce 'down' edilip ardından 'up' duruma getirilir. Örneğin:

```
# ifconfig le0 down
```

```
# ifconfig le0 144.122.199.100 up
```

komutları ile Ethernet ara yuz önce kapatıldı sonra adres değişikliği yapılarak açıldı.

Bu noktaya kadar verilen bilgiler ve örnekler ile TCP/IP protokolüne sahip UNIX tabanlı bilgisayar sistemimiz bir Ethernet ağına bağlandı ve aynı ağ üzerinde yer alan diğer bilgisayarlar ile iletişime geçti. 'ifconfig' komutunun daha başka özellik ve yeteneklerinin olmasına karşın şu aşamada o detaylara girmiyoruz. Bu noktadan sonra yerel ağımızın seri hatlar üzerinden uzak bir noktadaki başka bir ağa yani İnternet'e nasıl bağlanabileceğini anlatacağız.

6.4 Seri hatlar üzerinde TCP/IP Konfigürasyonu

TCP/IP protokolu çok çeşitli fiziksel ortamlarda çalışabilmektedir. Yukarıdaki BÖLÜMde Ethernet ağlar üzerinde nasıl konfigürasyon yapılacağı anlatıldı, şimdi ise uzak iletişim hatları üzerinden başka bir ağ ile bağlantının nasıl yapılacağı anlatılacaktır.

Seri arayüz bilgiyi tek bir hat üzerinden seri bitler olarak yollayan bir ortamdır. Her bilgisayar sisteminde en az bir veya iki seri arayüz çıkışı bulunmaktadır. Bu çıkış üzerinden iki nokta arasındaki iletişimi sağlamak için modem ya da benzeri bir aygıt kullanılır.

Günümüzde iletişim teknolojilerinin çok hızlanması ve bunun yanında fiyatların düşmesi ile beraber telefon hatları üzerinden evlerden dahi ağ bağlantıları yapılabilir duruma gelmiş ve TCP/IP için standart geniş alan bağlantısı (WAN) protokolları geliştirilmiştir. Bu protokoller SLIP (Serial Line IP) ve PPP'dir (Point-to-Point Protocol).

SLIP, PPP protokolünden önce ortaya çıkan ve standart dışı bir İnternet protokolüdür. Bunun yanında PPP, SLIP'den sonra ortaya çıkmıştır ve İnternet'in standart seri hat protokollarından birisidir. SLIP önceden ortaya çıkması ve pek çok UNIX sisteminin parçası haline gelmesi sebebi ile çok yaygın olarak kullanılmaktadır.

Burada her iki protokolün bir UNIX ortamında nasıl konfigüre edileceği örneklerle anlatılacaktır.

6.4.1 SLIP kuruluşu

Ağa bağlı bilgisayarınızın SLIP amaçlı kullanım için kuruluşunun Ethernet kuruluşundan pek bir farkı yoktur. Ancak SLIP'e has bazı komutları vardır, bunun yanında PPP gibi standart olmayışından dolayı bazı komutlar sistemden sisteme değişebilmektedir. En çok kullanılan komutlar: 'slattach' ve 'sliplogin' komutlarıdır.

- slattach

Bu komutun kullanım ve fonksiyonu 'ifconfig' komutuna çok benzer.

```
# slattach /dev/tty001 144.122.199.200 144.122.199.201
```

Yukarıdaki örnekte 144.122.199.200 İnternet adresi /dev/tty001 seri portuna verildi. 144.122.199.201 adresi ise seri hattın diğer uçundaki bilgisayarın İnternet adresidir.

Örnekten de görüldüğü gibi 'slattach' komutu ile ağ arayüzü standart ismi olan sl01 yerine /dev/tty001 seri port tanımlanır.

Ancak 'netstat' komutu ile SLIP arayüzü kontrol edildiğinde arayüzün ismi (sl01) ile ilgili bilgi verir.

Bir arayüzden SLIP kullanımını kaldırmak için ise genelde kullanılan komut 'sldetach' komutudur.

```
# sldetach sl01
```

Yukarıdaki komut ile bu arayüz artık normal terminal arayüzü olarak kullanılır (bu komutta ağ arayüzü isminin kullanıldığına dikkat edin).

Bazı UNIX sistemlerde SLIP bağlantının dial-up telefon hatları üzerinden yapılabileceği göz önünde tutularak 'slattach' komutuna gerekli eklenti yapılmıştır. Örneğin IBM AIX sistemlerde :

```
# slattach /dev/tty1 ""ATZ OK \pATDT5551212 CONNECT""
```

komutu ile karşıdaki sistemin telefon numarası çevrilip bağlantı kurulmaktadır. Ancak slattach komutunda bu yeteneğe sahip olmayan sistemler dial-up turu bağlantılarda 'cu' veya 'tip' gibi programlar ile önce iki nokta arasındaki iletişim sağlanmalı sonra 'slattach' çalıştırılmalıdır.

- sliplogin

'sliplogin' ŞUN sistemlerde kullanılan slipware yazılımının SLIP bağlantıları sağlayan komutudur. Kullanımı 'slattach' komutuna benzer:

```
# sliplogin 144.122.199.200 144.122.199.201 < /dev/ttyb
```

Bu örnekteki ilk adres bilgisayarımızın üzerindeki ara yüzün adresi, ikinci adres ise SLIP bağlantının yapıldığı bilgisayarın adresidir. Yine benzer şekilde ara yüzün adı yerine seri port (/dev/ttyb) bu komutta kullanılmıştır.

6.4.2 PPP kurulumu

Bir bilgisayarın seri hat üzerinden PPP protokolunu kullanarak ağ bağlantısını sağlamak için 'ppp' komutu kullanılır.

Örneğin /dev/ttya seri portunu PPP olarak konfigüre etmek için

```
# ppp 144.122.199.200 144.122.199.201 /dev/ttya &
```

komutunu girmek yeterlidir. Böylece komutun çalıştırıldığı bilgisayarın seri arayüzü 144.122.199.200 adresini ve karşı taraftaki bilgisayarda 144.122.199.201 adresini alır. Ancak PPP'nin dinamik adresleme yeteneğinden dolayı karşı tarafın adresini vermek bir zorunluluk değildir. Örneğin :

```
# ppp 144.122.199.200: /dev/ttya &
```

komutu ile PPP seri porta 144.122.199.200 adresini verir. Ancak diğer bilgisayarın İnternet adresi bağlantı kurulduktan sonra karşı taraftan öğrenilir.

Dial-up telefon hatları üzerinden yapılan bağlantılarda SLIP'de olduğu gibi 'cu' veya

'tip' gibi programlar ile ilk iletişim kurulur.

7. İNTERNET Bağlantısı İçin Alternatif Çözümler

İnternet bugün için gerek kullanıcı sayısı ve gerekse sağladığı olanaklar bakımından dünyanın en yaygın ve etkin bilgisayar ağıdır. Hemen her türlü bilgisayarın birbiri ile olan iletişimini en kolay ve güçlü şekilde sağlayan bir çözümdür. İnternet üzerinde, eğitim ve araştırma kurumlarından, ticari, hükümet ve askeri kurumlara kadar yaygın bir yelpaze içinde çok değişik onbinlerce bilgisayar ağı yer almaktadır. Böyle muazzam büyüklükteki bir bilgiler kaynağından ülkemizden de mümkün olduğu kadar çok sayıda kişinin yararlanmasının zamanı gelmiş ve hatta geçmektedir. Eğer amaç bilgi çağına ulaşmak, ona ayak uydurmak ise bu konuda elimizdeki en önemli ve en kolay ulaşılabilir kaynaklardan biri İnternet'tir. Bu BÖLÜMde, bu büyük bilgi kaynağına ulaşmanın yolları, kurum ya da kişilerin İnternet bağlantısını sağlamak için ne yapmaları gerektiği, alt yapı olarak nelere ihtiyaçları olacağı ve değişik bağlantı yollarından hangilerini kullanabilecekleri anlatılacaktır.

İnternet ağına ulaşmak isteyen kişi ve kurumların bu bağlantıyı gerçekleştirebilmesi için temel bazı konularda karar vermesi gerekmektedir. Bunların en önemlisi bağlantı türüdür. Temel bağlantı türlerini genel olarak iki sınıfa ayırabiliriz.

A - Kişisel (veya tek kullanıcı) bir bilgisayar ile yapılacak terminal turu bağlantı.

B - Bir yerel ağ ya da çok kullanıcı bir bilgisayar ile yapılacak bağlantı (Düğüm- Node ya da Geçiş Kapısı-Gateway olmak).

Yukarıdaki bağlantı türleri de kendi içlerinde, kullanılacak donanım ve PTT imkanları nedeni ile değişiklik gösterirler.

Sırayla bağlantı türlerini ayrıntileri ile inceleyelim.

7.1 -Kişisel (veya tek kullanıcı) bir bilgisayar ile terminal türü bağlantı

İnternet'e bağlanmak isteyen kişi veya kurumların kendi bünyelerinde kurulu bir bilgisayar ağı yoksa ve sadece tek kullanıcı bir bilgisayar üzerinden İnternet bağlantısını yapmak istiyorlarsa bu durumda İnternet bağlantı hizmeti veren bir noktaya (Servis Sağlayıcı-SS) bağlanmak için müracaat edebilirler Bu tür kullanıcıların İnternet bağlantıları için TR-NET tarafından kurulmuş olan ve işletilen bilgisayarlar üzerinde bir kullanıcı kodu açılır. Kullanıcılar aşağıda anlatılacak olan değişik bağlantı yolları ile bu sistemlere ulaştıklarında hemen hemen tüm İnternet servislerini kullanabilecekleri bir ortama girerler. Bu adımdan sonra dünyanın herhangi bir noktasına bağlanıp dosya çekebilir, elektronik posta ile mektup gönderebilir, kütüphane taraması yapabilir, çeşitli konulardaki bilgi bankalarına ulaşabilir ya da burada sözü edilmeyen sayısız hizmetten yararlanabilirler.

İnternet bağlantısının sağlanması için gerekli donanım sadece bir bilgisayar ve bir modemden (2400 bps ile 14400 bps hızları arasında çalışabilen, tercihen V.32bis standardında) ibarettir.

Fiziksel bağlantının sağlanabilmesi için iki yol mevcuttur.

1- PTT Dial-up telefon hatları: TR-NET tarafından işletilen İnternet'e bağlı sistemlerin telefon numaralarını çevirip bağlantı kurmak.

2- PTT X.25-ITI (Turpak-Intelligent Terminal Interface) servisi: X.25-ITI servisinden yararlanıp TR-NET tarafından işletilen PAD cihazı yolu ile İnternet'e bağlantı kurmak. (X.25-ITI aboneliği telefon başvurusu gibi bir başvuru ile PTT'ye yapılır. Standart başvuru ücreti, aylık abonelik ücreti ve kullanım ücreti ödenir)

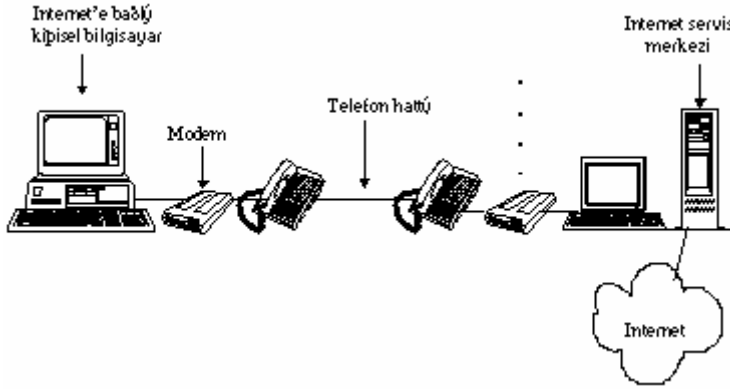
7.1.1Gerekli Yazılım ve Donanım

Bağlantı için gerekli donanımın sağlanıp, hangi PTT imkanı ile sisteme ulaşılabileceğine karar verildikten sonra geriye sadece bağlantı için hangi yazılımın kullanılacağı kalmaktadır. Piyasada bulunan hemen hemen bütün Terminal Benzetim (Emülasyon) programları (Procomm, Bitcom, Windows Term. Emul., Softerm gibi) İnternet bağlantısı için sorunsuz olarak kullanılabilirler. Bu yazılımlar genellikle satın alınan modem cihazı ile beraber verilmektedir. İnternet bağlantısını sağlamak için gerekli yazılım konfigürasyonları çok basit olup aşağıdaki özelliklerin girilmesi yeterlidir:

```
Number of Data Bits    = 8
Parity                 = No
Stop Bits              = 1
```

Emulasyon
Speed

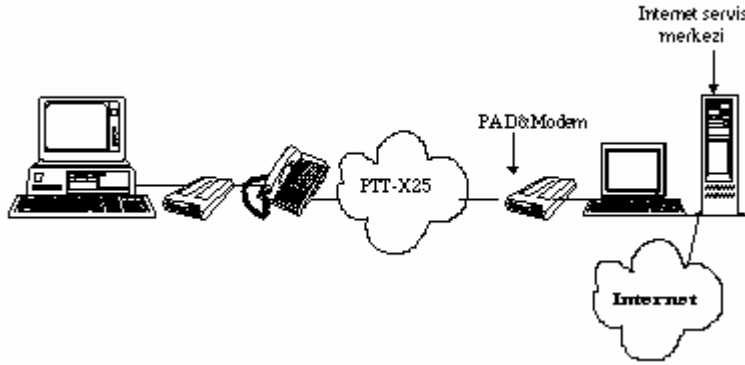
= VT100
= Modemin özelliklerine bağlı
olarak 2400 ile 14400 bps



arasındaki herhangi bir hız.

Çizim-18 ve Çizim-19'de her iki bağlantı turu de şekillerle gösterilmektedir :

Çizim-18. Dial-up telefon hattı ile bağlantı



Çizim-19. X.25 İTİ ile bağlantı

Ayrıca bazı çok kullanıcılı bilgisayarlarda da TCP/IP yazılımı bulunmadığı için bu sistemlerin yine yukardaki yollarla terminal emulasyonu yöntemi ile İnternet bağlantısı sağlanabilir.

Dial-up telefon hatları üzerinden yapılan bağlantılarda göz önüne alınması gereken bir noktada çok sayıda kullanıcının kısıtlı sayıdaki telefon hatlarını paylaşmalarıdır. Bu problem TR-NET tarafından hat sayısı artırılarak giderilmeye çalışılmaktadır.

7.2 - Bir yerel ağ ya da çok kullanıcılı bir bilgisayar ile yapılacak bağlantı

Bir yerel ağ ya da çok kullanıcılı bir sisteme sahip kuruluşların İnternet bağlantılarının sağlanması için de değişik bağlantı alternatifleri mevcuttur. Birden fazla kişinin aynı anda İnternet ağının imkanlarını kullanması durumunda bağlantı turunu seçerken cevap verilmesi gereken bir kaç nokta vardır. Bunlar:

- Bu bağlantıyı kaç kişi aynı anda kullanacak?
- Günde kaç saat bağlantı yapılacak ve hangi yoğunlukta kullanılacak?
- Hangi tür servisler kullanılacak?
- Kurum dışarıya elinde bulunan bir takım bilgi kaynaklarını açacak mı?

Tüm bu soruların cevapları bağlantı turunun belirlenmesini sağlamak için önemli kriterlerdir. Örneğin, çok yoğun bir kullanımda bulunacak bir kurumun X.25 yerine kiralık hat ile bağlanması daha uygun olurken, günde bir kaç kere bağlanıp sadece elektronik-posta okumak ve/veya Usenet/News gibi az sayıda İnternet olanağından yararlanmayı düşünen bir kurum için dial-up bağlantı en uygun çözüm olmaktadır.

7.2.1 . Fiziksel Bağlantı Seçenekleri

Değişik bağlantı tiplerini inceleyecek olursak temel olarak 3 bağlantı seçeneği olduğunu görürüz:

- 1 - Kiralık hat

2 - X.25

3 - Dial-up

7.2.1.1. Kiralık hat:

İnternet trafiği çok yoğun olan ve çok sayıdaki kullanıcıya aynı anda İnterneti kullandırmak isteyen kurumlar için en uygun çözümdür. İnternet'i kullanacak olan kurum ile TR-NET servis merkezi arasında PTT'den uygun hızda bir hat kiralanır ve İnternet bu hat üzerinden kullanılır. Bu çözümde yine kurumun bulunduğu yerin TR- NET servis merkezlerine olan uzaklığı ile oranlı olarak hat kirası artmaktadır. Şehirlerarası bağlantılar için oldukça pahalı olan bu bağlantı sekli genellikle büyük kuruluşların İnternet bağlantıları için kullanılmaktadır.

Kiralık hat bağlantısını yapmak isteyen kurumların dikkat etmesi gereken ikinci nokta bu tur bağlantının iki adet modem gerektirmesidir. Kurum hem kendi tarafında ve hem de TR-NET servis merkezinde kullanılmak üzere iki modem'e sahip olmalıdır. Ayrıca modem'in bağlanacağı bos bir port'un TR-NET yönlendirici cihazlarında bulunması gerekmektedir. Şu anda var olan bos port'lar sadece İnternet'e bağlanacak Üniversitelere ayrıldığı için diğer kurumların bu gerekli port'u da sağlamaları gereklidir.

7.2.1.2- X.25 bağlantı:

X.25 turu bağlantı daha önce de belirtildiği gibi yüksek trafik yaratmayan, orta büyüklükteki kurumlar için oldukça uygundur. Ancak X.25 hatlarının ücretlendirmesi doğrusal olarak arttığı için belli bir trafik yoğunluğunun üzerinde kiralık hat daha ekonomik bir çözüm olmaktadır. Bu bağlantının sağlanabilmesi için kurumun elindeki bilgisayarın ya da bilgisayar ağı cihazının (yönlendirici gibi) X.25 üzerinden IP paketlerini geçirme özelliğinin bulunması gereklidir. Ayrıca uygun özelliklere sahip bir adet modem de gereklidir. Uygun verimin alınabilmesi için X.25 hattının hızının en az 14.400 bps olması önerilmektedir.

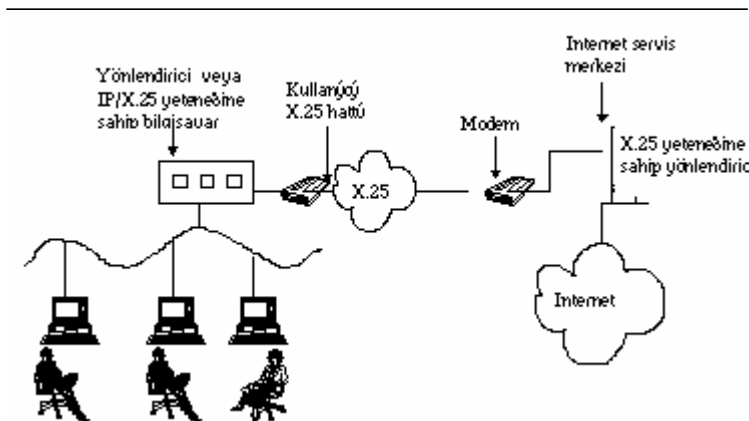
7.2.1.3- Dial-up bağlantı

Yerel ağın TR-NET merkezlerine olan uzaklığına ve kullanım yoğunluğuna göre dial-up telefon hatları ile de LAN bağlantısı sağlanabilir. Özellikle şehir içi LAN bağlantısı için çok uygun bir bağlantı alternatifi olan bu çözüm için TR-NET merkezinde bir port, bir telefon hattı ve TR-NET merkezi ile kurumu birbirine bağlamak üzere iki adet modem gerekmektedir.

7.2.2. Gerekli Yazılım ve Donanım

Bağlantı için gerekli fiziksel altyapı seçimi yapıldıktan sonra nasıl bir donanım ve yazılımın bu amaçla kullanılacağı sorusu gündeme gelir. Tüm bu yazılım ve donanımın temel görevi IP yönlendirme işlemini yapmaktır. Yani yerel ağdan gelen ve İnternet'e gitmesi gereken paketleri dış hat (X.25, kiralık hat, dial-up telefon hattı) üzerinden İnternet'e ve dışardan (yani İnternet'den) gelen bilgiyi yerel ağ üzerindeki ilgili bilgisayara yönlendirmektir (bu yönlendirme işleminin nasıl yapıldığı daha önceki BÖLÜMLerde detaylı olarak anlatılmıştı). Bu amaçla kullanılacak çözümler için değişik alternatifler mevcuttur. Bilgisayar ağları konusunda uzmanlaşmış bazı şirketlerin ürettikleri cihazlar bağlantı için kullanılabilmesi gibi ücretsiz temin edilebilen bazı yazılımlar ve çok ucuz elde edilebilecek donanımlar ile de İnternet bağlantısı sağlanabilir.

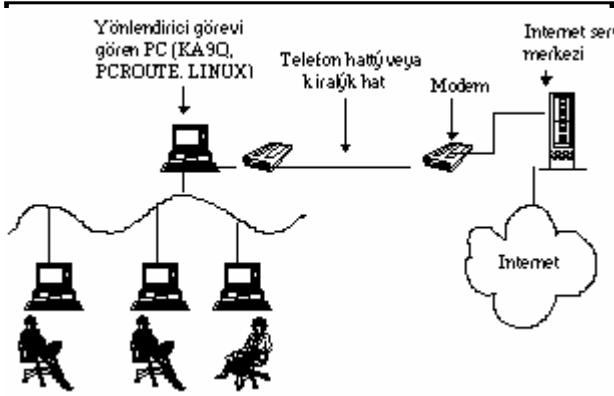
X.25 turu bir bağlantı için çok fazla bir seçenek bulunmamaktadır. Zira bu tur bağlantı X.25'e özgü özel yazılım ve donanım gerektirmektedir (bazı sistemler donanıma ihtiyaç duymamakta sadece yazılım yeterli olmaktadır). Çok kullanıcıli bir bilgisayar ile bağlantı yapmak isteyen kurumlar sistemleri üzerinde çalışan böyle bir yazılım ve donanımın bulunup bulunmadığını ve fiyatını cihazın satıcısı olan ilgili firmadan öğrenmelidir. Benzer şekilde, bağlantı için bir yönlendirici kullanılacaksa yönlendirici üzerinde de X.25 yazılım desteği bulunup bulunmadığı detaylı olarak araştırılmalıdır. Çizim-20'de bu bağlantı turu şekil üzerinde gösterilmektedir.



Çizim-20 X.25 türü bağlantı

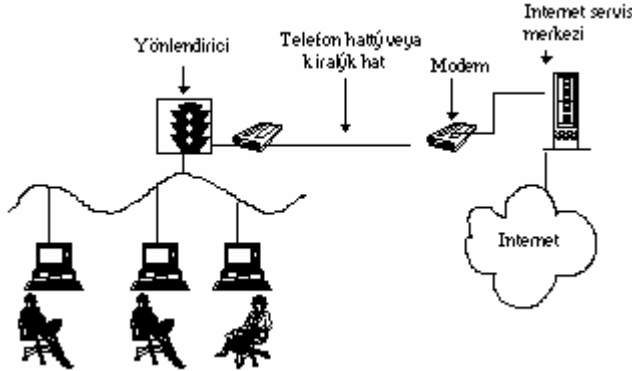
Kiralık hat ve Dial-up turu bağlantılar için alternatif cihaz yelpazesi daha geniştir. İnternet bağlantısı sağlamak için yazılmış çok sayıda ücretsiz yazılım mevcut olup bu yazılımların performansı da oldukça iyidir. Bu noktada ücretsiz ya da en az harcama ile sağlanacak bir çözüm ile nispeten pahalı cihazlar arasında yapılacak seçimde hassas bir denge bulunmaktadır. Yoğun bilgisayar trafiğine sahip olan ve yüzlerce bilgisayardan oluşmuş bir ağ bağlantısı için tabii ki ücretsiz yazılımlar bir noktadan sonra yetersiz kalmaktadır.

Çizim-21’de de gösterilen ücretsiz edinilebilecek yazılımların kuruluş ve kullanımı ile ilgili biraz daha detaya girecek olursak;



Çizim-21 Ücretsiz yazılımlar ile gerçekleştirilen bağlantı

Bu tür yazılımlar genellikle minimum konfigürasyona sahip bir kişisel bilgisayar üzerinde çalışmaktadır. Örneğin üzerinde seri portu ve Ethernet kartı bulunan bir 80286 PC üzerine kurulan yazılımlar arasında en popüler olanları PCROUTE ve KA9Q’dur. Bu yazılımlar kullanılarak SLIP (Serial Line IP) protokolu ile seri port üzerinden kiralık hat ya da telefon hatları kullanılarak İnternet’e bağlanılabilir. Bir diğer alternatif, güçlü bir PC (örneğin 8MB hafıza, 100 MB dışıe sahip bir 80386) üzerine kurulabilen ücretsiz (shareware) UNIX işletim sistemi LINUX ile oldukça iyi sonuçlar alınabilir. Daha önce de belirttiğimiz gibi büyük bir ağ yapısına sahip kuruluşlar (Büyük Üniversiteler ve şirketler gibi) ucuz PC tabanlı İnternet bağlantısı çözümleri yerine bu amaçla üretilmiş profesyonel cihazlar kullanmaktadırlar. Pek çok iletişim protokolunu aynı anda yönlendirebilen, üzerine pek çok arayüz takılabilen ve aynı anda pek çok noktanın birbirleri ile olan bağlantısını sağlayabilen yönlendirici cihazları kendi içlerinde kullanım amacına göre geniş bir yelpazeye sahiptir. Bu tür bir bağlantı Çizim-22’de gösterilmektedir.



Çizim-22 Yönlendirici ile gerçekleştirilen bağlantı

7.3 Fiziksel Bağlantı Sonrası

Bir yerel ağın bağlantısının tam anlamıyla yapılabilmesi için fiziksel bağlantı ve gerekli yazılım donanımın yanı sıra yerine getirilmesi gereken son bir kaç nokta daha vardır. Bunlar :

- IP-numarası edinilmesi,
 - Kurum alt-domain adının belirlenmesi,
 - DNS ve SMTP kurulması,
- olarak sıralanabilir.
- a-IP numarası edinilmesi:

Her kurum kendi yerel bilgisayar ağında kullanmak üzere bir IP adresine sahip olmalıdır. Kurumun bilgisayar ağına bağlı bilgisayar sayısına ve tahmin edilen genişleme sayılarına göre uygun miktarda IP adresi TR-NET NCC (Turkish İnternet - Network Coordination Center) tarafından ilgili kuruma tahsis edilir. Yurt dışından bir blok halinde Türkiye’nin kullanımı için ayrılan IP adreslerinin dağıtımı Türkiye İnternet Proje Grubunca (TR-NET NCC) yapılmaktadır. Bilindiği gibi uluslararası platformda varolan İnternet adresleri hızla tükenmektedir. Dolayısıyla A ve B-sınıfı IP adres dağıtımı tüm dünyada yapılmamakta sadece Ç-sınıfı adresler dağıtılmaktadır. Genellikle kurulu olan basit yerel ağlarda Ethernet teknolojisi kullanılmaktadır ve bir inçe Ethernet kablosu ile kurulan Ethernet ağı segmentinde en fazla 30 kişisel bilgisayar yer almaktadır. Ancak bir Ç-sınıfı adres ile 254 tane bilgisayarı adreslemek mümkündür. Bir Ç-sınıfı adresin subnet metotları kullanılmadan böyle bir segmente verilmesi 224 adet adresin boşa gitmesi anlamına gelir. Dolayısıyla kurumlar

kendilerine verilen adres alanlarını subnet yönteminden yararlanarak parçalarlarsa daha verimli kullanmış olurlar. Subnet konusu için daha önceki BÖLÜMLerde gerekli teknik açıklamalar detayları ile verilmiştir.

b-Kurum alt-domain adının belirlenmesi

Bilindiği gibi Türkiye'deki İnternet yapısında en üst seviye domain adı olarak ISO'nun ülke standart kısaltması olan .tr kullanılmaktadır. Bu seviyenin altında kalan domain isimleri İnternet bağlantısı yapılacak kurumun özelliğine göre kararlaştırılır. Bugün için var olan alt-domain ler :

.EDU	=	Eğitim ve araştırma kurumleri
.COM	=	Ticari kurumlar
.GÖV	=	Devlet kurumları
.MIL	=	Askeri kurumlar
.NET	=	Ağ işletim ve yönetim merkezleri
.ORG	=	Yukarıdakiler dışındaki kurumlar.

İkinci seviye alt domain adının belirlenmesinden sonra üçüncü seviye yani kurumu tanımlayan domain'in belirlenmesi gereklidir. Burada nasıl bir kısaltma kullanılacağı seçimi kurumun kendisine kalmıştır. Örneğin bu yapı

ODTU için	metu.edu.tr
Merkez Bankası için	tcmb.göv.tr
TUBITAK için	tubitak.göv.tr

şeklinde belirlenmiştir. Eğer bağlanan kurum içinde ayrı birimler varsa bunlara da ayrı domain isimleri verilebilir. Mesela:

ODTU Bilgisayar Merkezi için	cc.metu.edu.tr
ODTU Matematik BÖLÜMu için	math.metu.edu.tr
TUBITAK TETM için	tetm.tubitak.göv.tr
TUBITAK Marmara araştırmamam.	tubitak.göv.tr

c-DNS ve SMTP Kurulması

DNS (Domain Name Sistem) İnternet bağlantısının yapılması aşamasında çok gerekli olmasa da özellikle ağ çalışmaya başladıktan sonra gerek duyulan bir servistir. DNS, Elektronik posta yollanması ve sembolik adreslere

(knidos.cc.metu.edu.tr gibi) uzak bağlantı (telnet, ftp vs.) yapılması esnasında kullanılan önemli bir servistir. Çok önemli olan bu konuda kurumun gerekli çalışmayı tamamlayıp kendi DNS'ini çalıştırması sağlıklı bir yapı için önemli bir gereksinimdir. Ancak İnternet bağlantısı yapan her kurumun muhakkak DNS kurması zorunlu diye de bir şart yoktur. Zira kurum sadece 1-2 bilgisayarını İnternet ağı üzerine bağlamışsa bu durumda TR-NET ile görüşüp bu makinaları için DNS hizmetini Ağ İşletim Grubundan alabilir.

SMTP (Simple Mail Transfer Protokol) ise kurumun İnternet üzerinden elektronik- posta almasını ve yollamasını sağladığı için aynı şekilde çok gerekli bir servistir.

Bu iki servisin kurulması ile ilgili detaylar sistemden sisteme değiştiği için tüm konfigürasyonlar sistem yöneticisi tarafından yapılmalı ve bağlanan bilgisayar sistemleri ile ilgili dökümantasyonda belirtilen talimatlara uyulmalıdır.

İnternet Bağlantısı İçin Kullanılacak İdeal Bilgisayar Sistemleri

İnternet bağlantısı için kullanılacak bilgisayarın öncelikle TCP/IP protokoller setine sahip olması gerekmektedir. Bu setin ana elemanları Telnet, FTP ve SMTP gibi kullanıcıya hizmet veren servisler olup bunun yanında DNS (Domain Name Sistem) gibi önemli yan servislerinde bulunması tercih edilir. Hem genel amaçla kullanılacak hem de ağ servislerini (LAN ve WAN) sağlayabilecek bilgisayarlar için en ideal çözüm UNIX tabanlı sistemlerdir. Bu sistemler hem endüstri standardı olmuş açık yapıları ve hem de TCP/IP protokoller setini doğal olarak barındırmaları nedeni ile en uygun çözümdürler.

7.4 Personel Gereksinimi

İnternet bağlantısında en önemli konulardan biri de bilgisayar ağını kontrol edecek ve onu sürekli çalışır tutacak insan gücüdür. Bilgisayar ağından en yüksek verimin alınabilmesi için kurumun büyüklüğüne bağlı olarak en az bir (tercihan Bilgisayar Mühendisi), kurumun büyüklüğüne göre gerekirse daha çok sayıda personel bu iş ile sorumlu olmalı ve konu ile ilgili her türlü konfigürasyon, IP adresleme, yönlendirme (routing), servislerin kuruluşu, kullanıcı eğitimi ve dökümantasyon çalışmalarını yapmalıdır.

7.5 Dökümanların Okunması

TR-NET merkezinde değişik kurumlardan gelen bağlantı isteklerini yerine getirmek ve sürekli olarak İnternet kullanıcılarının sayısını yükseltmek bu konuda emeği geçen kişilerin en çok zevk aldığı noktadır. Ancak gerek bağlantısını yapan ve gerekse yapmak için girişimde bulunan kurum ve kişilerin en büyük eksiklikleri ellerindeki dökümanları okumadan, gerekli çalışmayı ve bilgi birikimini sağlama çabası göstermeden, teknik olarak bilgisi olduğunu bildiği kişilere sorarak öğrenme yoluna gitmeleridir. Bu tabii ki soran kişi açısından pratik bir yol olmaktadır ama yüzlerce kişinin bağlı olduğu bu servis üzerinde tüm soruları cevaplamının ne kadar zor ve zaman alıcı olacağıda çok belirgindir..

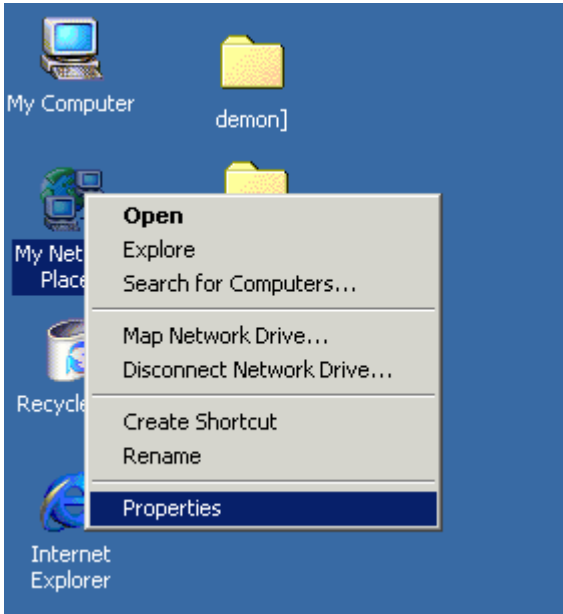
BÖLÜM2:İNTERNET UYGULAMA PROGRAMLARI

WİNDOWS 2000 WEB SERVER KURULUMU

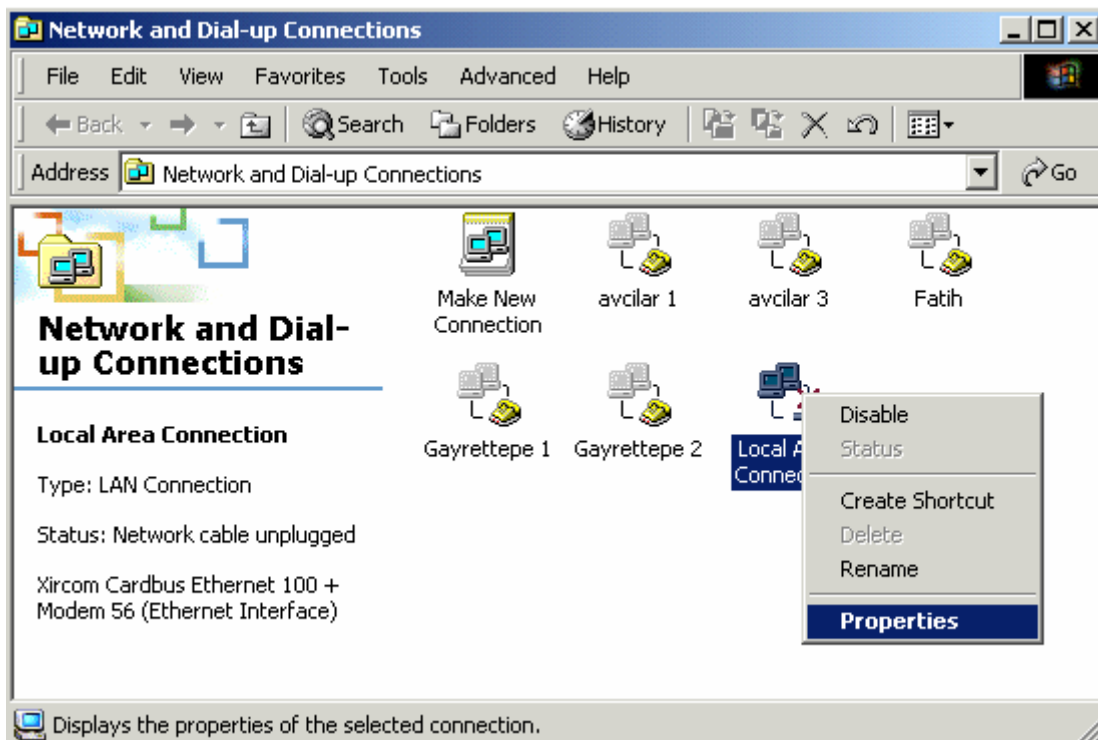
1- Windows 2000 kurulacak. (standart)

2- Server a alınan Ip numarası verilecek

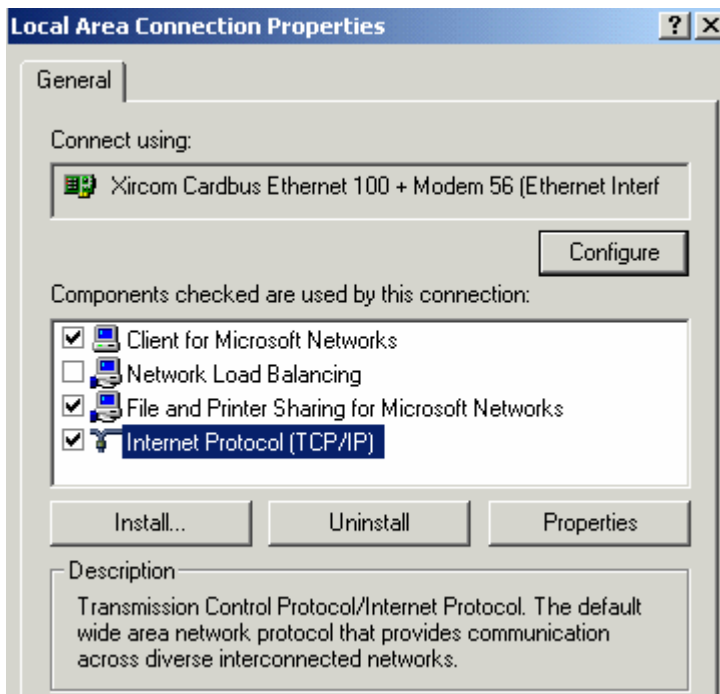
a- Netwok Plaçe sağ çlıkleyerek properties ine girilir.



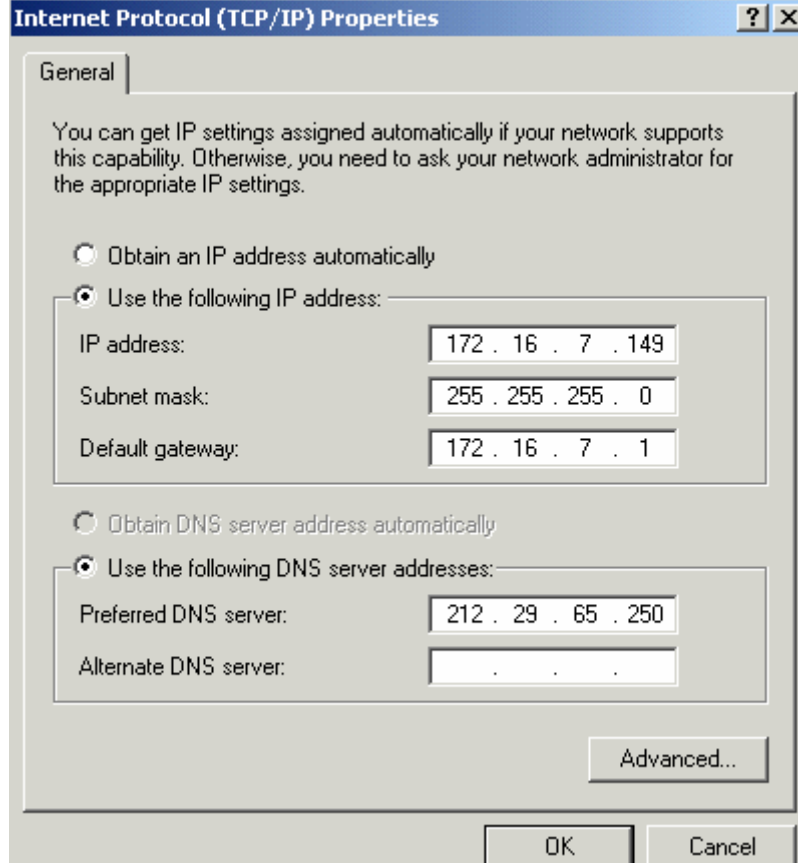
b- Local Area Connection properties ine girilir.



C- İnternet Protocol (TCP-IP) properties ine girilir.

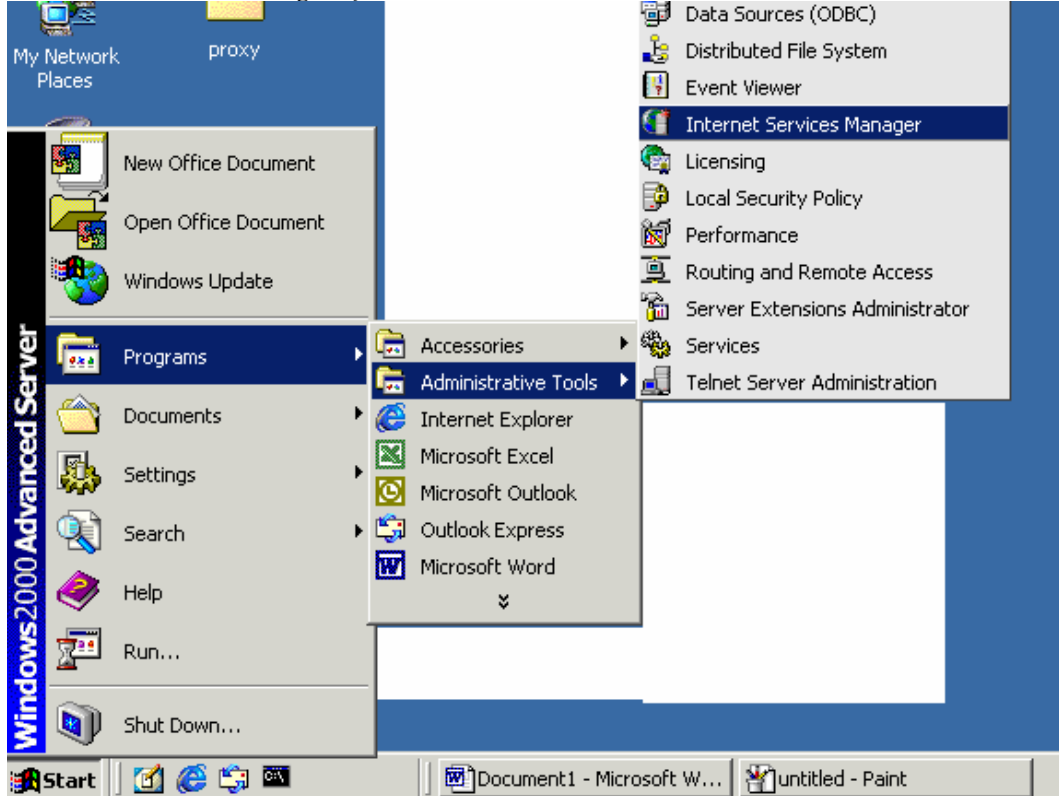


d-dns serverdan alınan domain name ip adresi ve network ayarları gerekli yerlere girilir.

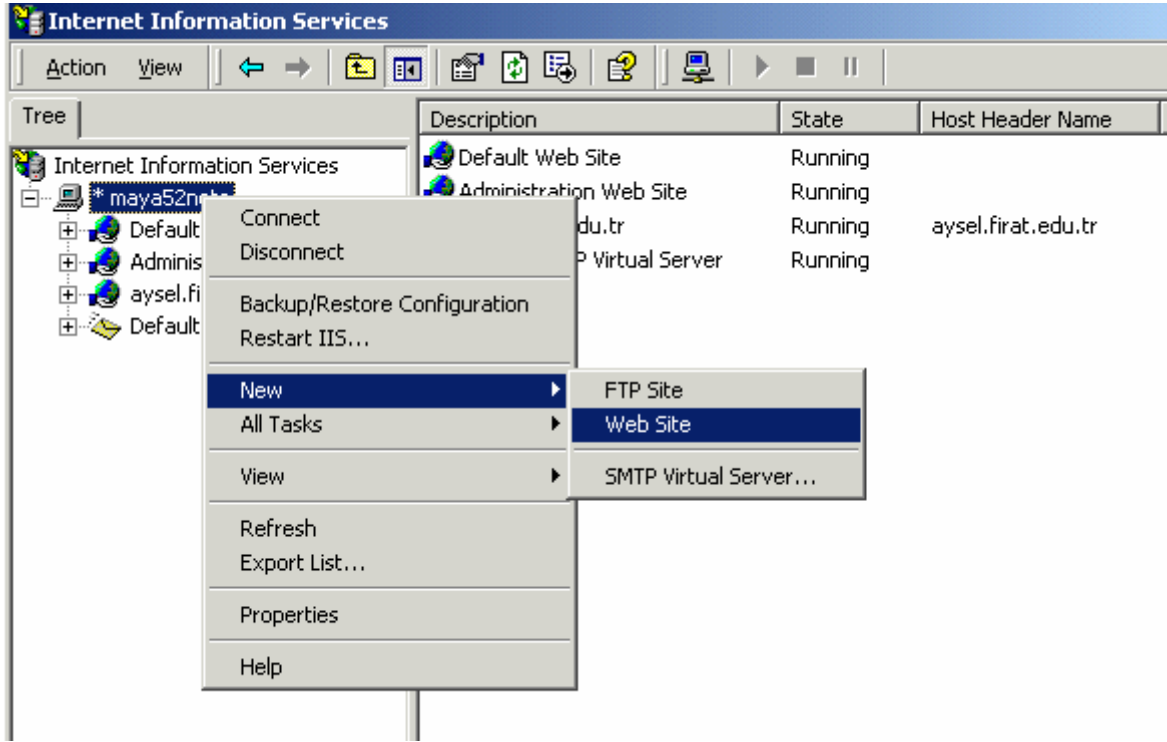


3- İnternet Service manager dan sayfa ayarlanması

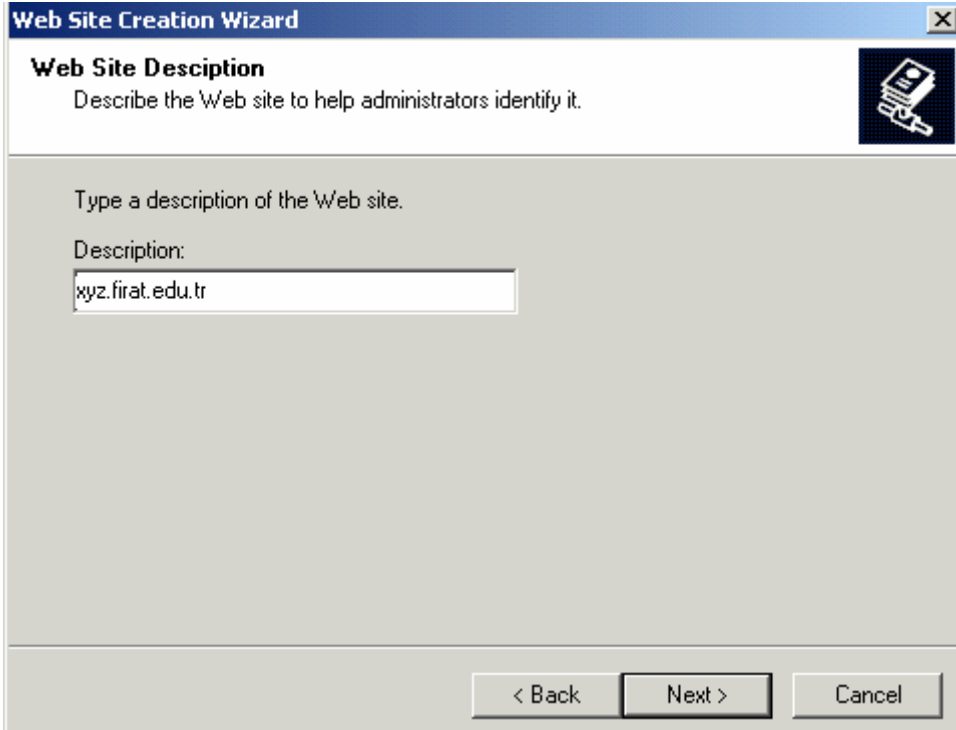
a- İnternet Service manager açılır.



b- Server name sağ tıklayarak sırasıyla **new> web site** seçilir.



c- Description kısmını oluşturulacak sayfanın açıklaması yazılır. Kolaylık açısından sayfanın adresi girilebilir.



d- ip adres kısmına domain name`e verilen ip adresi verilir.Port kısmı 80 olarak bırakılır.Host header name kısmına sayfanın internet adresi girilir.

Web Site Creation Wizard [X]

IP Address and Port Settings

Specify IP address and port settings for the new Web site.

Enter the IP address to use for this Web site:
127.0.0.1

TCP port this web site should use: (Default: 80)
80

Host Header for this site: (Default: None)
xyz.firat.edu.tr

SSL port this web site should use: (Default: 443)

For more information, see the IIS Documentation.

< Back Next > Cancel

e- Path kısmına sayfa dosyalarının saklanacağı yol girilir.

Web Site Creation Wizard [X]

Web Site Home Directory

The home directory is the root of your Web content subdirectories.

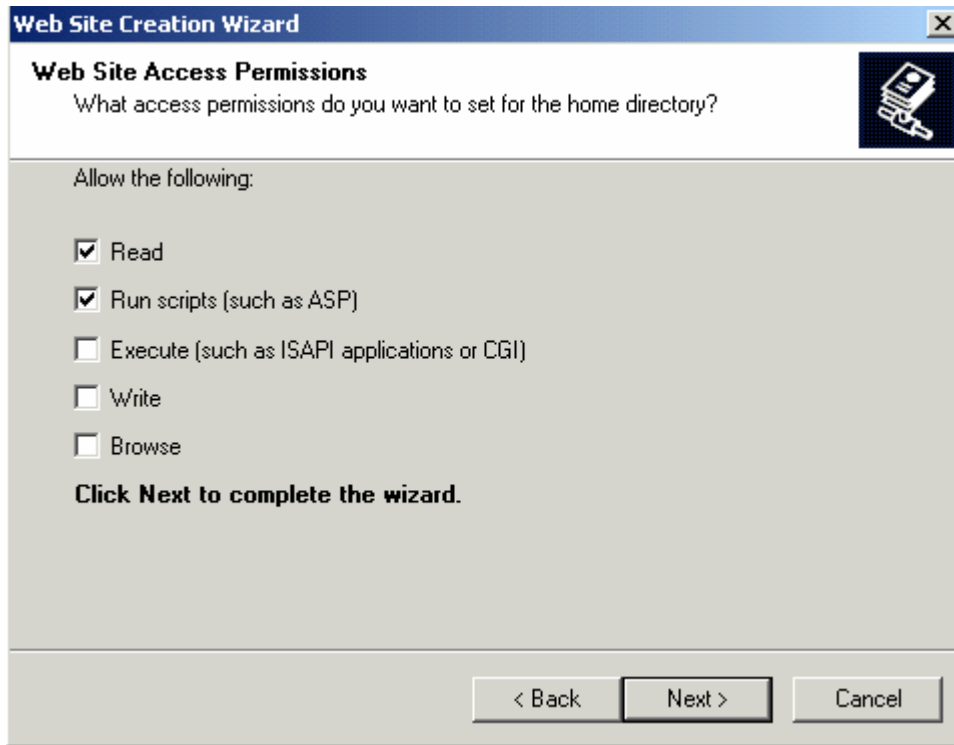
Enter the path to your home directory.

Path:
E:\inetpub\wwwroot\xyz.firat.edu.tr Browse...

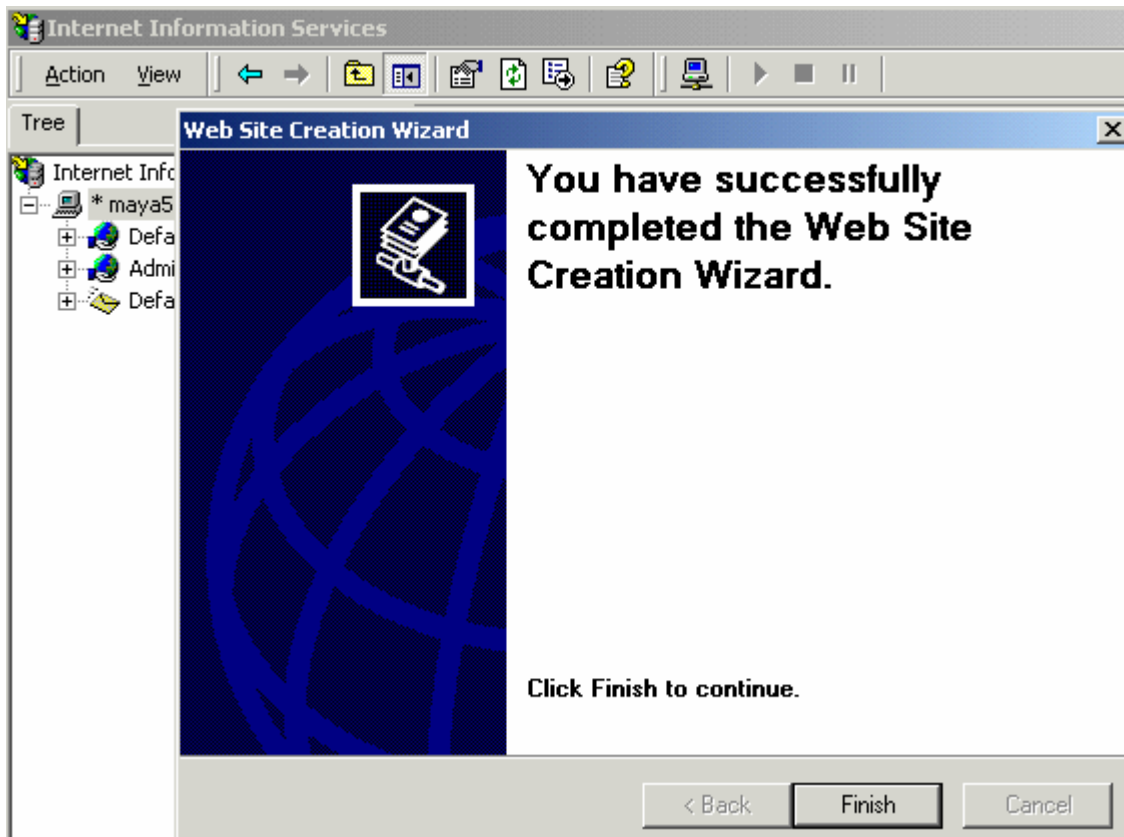
Allow anonymous access to this Web site

< Back Next > Cancel

f- Gelen pencerede herhangi bir değişiklik yapılmadan next kliklenir.



ğ- finish seçilerek işlem bitirilir.

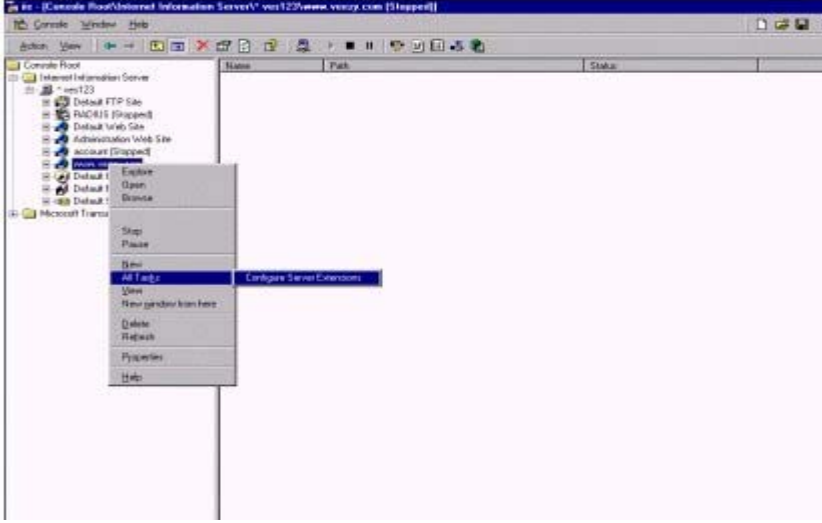


4 - Frontpage Server Kurulum

Yapacağımız ayarlar ile Front Page ile Sayfanın bulunduğu foldera istenilen user'lerin bağlanması sağlanacaktır. Bu konu sayfanın güvenliği açısından önemlidir. Kullanıcı adı ve şifreleri gizli olmalıdır.

Belli periyodlarla değiştirilmelidir. şifreler minimum 8 karakter olmalı , büyük küçük harf kullanılmalı , sayısal ve alfabetik karakterler kullanılmalıdır.

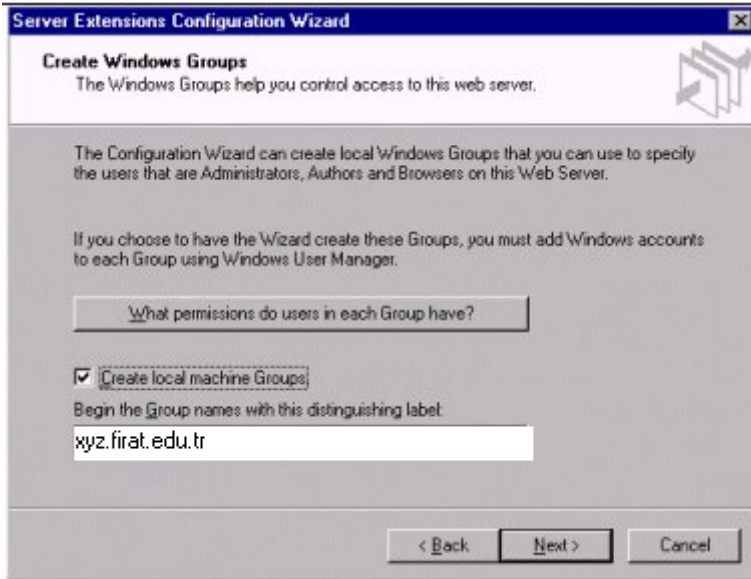
a. Front Page Server Extensionlarını konfigür edeceğimiz sayfanın üzerine gelerek sağ tıklayıp Task kısmından “Configüre server Extensions” seçilir.



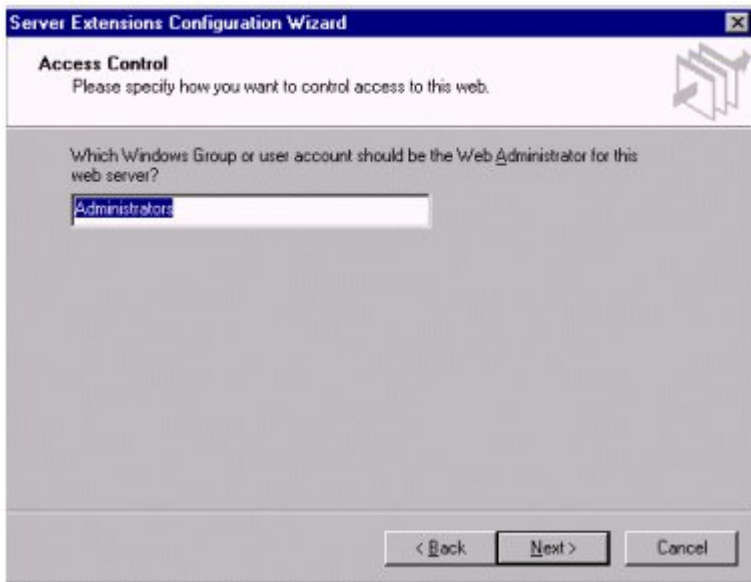
b. “Next” diyerek geçiniz.



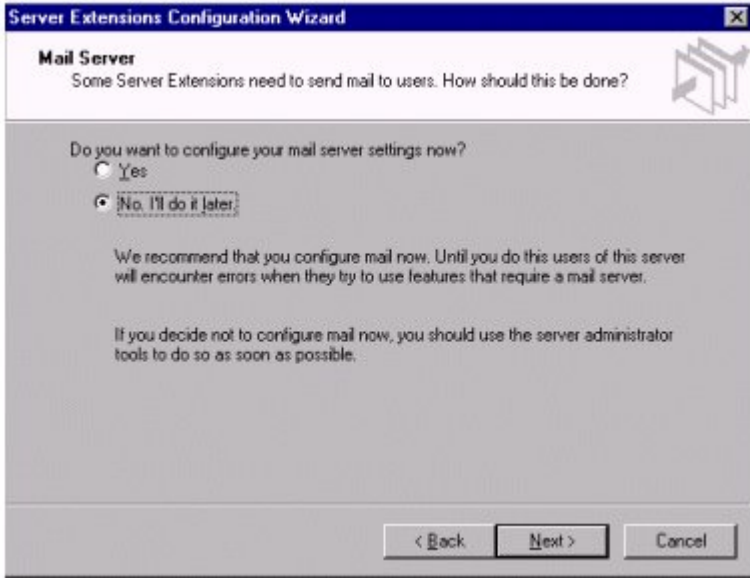
c. User Manager For Domains te www.xyz.firat.edu.tr Admins , Authors ve Browsers grupları yaratılır



d. Administrator grubu web sayfasının default admini olarak atanır.



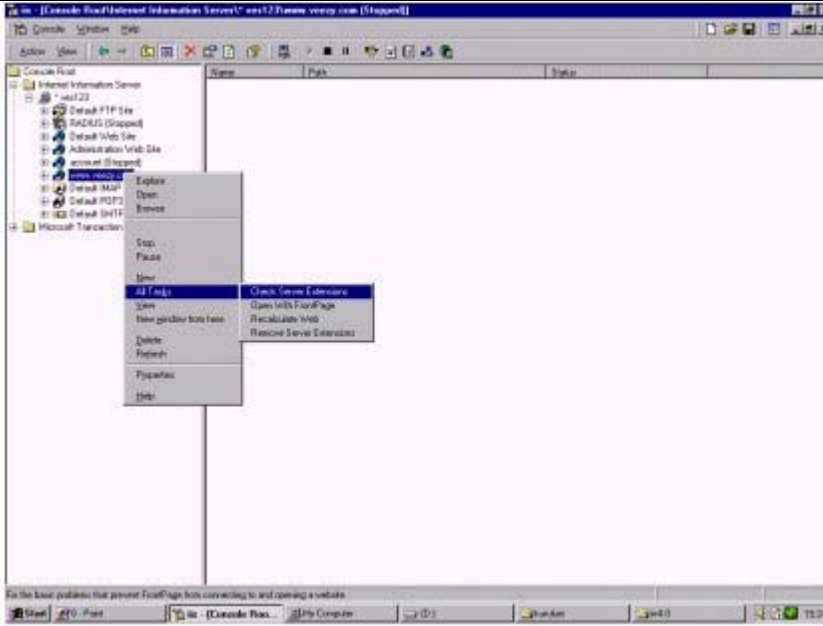
e) Mail server ile ilgili olan settinglere "No" diyerek geçilebilir."Yes" denilmesi halinde sayfa üzerinden mail gönderilmesi ile ilgili mail settinglerini yapılması gerekmektedir.



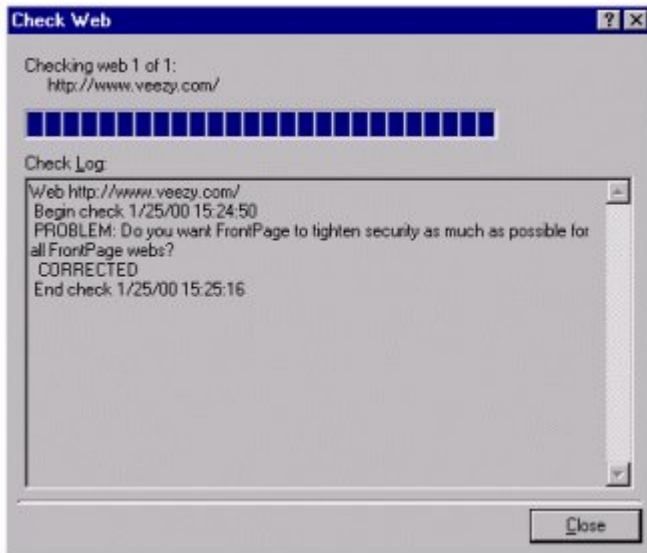
f. FP Server Extensions konfigurasyonunun tamamlandığına ve sayfanın edit edilmesi ile ilgili gerekli Nt user gruplarını açıldığını belirten ekran gelir. “Finish” diyerek konfigurasyonu tamamlayınız.



g. Server Extensionlarının konfigurasyonunun tamamlanmasından sonra Fp ile güvenli bir bağlantının sağlanması için sayfanın server extensionlarının kontrol edilmesi gerekmektedir. Bu işlem için sayfanın üzerine gelip sağ tıklayınız ve çıkan menüden “All Tasks” / “Check Server Extensions” tıklanarak bu işlem başlatılır. Güvenliğinden şüphe duyulan siteler için bu işlem gerektiğinde yapılır.



h. Sayfanın Fp securitysi doğrulandıktan sonra “close” diyiniz.



i. Yeni açılan sayfaya Front Page erişimi verdiğimiz kişiye yeni bir kullanıcı Accountu yaratıp gerekli hakları vermemiz gerekmektedir. Bu nedenle MMC üzerindeki User Manager for domains yada j- Start/Programs/Administrative Tools(Common)/User Manager For Domains seçilerek User Manager’ a gireriz.

User Manager

User Policies Options Help

Username	Full Name	Description
Administrator		Built-in account for administering the computer/domain
Guest		Built-in account for guest access to the computer/domain
aysel emine	aysel emine	ogrenci /firat universitesi

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Users	Ordinary users
xyz.firat.edu.tr Admin	
xyz.firat.edu.tr Author	
xyz.firat.edu.tr Browser	

j. "Groups" kısmına tıklayınız.

User Properties

Username: aysel emine

Full Name: aysel emine

Description: ogrenci/firat universitesi

Password: [Redacted]

Confirm Password: [Redacted]

User Must Change Password at Next Logon

User Cannot Change Password

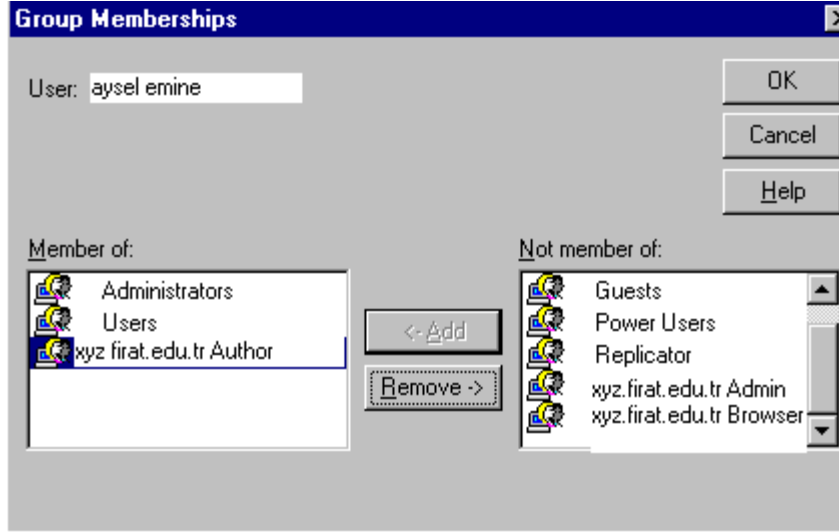
Password Never Expires

Account Disabled

Account Locked Out

Groups Profile Dialin

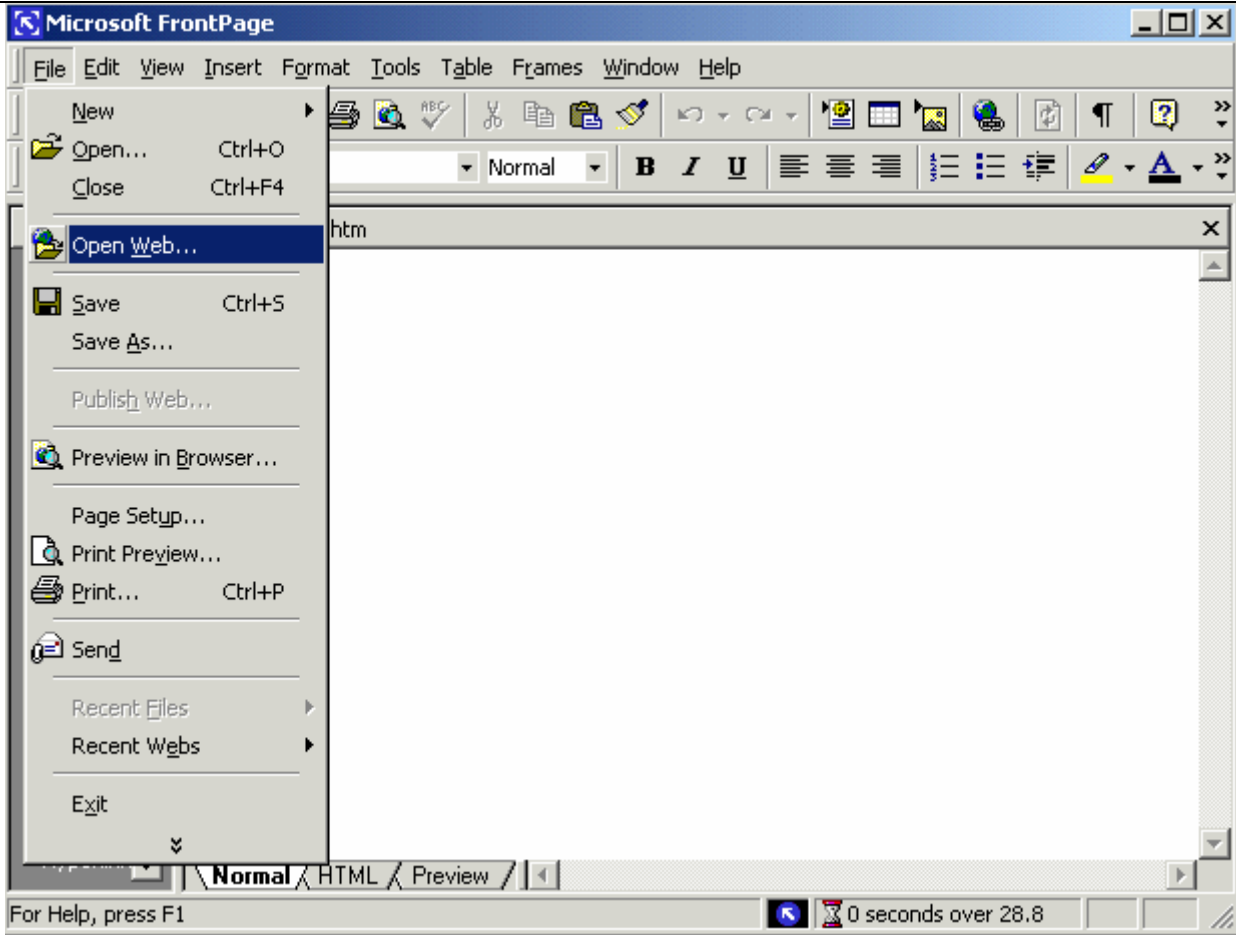
k) .Front Page erişim hakkı verilecek olan web editorlerine sayfa için Author haklarının verilmesi yeterlidir.Admin haklarını verilmesi durumunda security ile ilgili sorunlar yaşanabilir.



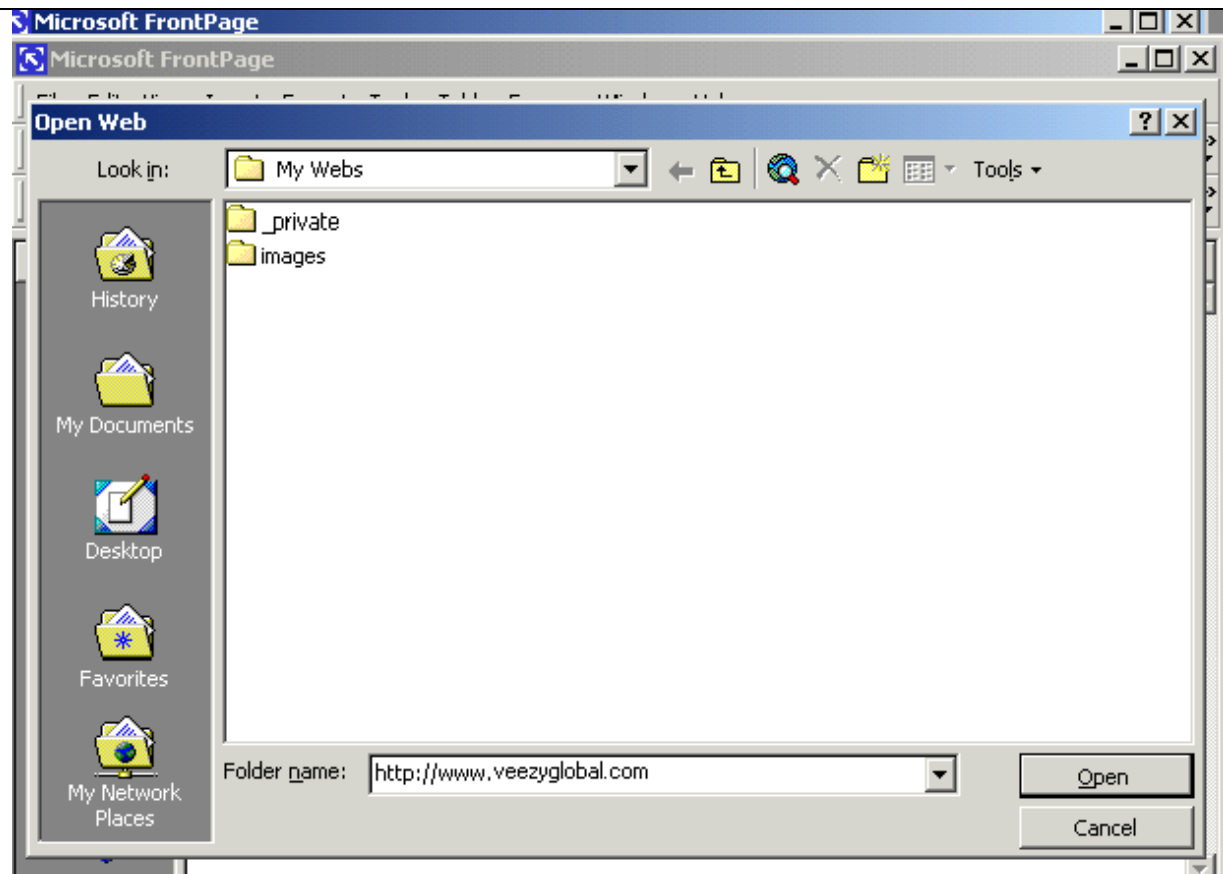
1.)Web editorünün bulunduđu gruplara xyz.firat.edu.tr Authors grubunda eklenerek Fp erişimi verme işlemi tamamlanmış olur.

5. Front Page Ile Sayfaya Login olma:

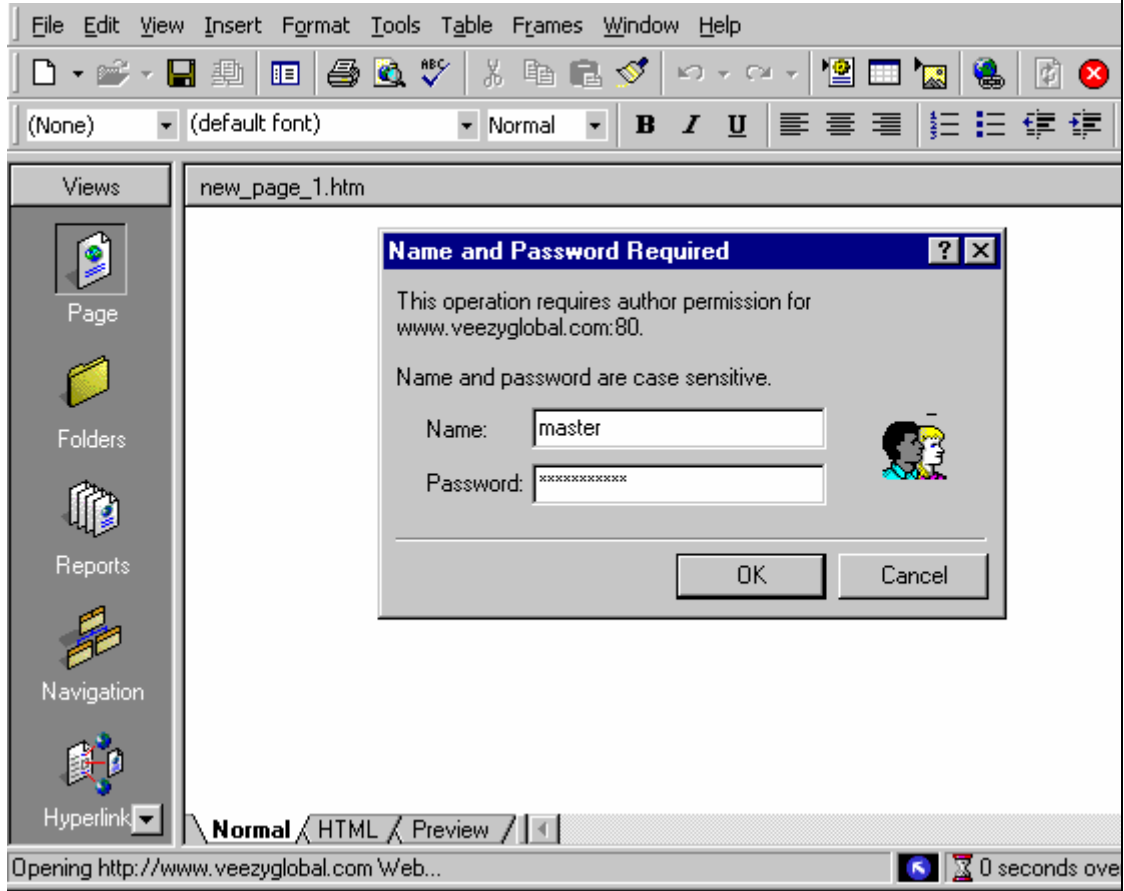
A - Front Page 2000 programı açılarak File > Open Web seceneđi seçilir.



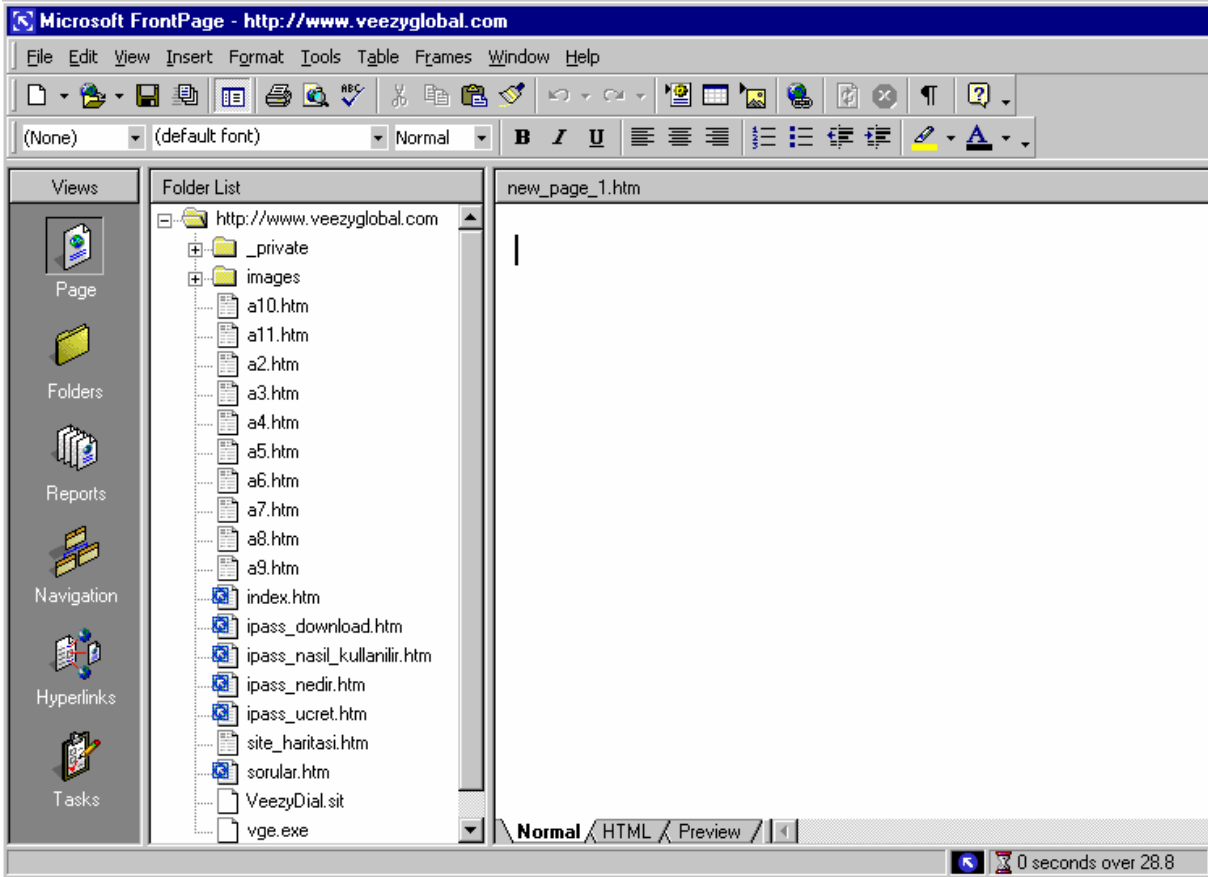
B - Open Web penceresinden Folder Name kısmına <http://www.veezyglobal.com> yazılarak "Open" tuşu seçilir. Baftaki "http://" girilmesi zorunludur.



C – ilgili sayfanın Front Page Server Extension ‘leri tanımlandıysa aşağıdaki gibi pencere ekrana gelir. İzin verilen bir kullanıcının kullanıcı adı ve şifresi girilerek “ OK” tuşuna basılır



D – Yetkiniz varsa ve şifreyi doğru girdiyse ilgili sayfanın dosyalarına erişirsiniz.



6- Windows NT Load Balance:

Bu sistem Web Sayfalarının kesintisiz hizmete devam edebilmesi için uygulanan Nt servislerinden biridir..

