3. Linux Ağ Yönetimi I

3.1 TCP/IP Ağ Kavramları

Diğer açık sistemler gibi Linux'un da en büyük özelliklerinden biri ağ protokolleri ve uygulamalarının sistemin en doğal parçalarından biri olmasıdır. Dolayısıyla ağ yapısını bilmeyen bir yöneticinin, açık sistemler üzerindeki bilgisini daha da geliştirebilmesi mümkün değildir. Bu bölümde anlatılacaklar Linux üzerinde ağ yönetimi ve TCP/IP'ye bir giriş yapılmasını sağlayacaktır.

3.1.1 Temel TCP/IP

TCP/IP, ilk defa ABD'de ARPANet (Advanced Research Projects Agency Network) adı altında, askeri bir proje olarak geliştirildi. Önceleri askeri amaçlı düşünülen proje önce ünivesiteler tarafından kullanılmaya başlandı. Ardından ABD'nin dört bir yanında birbirinden bağımsız geliştirilen ağlar, tek bir omurga altında NSFNet olarak adlandırıldı ve ulusal boyutu aşarak dünyaya yayıldı. İnternet'in doğuşu da bu tarihe denk gelir.

Bir sokak üzerinde yeralan evlerin adresleri gibi, İnternet'e bağlı olan her makinanın da bir adresi vardır. Bu adres sayesinde bir bilgisayardan diğerine ulaşmak mümkün olur. İnternet adresi 4 bayttan (32 bit) ibaret olup yazılırken her bayt arasına bir nokta konulur. En çok kullanılan bu gösterim şekline örnek olarak, İTÜ'deki bir bilgisayarın adresi olan `160.75.90.1`'yi verebiliriz.

Bununla beraber, 4 baytlık numaraların kolayca hatırlanmasının mümkün olmadığından, İnternet üzerindeki makinalara alfanümerik adlar da verilebilir. Yukarıda örneğini verdiğimiz adresin ismi, *devinim.be.itu.edu.tr*'dır. ilk noktaya kadar olan kelime, makina adıdır (yukarıdaki örnekte *devinim*), bundan sonraki noktayla ayrılmış bölümler özelden genele doğru makinanın ait olduğu kurum, kurumun tipi ve ülke gibi bilgiler içerir. Bu adlandırma yöntemiyle ilgili ayrıntılı bilgiyi Alan İsimlendirme Sisteminin (Domain Name System - DNS) anlatıldığı bölümde bulabilirsiniz.

İletişimin en basit şekli olan iki kişi arasındaki konuşmayı göz önüne alalım burada iletişim kurmaya çalışan her kişi soyut anlamda bir "**node**" veya "**düğüm**" oluşturur. Bu "**node**"lar arasındaki bilgi iletişimi için kullanılan mesafede (yol) "**edge**" veya "**bağlantı**" olarak adlandırılır. Eğer bir bilgi ağından bahsediliyorsa iletişim için kullanılan şeyler bilgiyi içermektedir diyebiliriz. Ağ kavramı daha genel bir içeriğe sahip olup pek çok farklı konuda ağ oluşturulması mümkündür, örneğin su, petrol, doğalgaz boru ağları gibi. Eğer

sözünü ettiğimiz "**node**"lar bilgisayar ve "**edge**"ler ise fiber optik kablolar veya koaksiyel kablolar olursa bir bilgisayar ağından söz edebiliriz.

Bilgisayar Ağları: Bilgisayar ile yazıcının bağlantısı, bilgisayar ağı için bir örnek teşkil eder. Bilgisayar ağları aşağıdaki özelliklere göre sınıflandırılırlar.

» Coğrafi Sınıflandırma: Coğrafi sınıflandırma, bilgisayar ağının bulunduğu yer bakımından yapılan sınıflandırmadır. Bilgisayar ağı sadece bir bina içinde yada kampus gibi bir alan içerisindeyse ve bilgisayarların birbirini görmesi için telefon yada radyo bağlantısı gerekmiyorsa, LAN (Local Area Network) olarak isimlendirilirler. Örnek olarak İTÜ deki bilgisayar laboratuvarlarına LAN diyebiliriz. Ayazağa kampusündeki tüm bilgisayar ağlarıda bir LAN'dır.

Eğer ağ bağlantılarının bir kısmı coğrafi bakımdan uzak yerlerdeki bilgisayarlara ulaşmak için telefon yada radyo bağlantısı kullanılıyorsa bu tür ağlara da WAN (Wide Area Network) denir. Örnek olarak İTÜ Maçka kampüsü ile Ayazağı kampüsü arasındaki ağ WAN olarak düşünülebilir. Ayrıca bankaların şubeleri arasındaki bilgisayar ağı WAN'a güzel bir örnek teşkil eder.

» Topolojik sınıflandırma: Bilgisayar ağları topolojisine göre yani ağın geometrik yapısına göre de sınıflandırılır. **Bus**, **ring** ve **star** topoloji olmak üzere üç tür topoloji vardır. Bu topoloji türleri temel olarak LAN'da kullanılırlar.
Bus topolojide bütün bilgisayarlar bus yada backbone olarak isimlendirilen tek bir kabloya bağlanmıştır. Bu tip ağlara bus ağlar denir. Kısa mesafeler için kurulumu kolay ve ucuz bir yöntemdir. Terminatör denilen bir aletle kablonun iki ucu sonlandırılmalıdır.

Ring ağ adında anlaşılacağı gibi yüzüğe benzer şekilde ağdaki bilgisayarların bir döngü içerisinde peş peşe bağlanmasıdır. Bu topolojide her bir makine iki makineye bağlanmış durumdadır. Bu tür ağları kurmak pahalı ve zordur.

Star topolojide ise her bir makine merkezde **hub** denilen bir alete bağlanırlar. **Hub**'lar bir makinedan gelen paketleri topolojiye bağlı tüm makinelere gönderirler. Eğer pasif **hub**'lar kullanılırsa bir makineden gelen mesaj üzerinde hiçbir işlem yapmadan tüm makinelere gönderilir. Ama aktif bir takım cihazlar kullanılırsa bir makineden gelen mesajın mantıksal olarak ilgili porta gönderilmesi sağlanarak mesaj trafiği azaltılabilir. Aktif hubları kullanmak pasif hublara göre daha pahalıdır.

» Protokol Tabanlı Sınıflandırma: Protokol, ağdaki bilgisayarların bir biri ile konuşmasını sağlayan kurallar topluğudur. LAN'larda kullanılan en çok popüler iki protokol Ethernet ve IBM token ring network tür.

Ethernet Xerox şirketi tarafından DEC ile işbirliği yapılarak 1976 yılında geliştirilmiştir. Ethernet protokolü star yada bus topolojiyi kullanır. Ethernet 10Mbps (MegaBit Per Second) data transferini destekler. Ethernetin daha yeni bir versiyonu olan 100Base-T 100Mbps data transferini desteklerken, en son versiyonu olan Gigabit Ethernet 1000 Mbps lik data tranferini desteklemektedir.

Ethernet'in LAN'da kullanılan birkaç tane adaptasyonu vardır. Bunlardan biri Thinnet olarak ta isimlendirilen 10Base-2 Standard'tir. 50 Ohm'luk koaksiyel kabloyla 185 metreye kadar kullanılabilir. 10Base-2 Standard'ta ise koaksiyel kablo uzunluğunu 500 metreye kadar uzamasına izin verir.

IBM token ring network ise ring topolojide kullanılır. IBM tarafından geliştirilmiştir. Ring 'e bağlı bilgisayarlarda datanın transferini sağlar.

» Mimari Tabanlı Sınıflandırma: Bilgisayar ağları kullanılan mimariye göre de sınıflandırılırlar. Temelde **peer to peer** ve **client/server** olmak üzere iki tür mimari vardır.

Peer-to-peer mimaride iki makinenin de birbirilerine karşı sorumlulukları eşittir. Ucuz bir mimaridir. **Client/server** de ise server olacak makinenin yeterli RAM i olmalı ayrıca işlemci hızı da yeterli olmalıdır. **Client/server** mimaride server makinenin sorumluğu daha fazladır.

Linux veya herhangi Unix ürünü için bilgisayar ağında bir görev yapılmaya çalışılsa TCP/IP kaçınılmaz olarak devreye girer. TCP/IP'nin ne olduğuna bakmadan önce biraz ağ terminolojisine bakmakta fayda vardır.

SUNUCULAR: Bir sunucu size dosyalar, kaynaklar ve servisler sağlayan herhangi bir makinedir. Bu durum gerçekte client/server sistemlerinin temelinide oluşturur öyleki bir makine (client) bir diğer makineden (server/sunucu) birşey talep eder. Bir makina hem client hemde çoğu zaman sunucu olabilir. Server'in daha yaygın tanımında, server/sunucu tüm büyük uygulama programlarını ve dosyalarını tutan güçlü bir makina olarak yerel LAN (local area Network)'da görev alır. Aşağıdaki diğer makineler ile ilgili dosyalara erişmek için bu sunucuya bağlanırlar. Ağın bu türünde tek bir makina genellikle sunucu olarak görev alır (diğer makineler client olurlar). Büyük sunucu-tabanlı ağlarda spesifik görevler için spesifik sunucular görev alır. Örneğin; bir sunucu ağ için tüm dosyaları organize ederken (dosya sunucusu) gibi.

CLIENTS: Bir client, bir sunucudan herhangi bir şeyi talep eden bir makinadır. **client/server** tipi ağlarda, bir client server'a bir talebi ileten ve belirli bir süreci başlatan bir makinadır.

NODE'LAR (DÜĞÜMLER): Bir sunucu ve belirli bir sayıda PC'nin oluşturduğu küçük ağlar oldukça yaygındır. Bu ağdaki her PC bir node (düğüm) olarak adlandırılır. Bir node ağın boyutu ne olursa olsun bu ağa bağlanan herhangi bir bilgisayarı temsil eder. Çünkü her makinanın bağlandığı ağda kendisini unique olarak tanımlayacağı bir ismi ve numarası vardır.

YEREL VE UZAK KAYNAKLAR (RESOURCES): Yerel bir kaynak, yazıcı, modem, tarayıcı veya sabit disk gibi makinamıza bağlanmış herhangi bir araçtır. Çünkü makinamızın ağ'a çıkıp bir araç temin etmesi mümkün olmadığından bunlara yerel araç ve kaynaklar denir. Aynı mantığı takip edersek, ağ üzerinden ulaşılabilen herhangi bir araç uzak bir kaynaktır. Örneğin yüksek-hızlı renkli bir lazer yazıcı ağda uzak bir kaynaktır.

AĞ İŞLETİM SİSTEMİ (NOS): Bir ağ işletim sistemi-sıklıkla (NOS olarak adlandırılır) ağdaki tüm makinalar arasında etkileşimleri kontrol eder. NOS, ağ ortamı (koaksiyel veya bükülü kablo çifti veya optik kablolar) üzerinden gönderilen bilginin kontrolünden sorumludur. Bir makinadan gelen veri paketlenir ve diğerlerine yollanır, bu arada iki veya daha fazla sayıda makine aynı anda bilgi yollamak istediğinde bu durumu NOS kontrol eder. Bunlara ilave olarak, paylaşımlı aygıtların (örneğin lazer yazıcı, tarayıcı ve CD-ROM sürücüleri gibi) çalışmalarını organize eder. Tek bir sunucuya sahip LAN'lardan NOS sunucu üzerinden çalışır. NOS'un ana kısmı sunucu üzerinden çalışırken daha küçük client yazılım paketleri ağ üzerindeki her bir client üzerine yüklenir.

TCP/IP üzerinde çalışan bir linux ağı gibi tek bir sunucu kullanmayan daha büyük ağlarda, NOS her makinanın yazılımının bir parçası olabilir. Örneğin, linux, her zaman mevcut olacak şekilde TCP/IP için işletim sisteminin çekirdeğinde oluşturulan ağ yazılımına sahiptir. Bir TCP/IP ağına bağlanmak isteyen bir PC'de TCP/IP protokolünü koordine eden bir yazılım paketinin kurulmuş olması gerekir.

AĞ PROTOKOLLERİ: Ağ protokolü, ağ üzerindeki makinaların etkileştiği işletim sisteminin adıdır. Örneğin bir UNIX sisteminde, TCP/IP en yaygın protokoldür. TCP/IP bir ağ protokolüdür. Novell Networe genellikle IPX (Inter Packet Exchange) olarak adlandırılan bir ağ protokolü kullanır. Farklı protokoller çoğunlukla iletişimde benzer yaklaşımı kullanırlar: Bilgiyi bir paket olarak adlandırılan veri bloklarında toplarlar ve bunu ağ boyunca yollarlar. Ancak paketin hazırlanış biçimi, ve doğrultusunu kontrol etmek ilave edilen bilginin türü her NOS ile farklılık gösterir.

AĞ ARAYÜZ KARTI: Ağ arayüz kartı (Network Interface Card, NIC) genellikle PC'niz içindeki bir slot'da kullanılan bir adaptördür. Bu kart, arasındaki bir veya

daha fazla bağlantı noktası aracılığıyla ağa bağlantıyı koordine eder. En yaygın ağ bağlantıları, kablolu TV'dekine benzer şekilde koaksiyel kabloyla telefon prizine benzer bir yapıdadır.

BRIGES, ROUTERS VE BROUTERS: Bridge ve Router, iki veya daha fazla ağı birbirine bağlayan makinelerdir. Bridge ile Router arasındaki fark şöyledir:
Bridge sadece aynı ağ işletim sistemiyle çalışan iki yerel ağı (LAN) bağlar (diğer bir deyişle, daha büyük ağ üzerindeki yükü azaltmak için iki LAN arasında köprü vazifesi görür) oysa Router farklı ağ işletim sistemi kullanan LAN'ların bağlantısında kullanılır. Router, barındırdığı yazılım ile farklı NOS paketlerini bir diğerine dönüştürür. Bir Router, bir Bridge'den daha karmaşık bir aygıttır, öyleki bilgi paketlerini varış noktalarına nereden ve nasıl yallayacağı hakkında karar verebilir. Brouter kısmen yeni bir aygıt olup hem Router hemde Bridge özelliklerini bünyesinde barındırır.

GATEWAYS: Bir gateway küçük bir ağ ile daha büyük ağ arasında (örneğin internet'e bağlanan LAN gibi) bir arayüz görevi gören bir makinadır. Gateway'ler aynı zamanda küçük LAN'ları daha büyük LAN'lara bağlanmasındada kullanılırlar (örneğin büyük şirketlerin ofis-tabanlı LAN'larını şirketin daha büyük mainframe ağına bağlantısında kullanılırlar). Genellikle, gateway yüksek-hızlı ağ kablosuna veya backbone (omurga) olarak adlandırılan ortama bağlantı kurar. Daha formal olarak, bir gateway iki ağ arasında protokol dönüşümünü gerçekleştirir.

3.1.2 Protokoller

En basit terimiyle TCP/IP bir ağ protokol ailesinin adıdır. Protokoller kurallar kümesidir, öyleki tüm şirketler ve yazılım ürünleri bu kurallara uynak durumundadırlar çünkü ürünlerinin diğerleri ile uyumlu olarak çalışabilmesi gerekmektedir. Protokol, bir yazılımın diğerleriyle nasıl iletişim kuracağını belirler. Bir protokol tüm paketin herbir kısmının bilgi transferini nasıl yöneteceğinide tanımlar. TCP/IP, **T**ransmission **C**ontrol **P**rotokol/**I**nternet **P**rotocol açılımının kısaltılmış hali olup gerçekte iki ayrı protokolden oluşur. TCP/IP bir ağın yazılım bileşeni olarak tasarlanmıştır. TCP/IP protokol ailesinin kısımlarının hepsi, elektronik posta yollamak, dosya transferi, uzaktan erişim servislerini sağlamak, mesajları yönlendirmek ve ağ çökmelerini kontrol etmek gibi özel amaçlara yönelik görevlere sahiptir. TCP/IP ile irtibatlandırılmış farklı servisler ve fonksiyonlar amaçlarına göre gruplandırılabilir. Taşıma protokolleri (Transport protocols) verinin iki makine arasındaki hareketini kontrol eder ve aşağıdakileri içerir:

- TCP/IP(Transmission Control Protokol): Bir bağlantı-tabanlı servis olup, anlamı yollayıcı ve alıcı makinalar her zaman birbirleriyle bağlantılı ve iletişim halindedir.

- UDP(User Datagram Protocol): Bağlantısız bir servis olup, anlamı verinin makinalar birbiri ile temasta olmaksızın yollanıp alındığı anlamındadır.

Routing protokolleri verinin adreslenmesini ve varacağı noktaya en uygun nasıl ulaşacağının saptanmasını kontrol eder. Ayrıca büyük mesajların daha sonra tekrar biraraya getirilebilecek şekilde parçalara bölünmesini kontrol ederler.

- IP(Internet Protocol): Verinin gerçek transferini kontrol eder.

- ICMP(Internet Control Message Protocol): IP'nin hata mesajını ve Routing'i etkileyen ağ donanımındaki değişiklikler gibi durum mesajlarını kontrol eder.

- RIP(Routing Information Protocol): Bir mesajı teslim etmek için en iyi yolu saptayan protokollerden birisidir.

- OSPF(Open Shortest Path First): Routing'i saptayan bir alternatif protokoldür.

Ağ adres protokolleri makinaların hem tek bir numara hemde tek bir isimle adresleniş şeklini kontrol eder.

- ARP(Address Resolution Protocol): Ağdaki makinaların unique sayısal adreslerini saptar.

- DNS(Domain Name System): Makina isimlerinden sayısal adreslerini saptar.

- RARP(Reverse Address Resolution Protocol):Ağ üzerinde makinaların adreslerini saptarlar, fakat ARP'den geriye doğrudur.

Kullanıcı servislerini bir kullanıcının (veya bir makinanın) kullanabileceği makinalardır.

- BOOTP(Boot Protocol): Bir sunucudan boot bilgisini okuyarak bir ağ makinasını başlatır

- FTP(File Transfer Protocol): Bir makinadan diğerine dosyaları transfer eder.

- TELNET: Bir makina başındaki kullanıcının bir diğer makinaya sanki o makinanın başında oturuyormuş gibi bağlantı kurması için uzak erişimlere izin verir.

Gateway Protokolleri, yerel ağlar için veri akışını kontrol etmesi kadar, ağın routing iletişimine ve durum bilgisini elde etmeye yardımcı olur.

- EGP(Exterior Gateway Protocol): Dış ağlar için routing bilgisini transfer eder.

- GGP(Gateway-to-Gateway Protocol): Gateway'ler arasında routing bilgisini transfer eder

- IGP(Interior Gateway Protocol): İçerdeki ağlar için routing bilgisini transfer eder.

Aşağıdaki Protokoller önceki ifade edilen katagorilere girmemektedir, fakat bir ağ üzerinde önemli servisler sunarlar:

- NFS(Networking File System): Bir makina üzerindeki klasörlerin bir diğeri üzerine bağlanmasına (mount edilmesine) ve kullanıcının sanki o yerel makinadaymış gibi erişmesine izin verir.

- NIS(Network Information Service): Ağ boyunca kullanıcı hesaplarını düzenler, girişleri (logins) kolaylaştırır, ve şifre bakımını temin eder.

- RPC(Remote Procedure Call): Uzak makinalardaki uygulama programlarının basit ve verimli bir biçimde birbiri ile iletişim kurmasına izin verir.

- SMTP(Simple Mail Transfer Protocol): Makinalar arasında elektronik posta transferi sağlayan bir protokoldür.

- SNMP(Simple Network Management Protocol): Ağ hakkında ve ağa bağlanan aygıtlar hakkında durum mesajı yollayan bir yönetici servisidir.

TCP/IP içindeki farklı protokoller, internet organizasyonunun bir üyesi olan yönetim standartları oluşumu tarafından işletilir.

IP paketlerinin her biri kendi başlarına aradaki ağ cihazları tarafından yönlendirileren paket içinde belirtilen adrese ulaştırılır. Bu sırada fiziksel ağ farklılıklarından kaynaklanan paket parçalanmaları (fragmentation) ve bunların yeniden birleştirilmeleri aradaki ağ cihazlarının aşırı yüklenmelerini önlemek gibi görevler de IP katmanı tarafından gerçekleştirilir. IP, bağlantı temelli (connection oriented) bir ağ protokolü değildir. Bunun yanı sıra IP paketlerin içeriklerinin doğruluğunu da garanti etmez. IP katmanı sadece başlık kısmında oluşan hataları bulur ve düzeltir. Internet üzerinde yönlendirme, yukarıda sözü edilen adreslerden yararlanılarak yapılır.

Kullanıcı uygulamalarının IP katmanına doğrudan ulaşımları yoktur. IP ve uygulama programları arasındaki bağlantıyı sağlayan iki protokol vardır: *Transmission Control Protocol (TCP)* ve *User Datagram Protocol (UDP)*. TCP, IP katmanının sağlamadığı bağlantı temelli, güvenilir servisi sağlar. TCP kullanarak ağ üzerinden veri aktaran programlar, bir dosyadan okuyormuş ya da yazıyormuş gibi güvenle ağ bağlantısını kullanabilirler. Arada oluşan hatalar TCP tarafından onarılır. IP protokol katmanına uygulama programları doğrudan erişemediklerinden, hata kontrolü ve bağlantı gerektirmeyen yada bu işlemleri kendileri gerçekleştirmek isteyen uygulamalar *UDP* kullanarak ağ üzerinden iletişim sağlarlar.

Yukarıdaki protokollerin yanı sıra İnternet standardı olmuş birçok uygulama protokolü de vardır. Bunlar arasında, *TELNET*, *FTP*, *SMTP* ve *HTTP* gösterilebilir. İnternet üzerinde paketlerin son makinaya ulaştıktan sonra, ilgili uygulama programına ulaşabilmesi için *port* adı verilen sanal numaralar kullanılır. Servis veren uygulamalar, önceden belirlenmiş standart port numaraları kullanırlar. Örnek olarak SMTP 25 numaralı TCP portunu, talk ise 518 numaralı UDP portunu kullanır. Sisteminizin kullandığı port numaraları ve bunların isimlerini **`/etc/services`** dosyasından görebilirsiniz.

TCP/IP, İNTERNET VE TABAKALAŞMIŞ MİMARİ

Internet tek bir ağdan ziyade TCP/IP yoluyla iletişim kuran pek çok ağın toplamından oluşmuştur. TCP/IP ve internet çok yakından kaynaşmıştır öyleki TCP/IP'nin mimarisi sık sık internet mimarisi olarakta adlandırılır. Hemen hemen ARPAnet olarak internetin başlangıcından beri mevcut protokollerin ağın taşımak zorunda olduğu yağun trafiği kaldıramadığı çok açık hale gelmişti, böylelikle yeni bir proje ile yeni iletişim protokolleri geliştirildi. TCP/IP protokolleri ilk 1973 yılında önerildi ve 1982 yılında standart haline getirildi. Tabakalaştırılmış mimari ile her servis kümesini bir diğerinden izole etmek mümkün hale gelmiştir. Bu yaklaşımla, her tabaka diğerinden bağımsız olup bir servisteki değişikliğin diğer servisler üzerine olumsuz bir etkisi önlenmiş olmaktadır. Yeni servisler geliştirildikçe, yazılım sistemini geliştirmeksizin ilave etmek yetmiştir. Belkide daha önemlisi, tabakalı mimari ile, çok spesifik görevler için küçük ve verimli program kümecikleri geliştirmek mümkün olmuştur. Belirli bir görevi basitleştirmek için her tabaka örneğin gönderilen bir elektronik posta mesajının önüne ve arkasına bir veri bloğu ilave eder bu blok hangi tabakanın bu işe karıştığı bilgisini içerir ve diğer tabakalar için ilave bilgiler bulunur. Sonunda mesajı alan makina gelen mesajı doğru bir şekilde açabilmek için bu bilgilere ihtiyaç duyar. Bu esnada mesajın içindeki veri ihmal edilir. Bu duruma "encapsulation" adı verilir, öyleki her tabaka orjinal mesaja ilave olarak bir bilgi kapsülü ekler. Her tabaka kendi encapsülasyonunu

gerçekleştirir ve yukarıdaki tabakadan gelen mesaja başlık ve kuyruk bloklarını ekler. Bu durum mesajın ağ üzerinde ilerlemesiyle bir kaç küme başlık ve kuyruk orjinal mesaja eklenmiş olur.

DOMAIN NAME SYSTEM (DNS)

Bir şirket veya organizasyon Internet'i kullanmak isterse, şirket veya organizasyonu doğrudan internet sistemine bağlayıp bağlamıyacaklarına veya bu bağlantıyı sağlayan başka bir şirket üzerinden yapıp yapmayacaklarına karar vermeleri gerekmektedir. Çoğu şirket bunu servis sağlayıcı olarak adlandırılan bir diğer şirket üzerinden gerçekleştirir. Çünkü bu malzeme, yönetim ve diğer maliyetleri düşürür. Eğer şirket veya organizasyon doğrudan internete bağlanmak isterse kendilerini tek bir şekilde tanımlayan kimlik almaları gerekir. Örneğin ABC şirketi elektronik postayla haberleşmek istediğinde **abc.com** internet adresini kullanmak isteyebilir. Bu "**domain name**" olarak adlandırılan tekil kimlikleri elde etmek için şirket veya organizasyon internete erişimi kontrol eden oluşuma bir talepte bulunur. Bu oluşum **Network Information Center (NIC)**'dir. Eğer **NIC** şirketin adını onaylarsa internet veri tabanına ilave edilir. **Domain Name System (DNS)** mesajların adreslenmesine yardımcı olan TCP/IP protokol ailesi tarafından sağlanan bir hizmettir. Eğer bozo@clowns-r-us.com gibi bir posta adresiniz varsa DNS sistemi bu sembolik ismi veritabanındaki domain name'e bakarak dönüştürür. DNS sizi IP adresi yerine daha basit domain name'ler kullanmanıza izin verir. Internet üzerinde bir kullanıcıya mesaj yollamak için genel yapı **username@damain-name** şeklindedir. DNS gerçekte IP adresinin sadece Network kısmı ile ilgilenir.

3.1.3 İnternet Adresleri

İnternet üzerinde genel olarak 3 sınıf adres vardır. Avrupa'da RIPE (**R**éseaux **IP** **E**uropéens) tarafından dağıtılan bu adresler daha sonra o yerin ağ yöneticisi tarafından uygun şekilde bölünebilir. Bu bölümlendirmeye "subnetting" işlemi adı verilir. Bu sayede ağlar gruplanarak herbirisinin yönetimi bağımsız hale getirilmiş, aynı zamanda da kısıtlı olan IP adresleri daha verimli bir şekilde kullanılmış olur.

Üç çeşit İnternet adresi şunlardır :

- **A sınıfı İnternet adresi:** Adresin ilk baytı (8-bits) 1 ile 126 arasında bir sayıdır. Bu adrese verilen yetkiyle toplam 2^24 makina adreslenebilir. Dünya üzerinde 126 tane A sınıfı adres vardır.

- **B sınıfı İnternet adresi:** Adresin ilk baytı 128 ile 192 arasında bir sayıdan oluşur. Bu adresin subnetlere bölünmesiyle 65534 farklı makina adreslenebilir.

- **C sınıfı İnternet adresi:** Adresin ilk baytı 192 ile 223 arasındadır. C sınıfı bir adres blokuyla bağlı 254 bilgisayar adreslenebilir.

Her makina TCP/IP tabanlı bir ağa bağlandığında sisteme tek bir şekilde tanımlanmış olması gerekir. İnternet, ağları "internet adresleri" atayarak veya daha uygun bir şekilde ağ üzerindeki her şirket veya organizasyona bir IP adresi vererek tanımlar. IP adresleri, herbiri 8-bit olan 4 alanın bir araya geldiği ve toplam 32-bit uzunluğundaki adreslerdir. Bu durum toplam dört alanın herbirinin 0'dan 255'e kadar değişen bir rakam olmasına neden olur. Bu dört kısım "dotten quad" olarak adlandırılan bir notasyonla birleştirilir. Örneğin; "255.255.255.255" ve "147.120.3.28" "dotten quad" IP adresleridir. IP adresleri gerçekte iki kısımdan oluşmuştur: Network number(Ağ sayısı) ve Host number.
Maksimum esneklik sağlayabilmek için IP adresleri "Class A", "Class B", "Class C", "Class D" ve "Class E" olarak adlandırılan kullanıcı boyutuna göre atanmıştır ve özel amaçları vardır. IP adreslerinde toplam 32-bit boyutu olduğuna göre ve her kısım 8-bit'den oluştuğuna göre 1 veya daha fazla bit 32-bit'lik IP adresinin sınıf tipini tanımlamak için kullanılır.
Üç sınıfın ayrıştırması aşağıdaki gibidir:

- Class A : network 7 bits ; host 24 bits
- Class B : network 14 bits ; host 16 bits
- Class C : network 21 bits ; host 8 bits

Bir class A adresinde, network adresi 7-bit iken host adresi 24-bit dir. Bu çok büyük organizasyonlar için yeterli host adresine izin vermektedir (16 milyon farklı adres). Elbette, maksimum 128 adet bu tip Class A adresi vardır. Class B'de 16-bit'e izin verilmiştir, buda 65000 host demektir. Class C tipi IP adreslerinde maximum 254 host'a izin verilmektedir.

Ne zaman internet üzerinde herhangi bir yerdeki host'a bir mesaj yollanırsa, onu yollayan host ile varış yerini göstermek için IP adresi kullanılır. Şanslıyız ki *Domain Name System* olarak adlandırılan diğer bir TCP/IP servisinden dolayı kendinizin bu IP adreslerini takip etmenize gerek yoktur.

A ve *B* sınıfı adreslerin hepsi dağıtılmış ve şu anda internet *C* sınıfı adreslerde de sıkıntı çekilmektedir. Adres yetersizliğine çözüm getirmek amacıyla *IPv6* ya da *IPNG* adlarıyla daha uzun İnternet adresleri kullanan protokoller geliştirilme ve test aşamasındadır.

Bir İnternet adresi iki kısımdan meydana gelir: *ağ adresi* ve *düğüm adresi*. Her makina, bir ağ üzerinde bulunur ve bu adres "ağ adresi" olarak adlandırılır. Üç sınıf (A, B ve C) İnternet adresinin ağ ve düğüm adresleri farklı farklıdır. A sınıfı İnternet adreslerinde ağ adresini 1 bayt tayin eder. Örnek olarak hayali yazılan 74.198.59.33 makinasını tanımlayan ağ adresi 74'tür. Ağ adresi uzun halde yazıldığı zaman kalan 3 baytın yerine 0 konur. Bu durumda yukarıda adı geçen makinaya ait ağ adresi 74.0.0.0 olacaktır. Çoğunlukla ağ IP'leri Class B ve C türündendir. IP adresleri ile bir şirketin ait olduğu sınıf tipini söylemek mümkündür. Böylece, örneğin host makinanızın IP adresi eğer 147.14.87.23 ise makinanız Class B ağındadır ve ağ adresi 147.14'dür, ve bu ağda host'unuzun belirleyici numarası 87.23'dür. Eğer IP adresi 221.132.3.123 ise, makine Class C ağında 221.132.3 ağ adresi ile ve 123 host numarası ile yer alır. Ağ adresinden geriye kalan düğüm adresi, bir makinanın İnternet sınıfına göre 1, 2 veya 3 bayttan ibaret olabilir. Örnek olarak,

195.12.288.3 makinasının (C sınıfı) ağ adresi 195.12.288.0, düğüm adresi 3'tür.
130.11.195.62 makinasının (B sınıfı) ağ adresi 130.11.0.0, düğüm adresi 195.62'dir.

Düğüm adresleri yerine 4 baytı da kullanmak da olası. Yukarıdaki iki örnek için düğüm adreslerini sırasıyla 195.12.288.3 ve 130.11.195.62 olarak kabul edebiliriz.

Yukarıda sözedilen *subnetting* (alt ağlara ayırma), çok sıkça kullanılan bir yöntem olup getirdiği birtakım kolaylıklar vardır. Büyük bir iletişim ağı alt ağlara ayrılırsa, kontrol edilmesi daha kolaylaşır.

Bir kuruluş, kendine ait olan B sınıfı adresi subnet'lere bölmek isteyebilir. Gerekli düzenlemeleri yaparak bir B sınıfı adresi (örneğin) 255 adet alt adrese ayırabilir. ODTÜ'nün NIC'den aldığı 144.122.0.0 ağı, 254 parçaya bölünmüş, bu parçalardan 144.122.71.0 alt ağı Bilgisayar Mühendisliği bölümüne, 144.122.34.0 alt ağı Kimya Mühendisliği bölümüne verilmiştir. Yine İTÜ NIC'den 160.75.0.0 ağını almıştır. Bundan sonra her bölüm kendi ağı ve üzerindeki makinelerden sorumlu olur.

3.1.4 İnternet'e Bağlanma

Linux'u İnternet'e bağlamak ilk aşamada biraz zor görünse de biraz teori, biraz pratik yardımıyla mantık kolayca anlaşılabilir. Ağlar, bilgisayar sistemlerinde hata olma olasılığı en yüksek, en çok sorunun çıktığı alandır. Bu bölüm, özelde bir ethernet kartı ile bağlantı yapıldığı varsayılarak anlatılmıştır. Ancak anlatılan birçok kavram herhangi bir yapıdaki İnternet bağlantısı için geçerli olacaktır.

Öncelikle çekirdeği -daha önce yapmamışsanız- ağ bağlantısına destek verecek şekilde tekrar derleyin (Genelde Linux sürümleri bu desteği sağlayacak şekilde gelir). Bunun için gerekli birkaç soruya "y" cevabı vermek yeterli olacaktır :

```
CONFIG NET ? [ Y/n]  y
...
TCP/IP networking (CONFIG_INET) [ Y/n/?]  y
...
Network device support (CONFIG_NETDEVICES) [ Y/n/?]
...
Ethernet (10 or 100Mbit) (CONFIG_NET_ETHERNET) [ N/y/?]  y
...
Other ISA cards (CONFIG_NET_ISA) [ N/y/?]  y
...
NE2000/NE1000 support (CONFIG_NE2000) [ N/y/m/?]  y
```

Yukarıdaki örnekte ethernet kartınızın NE2000/NE1000 ya da uyumlu bir kart olduğu var sayılıyor. Kartınızın marka/modeline uygun seçeneneğe ‘y’ cevabı vermelisiniz. Ethernet kartlarının dışında bağlanma yönteminize bağlı olarak çekirdeği *PPP*, *SLIP*, *Token Ring* gibi bir destekle derlemeniz gerekebilir. Bunları *modül* olarak derlemeniz de mümkündür.

Tabii ki çekirdeği derlemek yetmiyor, derleme aşamasından sonra ağ desteğine sahip olan çekirdek ile makinanın açılması gerekir. Bağlantıyı gerçekleştirmek için ağ sorumlusundan bazı önemli bilgileri almalısınız. Makinanızın *IP adresi* bunların başında gelir. Diğer gerekli bilgiler de *subnet mask* ve *broadcast adresi* dir.

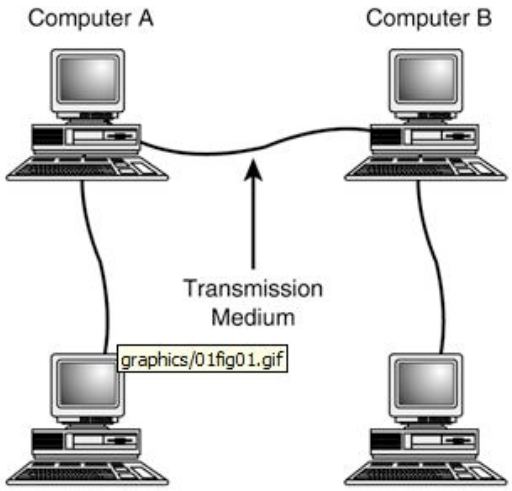
DNS adres çözümleyici olarak çalışan DNS makinası ve makinanızı İnternet'e bağlayacak olan yönlendiricinin IP adreslerini de biliyor olmalısınız. Bu aşamadan sonra konfigürasyon işlemlerine geçilebilir.

3.2 TCP/IP

TCP/IP ağ ile iletişim kurabilmeyi destekleyen protokollerin olşuşturduğu bir sistemdir. Bir protokol nedir sorusunun sorulmasından önce bir ağ nedir sorusunun cevaplanması gerekmektedir.

Ağlar ve Protokoller

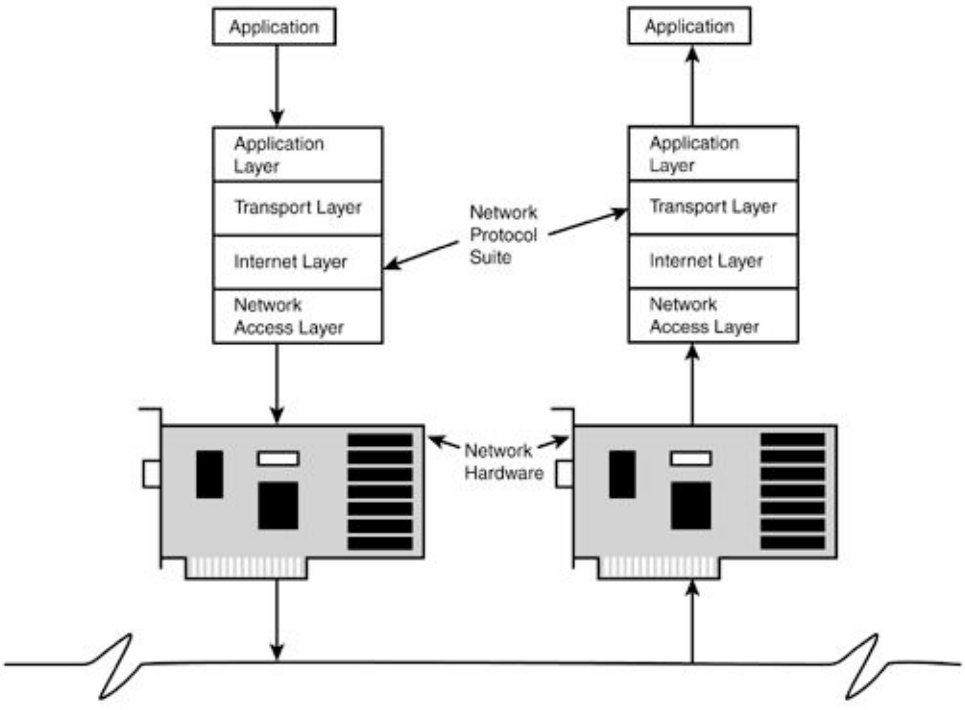
Bir ağ, bir iletim ortamında haberleşen bilgisayarların ve bilgisayar benzeri cihazların toplamıdır. Resim 1 de basit genel bir ağ resmi vardır.



Resim 1

Bir ağ ortamında istekler ve veriler bir bilgisayardan bir bilgisayara bir iletim ortamında (bir ağ kablosu veya telefon hattı) iletilerek geçer. Şekil 1 de A bilgisayarı B bilgisayarına veri gönderebilmeli veya ondan bir istek yapabilmelidir. B bilgisayarıda A nın mesajınıu anlayabilmeli ve ona cevap verebilmelidir.

Bir bilgisayar dış dünya ile bir yada birden fazla uygulamanın belirli görevleri ve giriş-çıkış işlemleri yapabilmesi aracılığı ile iletişim kurar. Bu bilgisayar eğer bir ağa dahilse bu uygulamalardan bazıları, ağdaki diğer bilgisayarlar üzerinde çalışan uygulamalarla iletişim kurma yeteneğine sahip olmalıdır. Bir ağ protokolü veri transferinin karmaşık işlemlerini düzenlemeye yarayan bir sistemdir.Veri bir uygulamadan diğer uygulamaya gönderilirken, önce bilgisayarın donanımından geçer, veri iletim ortamında iletilerek alıcı bilgisayarın ağ donanımına gelir ve oradan uygulamaya iletilir. (Resim 2)



Resim 2

TCP/IP protokolleri ağ iletişimi işleyişini tanımlar ve daha önemlisi verinin içinde ne gibi bilgiler olacağı ve bir verinin nasıl görüneceği konularını açıklar. TCP/IP ve ilişkide olduğu protoller verinin bir ağ üzerinde nasıl işleneceği, iletileceği ve hedef sistemde nasıl karşılanacağını tanımlayan tam bir sistem oluştururlar. Bu tür birbiriyle ilişkili protokollerin oluşturduğu sistemler Protokol Suiti (takım) olarak isimlendirilirler.

TCP/IP iletimlerinin biçimlendirilmesi ve işlenmesi aslında üretici firmanın sağladığı bir yazılım bileşenidir. Örnek olarak Microsoft un TCP/IP si bir TCP/IP ağında, Windows sistemi yüklenmiş bilgisayarların nasıl iletişim kuracağını belirler. Elinizdeki dökümanı okurken şu iki husus devamlı hatırda olmalıdır:

- TCP/IP standartı, TCP/IP ağları üzerindeki iletişimin kurallarını belirleyen bir sistemdir.
- Bir TCP/IP uygulaması, bir bilgisayarın TCP/IP ağına iştirak edebilmesini sağlayan bir yazılım bileşenidir.

TCP/IP standartlarının amacı, versiyon ve üretici bağımsız olarak bütün TCP/IP uygulamalarının uyumluluğunu sağlamaktır.

TCP/IP Özellikleri

TCP/IP bir çok önemli özelliğe sahiptir. En önemlilerinden biri TCP/IP nin aşağıdaki konulara olan yaklaşımıdır.

- Mantıksal Adresleme
- Yönlendirme
- İsim servisi
- Hata ve akış kontrolü
- Uygulama desteği

Mantıksal Adresleme

Bir ağ adaptörü tek ve kalıcı bir fiziksel adrese sahiptir. Fiziksel adres, ağ adaptörü fabrikada üretilirken verilen bir numaradır. Bir yerel ağ da alt seviye donanım protokolleri veriyi bu fiziksel adresleri kullanarak iletir. Bir çok değişik ağ tipi vardır ve hepsinin veriyi iletme/alma yolları farklıdır. Basit bir ethernet ağında, bilgisayar mesajları direk iletim ortamının üzerine gönderir. Her bilgisayardaki ağ adaptörü bir mesajın kendi fiziksel adresine gönderilip gönderilmediğini anlamak için ağdaki bütün iletişim trafiğini dinlerler.

TCP/IP protokollerden oluşan bir sistemdir ve bir protokolde kurallar ve prosedürlerden oluşan bir sistemdir. Çoğu zaman, iletişim kuran bilgisayarların donanım ve yazılımları TCP/IP letişimi için kuralları taşır.

TCP/IP Protokol Sistemi

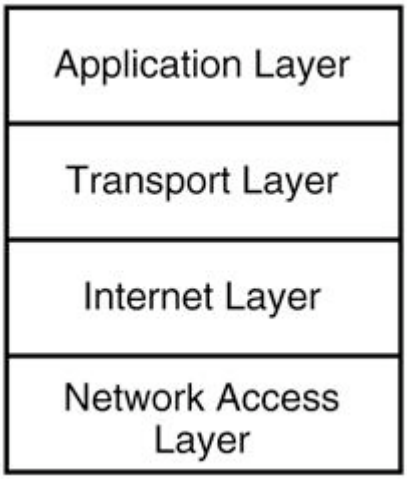
TCP/IP yi oluşturan elemanları incelemeden önce, bu sistemin sorumluluklarına kısaca bir göz atalım:

- Verinin iletim ortamında efektif bir biçimde iletilebilmesi ve kolaylıkla yönetilebilmesi için parçalara bölmek.
- Ağ adaptörü donanımı ile birlikte arayüz oluşturmak.
- Adresleme: Veri gönderen bilgisayar veriyi alıcı bilgisayara gönderebilmeli. Alıcı bilgisayar kendisine gelen mesajı anlayabilmelidir.
- Veriyi fiziksel olarak ayrı bile olsalar değişik ağlara gönderebilmek.
- Hata kontrolü, akış kontrolü ve onaylama: Güvenilir bir iletişim için gönderici ve alıcı bilgisayarlar hatalı iletimlere tanımlayabilmeli ve düzeltebilmeli ve bu sayede akış kontrolü yapabilmelidirler.
- Bir uygulamadan veri alıp ağa iletebilmek.
- Bir ağdan veri alıp uygulamaya iletebilmek.

Bu görevleri yerine getirebilmek için, TCP/IP yaratıcıları modüler bir tasarım yapmıştır. TCP/IP protokol sistemi teorik olarak birbirinden bağımsız çalışan bileşenlere ayrılmıştır. Her bir bileşen iletişim sürecinin bir bölümünden sorumludur.

Modüler tasarımın avantajı, üreticilerin protokol yazılımlarını kolaylıkla spesifik donanım ve işletim sistemlerine adapte edebilmeleridir. Örnek olarak Ağ Erişim (Network Access) katmanı Token Ring veya Ethernet gibi spesifik yerel ağ mimarileri için fonksiyonları içerir. Modüler yapı sayesinde Microsoft gibi üreticiler Token Ring ağları için tamamen farklı bir yazılım geliştirmek zorunda kalmaz. Sadece Ağ Erişim katmanında değişiklik gereklidir, üst katmanlar bundan etkilenmez.

TCP/IP protokol sistemi her biri spesifik görevler yapan katmanlara bölünmüştür (Resim 3). Bu model veya yığın, TCP/IP nin ilk günlerinden kalmadır ve bazen TCP/IP modeli olarak adlandırılır. Resmi TCP/IP protokol katmanları ve fonksiyonları aşağıda açıklanmıştır:



Resim 3

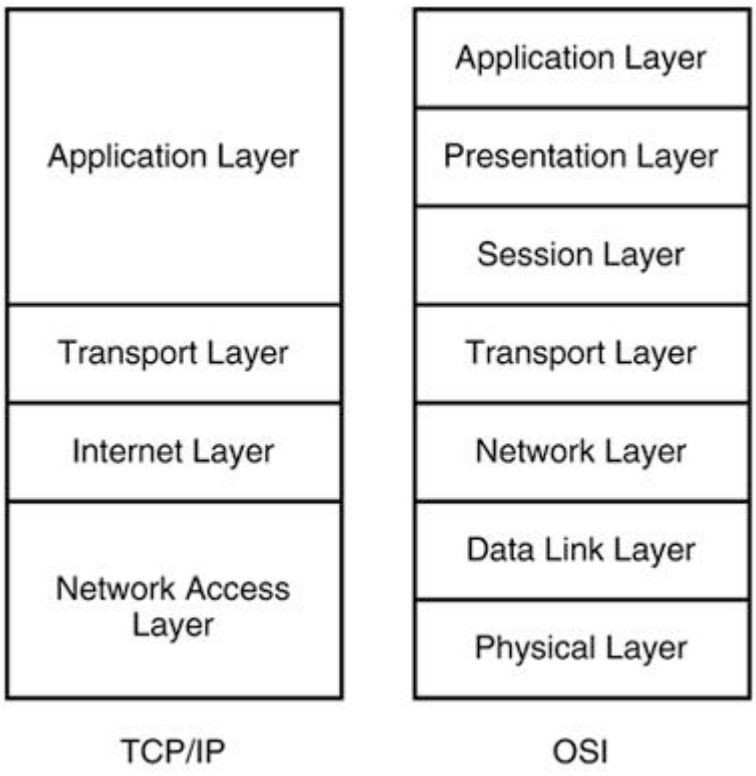
- Network Erişim Katmanı --- Fiziksel ağa bir arayüz sağlar. Veriyi iletim ortamı için düzenler ve fiziksel adrese dayanarak adresleme yapar. İletilen veri için hata kontrolü yapar.
- İnternet Katmanı --- Donanımdan bağımsız mantıksal adresleme yapar, bu sayede veri değişik fiziksel ağlar arasında iletilebilir. Trafiği azaltmak için yönlendirme sağlar ve veri iletimine destek verir. Fiziksel ve matıksal adresler arasında bağlantı kurar.
- Transport Katmanı --- Inter-network`ler için, akış ve hata kontrolü ile onay servisleri sağlar. Ağ uygulamaları için bir arayüz gibi davranır.
- Uygulama Katmanı --- Dosya transferi, uzaktan erişim ve Internet aktiviteleri gibi uygulamalar sağlar. Aynı zamanda ağ uygulamaları için programlama arabirimlerini destekler. (API desteği)

TCP/IP ve OSI Modelleri

Ağ endüstrisi ağ protokol yapısı için OSI (Open Systems Interconnection) adı verilen standart yedi katmanlı bir modele sahiptir. OSI modeli ISO (Internation Standards Organization) nun çalışmalarıyla, ağ protokollerinin tasarımlarını starndart hale getirmek ve yazılım geliştiriciler için protokol standartlarına açık erişim için hazırlanmıştır.

TCP/IP, OSI standartları ortaya çıkmadan önce zaten geliştirilme yolunda ilerliyordu ve OSI ile uyumsuz olduğu söyleniyordu. Fakat iki modelinde benzer amaçları vardı. OSI modeli büyüme aşamasında oldukça etki yarattı ve OSI terminolojisi TCP/IP için kullanılmaya başlandı. Aşağıdaki şekil (Resim 4) TCP/IP modelinin dört katmanlı yapısı ile OSI nın yedi katmanlı yapısı

arasındaki ilişkiyi göstermektedir. OSI modeli Uygulama Katmanı nı üç ayrı katman olarak tanımlamıştır: Uygulama, Sunum, Oturum. Ayrıca OSI Ağ Arabirimi Katmanını Veri Link katmanı ve Fiziksel Katman olarak ikiye bölmüştür. Artan katman sayısı daha fazla karmaşıklık getirmiştir fakat aynı zamanda yazılım geliştiriciler için spesifik servislere odaklanmayı kolaylaştırmıştır.



Resim 4

OSI modelinin yedi katmanı şöyledir:

- Fiziksel Katman --- İletilecek veriyi elektriksel veya analog sinyallere dönüştürür, veri iletimini gözetler.
- Veri Link Katmanı --- Ağ adaptörüne arabirim sağlar, ağ için mantıksal adresleri barındırır.
- Ağ Katmanı --- Mantıksal adresleme ve yönlendirmeyi destekler.
- Transport Katmanı --- Hata ve akış kontrolü sağlar.
- Session katmanı – İletişim kuran bilisayarlar üzerinde iletişim kuran uygulamalar arasında session açar.
- Sunum Katmanı --- Veriyi standart formata dönüştürür, varsa sıkıştırma ve şifreleme işlemlerini yönetir.

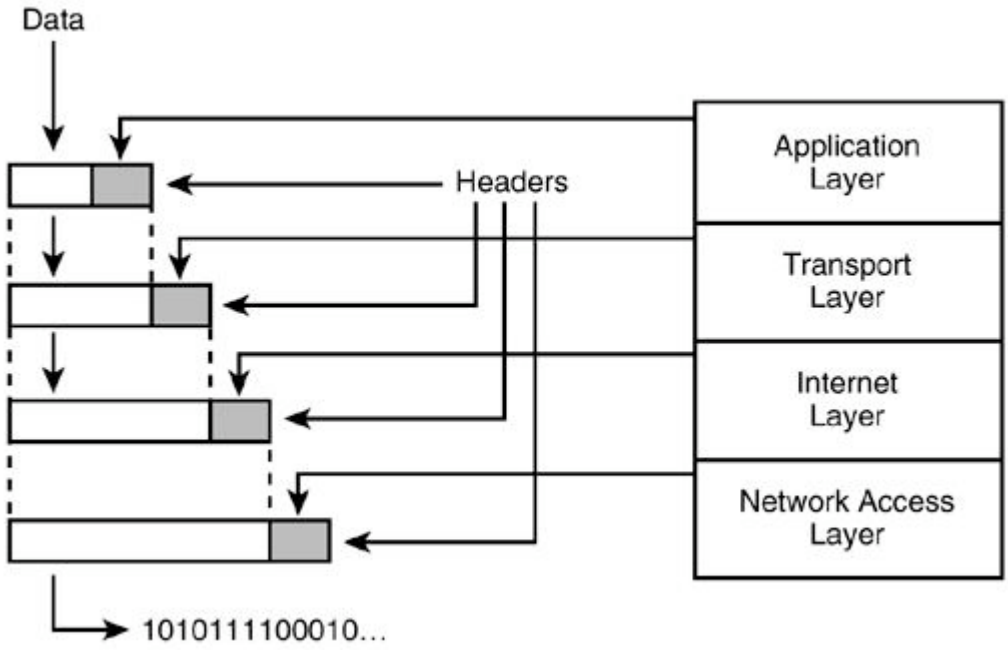
- Uygulama Katmanı --- Uygulamalar için ağ arayüzü sunar, dosya transferi için ağ uygulamalarına destek verir.

Şunu unutmamakta fayda var; TCP/IP ve OSI modelleri uygulama değil standartlardır. TCP/IP nin gerçek hayattaki uygulamalarının hepsi doğrudan modellere hitap etmeyebilir.

OSI ve TCP/IP modelleri en çok Transport ve Internet (OSI deki Ağ Katmanı) katmanlarında benzeşir. Bu katman protokol sistemimin en kolay tanımlanabilen ve en kolay ayırt edilebilen bileşenlerine sahiptir ve protokol sistemlerinin bazen Transport veya Ağ katmanı protokolleri olarak isimlendirilmesi tesadüf değildir. TCP/IP protokol sistemi TCP, transport katmanı protokolü, ve IP , Internet/Ağ katmanı protokolü, ile isimlendirilmiştir.

Veri Paketleri

Bir başka unutulmaması gereken nokta her katman bütün bir iletişim prosesi içinde bir role sahiptir. Her katman kendi rolu için o katmanda geçerli servislere sahiptir. Dışarı gönderilecek bir ileti için veriye her katmanda başlık (header) adı verilen bir bilgi eklenir. Başlık ve bilgi içeren küçük bir veri paketi bir alt katmanda o katmanın header bilgisi ile tekrar paketlenir. Bu işlem Resim 5 de görülmektedir. Veri hedef bilgisayara ulaştığında bu işlem tersten başlayarak gerçekleşir. Veri yığın içinde yukarı doğru çıkarken her katman kendisine ait başlık bilgisini açar ve içindeki bilgiyi kullanır.



Resim 5

Veri yığın içinde aşağı doğru hareket ettikçe, iç içe geçmiş Rus bebekleri gibi bir efekt oluşturur. Alıcı tarafında veri paketleri tek tek açılır ve veri yığın boyunca üste doğru hareket eder. Her katman kendi ismine karşılık gelen başlık kısmını açar ve içindeki bilgiyi kullanır. Her katmandaki fonksiyonlar farklı olduğu için veri her katmanda değişik bir form alır.

Veri paketi her katmanda farklı bir görünüm kazanır. Her katmanda değiştirilen paketler için kullanılan isimler aşağıdadır.

- Uygulama katmanında yaratılan paket Mesaj adını alır.
- Transport Katmanında yaratılan ve Uygulama Katmanı Mesajını sarmalayan paket, Transport Katmanının TCP protokolünden geliyorsa segment, UDP protokolünden geliyorsa Datagram adını alır.
- Internet katmanındaki Transport katmanından gelen segment sarmalayan paket datagram adını alır.
- Ağ Erişim katmanındaki, datagramı sarmalayan ve belki parçalara bölen paket frame (çerçeve) olarak adlandırılır. Bu çerçeve daha sonra Ağ Erişim katmanının alt seviyelerinde bit akışı na çevrilir.

Protokol ve Donanımlar

Ağ erişim katmanı TCP/IP katmanları arasında en gizemli ve en az düzenli olan katmandır. Ağ Erişim katmanı veriyi fiziksel ağa hazırlamak için bütün servisleri ve fonksiyonları yönetir. Bu sorumluluklar şöyle sıralanabilir:

- Bilgisayarın ağ adaptörü ile arayüz oluşturmak
- Veri iletimini uygun erişim metodları araçları ile koordine eder.
- Veriyi frame (çerçeve) olana kadar düzenler ve frame i iletim ortamına gönderebilmek için elektriksel veya analog sinyallere dönüştürür.
- Gelen frame leri hata kontrolü için denetler.
- Çıkan frame lere, alıcı bilgisayar kontrol edebilsin diye hata kontrol bilgileri ekler.
- Gelen frame için onay bilgisi yollar ve giden frame için onay bigisi gelmediyse frame i tekrar yollar.

Tabiki giden frame için gerçekleşen herhangi bir düzenleme işlemi, alıcı bilgisayara ulaştığında tersten olarak yapılmalıdır.

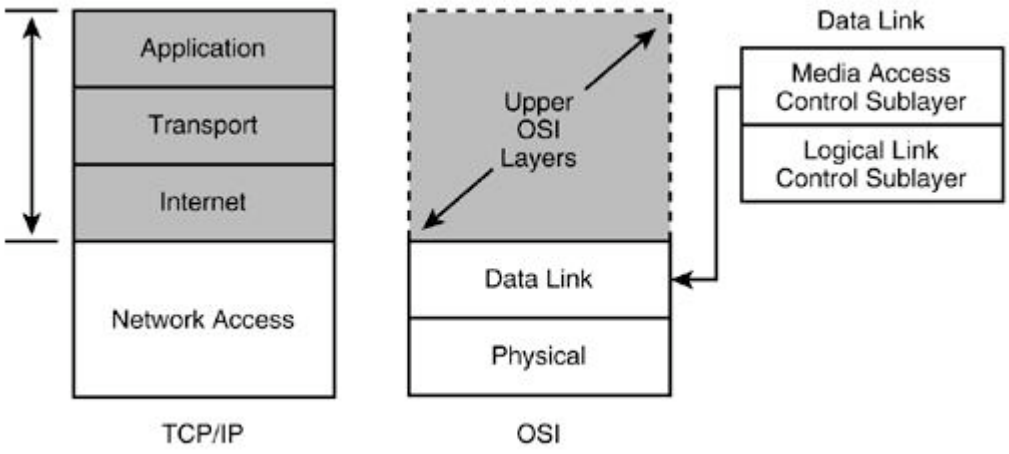
Ağ Erişim katmanı ağ donanımı ile arayüz oluşturmak ve iletim ortamına erişim için kullanılan prosedurleri tanımlar. TCP/IP nin Ağ Erişimi katmanının yüzeyinde; donanım, yazılım ve iletim ortamı arasında geçen karmaşık bir ilişki vardır. Ne yazıkki, en azından kısa ve özlü bir tanım için, herbirinin kendine özgü araçları olan çok sayıda fiziksel ağ tipi vardır ve bunlardan en azından bir tanesi Ağ Erişimi katmanı için temeli oluşturabilir. Bir kaç örnek olarak:

- Ethernet
- Token ring
- FDDI
- PPP (Point-to-Point Protocol, bir modem aracılığı ile)
- Kablosuz ağlar

Ağ Erişim Katmanı ve OSI Modeli

TCP/IP resmi olarak yedi katmanlı OSI modelinden bağımsızdır ancak genel çerçevede protokol sistemlerini anlamak için sık sık OSI modeli kullanılmaktadır. OSI genel kavramı ve terminolojisi özellikle Ağ Erişim katmanı için tartışılmaktadır çünkü OSI modeli bu katman için ek alt bölümler getirmektedir. Bu alt bölümler bu katmanın çalışması hakkında biraz daha fazla bilgi sunmaktadır. OSI modeli ağ üreticileri için oldukça etkileyici olmuştur ve son yıllarda NDIS ve ODI gibi çoklu protokol standartlarına olan eğilim OSI modelin sağladığı terminolojiye olan ihtiyacı gündeme getirmiştir.

Resim 6 da görüldüğü gibi TCP/IP Ağ Erişim katmanı OSI nın Fiziksel ve Data Link katmanlarını aşağı yukarı karşılamaktadır. OSI nin Fiziksel Katmanı framelerin iletim ortamına uygun bit akışlarına dönüştürmekten sorumludur. Başka bir deyişle, OSI Fiziksel Katmanı asıl iletimi gerçekleştiren elektriksel veya analog sinyalleri yönetir ve organize eder. Alıcı tarafında bu sinyaller tekrar bir araya getirilerek frame ler oluşturulur.



Resim 6

OSI Data Link katmanı iki alt katmana bölünerek iki ayrı fonksiyonları gerçekleştirir:

- Media Access Control (MAC) – Bu alt katman ağ adaptörü ile bir arayüz sağlar. Ağ adaptörü sürücüsü genellikle MAC sürücüsü olarak adlandırılır ve fabrikada verilen donanım adres genelde MAC adresi olarak adlandırılır.
- Logical Link Control (LLC) -- Bu alt katman ağa gönderilen frameler için hata kontrol fonksiyonları gerçekleştirir ve ağ üzerinde iletişim kuran cihazlar arasındaki linkleri yönetir.

Ağ Mimarisi

Pratikte, yerel ağlar protokol katmanları bağlamında düşünülmez fakat bundan kastedilen yerel ağ mimarisi veya ağ mimarisidir. (Bazen bir ağ mimarisi yerel ağ tipi veya yerel ağ topolojisi için kullanılır) Bir ağ mimarisi, ethernet gibi, ortam erişimi, fiziksel adresleme ve bilgisayarların iletim ortamı ile ilişkisini yöneten bir çok spesifikasyon getirir. Bir ağ mimarisi için karar vermeye çalıştığınızda, aslında Ağ Erişim katmanı tasarımı için karar vermeye çalışıyorsunuz demektir.

Bir ağ mimarisi fiziksel bir ağ için bir tasarım ve o fiziksel ağ üstünde olacak iletişimi tanımlayan spesifikasyonlar toplamı demektir. İletişim detayları fiziksel detaylara bağlıdır ve böylece spesifikasyonlar komple bir paket oluşturur. Bu spesifikasyonlar aşağıdaki hususları içerir:

- **Erişim Metodu** --- Bir erişim metodu, bilgisayarların bir iletim ortamını nasıl paylaşacaklarını belirleyen bir dizi kuraldan oluşur.
- **Veri Çerçevesi Formatı** --- Internet katmanından IP-seviyesi datagram`ı bir veri çerçevesi içinde öntanımlı bir formatta sarmalanmıştır. Başlık içinde kalan bilgi verinin fiziksel ağ üzerinde iletimi için gereklidir.
- **Kablolama Tipi** – Bir ağda kullanılan kablo tipinin, adaptör tarafından iletilen bit akışının elektriksel özellikleri gibi dizayn parametreleri üzerinde etkisi vardır.
- **Kablolama Kuralları** --- Protokoller, kablo tipi ve iletilen bit akışının elektriksel özelliklerinin kablonun maksimum ve minimum uzunluğu ve kablo bağlantı spesifikasyonları üzerinde etkileri vardır.

Kablo tipi ve konnektörlerin tipi gibi detaylar Ağ Erişim katmanının doğrudan sorumlulukları arasında değildir ancak Ağ Erişim katmanının yazılım bileşenlerini geliştirmek için, yazılım geliştiricilerin fiziksel ağ için bir takım karakteristikleri varsaymaları gerekmektedir. Bu yüzden ağ erişim yazılımı spesifik donanım tasarımı ile birlikte gelmektedir.

Internet Katmanı: Adresleme ve İletim

Bir bilgisayar ağ ile bir ağ adaptör kartı aracılığı ile iletişim kurar. Ağ arabirim cihazı eşi olmayan bir fiziksel adres sahiptir ve o fiziksel adrese gönderilen veriyi alabilmesi için tasarlanmıştır. Fiziksel adres kart üretilirken içine/üzerine yazılır. Ethernet kartı gibi bir cihaz daha üstteki protokol katmanları ile ilgili herhani bir detay bilmez. Kendi IP adresini yada gelen frame`in Telnet içinmi yoksa FTP içinmi gönderildiğini bilmez. Sadece frame`leri dinler, kendi fiziksel adresine gönderilmiş bir frame bekler ve gelen frame`i yığının üst katmanına geçirir.

Bu fiziksel adres şeması tek bir yerel ağ için çok iyi çalışır. Bir kaç bilgisayardan oluşan ve başka bir şey ile bölünmeyen bir ortamda çalışmak için fiziksel adresten başka bir şeye ihtiyaç duymaz. Veri bir ağ adaptöründen diğerine doğrudan geçebilir. (NetBEUI protokolu bu tarz ağlar için en uygun protokoldur)

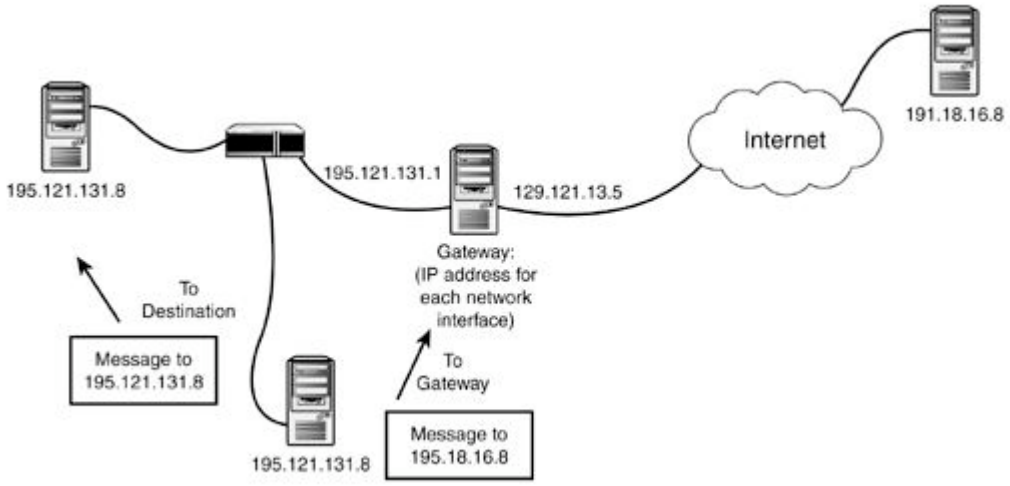
Ne yazıkki, yönlendirilmiş bir ağda, veriyi fiziksel adresler kullanarak iletmek mümkün değildir. Fiziksel adrese iletişim için gerekli olan keşif yayınları (discovery broadcast) yönlendirici arayüzünde çalışmaz.

Bu yüzden TCP/IP fiziksel adresi görünmez kılıp yerine ağı organize etmek için fiziksel ve hiyerarşik bir adresleme şeması kullanır. Bu mantıksal adresleme yapısı Internet Katmanında IP protokolu tarafından yönetilir. Bu mantıksal adres IP adresi olarak adlandırılır. Başka bir Internet katmanı protokolü olan ARP (Address Resolution Protocol) Ip adreslerini fiziksel adreslerle eşleştiren bir tablo tutar. Bu ARP tablosu kart üzerindeki fiziksel adresle IP adresi arasından bir linktir.

Yönlendirilmiş bir ağda (Resim 7) TCP/IP yazılımı veriyi ağa gönderirken şu stratejiyi izler:

- Alıcı bilgisayar gönderici bilgisayarlar aynı ağ segmentindeyse, gönderen bilgisayara paketi doğrudan alıcı bilgisayar gönderir. IP adresi ARP ile fiziksel adrese çözülür ve veri doğrudan hedefin ağ adaptörüne yollanır.
- Hedef bilgisayar gönderici/kaynak bilgisayar dan farklı bir ağ segmentindeyse aşağıdaki işlem başlar:
    - Datagram geçite yönlendirilir. Geçitler yerel bir ağdan diğer ağ segmentlerine datagram iletimine izin veren cihazlardır. Geçit in adresi fiziksel adrese ARP ile dönüştürülür ve veri geçitin ağ adaptörüne yollanır.
    - Datagram geçitten geçerek başka bir ağ segmentine yönlenir. Hedef adres yeni segmentteyse verilen hedefine yollanır aksi taktirde başka bir geçite yönlendirilir.

- Veri, hedef IP adresin fiziksel adrese ARP ile dönüştüreleceği ağ segmentine kadar bir çok geçitten geçmek zorunda kalabilir.



Resim 7

Veriyi karmaşık yönlendiricili bir ağa iletmek için Internet katmanı protollori şunları gerçekleştirmelidir:

- Ağ üzerindeki her bilgisayarı tanımlayabilmek.
- Bir mesajın geçitten geçmesi gerektiğine karar verebilmeli.
- Donanım-bağımsız olarak hedef ağ segmentinin tanımlanması.
- Hedef IP adresinin fiziksel adrese dönüştürülebilmesi ve iletimin gerçekleşebilmesi.

Internet Protokolü (IP)

IP protokolü, hiyerarşik, donanım bağımsız bir adresleme sağlar ve verinin karmaşık, yönlendirilmiş bir ağ üzerinde iletimi için servisler sunar. Bir TCP/IP ağı üzerindeki her ağ adaptörü eşi olmayan bir IP adresine sahip olmalıdır.

TCP/IP nin tanımlarında genellikle bir bilgisayarın IP adresine sahip olmasından bahsedilir çünkü çoğu zaman bir bilgisayar tek bir ağ adaptörüne sahiptir. Fakat birden fazla ağ adaptörüne sahip bilgisayarlar da oldukça yaygın kullanılmaktadır. Yönlendirici veya proxy olarak kullanılan bilgisayarlar birden fazla adaptöre sahip olmalıdırlar bu yüzden birden fazla IP adresine sahip olurlar. Ayrıca çoğu işletim sisteminde bir adaptöre birden fazla IP adresi atamak mümkündür.

Bir ağ üzerindeki IP adresleri organize edilmiştir, böylece bir bilgisayarın konumunu IP adresine bakarak bilebiliriz. Başka bir deyişle adresin bir kısmı

genel bir konumu belirten Posta Kodu gibi, diğer bir kısmıda genel bir alanda spesifik bir konumu belirten Sokak ismi gibidir.

Bu yüzden IP adresi iki parçaya bölünmüştür:

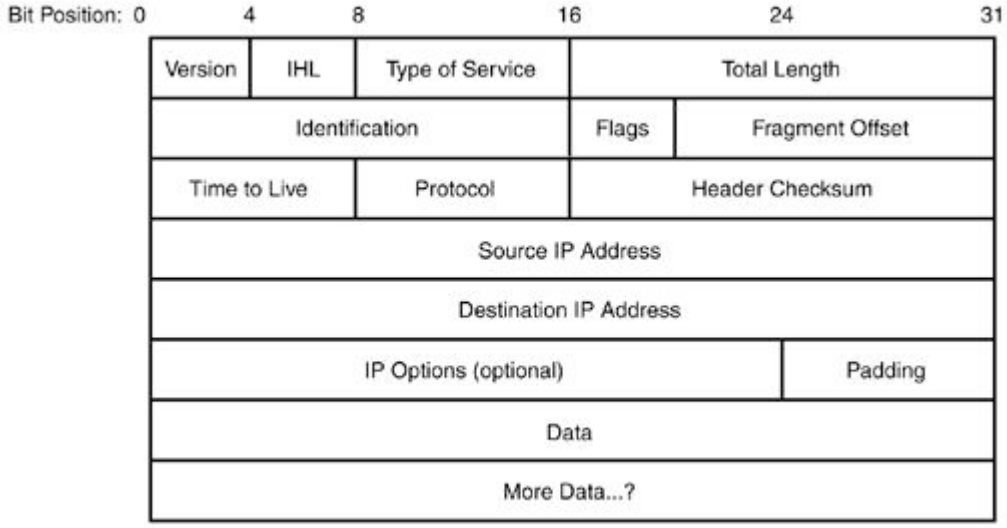
- Ağ Kimlği
- Bilgisayar Kimliği

Ağın yöneticileri ek bir hiyerarşik yapı olan Alt Ağ Kimliği kullanabilir.

Bir protokol yazılımının IP modülü, adresin kendisinden hangi bölümün ağ kimliği hangi bölümün bilgisayar kimliği olduğunu anlayabilir.

IP Başlık Alanları

Bütün IP datagram ları bir IP başlığı ile başlar. Kaynak bilgisayardaki TCP/IP yazılımı IP başlığını kurar. Hedef bilgisayardaki yazılım ise bu başlığın içindeki bilgiyi kullanarak datagram`ı işler. IP başlığı, kaynak ve hedef bilgisayarların IP adresleri, datagramın boyu, IP versiyon numarası ve yönlendiricilere özel bilgiler gibi bir çok bilgi içerir. Bir IP başlığı için minimum boyut 20 bit`dir. Resim 8 IP başlığı içeriğini gösterir.



Resim 8

Şekil deki başlık alanları aşağıdakilerdir:

- Versiyon --- Bu 4 bitlik alan hangi IP versiyonunun kullanıldığını belirtir. Şu andaki versiyon 4 tür. İkili düzendeki karşılığı 0100 dır.
- Internet Başlık Uzunluğu – Bu 4 bit lik alan IP başlığının uzunluğunu 32 bit kelime olarak verir. Minimum başlık uzunluğu 32 bit kelimedir. 5 in ikili düzen karşılığı 0101 dir.
- Servis Tipi --- Kaynak IP si özel yönlendirme bilgisi içerebilir. Bazı yönlendiriciler bu alanı görmezden gelebilir fakat QoS servisinin belirmesiyle bu servisin önemi artmıştır. Bu 8 bitlik alanın amacı bir yönlendiriciden geçmek için bekleyen datagramlar arası öncelik sırasını belirlemektir. Günümüzdeki çoğu IP uygulaması bu alanı sıfırlar ile doldurur.
- Toplam Uzunluk – bu 16 bitlik alan octet olarak IP datagramın uzunluğunu belirtir. Bu uzunluk IP başlığını ve veri yük dağılımını içerir.
- Tanımlama --- Bu 16 bitlik alan kaynak IP tarafından mesajlara verilen artan ardışık sayılardır. Bir mesaj IP katmanına gönderildiği zaman tek bir datagramın içinde tutulmak için büyüktür, IP mesajı bir çok datagram a böler ve hepsine aynı tanımlama numarasını verir. Bu numara verinin alımı ve tekrar oluşturulması için kullanılır.
- Bayrak --- bayrak (Flag) alanı parçalanma olasılıklarını tutar. İlk bit kullanılmaz ve her zaman sıfırdır. Sonraki bir DF (Parçalama) bayrağıdır. DF bayrağı parçalanmaya izin verilip verilmeyeceğini belirtir. Bir sonraki bayrak MF, alıcıya bir çok parçalanmanın sırada olduğunu belirtir. MF sıfırsa datagram hiç bir zaman parçalanmaz.
- Yaşam Ömrü --- Bu bit alanı saniye cinsinden veya geçilen yönlendirici sayısı cinsinden datagramın ömrünü belirtir. Her yönlendirici bu alanı en az 1 azaltır veya saniye cinsinden gecikme sağlar. Bu alan sıfır olduğunda datagram kullanım dışı olur.

Bir datagram hedefine ulaşmadan önce 5 adet yönlendiriciden geçiyorsa hedef için 5 hop uzakta denilebilir.

- Protokol – 8 bit lik bu alan protokolun veri yük paylaşımını alacağını belirtir. Aşağıda kullanılan genel protokol değerleri vardır:

Protocol Name	Protocol Identifier
ICMP	1
TCP	6
UDP	17

- Başlık Sağlama – Bu alan başlığın geçerliliğini doğrulamak için kullanılan 16 bitlik bir değerdir. Bu alan her yönlendiricide TTL her azaldığında tekrar hesaplanır.
- Kaynak IP Adresi --- Bu 32 bit lik alan datagramın kaynak adresini tutar.
- Hedef IP Adresi --- Bu 32 bitlk alan datagramın hedef adresini tutar ve hedef IP tarafından doğru iletişimin kontrolü için kullanılır.
- IP Seçenekleri – Bu alan test, hata ayıklamak ve güvenlik için başlık seçeneklerini destekler.
- IP Veri YükDağılımı --- Bu alan genellikle TCP, UDP, ICMP veya IGMP ye iletilen veriyi tutar.

IP Adresleme

Bir IP adresi 32 bitlik ikili düzen adresidir. Bu 32 bitlik adres 8 bitlik octet adı verilen segmentlere bölünmüştür. İnsanlar 32 bitlik veya 8 bitlik ikili düzen adreslerle çalışmayı pek beceremezler bu yüzden IP adresi hemen her zaman noktalı ondalık şekilde ifade edilir. Bu formatta her octet karşılığı ondalık sayı yazılır bu 4 alan noktalarla birbirinden ayrılır. 8 ikili düzen bitleri 0 ile 255 arası herhanbir bir sayı temsil edebilir böylece ondalık sayılar 0 ile 255 arasındadır. Noktalı ondalık bir IP adresi şöyle görünmektedir: 209.124.124.15

IP adresinin bir bölümü ağ ID si için bir bölümüde bilgisayar ID si için kullanılır. Çoğu IP adresi aşağıdaki adres sınıflandırması içinde kalmaktadır:

- A Sınıfı Adresler --- IP adresinin ilk 8 bit i ağ ID si için kullanılır. Geri kalan 24 bit makina ID leri içindir.
- B Sınıfı Adresler – IP adresinin ilk 16 bit i ağ ID si geri kalan 16 bit i makina ID si içindir.
- C Sınıfı Adresleri --- IP adresinin ilk 24 bit i ağ ID si için geri kalan 8 bit i makina ID si içindir.

Daha fazla bit daha fazla kombinasyon demektir. Tahmin edeceğiniz gibi A sınıfı az sayıda ağ ID si ve çok büyük sayıda makina ID si sağlamaktadır. Bir A sınıfı ağ yaklaşık 2^{24}, veya 16,777,216 makina ID si sağlayabilir. Bir C sınıfı ağ ID si yaklaşık 2^{8}, veya 256 tane makina ID si sağlayabilir.

Bir bilgisayarın yada yönlendirici bir IP adresinin sınıfını nasıl yorumlayabiliyor diye soru sorulabilir. TCP/IP nin yaratıcıları adres kurallarını yazarken bir adresin sınıfının adresin kendisinden belli olabileceği şeklinde yazmışlardır. İkili adresin ilk bir kaç bit i adresin sınıfı hakkında bilgi verebilir. Adresler aşağıdaki şekilde yorumlanabilir:

- 32 bit lik ikili adres 0 la başlıyorsa adres A sınıfına dahildir.
- 32 bit lik ikli adres 1 0 la başlıyorsa adres B sınıfına dahildir.
- 32 bit lik ikili adres 110 la başlıyorsa adres C sınıfına dahildir.

Bu şema noktalı ondalık gösterime kolaylıkla dönüştürülebilir çünkü bu kurallar ondalık noktalı adreslerin ilk terimini sınırlamaya yardımcı olmaktadır. Örnek olarak bir A sınıfı adres ilk oktet in en solunda 0 a sahip olmalıdır bu yüzden ondalık noktalı düzende ilk terim 127 yi geçemez. Aşağıdaki tabloda de A, B ve C sınıfına ait adres aralıkları görülmektedir.

A, B ve C Sınıfları için Adres Aralıkları

Address Sınıfı	ikili Adresin Başlangıcı	Noktalı Ondalık Sayının Başlangıcı	Adresler
A	0	0 – 127	10.0.0.0 - 10.255.255.255 127.0.0.0 - 127.255.255.255
B	10	128 – 191	172.16.0.0 - 172.31.255.255
C	110	192 – 223	192.168.0.0 - 192.168.255.255

Ağ yöneticisi ağı küçük alt ağlara bölebilir (subnetting). Bu yöntemde makina ID lerinin bazı bit lerini ödünç alıp ekstra ağlar yaratılır.

Çoğu TCP/IP iletişimi ya makinadan makinaya yada broadcast olarak gerçekleşir. Diğer yandan D sınıfı adresler çoklu yayınlar içindir. Birçoklu yayın bir ağın belli bir kısmına gönderilen bir mesajdır.

IGMP, çoklu yayın ve D sınıfı adresi birleşiminde kullanılan Internet katmanı protokolüdür.

E sınıfı adresler deneysel çalışmalar için ayrılmıştır. Normalde kullanılmaz.

Özel IP Adresleri

Bir kaç IP adresi özel anlamlara sahiptir ve spesifik makinalara verilemezler. Bütün makina ID alanları sıfır olan bir adres ağın ID sidir. Örnek olarak 129.152.0.0 adresi B sınıfı bir ağa aittir ve ID si 129.152 dir.

Bütün makina ID alanları 1 olan adres yayın adresidir. Bir yayın; bir ağdaki bütün makinalara yollanan bir mesajdır. 129.152.255.255, ID si 129.152 olan B sınıfı bir ağ için yayın adresidir.

255.255.255.255 adresi yine yayın adresi olarak kullanılabilir.

127 ile başlayan adresler loopback adresleridir. Bir loopback adrese gönderilen mesaj TCP/IP yazılımının kendisine gönderilmiş olur. Loopback adresi TCP/IP yazılımının çalıştığını doğrulamak için kullanılır. En yaygını 127.0.0.1 dir.

RFC 1597 bazı adresleri özel ağlar için ayırmıştır. Bu adresler Internete bağlı olmayan adresler olarak kabul edilir ve adreslerin tek olmasına gerek yoktur. Günümüz dünyasında bu özel adresler bir ağ dönüştürücü cihazının arkasında tutulan korumalı ağlarda kullanılmaktadır.

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Adres Çözümleme Protokolü - ARP

Yerel bir ağdaki bilgisayarlar IP adreslerini fiziksel adresler ile eşleyebilmek için ARP adı verilen bir Internet katmanı protokolu kullanırlar. Bir makina alıcı makinanın adaptorünün fiziksel adresini bilmesi gerekmektedir. Bu yüzden ARP çok önemli bir protokoldür. Fakat TCP/IP, ARP ve diğer bütün fiziksel adres çözümleme işleminin kullanıcılara görünmemesi için tasarlanmıştır. Kullanıcı söz konusu olduğunda bir ağ adaptörü IP adresi ile tanımlanır.

Bir ağ segmentinde bulunan her makina ARP tablosu veya ARP belleği adı verilen bir tablo ya sahiptir. Bu tablo ağda bulunan diğer makinaların IP adreslerini fiziksel adresler ile ilişkilendirilir. Bir makina ağdaki başka bir makina bir veri göndermek istediğinde hedef bilgisayarın fiziksel adresi ARP tablosunda varmı yokmu kontrol edilir. ARP tablosu dinamik olarak oluşur.

Transport Katmanı

TCP/IP Internet katmanı verinin ağ boyunca iletimine olanak sağlayan adresleme bilgilerini sağlayan bir çok yararlı protokole sahiptir. Adresleme ve yönlendirme buna rağmen resmin sadece bir parçasıdır. TCP/IP nin geliştiricileri Internet katmanından başka bir katmana ihtiyaçları olduklarını biliyorlardı, IP ile koordineli çalışarak daha fazla özellik sağlayan başka bir katman. Spesifik olarak aşağıdaki özellikleri sağlayan Transport katmanını istiyorlardı:

- Ağ uygulamaları için bir arayüz --- Ağ uygulamalarının ağa erişimini sağlayacak bir yol. Tasarımcılar veriyi sadece bir makina için değil aynı zamanda belli bir uygulamaya gönderebilmeyi istediler.
- Multiplexing/Demultiplexing için bir mekanizma. Multiplexing, Değişik uygulamalar ve bilgisayarlardan veri kabul edip bunu doğru uygulamaya

iletmekten sorumludur. Başka bir deyişle, Transport katmanı aynı anda birden fazla ağ uygulamasını desteklemeli ve Internet katmanına gidecek veriyi yönetebilmeli. Hedef bilgisayar tarafında ise Transport katmanı Internet katmanından veri alabilmeli ve değişik uygulamalara yönlendirebilmeli. Bu özellik demultiplexing olarak bilinmektedir. Örnek olarak bir Web tarayıcısı, bir e-posta istemcisi gösterilebilr.

- Hata-kontrolü, akış-kontrolü ve doğrulama. Protokol sistemi alıcı ve gönderen bilgisayarlar arasında veri iletimininden emin olacak bir genel şemaya sahip olmalıdır.

Son madde en açık uçlu olan maddedir. Kalite teminatı problemi her zaman fayda-maliyet probleminin dengeleyicisi olmuştur. Ayrıntılı bir kalite teminatı sistemi iletimden emin olma yüzdenizi arttırır fakat bunun karşılığında artan ağ trafiği ve yavaş işlem zamanları alırsınız. Çoğu uygulama için bu ek teminat sistemini kullanmaya değmez. Transport katmanı bu yüzden ağ için, her birinin destekleyen uygulamalar için arayüz ve multiplexing/demultiplexing özellikleri olan iki yol sunar fakat ikisininde kalite teminatı sistemine yaklaşımı oldukça farklıdır:

- Transport kontrol Protolü – TCP geniş çapta hata kontrol ve akış kontrol özellikleri sunarak verinin başarılı şekilde iletildiğinden emin olur. TCP bağlantı yönelik bir protokoldür.
- User Datagram Protokol --- UDP oldukça basit hata kontrol mekanizması sunar ve TCP nin geniş kontrol özelliklerinin gerekli olmadığı durumlar için tasarlanmıştır. UDP bağlantı bağımlı bir protokol değildir.

Transport Katmanı Kavramı

TCP ve UDP nin detaylı tartışmasına girmeden önce bazı önemli noktaları vurgulamakta fayda var:

- Bağlantı yönelik ve bağlantı bağımsız protokoller
- Portlar ve soketler
- Multiplexing

Bağlantı Yönelimli – Bağlantı Bağımsız Protokoller

Herhangi bir durum için uygun bir seviye kalite teminatı sağlamak için yazılım geliştiriciler iki değişik ağ protokolü tasarlamışlardır:

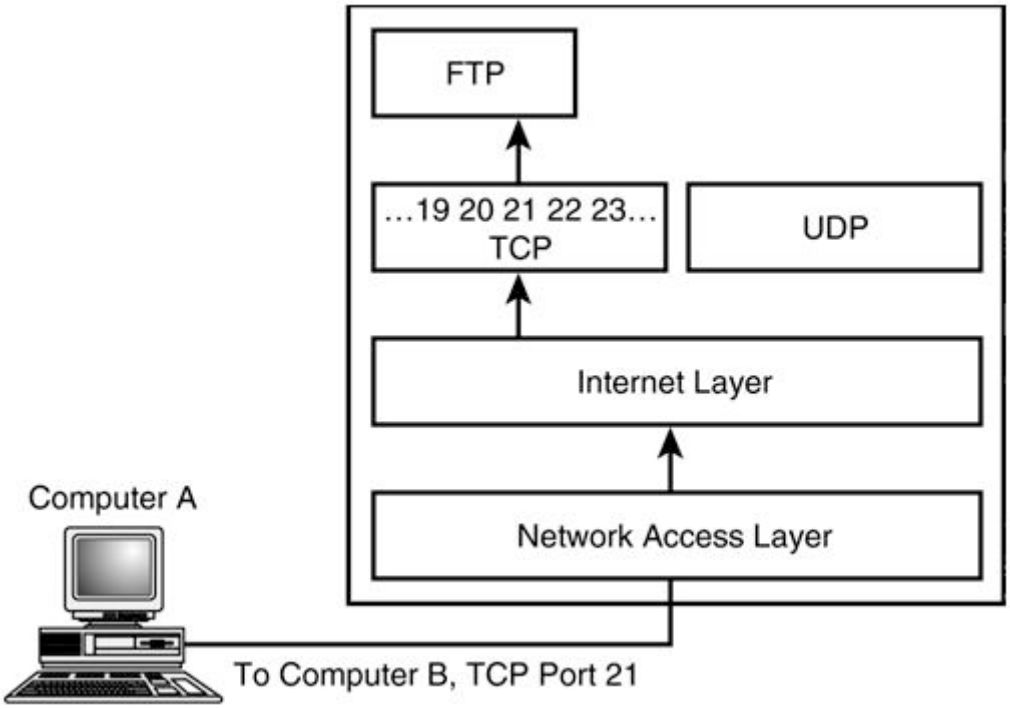
- Bağlantı yönelik protokol iletişim kuran bilgisayarlar arasında bir bağlantı kurar, yönetir ve iletim boyunca bu bağlantıyı gözetler. Başka bir deyişle her gönderilen paket için bir onay mesajı alınır ve gönderen makina giden

paketin hatasız gittiğinden emin olmak için bu bilgileri kaydeder. İletim bittiğinde iki makinada bağlantıyı kapatır.

- Bağlantı bağımsız protokol tek yönlü datagramı hedefine yollar ve karşı makinanın veriyi alıp almadığı ile ilgilenmez. Alıcı makina veriyi alır ve kaynak makinaya herhangi bir durum raporu göndermek ile ilgilenmez.

Portlar ve Soketler

Transport katmanı ağ uygulamaları ve ağ arasında bir arayüz sağlar ve veriyi belirli uygulamalara doğru adreslemek için bir metod sağlar. TCP/IP sisteminde uygulamalar veriye TCP veya UDP üzerinden port sayıları kullanarak erişirler. Bir port Transport katmanından uygulamaya veya uygulamadan Transport katmanına bir yol olarak hizmet eden önceden belirlenmiş bir adrestir. (Resim 9). Örnek olarak bir istemci bilgisayar bir sunucunun FTP uygulaması ile TCP 21 portu üzerinden iletişim kurar.



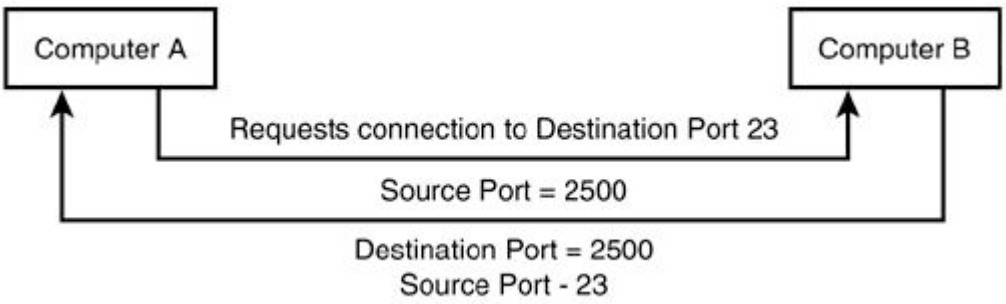
Resim 9

Transport katmanının uygulama-spesifik adresleme şemasına yakından bakarsak, TCP ve UDP verileri aslında soket adı verilen bir yapıya adreslenmiştir. Bir soket IP adresi ile port numarasının birleşmesinden

oluşmaktadır. Örnek olarak 111.121.131.141.21 ifadesi 111.121.131.141 IP adresli bilgisayarın 21 numaralı portunu göstermektedir.

Aşağıdaki örnek bir bilgisayarın soket aracılığı ile hedef makinadaki bir uygulamaya nasıl eriştiğini gösterir (Resim 10):

- A bilgisayarı B bilgisayarındaki bir uygulama ile bilinen bir port aracılığı ile bağlantı kuruyor. Bilinen port ICANN tarafından spesifik bir uygulamaya atanan bir port nuımarasıdır. IP adresi ile birleşen port numarası A bilgisayarı için bir hedef adresi oluşturur. İstek B bilgisayarına A ya cevap döndürürken hangi port numarasını kullanacağı bilgisini içeren bir veri alanına sahiptir. Bu A bilgisayarının kaynak soket adresidir.
- B bilgisayarı A dan gelen istek paketini alıyor ve A nın kaynak adresi olarak adreslediği soketi cevap olarak yönlendiriyor. Bu soket B den A ya gönderilen mesajlar için bir hedef adresi oluyor.



Resim 10

TCP ve UDP yi Anlamak

TCP/IP nin güvenirlilik UDP nin hız için yapıldığı söylenebilir.Telnet veya FTP gibi etkileşimli seansları desteklemesi gereken uygulamalar TCP kullanmaya meğillidir. Kendi hata kontrol mekanizmaları olan ve daha fazla hata kontrolüne ihtiyaç duymayan uygulamalar UDP kullanmaya meğillidir.

Bir ağ uygulaması tasarlayan bir yazılım geliştirici TCP veya UDP kullanmayı seçebilir. UDP nin daha basit olan kontrol mekanizmaları sınırlandırıcı olarak düşünülmemelidir. Hepsinden önce daha az kalite teminatı daha az kalite anlamına gelmez. TCP nin sağladığı ekstra kontroller çok sayıda uygulama için tamamen gereksizdir. Hata ve akış kontrolunun gerekli olduğu yerlerde bazı

geliştiriciler bu kontrolleri yazılımın kendisine yaptırmakta ve ağ erişimi için UDP yi tercih etmektedirler. TCP/IP nin RPC si gibi UDP tabanlı servisler gelişmiş uygulamaları destekleyebilir fakat hata ve akış kontrol görevlerini TCP yerine o uygulamalar yapar.

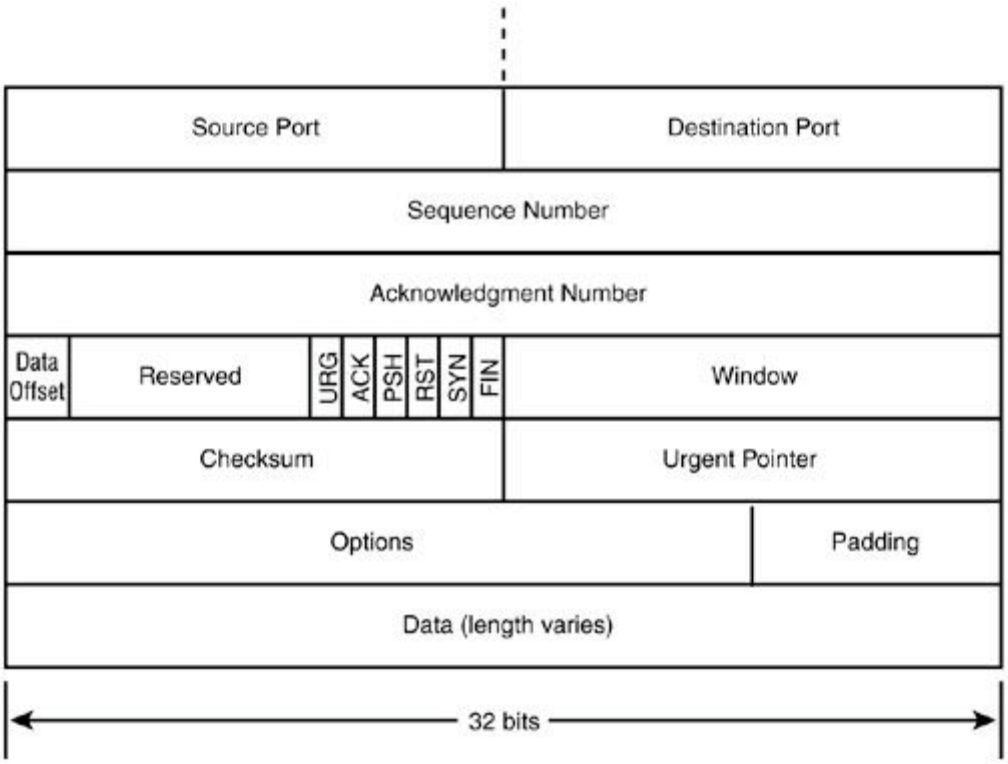
TCP: Bağlantı Yönelimli Transfer Protokolü

TCP belirtilmesi gereken bir kaç tane daha önemli özellik barındırmaktadır:

- Akış yönelimli İşleme -- TCP bir akıştaki veriyi işler. Başka bir deyişle TCP ön formatlı bir blok olarak almak yerine veriyi her seferde bir byte alır. TCP veriyi değişken uzunluklu segmentler olarak formatlar.
- Veri hedef makinaya sıralı bir şekilde gelmez ise, TCP modülü verinin orjinal sırasını tekrar ayarlayabilir.
- Akış Kontrolü --- TCP nin akış kontrol mekanizması hedef bilgisayarın veri alış kapasitesini aşmamak veya az kullanmamak üzere veri iletimini kontrol eder.

TCP Data Formatı

TCP başlık formatı Resim 11 de gösterilmiştir. Yapının karmaşıklığı TCP nin karmaşıklığını ortaya çıkarmaktadır.



Resim 11

Başlıktaki alanlardan bazılarının açıklamaları şöyledir:

- Kaynak Portu (16 bit) --- Kaynak makinadaki uygulamaya atanan port numarası.
- Hedef Portu (16 bit) --- Hedef makinadaki uygulamaya atanan port numarası.
- Sıra Numarası (32 bit) --- SYN flag`ı 1 olarak değer almamışsa ilk byte`ın sıra numarası. SYN flag`ı 1 ise, Sıra Numarası alanı başlangıç sıra numarasını (ISN) verir, ISN sıra numaralarını senkronize etmek için kullanılır.
- Onay Numarası (32 bit) --- Gelen segmenti onaylayan numaradır.
- Kontrol flag leri (Her biri 1 bit) --- Kontrol flagleri segment ile ilgili özel bilgiler verirler.
    - URG --- 1 değeri segmentin acil olduğunu ve Urgent Pointer alanının önemli olduğunu belirtir.
    - ACK --- 1 değeri Onay Alanının anlamlı olduğunu belirtir.
    - PSH --- 1 değeri TCP yazılımına o ana kadar gönderilen bütün verilerin hedef uygulamaya iletilmesini belirtir.
    - RST --- 1 değeri bağlantıyı tekrar kurar.
    - SYN --- 1 değeri sıra numaralarının senkronize olacağını belirtir.
    - FIN --- 1 değeri kaynak makinanın gönderecek başka verisi kalmadığını belirtir. Bağlantıyı kapatmak için kullanılır.
- Pencere (16 bit) --- Akış kontrolü için bir parametredir. Son onaylanan sıra numarasından sonra bir dahaki onay a kadar serbset olarak gönderilebilecek sıra numarası aralığıdır.
- Sağlama (16 bit) --- Segment in bütünlüğünü kontrol eden alan. Hedef bilgisayar bu alanda tutulan değerle, segment üzerinde yaptığı bir sağlama hesaplaması sonucunu karşılaştırır.
- Urgent Pointer (16 bit) --- Herhangi bir acil bilginin başlangıcını işaret eden offset pointer'ı.
- Data --- Segmentte iletilen veri.

TCP Bağlantıları

TCP içinde gerçekleşen her şey bir bağlantı durumunda gerçekleşmektedir. TCP veriyi bir bağlantı aracılığı ile gönderir ve alır. Bu bağlantı TCP kuralları dahilinde istek olarak yapılmalı, açılmalı ve kapanmalıdır.

TCP nin amaçlarından biri uygulamalara ağ erişimi için bir arayüz sağlamaktır. Bu arayüz TCP portları ile sağlanmakta bu portlar kullanılarak bir bağlantı sağlamak için, TCP arayüzü uygulamaya açık olmalıdır. TCP iki açık durumu desteklemektedir:

- Pasif Açık --- Herhangi bir uygulama TCP yi, bir TCP portundan gelecek bağlantılar konusunda bilgilendirir. Bu yüzden TCP den uygulamaya açılan yol gelen bağlantı isteğinin önceden bilinmesi ile olmaktadır.
- Aktif Açık --- Bir uygulama TCP den pasif açık durumunda olan başka bir bilgisayar ile bağlantı kurmasını ister.

Bağlantının Kurulması

Sıra numarası ve onay sisteminin çalışması için, bilgisayarlar sıra numaralarını senkronize etmelidirler. Başka bir deyişle B bilgisayarı bir zincir başlatmak için A nın başlangıç sıra numarasını (ISN) bilmek zorundadır. A bilgisayarı B nin başlatacağı herhangi bir veri iletimi için kullanacağı ISN i bilmek zorundadır.

Bu senkronizasyon 3 lü el sıkışma (3-way handshake) olarak adlandırılır ve TCP bağlantısının başlaması sırasında gerçekleşir. 3 lü el sıkışmanın üç aşaması aşağıdaki gibidir:

1. A bilgisayarı aşağıdaki bilgiler ile bir segment gönderir:

   SYN = 1
   ACK = 0

   Sequence Number = X (where X is Computer A's ISN)

   A aktif açık bilgisayarı SYN flag i 1 ve ACK flag i 0 olarak bir segment yollar. SYN senkronizasyon için küçüktür. Bu flag daha önce açıklandığı gibi bir bağlantı açma denemesi için anons yapar. İlk segment başlığı aynı zamanda A nın göndereceği veri için başlangıç sıra numarası ISN i içerir. B ye gönderilen ilk byte ın sıra nunarası ISN+1 olacaktır.

2. B bilgisayarı A nın segmentini alır ve aşağıdaki bilgiler ile bir segment i geri yollar:

   SYN = 1

   ACK = 1

   Sequence number = Y, where Y is Computer B's ISN

   Acknowledgment number = M + 1, where M is the last sequence number received from Computer A

   M, A dan gelen son sıra numarasıdır.

3. A bilgisayarı B nin ISN ini aldığını onaylayan bir segmenti B ye gönderir.

SYN = 0
ACK = 1

Sequence number = next sequence number in series (M+1)

Acknowledgment number = N + 1 (where N is the last sequence number received from Computer B)

N B den gelen son sıra numarasıdır.

3 lü el sıkışmanı ardından bağlantı açılır ve TCP modülleri veri gönderip ve alımını yukarda anlatılan zincir ve onay şeması dahilinde gerçekleştirir.

TCP Akış Kontrolü

TCP başlığındaki Pencere alanı bağlantı için akış kontrolü sağlar. Bu alanın amacı veri gönderen bilgisayarın veriyi, alıcı bilgisayarın, gönderici bilgisayarın gönderdiği hızda veriyi işleyememe olasılığı adına, hızlı veri göndermemesi ve böyle bir durumda veri kaybı olmamasını sağlamaktır. Bu metod kayan pencere metodu olarak adlandırılır. Hedef bilgisayar Pencere alanını kullanarak kaynak bilgisayarın son onaylanmış sıra numarasından beri göndermeye yetkili olduğu sıra numaraları penceresini tanımlar. Kaynak bilgisayar, bir sonraki onaya kadar o pencere dışında başka iletim yapamaz.

UDP – Bağlantı Bağımsız Transfer Protokolü

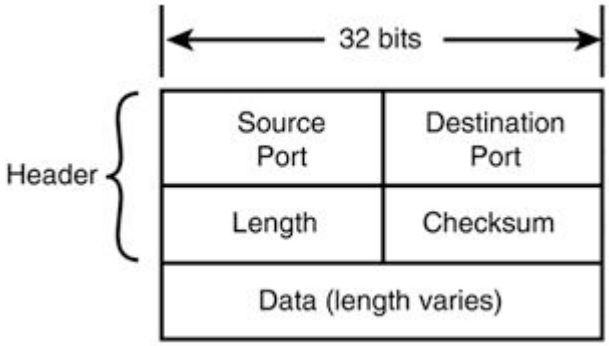
UDP, TCP ye göre çok daha basittir ve önceki bölümlerde listelenen fonksiyonlardan hiçbirini gerçekleştirmez. Fakat UDP için belirtilmesi gereken bir kaç konu vardır.

İlk önce, zaman zaman UDP nin hiç bir hata kontrol mekanizması bulunmaz denmesine rağmen aslında temel bir hata kontrol yapabilme yeteneği vardır. UDP yi sınırlı hata kontrol mekanizmasına sahip olarak kategorize etmek en iyisidir. UDP datagramı, hedef makinanın verinin bütünlüğünü kontrol edebilmesi için bir sağlama değeri içermektedir. Ayrıca, hedef UDP modülü bir aktif olmayan yada tanımlı olmayan porta yönlenmiş bir datagram alırsa, kaynak makinaya port un ulaşılamaz olduğunu belirten bir ICMP mesajı gönderir.

İkinci olarak, TCP nin sağladığı verinin sıraya konulma işlemini sağlamaz. Yeniden sıralama, segmentlerin değişik yollar kullanarak ve yönlendiricilerde gecikmeler yaşayarak gelebileceği Internet gibi büyük ağlarda önemlidir. Yerel ağlarda yeniden sıralama eksikliği genelde güvenimez bir özellik olarak karşılanmaz.

UDP protokolünün ana amacı datagram ları Uygulama Katmanı için açmaktır.Udp nin kendisi ufakta olsa bir başlık işlemi yapar. Bunu açıklayan RFC sadece 3 sayfador. Daha önce de belirtildiği gibi UDP kaybolan yada zarar görmüş datagramları yeniden iletmez, sırası bozulmş datagramları sıraya koymaz, birbirinin aynı gelen datagram ları ayırmaz, datagramların iletimini onaylamaz, bağlantı kurmaz ve kapatmaz. UDP ana amacı uygulamaların TCP nin karmaşıklığı olmadan datagram alıp vermelerini sağlayan bir mekanizma sağlamaktır. Uygulama eğer gerekliyse bunların hepsini kendi sağlayabilir.

UDP başlığı dört adet 16 bit lik alanda oluşur. (Resim 12)



Resim 12

Aşağıdaki liste bu alanları açıklar:

- Kaynak Port --- İlk 16 bit lik alandır. Datagramı gönderen uygulamanın port numarasını tutar. Burdaki değer hedef uygulama tarafından geri dönüş adresi olarak kullanılacaktır. Bu alan opsiyoneldir. Kaynak uygulama bu alanı port numarası ile doldurmazsa bütün 16 bit`in sıfırla doldurulması beklenir.
- Hedef Port --- bu 16 bit`lik alan hedef makina nın datagramı alacağı port numarasıdır.
- Uzunluk --- Bu 16 bit lik alan octet olarak UDP datagram ın uzunluğunu tutar. Uzunluk UDP başlığını ve veri yi içerir. UDP başlığı sekiz octet uzunluğunda olduğu için bu değer her zaman en az 8 olacaktır.
- Sağlama --- Bu 16 bit lik alan datagram ın iletim sırasında bozulup bozulmadığına karar verir. Sağlama ikili düzen de bir veri string i üzerinde yapılan özel bir hesaplamanın sonucudur. UDP için sağlama, UDP başlığı, UDP verisi ve çift sayıda bir octet uzunluğu elde etmek için sıfırla doldurulan octet ler temel alınarak hesaplanır.

Gerçek UDP başlığı kaynak veya hedef IP adresi içermediği için datagramın başka bir bilgisayar yada servise gitme olasılığı vardır. Pseudo-header hedef IP bilgisi sağlar ve böylece hedef bilgisayar UDP datagram ın yanlış gelip gelmediğini kontrol edebilir.

Uygulama Katmanı

Uygulama katmanı TCP/IP protokol sisteminin en üst katmanıdır. Uygulama katmanında ağ uygulamalarını yada TCP ve UDP portları aracılığı ile alt katmanlarla iletişim kuran servisleri bulabilirsiniz. Uygulama katmanının neden yığının bir parçası olduğu sorulabilir. Fakat unutmamak gerekirki, TCP/IP gibi katmanlı bir yapıda, her katman ağa bir arayüzdür.

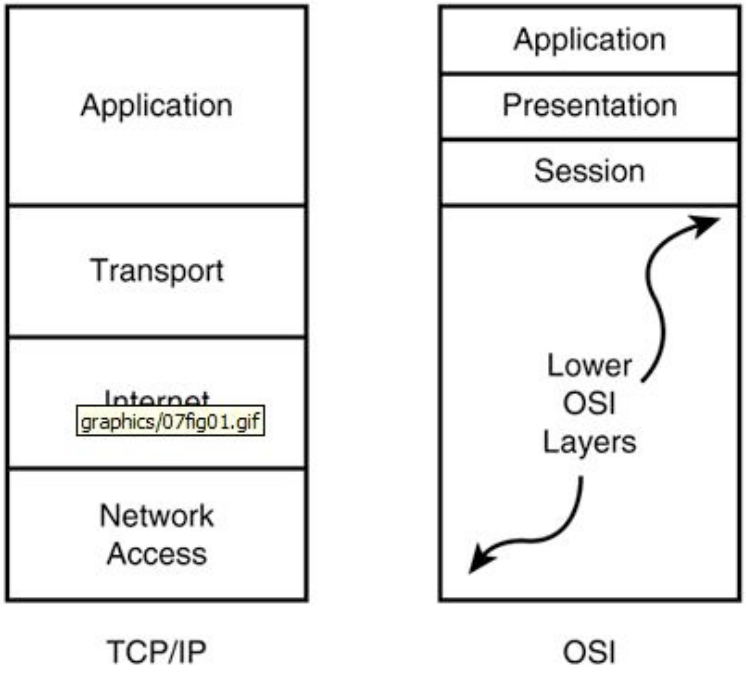
TCP/IP nin Uygulama katmanı gerçekte TCP ve UDP portlarına bigi önderen ve onlardan bilgi alan ağ yazılım bileşenlerinin karışımıdır. Bu bileşenler mantıksal olarak benzer veye eşit olma anlamında paralel değildirler. Bazı bileşenler ağ konfigürasyonu hakkında bilgi toplayan araçlardır. Diğer Uygulama katmanı bileşenleri bir kullancı ararimi sistemi veyab Uygulama Arabirimi (API) olabilir. Bazı Uygulama katmanı bileşenleri dosya veya yazıcı servisleri gibi ağ hizmetleri sunar.

TCP/IP nin Uygulama katman ile bunun OSI deki karşılığı olan katmanların bir karşılaştırması ile başlayalım.

TCP/IP Uygulama Katmanı ve OSI

Daha önce bahsedildiği gibi TCP/IP resmi olarak OSI nin yedi katmanlı yapısına uymamaktadır. OSI modeli buna rağmen ağ sistemlerinin geliştirilmesinde oldukça etkili olmuştur. Uygulama katmanı işletim sistemi ve ağ ortamları açısından geniş bir yelpaze çizer ve bu ortamların çoğunda ağ sistemlerini tanımlamak ve açıklamak için OSI modeli önemli bir araçtır.

TCP/IP nin Uygulama katmanı, OSI nin Uygulama, Sunum ve Oturum katmanlarına karşılık gelir. (Resim 13). OSI modelinin getirdiği alt bölümleme (1 yerine 3 katman) bazı ek organizasyon özellikleri sağlamaktadır.



Resim 13

TCP/IP nin Uygulama katmanına karşılık gelen OSI katmanlarının açıklamaları aşağıdadır:

- Uygulama Katmanı --- OSI nin uygulama katmanı kullanıcı uygulamaları için servisler sağlar ve ağ erişim desteği verir.
- Sunum Katmanı --- Sunum katmanı veriyi platform bağımsız bir formata dönüştürür ve dosya sıkıştırma ve şifreleme işlemlerini yönetir.
- Oturum katmanı --- oturum katmanı ağdaki bilgisayarlar üzerinde iletişim kuran uygulamaları yönetir. Bu katman Transport katmanında bulunmayan, tanıma ve güvenlik gibi bağlantılar ile ilgili bazı fonksiyonlar sunar.

Bütün bu servisler bütün uygulamalar için gerekli değildir. TCP/IP modelinde uygulamalar OSI alt bölümlerinin katmanlı bir yapıda olmasına ihtiyaç duymaz fakat genelde OSI nı Uygulama, Sunum ve Oturum katmanlarının sorumlulukları TCP/IP nin Uygulama katmanı sorumlulukları ile örtüşmektedir.

Kaynaklar

1. TCP/IP Illustrated Vol.1 – W. Richard Stevens
2. Illustrated TCP/IP – John Wiley & Sons

3. Teach Yourself TCP/IP in 14 Days – Sam's Publishing (Dökümanda kullanılan resimler bu kaynaktan alınmıştır)
4. TCP/IP Tutorial and Technical Overview – International Technical Support Organization

Düzenleyen

Ümit Yalçın Şen, EST 2003 – 2004, Y.Lisans Öğrencisi.

3.3 TCP/IP Konfigürasyonu

Linux sisteminin TCP/IP dosyalarını konfigüre etmeden önce birkaç ev temizliği adımı atmamız gerekmektedir. Bu adımların bazıları sistem yüklendiğinde sizin için otomatik olarak gerçekleştirilmiş olabilir. Linux ağ sisteminin bazı versiyonları **`/proc`** dosya sistemine dayanır. Ağ sistemini destekleyen çoğu linux çekirdeği sistem yüklendiğinde otomatik olarak **`/proc`** dosya sistemini oluşturur. Bu durumda yapacağınız tek şey bu sistemin çekirdek tarafından düzgün bir şekilde mount edilip edilmediğini kontrol etmeniz olacaktır. **`/proc`** dosya sistemi temel olarak ağ bilgilerini kolay elde etmek için çekirdeğe hızlı bir arayüzü noktası oluşturur ve buna ilave olarak ağ yükleme alt programı tarafından yaratılan ve genellikle, **`/proc/net`** alt dizininde önemli tabloları tutar. **`/proc`** dosya sisteminin otomatik olarak mount edilmesini temin etmek için **`/etc/fstab`** dosyasını mount komutunu kullanarak modifiye etmek gerekir. Aşağıdakine benzer satırlar için **`/etc/fstab`** dosyasındaki girdileri kontrol etmeliyiz.

```
none/proc  proc  defaults
```

Eğer böyle bir satır yoksa, **`/etc/fstab`** dosyasına ASCII editörü kullanarak bu satırı ilave etmelisiniz. Linux çekirdeğiniz tarafından **`/proc`** dosya sistemi oluşturulmamışsa Linux çekirdeğini yeniden derlemeli ve **`/proc`** opsiyonunu seçmelisiniz. Bunun için **`/usr/src/linux`** klasöründen aşağıdaki komutu çalıştırmalısınız.

```
$ make config
```

procfs desteği sorulduğunda buna yes opsiyonu ile yanıt vermelisiniz. TCP/IP konfigürasyonuna başlamadan önce yapmanız gereken bir diğer adım **hostname**'inizi kurmanızdır. Hostname'ini kurmak için

```
$ hostname name
```

burada **`name`** sizin yerel makinanız için istediğiniz sistem ismidir. Örneğin linux makinanız **`star.com`** domain'ine bağlanmış ise ve makinanızın ismi **`ata`** ise;

```
hostname ata.star.com
```

hostname isminin **/etc/hosts** dosyasında görünüyor olmasını kontrol ediniz. Pekçok ağ için doğrudan bilgiye ulaşmak istiyorsak **/etc/networks** dosyası faydalı olabilir. Bu dosya network isimlerinin ve IP adreslerinin listesini içerir. Makinanızdaki uygulama programları isimlerine dayanarak hedef ağları belirlemek istediklerinde bu dosyayı kullanabilirler. Bu dosya iki sütundan oluşur:

1. Uzak ağın sembolik ismi
2. Ağın IP adresi

Çoğu **/etc/networks** dosyaları en azından bir loopback sürücü girişine sahiptir. Örnek olarak;

```
Loopback        127.0.0.0
Merlin-net      147.154.12.0
BNR             47.0.0.0
```

Bu dosya ağ IP adresleriyle girilen iki ağa sahiptir.

TEMEL KURULUMLAR

Linux makinanızda TCP/IP kurmak için yapacağınız ilk adım ağ arayüzünü (veya arabirimini) erişilebilir kılmaktır. Bu **ifconfig** komutu ile gerçekleştirilir. **ifconfig** temel olarak çekirdeğin ağ tabakasını IP adresi vererek ağ arayüzü ile çalıştırır ve daha sonra arayüzü aktif yapmak için komutu çalıştırır, arabirim aktif olduğunda çekirdek arabirim boyunca veri alış-verişi yapabilir. Makinanıza loopback sürücüsü ve ethernet arabirimi dahil olmak üzere birkaç arabirim kurmak zorundasınız. **ifconfig** komutu sırayla herbir arabirim için kullanılır. Genel format şöyledir.

```
ifconfig  interface_type  IP_address
```

Burada **interface_type** interface aygıtının sürücü ismidir (örneğin **0** loopback için, **ppp** ppp için ve **eth** ethernet için). Bir kez **ifconfig** komutu çalıştırılırsa ve arayüz aktif olursa **route** komutunu kullanarak çekirdeğin routing tablosunda **route**'ları eklemek veya çıkarmak mümkündür. Bu yerel makinamızın diğer makinaları bulmasını temin eder. **route** komutunun genel formatı.

```
route add|del  IP_address
```

Burada **IP_address** etkilenecek uzak **route**'ı tanımlar. Herhangi bir zamanda çekirdeğin routing tablosunun mevcut içeriğini görüntüleyebilirsiniz bu **route** komutu ile gerçekleşir. Eğer sisteminiz sadece loopback sürücü ile kurulmuşsa aşağıdaki örnekteki gibi bir çıktı göreceksiniz.

```
$ route
     Kernel Routing Table
     Destination Gateway Genmask Flags MSS Window Use Iface
     Loopback * 255.0.0.0 U 1936 0 16 Lo
```

-n opsiyonu kullanarak sembolik isimler yerine IP adreslerini görüntüleyebilirsiniz.

```
$ route -n
     Kernel Routing Table
     Destination Gateway Genmask Flags MSS Window Use Iface
     127.0.0.1 * 255.0.0.0 U 1936 0 16 Lo
```

Tipik bir linux ağ konfigürasyonu birkaç arayüzü içerir loopback arayüzü her makinada bulunması gerekir. İster ethernet isterse diğer bir araç olsun network arayüzü mevcut olmalıdır (sadece bir loopback sürücüsü istemediğinizde). Bu anlatımımızda sisteminize loopback ve ethernet kartı kurmak için işlemlerimizi yapacağız.

LOOPBACK ARAYÜZÜNÜN KURULUMU

Loopback arayüzü ağa bağlanan her makinada mevcut olmalıdır. Loopback arayüzü her zaman 127.0.0.1 IP adresine sahiptir, bu nedenle **/etc/hosts** dosyası bu arayüzü barındırmalı loopback sürücüsü yazılım yüklenmesi esnasında çekirdek tarafından oluşturulabilir, bu nedenle **/etc/hosts** dosyasına bakalım:

```
127.0.0.1       localhost
```

Eğer bu satır mevcut ise, loopback sürücüsü yerindedir. Eğer bu satır mevcut değilse **ifconfig** komutu ile oluşturulur.

```
ifconfig  lo  127.0.0.1
```

Konfigürasyon hakkında emin değilseniz

```
ifconfig  lo
```

Aşağıdakine benzer birkaç satırı görmelisiniz.

```
ata:~#  ifconfig  lo
lo  Link  encap:Local Loopback
Inet addr:127.0.0.1 Bcast:127.255.255.255 Mask:255.0.0.0
UP BROADCAST LOOPBACK RUNNING MTU:2000 Metric:1
```

```
RX  packets:0  errors:0  dropped:0  overruns:0
TX  packets:12 errors:0  dropped:0  overruns:0
```

Bilinmeyen arayüz gibi hata mesajı alırsınız, bu ilave edilmeli. Aşağıdaki iki komuttan biriyle bu işlem gerçekleştirilir.

```
route  add  127.0.0.1
route  add  localhost
```

Loopback sürücüsünü kontrol etmek için **ping** komutu kullanılır. Aşağıdaki iki komuttan birisi kullanılabilir.

```
ping localhost
ping 127.0.0.1
```

Aşağıdaki gibi bir çıktı elde ederiz.

```
PING  localhost: 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0. tt1=255 time=1 ms
64 bytes from 127.0.0.1: icmp_seq=1. tt1=255 time=1 ms
64 bytes from 127.0.0.1: icmp_seq=2. tt1=255 time=1 ms
64 bytes from 127.0.0.1: icmp_seq=3. tt1=255 time=1 ms
64 bytes from 127.0.0.1: icmp_seq=4. tt1=255 time=1 ms
64 bytes from 127.0.0.1: icmp_seq=5. tt1=255 time=1 ms
64 bytes from 127.0.0.1: icmp_seq=6. tt1=255 time=1 ms
64 bytes from 127.0.0.1: icmp_seq=7. tt1=255 time=1 ms
^C
--- localhost PING statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip (ms) min/avg/max = 1/1/1
```

ping komutunun çalışması **Ctrl-C** ile 7 transmisyondan sonra kesilmiştir. İstediğiniz kadar devam etmenize izin verilir. Eğer "no replies" yanıtını ping komutundan alırsak o zaman 127.0.0.1 adresi veya **localhost** adı tanınmamıştır ve konfigürasyon dosyalarını tekrar gözden geçirmeli ve tekrar **route** girişi yapmalıyız.

ETHERNET ARABİRİMİNİN KURULUMU

Şimdi loopback sürücüsü yüklenmiş ve çalışır vaziyette. Aynı konfigürasyon sürecini ethernet sürücüsü için yapabiliriz yapılacak süreç tamamen aynıdır: Yani **ifconfig**'i kullanarak kernel'e arabirim hakkında bilgi verilir ve daha sonra ağ üzerindeki uzak makinalara yönlendirmeler ilave edilir. Eğer ağ ilave edilmişse bu bağlantıları **ping** komutu ile test ederiz. Başlamak için, **ifconfig** kullanarak ethernet arabirimini kuralım arabirimi aktif yapmak için, yerel IP adresinizle birlikte ethernet aygıt ismini kullanarak **ifconfig** komutu devreye sokulur.

```
ifconfig  eth0  147.123.20.1
```

Burada arabirim **/dev/eth0** ile ethernet aygıtınadır. Network mask değeri IP adresinden elde edileceğinden ayrıca belirtmeye gerek yoktur fakat yinede açık bir şekilde belirtmek isteniyorsa network keyword'ü ile komuta ilave edilebilir.

```
ifconfig eth0 147.123.20.1 network 255.255.255.0
```

arabirimi aşağıdaki komutla kontrol edilir.

```
     $ ifconfig eth0
eth0 Link encap 10Mps: Ethernet Hwaddr
inet addr 147.123.20.1 Bcast 147.123.1.255 Mask 255.255.255
UP  BROADCAST RUNNING MTU 1500 Metric 1
RX  packets:0  errors:0  dropped:0 overruns:0
TX  packets:0  errors:0  dropped:0 overruns:0
```

Bu çıktıdan broadcast adresinin yerel makinanın IP adresine dayanarak kurulmuştur. Bu LAN üzerindeki tüm makinalara TCP/IP tarafından bir defada ulaşılması için kullanılır. MTU (Message Transfer Unit) boyutu genellikle 1500 max. değerine kurulmuştur (Ethernet ağları için) daha sonra çekirdeğin yönlendirme tablosuna, çekirdeğin yerel makinanın ağ adresini bilebilmesi için bir satır ilave etmemiz gerekir. Bu aynı ağda diğer makinalara veri yollamasına izin verir. Bir defada tüm LAN'ı kurmak için **route** komutunu **–net** opsiyonu ile kullanalım:

```
route  add  -net  147.123.20.0
```

Bu komut 147.123.20 ağ adresiyle tanımlanan ağ üzerindeki tüm makinaları, çekirdeğin erişebilir makinalar listesine ekler. Eğer bu şekilde yapılmazsa geriye iki alternatif kalır birincisi tüm IP adreslerini elle girmek, ikincisi ise tüm ağ isimlerini ve IP adreslerini içeren **/etc/networks** dosyasını kullanmaktır. Örneğin, **foobar_net** isimli bir ağ için **/etc/networks** dosyasında bir giriş varsa, bu ağın tümünü yönlendirme (routing) tablosuna aşağıdaki komutla ilave ederiz.

```
route  add  foobar_net
```

Bu işlemden sonra, ethernet arabirimini devreye sokmak kalıyor. Bu adım elbette diğer makinalara bağlandığınızı ve en azından birisinin IP adresini bildiğinizi kabul etmektedir. Böylelikle **ping** komutu ile uzak makinadaki bağlantı seviyesi saptanmış olur. Eğer **ping** komutu düzgün çalışmazsa **netstat** utility devreye girer.

PLIP KONFİGÜRASYONU

PLIP (ParaleL port IP) arabirimi sadece iki makinayı paralel portları aracılığı ile bağlanması için kullanır. PLIP konfigürasyonu, TCP/IP'ninkinden farklıdır,

özellikle arabirim standart TCP/IP arabirimi değildir ve sadece iki makina karışmıştır. Şimdi, yerel linux makinamız **darkstar** ile **x-wing** olarak adlandırılan **mscelebi**'nin makinasını PLIP arabirimi ile bağlamayı düşünelim. İki makina bir null-paralel kablo ile bağlanır. Her iki makinanın sadece bir paralel portu vardır ve bu PLIP için kullanılır. PLIP konfigüre edildiğinde araçlar **/dev/plip1** olarak her iki makinadada kurulur. Her iki makina arasında PLIP arabirimini konfigüre etmek için tekrar **ifconfig** komutunu kullanalım. Bu komutla birlikte özel bir keyword "**pointtopoint**" kullanılır (bu network tipini tanımlayan point-to-point'in karmaşık yapısından farklıdır). Bağlantı için gerekli **ifconfig** komutu

```
ifconfig  plip1  x-wing  pointtopoint darkstar
```

Aygıtın **/dev/plip1**, uzak makinanın **x-wing** ve yerel makinanın **darkstar** olduğuna dikkat ediniz. Bu işlemden sonra **route** komutu ile çekirdek yönlendirme tablosu güncellenir.

```
route  add  x-wing  gw  darkstar
```

gw keyword'ü **darkstar**'ın **x-wing** makinasına bir gateway olduğunu gösterir.
Benzer komutlar diğer makinadada girilmelidir.

```
ifconfig  plip1  darkstar  pointtopoint x-wing
 route  add  darkstar  gw  x-wing
```