AĞ TOPOLOJİLERİ

Topoloji Nedir ? Bir ağdaki bilgisayarların nasıl yerleşebileceğini,nasıl bağlanacağını,veri iletiminin nasıl olacağını belirleyen gene yapıdır.

Fiziksel Topoloji : Ağın fiziksel olarak nasıl görüneceğini belirler.(Fiziksel Katman).

Mantıksal Topoloji : Bir ağdaki veri akışının nasıl olacağını belirler.(Veri İletim Katmanı).

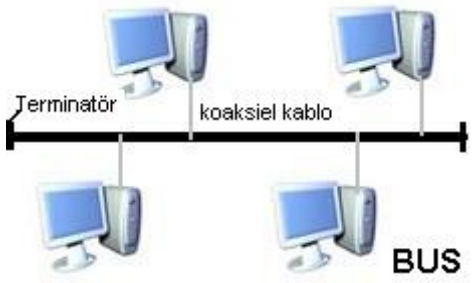
1) Yol (Bus) Topolojisi : Bütün makinelerin tek bir kabloya bağlı oldukları bir ağ türüdür.

Avantajları :

- Ağa bir bilgisayarı bağlamak daha kolaydır.
- Daha az uzunlukta kablo gerektirir

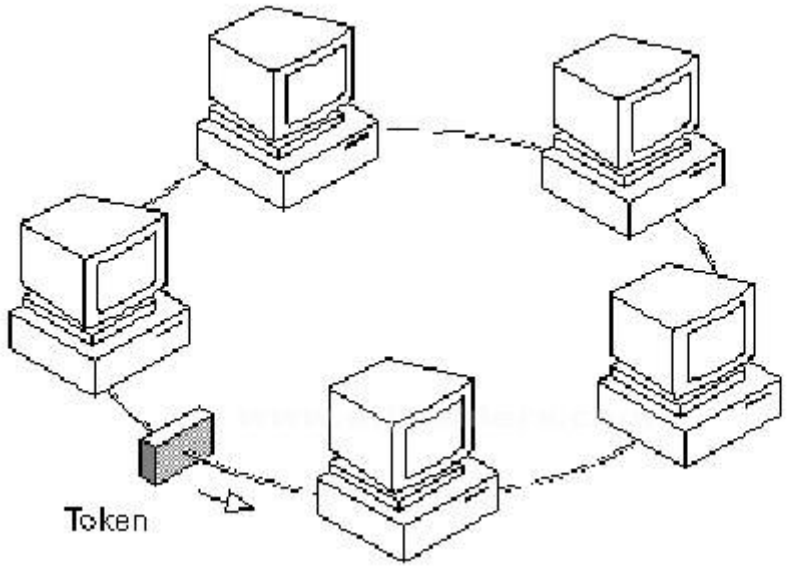
Dezavantajları:

- Hatanın yerinin belirlenmesi zor olmaktadır.
- Omurga kabloda bir bozulma veya kesilme olursa tüm ağ bağlantısı kesilir.
- Kablonun sonunda sonlandırıcı (Terminatör) olmalıdır.
- Tek başına tüm bir binanın ağ çözümü için genellikle kullanılmamaktadır.
- Çarpışma



2) Halka (Token Ring) Topolojisi:

- IBM tarafından geliştirilmiştir.
- Mantıksal olarak bir daire şeklinde tüm düğümlerin birbirine bağlanması.
- ,tüm cihazlar ağı oluşturan ve halka şeklinde dolaşan bir kabloya bağlıdırlar.
- Halka içindeki bir bilgisayar bozulursa tüm ağ bağlantısı kesilir.
- Çarpışma olasılığı düşüktür.
- Şu anda halka topolojilerinde UTP,STP kablo kullanılmaktadır.



3) Yıldız (Star) Topolojisi:

Tüm düğümlerin ortak bir merkeze (hub,swtich) bağlanmasıdır.Arızalı cihazların tespiti bu yapıda kolay olur.Hub veya Switch denilen kutulardaki yanan ışıklara bakarak hangi makinenin bağlantı sorunu olduğu daha kolay anlaşılabilir.

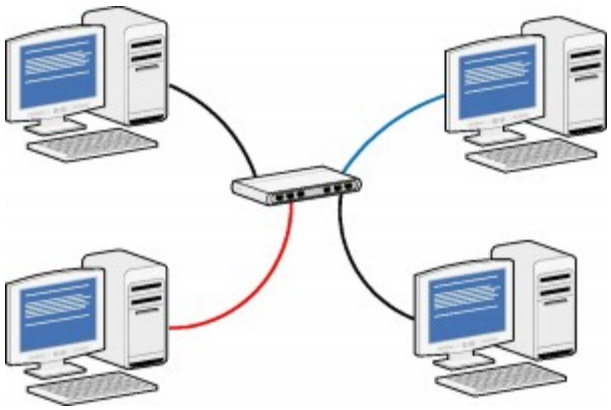
Avantjları :

- Ağı kurmak kolaydır.
- Bir bilgisayara bağlı kablo bozulduğunda ağın çalışması etkilenmez.
- Ağdaki sorunları tespit etmek kolaydır.

Dezavantajları:

- Hub kullanıldığında ağ trafiği artar.
- Doğrusala göre daha fazla kablo gerektirir.
- Hub veya swich bozulduğunda tüm ağ çalışmaz hale gelir.
- Hub ve switch gibi cihazlar nedeniyle doğrusala göre kurulumu daha pahalıdır.

Not: Hub,veriyi taşır ve ne olduğunda bakmaz.Switch ise veriye bakar ve veri trafiği daha hızlıdır.Çarpışma olmaz.



4) Ağaç (Tree) Topoloji:

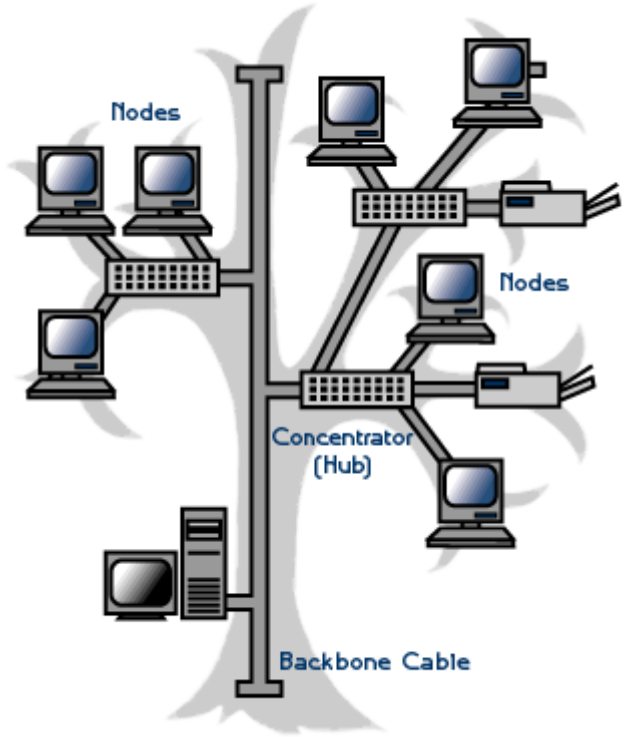
Genellikle yıldız topolojisindeki ağları birbirine bağlamak için kullanılır.Böylece ağlar büyütülebilir.Bir ağacın dalları farklı topolojilerdeki ağları temsil eder,ağacın gövdesi ile de bunlar birbirine bağlanır.

Avantajları:

- Her bir bölüme ulaşmak (segment) kolaydır.
- Bir çok çalışma grubu bir araya getirilebilir.

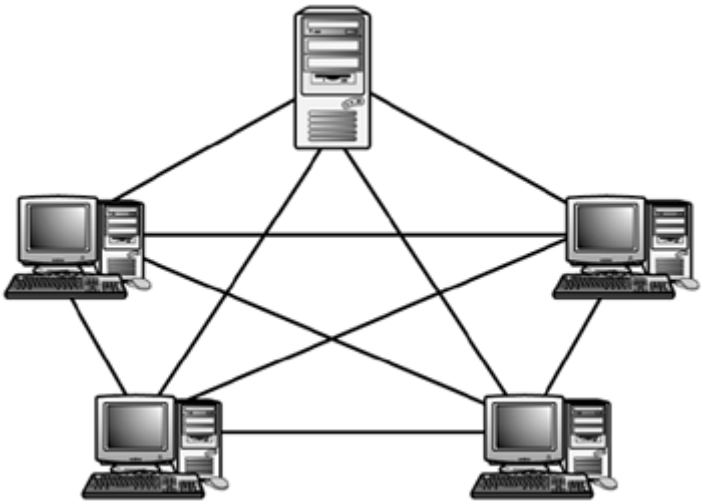
Dezavantajları:

- Her bir bölümün uzunluğu kullanılan kablo ile sınırlıdır.
- Omurga kablosu bozulduğunda bölümlerdeki ağ trafiği etkilenir.
- Kurulumu ve düzenlenmesi daha zordur.



5) Karmaşık (Mesh) Topoloji:

- Her noktanın birbirine bağlandığı çok güvenli bir network sistemi olan mesh yerleşim biçimi tamamen yada kısmen oluşturulabilir.Mesh yerleşim birimine pek rastlanmaz.
- Daha çok WAN'da kullanılır.
- Gerçek Mesh topolojide tüm düğümler ağ içerisinde birbirine bağlıdır.
- LAN'da kullanıldığında tüm düğümlerin birbirine mutlaka bağlı olması gerekmez.



Temel Ağ Cihazları

Birden fazla bilgisayarın bilgi paylaşımı, yazılım ve donanım paylaşımı, merkezi yönetim ve destek kolaylığı gibi çok çeşitli sebeplerden dolayı birbirine bağlandığı yapıya ağ (network) denir. Ağ yapılarını oluşturmak için çok çeşitli ağ cihazları kullanılabilir. Ağ yapılarında kullanılan başlıca cihazlar:

- Göbek (Hub)
- Anahtar (Switch)
- Tekrarlayıcı (Repeater)
- Köprüleyici (Bridge)
- Yönlendirici (Router)
- Güvenlik Duvarı Cihazları (Firewall)
- Erişim Noktası (Access point)
- NIC (Ağ Ara Birim Kartı)
- Modem

Göbek (Hub) : En basit ağ cihazlarından biridir. Kendine ait bir güç kaynağından beslenerek çalışır. Ağ sistemlerinde sinyallerin yeniden oluşturmasını ve yeniden zamanlanmasını sağlar. Kendisine bağlı olan bilgisayarlara paylaşılan bir yol sunar. (Kendisine gelen datayı bütün portlara gönderirler.) Bundan dolayı aynı anda haberleşmek isteyen ağa bağlı cihazların, hattın boşalmasını beklemeleri gerekir. 8 ile 24 arasında değişen port sayısına sahip cihazlardır. Bu cihazlar ağ yapılarında genellikle merkezi bir nokta oluşturmak ya da ağın güvenliğini arttırmak gibi amaçlarla kullanılırlar ve sadece bit düzeyinde işlem yapmalarından dolayı OSI modelinde 1. katman cihazlarıdır. Göbek cihazları için iki farklı sınıflandırma yapılabilir. Bu cihazlar genel olarak aktif ya da pasif olmak üzere 2 grupta incelenebilir. Aktif göbekler, gelen sinyali güçlendirerek çoklu kullanıcı ortamı için bölerken, pasif göbekler ise gelen sinyali güçlendirmeden sadece çoklu kullanıcı ortamı için bölerler. Bundan dolayı pasif göbekler kablo uzunluğunu arttırmak amaçlı kullanılmazlar.

Anahtarlama Cihazı (Switch) : Anahtarlama cihazları da göbek gibi kendisine bağlı bilgisayarlara yol sunar. Ancak göbek cihazlarından farklı olarak anahtarlamalı olarak yol sunarlar. Ağ yapısına dahil iki bilgisayar birbiri ile haberleşirken anahtarlama özelliğinden dolayı diğer bilgisayarlar da aralarında iletişim kurabilirler. Bundan dolayı göbek cihazlarına göre daha yüksek performans gösterirler. 8 ile 48 arasında değişen port sayısına sahip ve şaseli modelleri vardır. Şaseli anahtarlarda gerektiğinde port eklenebilir. OSI modelinde 2. katman cihazlarıdır. Paketleri MAC adreslerine göre yönlendirirler ve MAC adreslerine bağlı çarpışma alanları ayırırlar. Ağları birbirinden yalıtılmış kanallara bölerler ve özel bir durum olmadığı sürece gönderilen paket diğer kanallara karışmadığından trafiği bozmaz.

Tekrarlayıcı (Repeater) : Tekrarlayıcılar, bir ethernet segmentinden aldığı elektriksel veriyi yenileyerek ve ikili koda dönüştürerek diğer segmente ileten ağ cihazlarıdır. Bu yönüyle tekrarlayıcı(repeater), hem sinyal gücünün arttırılmasını, hem de elektriksel olarak bozulmuş sinyallerin iyileştirilmesini sağlar. Tekrarlayıcılar, telefon, telgraf, mikrodalga, optik haberleşme gibi pek çok sistemde kullanılmaktadır. Tekrarlayıcılar da göbekler gibi sadece bit seviyesinde işlem yaptıklarından OSI modelinde 1. katman cihazlarıdır.

Köprü (Bridge) : Köprüler aynı protokolü kullanan iki veya daha fazla bağımsız ağı birbirine bağlamak için kullanılan ağ cihazlarıdır. İki bağımsız ağ arasına konularak her iki tarafa da aktarılmak istenen verileri inceler. Eğer veri adresi ağdaki bir adres ile örtüşüyorsa verinin o ağa geçmesine izin verir; aksi durumlarda ise verinin ağa geçmesine izin vermez.

Yönlendirici (Router) : Programlanabilir ve gerekli ayarlar yapıldığında uzak bir ağa erişmek için mevcut birden fazla yol arasında kullanılabilecek en iyi yol (Best Determination Path) seçimini yapabilen ağ cihazlarıdır. Yönlendiriciler, bütün ağları ya da ağ bölümlerini birbirine bağlayabilir. OSI modelinde 3. katman cihazı olan yönlendiriciler gerekli arayüz modülleri kullanılarak OSI modelinde 2. katmanda çalışan birbirinden farklı iki ağ cihazını birbirine bağlayabilir. Sadece ağ adresi bilinen verilerin aktarılmasına izin vererek ağ trafiğini azaltırlar. Genel olarak dinamik yönlendiriciler ve statik yönlendiriciler olarak ikiye ayrılırlar. Dinamik yönlendiricilerde, rotalar otomatik olarak biçimlendirilir ve veri için en iyi rota yönlendirici tarafından seçilebilir. Statik yönlendiricilerde ise rotalar elle biçimlendirilir ve hep aynı rota kullanılır. Statik yönlendiriciler, dinamik yönlendiricilere göre daha güvenlidir. Dinamik yönlendiricilerde güvenliği arttırmak için elle biçimlendirme tercih edilebilir.

Güvenlik Duvarı (Firewall) : Özel ağlar ile İnternet arasında her iki yönde de istenmeyen trafiği önlemek amacı ile kullanılan ağ cihazlarıdır. Verimli olarak kullanılabilmeleri için İnternet ile özel ağ arasındaki tüm trafik cihaz üzerinden geçmeli ve gerekli erişim listeleri uygun bir stratejide hazırlanmış olmalıdır.

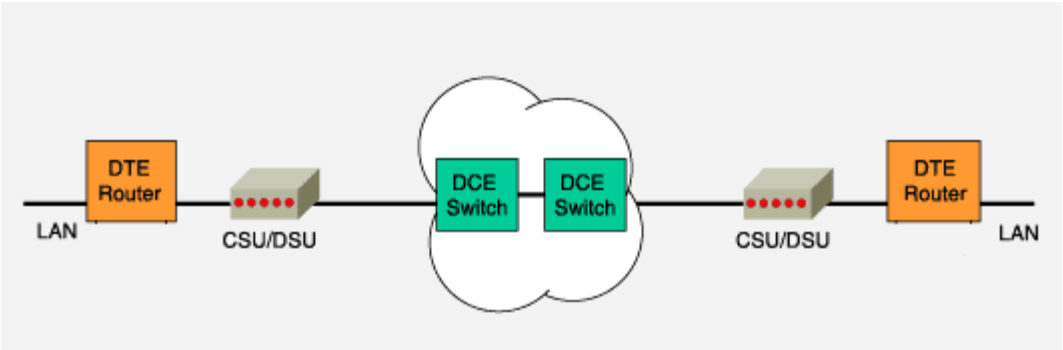
Access Point (Erişim noktası) : Erişim noktası cihazları kablolu bir ağa kablosuz erişim yapılmasını sağlayan cihazlardır. Göbek, anahtarlayıcı ya da kablolu yönlendiricilere takılarak kablosuz iletişimin sağlanması için gerekli sinyallerin oluşturulmasını sağlarlar. Bununla birlikte erişim noktaları, kablosuz ağ sinyallerinin güçlendirilerek kablosuz ağın etkin olduğu mesafenin artırılması amacıyla da kullanılabilir. Kablosuz iletişim özelliği olan yönlendiricilerin kullanıldığı sistemlerde, access point(erişim noktası) kullanımına gerek yoktur.

NIC (Ağ Arabirim Kartı) : Bilgisayarın bir ağa bağlanmasını sağlayan donanımdır. Genel olarak verilerin elektriksel sinyallere veya elektriksel sinyallerin verilere dönüştürülmesini sağlarlar. Bilgisayarın özelliklerine göre anakartla bütünleştirilmiş halde olabilir ya da anakart üzerindeki herhangi bir çevresel yuvaya takılı olabilir. Ağ arabirim kartı, ağda kullanılacak protokol çeşidi, sistem veriyolu ve fiziksel bağlantı çeşidine uygun olacak şekilde seçilmelidir. Ağ ara birim kartları kablo aracılığı ile ya da kablosuz olarak modem ile bağlantı kurarlar. OSI modelinde 1. ve 2. katmanda çalışırlar. Ağ arabirim kartları genel olarak 2 grupta incelenebilirler. Ethernet arabirim kartları kullanılan kablonun özelliğine göre aldıkları elektriksel sinyalleri ya da ışık dalgalarını sayısal verilere çevirir. Kablosuz (Wireless) arabirim kartları ise aldıkları elektromanyetik dalgaları sayısal verilere çevirir.

Modem : Bilgisayarın telefon hatları ile bağlantısını sağlayarak bilgisayarın ağa bağlanmasını sağlayan cihazlardır. Bilgisayardan aldıkları digital verileri analog sinyallere dönüştürerek telefon hatlarına aktarılmasını sağlarlar. Harici olarak bilgisayara takılarak kullanılırlar. Modemler genel olarak 4 grupta incelenebilirler.

- Analog modemler, ethernet kartından gelen dijital verileri telefon hatlarında iletilen analog işaretlere ya da telefon hatlarından gelen analog verileri sayısal verilere çevirirler. Günümüzde masaüstü ve dizüstü bilgisayarların İnternet erişimlerinin sağlanması için sıklıkla kullanılırlar.
- Dijital modemler ise verinin sayısal yapısı bozulmadan ulaşması istenen noktaya ulaştırırlar.
- ADSL modemler ise yapı itibari ile dijital ve analog modemlerden biraz daha farklıdır. ADSL sisteminde, bilinen bakır kablolama alt yapısı kullanılır. Telefon hattının her ucuna bir ADSL modem eklenerek veri alma (download), veri gönderme (upload) ve POTS (Plain Old Telephone Service – Düz Eski Telefon Hizmeti) olarak adlandırılan geleneksel telefon servis kanalı olmak üzere 3 farklı kanal oluşturulur. Normal telefon görüşmelerinizi yaparken 0 kHZ ile 4 kHz arasında değişen frekans aralığı kullanılırken, ADSL data iletimi için 4 kHz ile 1100 kHz aralığını kullanıldığından için İnternete bağlıyken aynı anda telefon görüşmesi yapmaya olanak sağlar.ADSL modemler sayısal verileri analog verilere çevirmeden doğrudan olduğu gibi iletir. Sistem asimetrik olarak çalıştığından veri alma ve veri gönderme için kullanılan bant genişlikleri birbirinden farklıdır.

- CSU/DSU modemler ise yerel alan ağlarında kullanılan veri çerçeveleri (data frame) geniş alan ağı çerçevelerine veya geniş alan ağı çerçevelerinini yerel alan ağı çerçevelerine dönüştürmek için kullanılır. Ayrıca geniş alan ağlarında verinin iletiminin sağlanması için veri iletiminin yapılacağı hattın iki ucunda saat darbesi (clock rate) değerlerinin aynı olması gerekir. Geniş alan ağı sistemlerinde saat darbesi değeri bu cihazlar tarafından belirlenir.



TCP/IP PROTOKOLÜ
TCP/IP NEDİR?
Protokol bir iletişim sürecinde bu bağlantıyı sağlayan noktalar arasındaki gidip gelen mesajlaşmayı düzenleyen kurallar dizisidir. Bu protokoller birbirleriyle iletişim içinde bulunan gerek donanım gerekse yazılımlar arasında oluşur. İletişimin gerçekleşmesi için her öğenin bu protokolü kabul etmiş ve uyguluyor olması gerekir.

TCP/IP 'de bu şekilde oluşan yüzden fazla bilgi iletişim protokolün toplandığı bir protkoller ailesidir. Bunlardan en önemlileri TCP (transmission control protokol) ve IP (ınternet protokol) olduğu için bu ismi almıştır.

Bir bilgisayar ağında kullanılan protokol ne olursa olsun aslında bilgisayarlar fiziksel adresleri ile birbirlerini tanır ve iletişimde bulunurlar. Bu fiziksel adres ağ kartı veya ağa bağlanmayı sağlayan herhangi bir donanım içinde hiçbir şekilde değiştirilmesi mümkün olmayan 48 bit olan bir numaradır. TCP/IP protokolünde diğer bilgisayarlardan farklı olarak her bilgisayar bir IP numarası alır.

Görünüşü 194.62.15.2 şeklindedir. İnternette bulunan her bilgisayarın kendine ait bir IP numarası vardır ve sadece ona aittir. IP adresleri 32 bitlik düzendedirler ama kolay okunabilmeleri için 8 bitlik 4 gruba ayrılmışlardır.

Internet üzerinde veri alış verişi yapan alıcı ve göndericiyi tanımlamaktadırlar. Veriler gönderilirken mutlaka gönderenin IP adresini taşırlar. Alıcının adresi de adresteki domain adrese göre çözümlenir ve gönderilir.

IP adres yapısının 2 bölümü vardır. Birincisi bilgisayarın bağlı olduğu özel bir ağın numarası ikincisi ise bilgisayarın özel numarasıdır. Veriler dolaşım sırasında router denilen yönlendiricilerden geçerken sadece bu özel ağın numarasına bakılır. IP adresleri a,b,c,d,e adı verilen beş sınıfa ayrılmıştır. A sınıfı adresleri ilk " oktet" ile belirlenir ve 2 ile 126 arasında olmalıdır. Örneğin 124.0.0.0 A sınıfı bir IP'dir. Aynı şekilde B ilk iki oktetle belirlenir ve ilk okteti 129 ile 91 arasındadır. C sınıfı ise ilk 3 okteti kullanır ve ilk okteti 192 ile 223 arasındadır. D ve E sınıfı IP 'ler ise kullanılmazlar zira sadece test amaçlıdırlar.

Bir örnek vermek gerekirse siz ISS' a telefon hattı ile bağlandığınızda ISS' nin ağına dahil oluyorsunuz. Daha evvel alınmış olan IP adresi havuzundan size bir IP adres veriliyor. Mesela IP adresiniz 194.62.15.2 ise, ISS nizin aldığı IP adresinin sınıfı C dir. Yani ilk 3 oktat içinde bulunduğunuz ağı , sonda bulunan oktat da sizin bilgisayarınızın o andaki adresini temsil eder.

ROUTER
Router internet üzerinde kullanılan paketleri varış oktalarına giderkenki bir sonraki uğrak noktalarını belirleyen bir donanım veya kimi zaman bir yazılımdır.

Router en az iki ağı birbirine bağlar ve paketlerin hangi yönde gideceğine bağlı olduğu ağların yapılarına ve durumlarına göre belirler. Routerlar olası her türlü yön hakkında ilgileri ve durumlarına ilişkin bir tablo oluştururlar. Bu bilgiyi paketlerin iletilmesi sırasında en güvenli ve en masrafsız yolu hesaplayarak yönlendirme işlemini gerçekleştirir.

INTERNET PROTOKOLÜ IP
Internet'te herhangi bir veri gönderirken veya alırken, örneğin e-posta yada web sitesi , mesajlar küçük paketlere bölünür. Her paketin üzerinde gönderenin ve alıcının IP adresleri

yazılı olarak bulunur. Her paket öncelikle bir “gateway” adı verilen bilgisayardan geçer. Bu bilgisayar paketlerin üzerindeki alıcının adresini okur ve buna göre paketleri yönlendirir. Bu işlem alıcının adresine en yakın bilgisayara kadar böyle devam eder. Bu en son bilgisayarda paketlerialıcı bilgisayar gönderir. Internet protokolüne göre yol alan bu paketler bir çok değişik yönden giderek alıcıya ulaşabilirler. Hatta paketler olması gerektiği sırada da alıcıya ulaşmayabilirler. Internet protokolünün amacı sadece bu paketleri göndermektir. Paketleri aski düzenine getirmek bir başka protokolün yani TCP nin görevidir.

DOMAIN NAME SYSTEM

IP adreslerinin ezberlenmemesinin zorunluluğu nedeni ile genellikle bilgisayarlar : “ host” adları ile anılırlar. Yani internet üzerindeki her bilgisayarın bir IP adresi bir de host ismi bulunur. Fakat iletişimin sağlanması için bu isimlerin tekrardan IP adreslerine çevrilmeleri gerekir. Bu yüzden bu çevirme işlemini yapması amacı ile DNS (domain name system) kullanılır. DNS internette bulunan her IP adresinin ve alan adını barındıran bir veri bankasıdır.bu sistem öyle korulmuştur ki bu veri tabanı bilirle kriterlere göre ayrılır ve sınıflandırılır.

Bir bilgisayarın alan adı isim.com şeklindedir. Ayrıca bulunduğu ülkeye göre sonunda ülkenin kodu da eklenir. Örneğin Türkiye’de bulunan bir alan adı şu şekilde olacaktır. “isim.com.tr”

Bu her alanla ilgili birer DNS sunucusu vardır. “Tr” domain’ ini alan bütün bilgisayarların listesi bir sunucuda tutulur. Örnek olarak sonu .com ile bitenler Amerika’da bir DNS sunucu bilgisayarda tutulur. Bu adresler sondan başa doğru ayrıştırılır. Yani “isim.com.tr” alan adı önce “tr” adına göre ayrılır ve diğer aynı adlı bilgisayarla birlikte düzenlenir. Eğer sonunda bir ülke kodu yoksa ki sadece Amerika’daki bilgisayarlar için geçerlidir direct “.com” adına bakılarak ayrıştırılır. Bunlara üst düzey domain de denilir.

.com Ticari Şirketler
.edu Eğitim kurumları
.org Ticari olmayan organizasyonlar
.net İnternet omurgası görevini üstlenen ağlar
.gov Hükümete bağlı kurumlar
.mil Askeri kurumlar

Bilgisayarımızda bir adres girdiğimiz zaman bu bilgiler direk olarak ilgili DNS sunucusuna ulaştırılır. Bu DNS sunucusu eğer bu bilgisayarın bilgisini içeriyorsa DNS istemcisine hemen ilgili adresin IP adresini ulaştırır.

ARP ADDRESS RESOLUTION PROTOKOL

Daha evvel bir ağ üzerinde gerçekte bütün iletişimin fiziksel adresler üzerinde gerçekleştiğinden bahsetmiştim. Yerel bir ağ üzerinde IP adresleri belirlenmiş bilgisayarlar mesajlaşmaya başlamadan önce normalde IP adresinin sahibinin fiziksel adresini sorgulamaya gelen bir yayın yaparlar. IP adresine sahip bilgisayar kendi fiziksel adresini içeren bir mesajı istemci bilgisayara gönderir ve böylece gerçek veri gönderimi bu adres üzerinden yapılmış olur.

IP ROUTING

Paket net ortamında yönlendirilmesi ve gönderilmesi işlemi internet protokolünün görevidir. Paketlerin üzerinde yazılı olan adreslere bakarak bunu bir yönlendirme tablosundaki bilgilerle karşılaştırılır ve yönlendirmeyi yapar. Bu tablonun oluşturulması görevi ise routing protokol ‘un görevidir. Routing protokolünde çeşitleri vardır. Ama bunlardan sadece bir tanesi internet yönlendirme domain ‘leri arasında bilgi alışverişi yapar.

ICMP
İnternet control message protocol

Bu protokol internet protokolün veri iletişimi sırasında beklenmedik bir olay gerçeklemesi halinde göndereni uyarma görevi üstlenmiştir. ICMP mesajlarına örnek vericek olursak:

Destination unreachable: bu mesajvarış noktası olan alıcı host'un erişilmez olduğunu belirtmek için kullanılır. Yani ağ tanımsız ya da ulaşılmaz halindedir.

Echo and echo reply: bu ik mesaj türü alıcının erişilebilir olup olmadığını anlamak için kullanılır. Gönderen bilgisayar alıcıya veri içeren bir echo mesaj atar. Karşılığında alıcı bilgisayardan cevap yani echo reply gelirse alıcı bilgisayarın ağ üzerinde erişilebilir olduğunu gösterir.

TCP
Daha önce belirttiğim gibi veriler küçük paketlere ayrılıp gönderilirken değişik yollardan ve değişik sıralar ile gönderilirler. Bu paketlerin sıralanmasını sağlayan protokolün adı TCP (transmission control protocol) 'dir. Örneğin bize gelen herhangi bir veri önce paketlere ayrılır. Bu paketleme işlemini gerçekleştiren TCP aynı zamanda bu paketleri doğru sırası ile numaralandırır ve adreslendirir, IP katmanına gönderir.artık gönderme işlemi sadece internet protokolünün elindedir. Paketler yola çıktıktan sonra birbirlerinden ayrılır ve farklı yönleri takip ederler. Bilgisayarımıza ulaştığında bizim bu paketleri bir bütün olarak ve tam sırasıyla görmemizi sağlayan gen TCP ' dir. Aynı zamanda TCP/IP 'nin en güvenilir protokol olmasını sağlayan işlevide yerine getirir. Paketlerin belirli bir kısmı ulaştıktan, eğer paketler sağlam ise, TCP bize bir onay gönderir. Eğer paketlerde bir sorun var ise bu onay gelmez ve biz bu verileri baştan göndermek zorunda kalırız. Yani diğer protokollerden farkı paketlere bir şey olması halinde biz bunu mutlaka biliriz ve eksikleri tekrardan göndermek suretiyle iletişimi kesin tamamlamış oluruz.

UDP
User datagram protokol TCP' nin aksine az güvenilir ama daha hızlı olmayı amaçlayan bir protkoldür. Bazı basit istem ve cevap ile işleyen uygulamalarda kullanılması işlemin daha hızlı gelişmesini sağlar.

UDP' nin yaptığı paket üzerinde bulunan IP numarasının yanına bir adet port numarsı eklemek ve böylece uygulamaların çalışması için gereken soketleri oluşturmak.

Internet' i oluşturan TCP/IP' nin bir başka katmanında bulunan bazı protokol ve uygulamalar şöyledir.

Telnet: "Telecommunication Network " ibaresinin kısaltılmışı kullanıcıya başka bir host a bağlanıp ağ üzerindeki diğer host lara ulaşma imkanı veren bir terminal protokolüdür.
FTP: "File transfer protocol" kullanıcıya kendi bilgisayarı ile başka bir bilgisayar arsında dosya transferi yapmasına olanak verebilen bir terminal protokolüdür.
ARCHİE: Kullanıcıya kayıtlı tüm anonymous FTP sunucularında belli bir dosyanın adını aramasına olanak veren bir araç.
GOPHER: İnsanlara mönü bazlı ve hiyerarşik bir ara yüz kullanarak veri repositories arasında arama yapılmasına olanak veren bir araç.
SMTP: "Simple mail transfer protocol " internet üzerinde elektronik olarak posta alım ve gönderim sağlayan standart bir protokol. SMTP internet üzerindeki e-posta sunucuları arasına ve herhangi bir bilgisayardan e-posta sunucusuna posta ulaşımını sağlar.

HTTP: "The hypertext transfer protocol" Internet üzerinde bilgi değişimini sağlayan baz protokol. WWW üzerinde bilgiler kullanıldığı sisteme bakmaksızın HTML formatında yazılır ve her sistem bu formatı tanır.
FINGER: Diğer kullanıcıların ya da hostlara internet üzerindeki durumunu öğrenmek için kullanılır.
POP: "The post office protocol" Bir kullanıcının e-posta programı ile sunucu arasındaki pop e-posta sunucusundan istemciye postaların alınmasını ve kullanıcıların kendi posta kutularını yönetmelerine olanak verir.
DNS: "The domain name system" Internet üzerinde buluna isimleri ve bunlara ait IP adreslerini düzenler. Aynı zamanda postaya isim sunucularında alan adları ile ilişkilendirilir.
SNMP: "The simple network management protkol" TCP/IP bazlı network araçlarını yönetmeye yönelik prosödürleri ve veri tabanlarını belirler. SNMP (RFC 1157) is widely deployed in local and wide area network.
PINK:" The packet internet groper" , bir sistemdeki kullanıcıya diğer bağlı bilgisayarların durumu ve mesajlaşma süresinde yaşanan gecikmeleri öğrenmesine olanak verir. ICMP echo mesajlarını kullanır.
WHOİS/NICKNAME: Kullanıcıya internet üzerindeki " domain " ve "domainler" hakkındaki irtibat bilgilerini derleyen veri tabanlarında arama yapma olanağı verir.
TRACEROUTE: Paketlerşn uzaktaki başka bir bilgisayara giderken ki yolunu takip edip öğrenmeye yarayan bir araçtır.

Alt Ağlara Bölme (Subneting)

Internet Protokolü (IP) vasıtasıyla haberleşmek durumunda olan tüm cihazlar bu haberleşmeyi sağlayabilmek için dinamik ya da statik mutlaka bir ip adresine sahip olmalıdırlar. Cihazlar ip adresleri vasıtasıyla diğer cihazlarla iletişim kurabilirler, ancak akış şeması sanıldığı kadar kolay değildir. Bunu bir örnek ile izah etmeye çalışalım; Bir okul düşünelim, bir öğretmen bu okulun tüm öğrencilerini tek bir sınıfta toplayıp ders verebilir mi? Oldukça güç olur değil mi, herkes konuşacak ama çok fazla gürültü olmayacak… Bu karmaşanın önüne geçebilmek için öğrenciler sınıflara dağıtılırlar ve her sınıfa bir öğretmen atanır.

Mevcut network yapısı genişleyince Broadcast etki alanı da büyüyecek ve tüm networkdeki bilgisayarlar yoğun bir Broadcast trafiğinin ortasında sıkışıp kalacaklardır. Bu da ağ performansını negatif yönde etkileyecektir.

IP adreslerini de yine aynı şekilde ortamda gürültü (Broadcast trafiği) olmaması ve iletişimin daha sağlıklı yapılabilmesi için ya da gereksinimlerden kaynaklanan çeşitli network senaryoları için alt ağlara ayırırız, bu işleme *Alt Ağlara Bölme* işlemi (*Subneting*) denilir.

Herhangi bir sınıf IP ağ adresinin uç bitlerinden bir kısmını alt ağ için ayırarak alt ağlar oluşturabiliriz.

Alt ağlara ayırma işlemi yaparken;

"-Gerek duyulan kullanıcı sayısı ve Gerek duyulan alt ağ sayısı" olmak üzere iki farklı kriter kullanalabiliriz. Genel olarak örneklerimizde gerek duyulan alt ağ sayısından yola çıkacağız.

Örneklere geçmeden önce bir kaç temel bilgiyi vermemiz gerekiyor;

a) Oktet

IP adresi, 32-Bit olarak toplam 4 bölümden (*oktet=bölüm*) oluşur ve her bir oktet 8 bitliktir. Her bir oktetin değeri onluk sistemde minimum 0, maksimum 255 olabilmektedir.

b) İkilik Sayı Sistemi

IP hesaplaması yapılırken onluk sayı sistemi ikilik sayı sistemine matematik kuralları çerçevesinde çevrilir, ancak bu konu burada bahsedilecek bir uzmanlık alanı değildir, lütfen detaylı bilgi için matematik konulu kaynakları inceleyiniz.

Ancak, size güzel bir tablo vereceğim:

7.bit	6.bit	5.bit	4.bit	3.bit	2.bit	1.bit	0.bit	Toplam 8 bit
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	Onluk karşılığı böyle hesaplanır
128	64	32	16	8	4	2	1	Onluk sistemdeki karşılığı
0	0	0	0	0	0	0	0	Onluk değeri 0 olan bir oktet
1	1	1	1	1	1	1	1	Onluk değeri 255 olan bir oktet
1	1	1	0	0	0	0	0	Onluk değeri 224 olan bir oktet

Yukarıdaki tabloya dikkat edecek olursanız, son satırda "1" bit değerine sahip olan onluk değerlerin toplanarak 224 oktet değerinin olarak ortaya çıktığını görebilirsiniz.

c) IP Adres Sınıfları

A sınıfı: 1 – 126 Öngörülen Ağ Maskesi:255.0.0.0

B sınıfı: 128 – 191 Öngörülen Ağ Maskesi:255.255.0.0

C Sınıfı: 192 – 223 Öngörülen Ağ Maskesi:255.255.255.0

D sınıfı: 224 – 239 Çoklu yayın (Multicast)

E sınıfı: 240 – 254 Araştırma için ayrılmıştır.

127: Loopback olarak ayrılmıştır ve bu sınıfların hiçbirisine dahil edilmemektedir.

172.16.122.204 ip adresi için Oktet ayrımı;

1.Oktet: 172 (Onluk) = 10101100 (İkilik)

2.Oktet: 16 (Onluk) = 00010000 (İkilik)

3.Oktet: 122 (Onluk) = 01111010 (İkilik)

4.Oktet: 204 (Onluk) = 11001100 (İkilik)

d) Network ID (Ağ Adresi)

172.16.122.0 yukarıdaki ip için ağ adresidir; "Aynı sınıf adresine sahip olan bilgisayarları temsil eden ve o grupta bulunan bütün bilgisayarlarda aynı olan bölümdür, IP olarak herhangi bir cihaza atanamazlar."

e) Broadcast Adresi

172.16.122.255 yukarıdaki ip için broadcast adresidir; “Herhangi bir ağda bütün adresleri temsil etmek için kullanılan adreslere Broadcast adres denir. Broadcast adresinin uç bölümünün bütün bitleri ağ adresinin tersine 1’dir.” Bu adresler de ağ adresi gibi ağdaki herhangi bir bilgisayara IP adresi olarak atanamazlar.

Network ID (Ağ Adresi) Nasıl bulunur?

Ağ adresi konusu biz sistemcilerin ve özellikle network işi ile içli dışlı olanların bilmesi gereken olmazsa olmaz bir konudur. Bir ip adresinin ağ adresini bulabilmek için; o ip adresi ile kendi Ağ Maskesinin (Subnet Mask) *“And / Ve”* işlemine tabi tutulması gerekmektedir. IP adresi ve Subnet mask ikilik sayı sistemine çevrilerek alt alta yazılır, her iki taraftada ‘1’ bit değerine sahip bölümler aynen (yani 1 olarak) aktarılır, diğerleri ise 0(sıfır) olarak değerlendirilir. Bir örnek verecek olursak;

Ip Address:	132.15.78.202	10000100	00001111	01001110	11001010
Subnet Mask:	255.255.0.0	11111111	11111111	00000000	00000000
Network ID:	132.15.0.0	10000100	00001111	00000000	00000000
Broadcast Address:	132.15.255.255	10000100	00001111	11111111	11111111

Network ID Karşımıza nerede çıkar?

Burada yazacağım örnekleri incelediğinizde Ağ adresinin nerede ve nasıl karşınıza bekçi gibi dikileceğini anlamış olacağınızı düşünüyorum. Ancak burada ikilik sayı sistemini kullanmayacağım, ben örneklerimi onluk sayı sisteminde anlatacağım.

Örnek-1: 192.168.10.17 ip adresine sahip bir terminal, yine kendi yerel ağında bulunan 192.168.10.18 ip adresli bir terminale erişmek istesin ve her ikisinin de Ağ Maskesi: 255.255.255.240 olsun.

Ağ adreslerine bakalım;

Client1 IP Adress	192.168.10.17
Subnet Mask:	255.255.255.240
Network ID:	192.168.10.**16**

Client2 IP Adress	192.168.10.18

Subnet Mask:	255.255.255.240
Network ID:	192.168.10.**16**

.17 ve .18 IP adreslerine sahip bilgisayarların aynı yerel ağ içinde konumlandırıldığını hatırlayalım. Yukarıdaki tabloda *And* işlemlerinde gördüğünüz gibi ağ adresleri aynıdır.

.17 olan pc, .18 e ulaşmak istediği zaman .18' in bulunduğu ağ adresini hesaplar ve görür ki ağ adresleri aynıdır. Sonra şunu der; "Hımm… demek bu bilgisayar ile ben aynı yerel ağ(LAN) içerisindeyim

(Local Area Network: LAN), o halde ağ geçidine gidip bu ip nin yerini sormaya gerek yok."

Sonuç: Haberleşme sağlanır, çünkü aynı ağ adresine sahipler.

Örnek-2:

Bu defa, farklı yerel ağlarda bulunan 192.168.10.17 ip adresine sahip bilgisayar 192.168.10.33 ip adresine sahip bilgisayara ulaşmak istesin ve Subnet Mask yine 255.255.255.240 olsun;

Ağ adreslerine bakalım;

Client1 IP Adress	192.168.10.17
Subnet Mask:	255.255.255.240
Network ID:	192.168.10.**16**

Client1 IP Adress	192.168.10.33
Subnet Mask:	255.255.255.240
Network ID:	192.168.10.**32**

(.17 ip adresli PC, .33 e ulaşmak istediği zaman .33 ü ve kendi ağ maskesini And işlemine tabi tutarak 33 ip'li PC nin hangi ağ adresinde olduğunu çözecek.)

.17 ip adresine sahip terminal, .33 ip adresine sahip olan terminalin ağ adresini hesapladı (192.168.10.**32)**ve bu Ağ adresi ile kendi Ağ Adresinin aynı olmadığını gördü, "Hımm, demek bu benim yerel ağda değil, o halde ben ağ geçidine gidip bir sorayım" der… Ve Router da

(ağ geçidi) 192.168.10.17 ip adresine sahip bilgisayarı 192.168.10.33 e götürür ve böylece haberleşme sağlanır.

Router bu iyiliği neden yaptı? Zira, görevi bu yönlendirmeyi yapmaktır. Adı üzerinde Router: Yönlendirici.

Dikkat: Demek ki Router, Ağ Adresi aynı olunca bir görev üstlenmiyor ama ağ adresleri farklı olunca görev alıyor.

Örnek-3: Yine, *farklı yerel ağlarda* bulunan 192.168.10.17 ip adresine sahip bilgisayar, 192.168.10.33 ip adresine sahip bilgisayara ulaşmak istesin, fakat bu kez Ağ Maskeleri 255.255.255.0 olsun!

Ağ adreslerine bakalım;

Client1 IP Adress	192.168.10.17
Subnet Mask:	255.255.255.0
Network ID:	192.168.10.0

Client2 IP Adress	192.168.10.33
Subnet Mask:	255.255.255.0
Network ID:	192.168.10.0

192.168.10.17 li ip 192.168.10.33 e ulaşmak istedi ve 192.168.10.33 ün Ağ Adresini hesapladı, baktı ki Ağ Adresleri aynı, "Demek ki bu benim ile aynı LAN içerisinde yer alıyor."

Ama nafile, çünkü bu adresler farklı LAN larda bulunuyorlar.

192.168.10.17 li bilgisayar .33 ip li bilgisayarı aradı taradı bulamadı, Router'a da gidip sormuyor!

Sonuç: iletişim sağlanamadı.

Yani sen iletişim kurmak istiyor musun, istemiyor musun, kararını verip ağ maskeni yazıyorsun.

Yukarıdaki açıklamalardan sonra Subneting konusuna geçiş yapabiliriz;

Bilgi:

'/24' değeri; Subnet Mask'ın sahip olduğu mevcut "1" sayısını ifade eder.

2^n: "iki üzeri n" diye okunur.

>= : "Büyük eşit" diye okunur.

***** "2^n-2>=Alt ağ sayısı" formulü ile n değeri bulunur. Bu n değeri, alt ağ bitini verecektir, yani burada bulunan değer öngörülen Subnet Mask'a eklenecek olan 1 lerin kaç tane olduğunu ifade eder.

Ekleme yapıldıktan sonra bulunan Subnet Mask, yeni Subnet Mask olacaktır.

(Yeni Subnet Mask: Eski Subnet Mask + n) |n:network, m: machine|

* 2^m-2 formulü ile bir aralığa atanabilecek ip sayısı bulunur, m değeri oktette kalan 0 sayısı kadardır. [m = host sayısı(uç bit)]

Örnek4:

192.168.0.0/24 ip aralığını 2 subnet (alt ağ) olacak şekilde ayıralım.

2^n -2 >=2 [subnet(alt ağ) sayısı] formulü ile n değerini 2 olarak buluruz.

2^2=4 ==> Mecburen 4 subnet' e bölmemiz gerekir.

N değeri artan bit değeridir. Yukarıdaki ip adresi C sınıfı bir ip adresi olduğundan öngörülen Ağ maskesi hesaplamadan önce:255.255.255.0 olacaktır.

Yeni(ortak) subnet mask: 255.255.255.11000000 (192) şeklinde olacaktır.

Bu durumda m:6 olacaktır. (8-n=>8-2=6) 2^6=toplam 64 ip (her alt ağ için)

Oktette kalan sıfır sayısı bize host id(m) yi verir, toplam 6 sıfır vardır ve bu durumda

2^6-2=62 (2^m-2) tane ip atanabilir.

X 1.Subnet	192.168.0.0	to	192.168.0.63
2.Subnet	192.168.0.64	to	192.168.0.127
3.Subnet	192.168.0.128	to	192.168.0.191
X 4.Subnet	192.168.0.192	to	192.168.0.255

2.Subnet kullanılabilir ilk subettir.

192.168.0.64 ip si 2.Subnet'in Network ID sidir ve ip olarak bir cihaza atanamaz.

192.168.0.127 ip si 2. Subnet'in Broadcast adresidir ve ip olarak bir cihaza atanamaz.

3.Subnet ise kullanılabilir son subnettir.

3.Subnet için Network ID: 192.168.0.128 and Broadcast Address: 192.168.0.191

Farklı kaynaklarda 2^n -2 formulü yerine 2^n formülünün kullanıldığını görebilirsiniz, ancak bu formüllerden bir tanesi yanlıştır denilemez.

Cisco'nun IOS-12 öncesi cihazlarında desteklenmediğinden dolayı 1.Subnet ve 4.Subnet kullanılamaz subnetlerdir. Her ne kadar IOS-12 ve sonrası sürümlerde bu subnetler kullanılabilir olsalar da, Cisconun 2008 eğitim dökümanlarına ve sınavlarına bakıldığında halen 2^n-2 formülünün esas alındığı görülmektedir. Bu nedenden ötürü makalemde hesaplama yapmayı uygun gördüm.

Örnek5:

172.17.128.255/18 adresinin sahip olduğu network id ve broadcast adresini bulalım;

Yukarıdaki ip adresi B sınıfı bir ip adresidir ve default ağ maskesi 255.255.0.0 dır. Ağ maskesinde iki tane 255, 8 + 8 =16 tane "1" değerine sahip olmak anlamına gelir. Yukarıdaki /18 değerinden 16 yı çıkardığınızda 2 bitin fazladan eklendiğini görürsünüz ki bu da yukarıdaki örneklerden hatırlayacağınız gibi artan bit değeridir. N=2 => 2^2=4 subnet e bölerek network id ve broadcast adresini bulalım;

N:2 ise m=6 olur 2^6=64

X 1.Subnet	172.17.0.0	to	172.17.63.255
2.Subnet	172.17.64.0	to	172.17.127.255
3.Subnet	172.17.128.0	to	172.17.191.255
X 4.Subnet	172.17.192.0	to	172.17.255.255

Yukarıdaki tabloda 3.Subnet e dikkat edecek olursanız 172.17.128.255 ip sinin 3.Subnet e ait olduğunu hemen görebilirsiniz. Bu durumda;

Sonuç: 172.17.128.255/18 için Network ID:172.17.128.0 – Broadcast Address: 172.17.191.255 olarak tespit edilir.

Subnet Mask: 255.255.192.0 dır.

Örnek6:

10.0.0.0/8 ip aralığı için 2 subnet oluşturalım.

2^n -2>=2 n=2 bit olarak bulunur.

255.192(11000000).0.0

m=6, 2^6=64

X 1.Subnet	10.0.0.0	to	10.63.255.255
2.Subnet	10.64.0.0	to	10.127.255.255
3.Subnet	10.128.0.0	to	10.191.255.255
X 4.Subnet	10.192.0.0	to	10.255.255.255