Temel Ağ (Network) Kavramları

Ağ (network) kavramı, var olan kaynakların kullanıcılar tarafından beraber kullanılması, bilgiye ortak ulaşmaları ve buna bağlı olarak da maliyet ve zaman tasarrufu sağlanılması gereksiniminden ortaya çıkmıştır. Bu temel kuraldan hareketle oluşan ağlar günümüzde uzaktaki bilgiye erişim (Web), kişisel iletişim (E-mail, ICQ, IRC, Video-konferans), interaktif eğlence (Web-Tv, oyunlar) gibi kavramlarla hayatımızda önemli bir yer kaplamaktadır. Bir ağın oluşabilmesi için minimum iki makineye, bunlara takılı olarak ağ kartlarına ve de bağlantıyı sağlamak içinde kabloya ihtiyaç vardır.

Ağların Gelişimi ve Ağ Teknolojileri

Ana Makine (MainFrame) Modeli:

Ağ kavramı ilk olarak Ana Makine (MainFrame) teknolojisi ile ortaya çıkmıştır. Ana makinenin kendi işlemcisi (CPU), sabit diski (harddisk), ve bunları kumanda etmek için bir ekranı ve klavyesi ve de terminallere bağlı seri portları vardı. Bu aptal terminaller (dumb terminal) sadece ekran ve klavyeden oluşurdu, yani bir deyişle pasif makinelerdi. Terminallerin yerel bir disk alanları da olmadığı için bilgiyi ana makine üzerinde saklarlardı. Tüm yük ana makinenin üzerindeydi ve bu yüzden çok pahalıydı. En büyük dezavantajı tabii ki güvenilir olmaması, yani ana makinede çıkacak bir sorunun tüm sistemi etkilemesi, terminallerin kendi başlarına işlem yapabilme kaabiliyetlerinin olmaması idi. Bu önemli sorun halen çok popüler olan İstemci/Sunucu (Client/Server) modelinin doğmasına yol açtı.

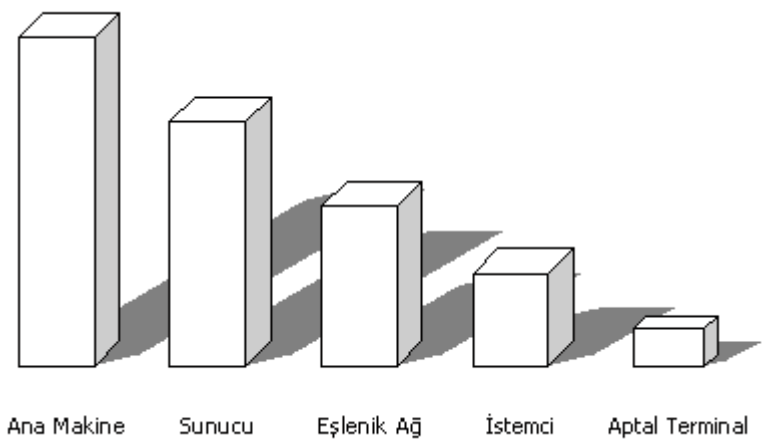
İstemci / Sunucu (Client/ Server) Modeli:

İstemci/Sunucu modeli ile pasif terminaller yerine kendi başlarına işlemler yapabilen ve kendi sabit disklerinde programlar saklayabilen makineler geldi. Böylece her istemci kendi başlarına belirli işlemleri yerine getirebilmekte, yetersiz durumda kaldıklarında ise o işe özelleşmiş olan sunuculara başvurmakta idiler. Örneğin her istemcide ofis uygulamaları, masa üstü yayıncılık, oyun programları kullanılması buna rağmen veri tabanı ya da web gibi uygulamalarda bir sunucuya erişilmesi gibi.

Eşlenik Ağ (Peer to Peer) Modeli:

İstemci/Sunucu modelinin gelişmesi ve yaygınlaşması ile birlikte istemcilerin daha ön plana çıktığı, özelleşmiş sunuculara ihtiyaç duyulmayan ağ örnekleri de ortaya çıkmaya başladı. Bu ağlarda makineler yaklaşık özelliklerde idi ve işleyiş olarak birbirlerine üstünlük sağlamıyorlardı. Örnek; tamamen Windows 95/98 kullanan ağlar.

Ağ Teknolojilerinde Güç Sıralaması



İnternetin Doğuşu

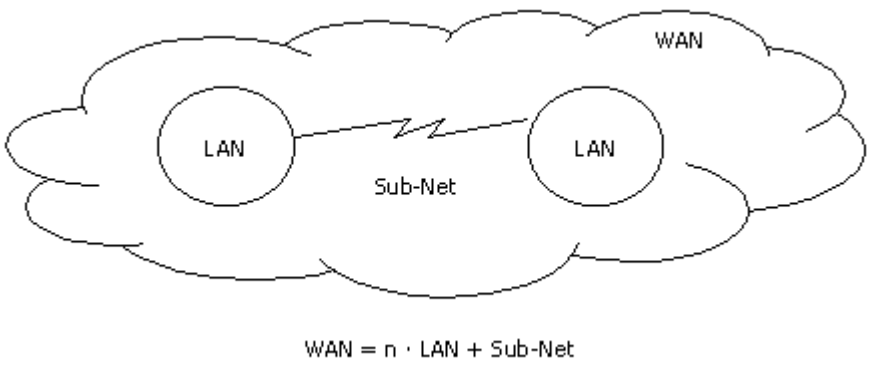
İnternet tam anlamıyla ağlar arası ağdır. Bu kavramı açmak gerekirse büyük küçük binlerce ağın birleşmesinden oluşmuş en büyük ağdır. Bir kişiye, kuruluşa, ülkeye özel değildir.
İnternet kavramı aslında 1969'da savaş sonrasında düşünülen DARPA (Defense Advanced Research Project Agency - İleri Düzey Savunma Araştırmaları Kurumu) isimli basit bir projeden ibaretti. Bu proje büyük bilgisayarları birbirine bağlamayı ve ne olursa olsun bu bağı koparmamayı amaçlıyordu. Klasik bir ağ tarzında, bu ağdaki tek bir bağlantının kopması veya ana sunucunun imha edilmesi durumunda bu ağ çökecektir. Bu yüzden teknisyenler istemci-sunucu modeli yerine her bilgisayarın birbirine eşit özelliklerde olduğu türdeş ağ modeli tercih ettiler. İlk bağlantı California ve Utah'ta olan 4 bilgisayar arasında idi. Yavaş yavaş üniversitelerin de bağlanmasıyla ağ giderek büyümeye başladı. Bu proje daha sonra ARPANET (Advanced Research Projects Agency Network) adını aldı. Sivil kişi ve kuruluşların da bağlanmasıyla tüm Amerikayı kapsamaya başladı. ARPANET in beklenenden fazla büyümesiyle askeri kısmı MILNET adıyla ayrıldı ve daha sonra da ARPANET gelişerek bügünkü adıyla INTERNET adını aldı.

Ağ Çalışma Prensipleri

Temel olarak ağlarda iki tip çalışma prensibi vardır:
Yayın (Broadcast): Ağa atılan bir paketin her bilgisayara gönderilmesi.
Noktadan noktaya (Point to Point): Ağa atılan bir paketin özel bir noktaya iletilmesi.
Ağların çalışma prensipi genelde yayın tarzındadır. Buna rağmen İnternet omurgası noktadan noktaya çalışmaktadır.

Büyüklüklerine Göre Ağlar

LAN (Local Area Network) Yerel Alan Ağı: Kurulabilecek en küçük çaplı ağ olmakla birlikte büyüklükleri bir oda veya bir binayla sınırlı kalmayıp 1 km'ye kadar çıkabilmektedir. Örneğin küçük ve orta dereceli kurumların ağları.
WAN (Wide Area Network) Geniş Alan Ağı: Aralarında 1 km'den fazla mesafe olan LAN ların birleşmeleriyle meydana gelirler. Türkiye'deki en meşhur WAN'lardan biri Turnet (Türkiye iç omurgası), bir diğeri Ulaknet'tir (Üniversiteler arası ağ).



WAN = n · LAN + Sub-Net

MAN (Metropolitan Area Network) Metropol Alan Ağı: WAN'ların şehir bazında ya da şehirler arası birleştirilmeleriyle oluşur, fakat günümüzde MAN kavramı kullanılmamakta, yerine WAN terimi tercih edilmektedir

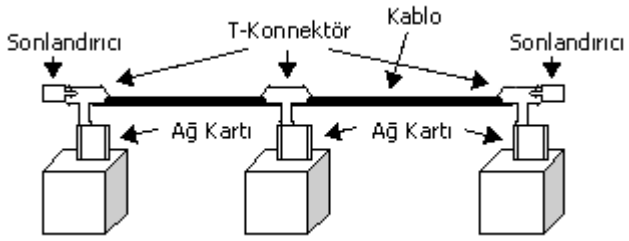
Mesafe Tablosu	
10 m	Oda
100 m	Bina
1 km	Fabrika / Kampüs
10 km	Şehir
100 km	Ülke
1000 km	Bölge
1000 km	Dünya

Ağ Topolojileri

Ağın fiziksel yapısı, kablolarla bağlantı şeklidir. Temel 3 topoloji vardır:

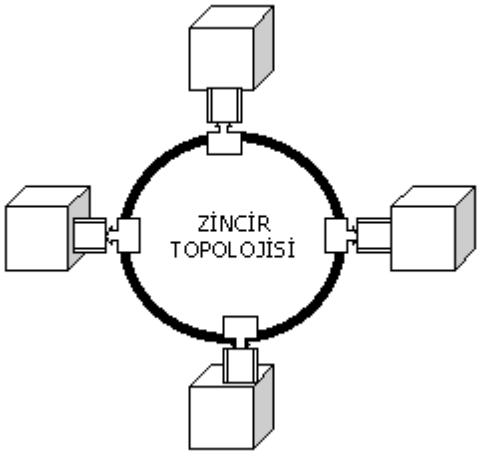
Kuyruk (Bus):

Doğrusal bir hat üzerinde kurulmuş bir yapıya sahiptir. Makineler kabloya T-konnektörler aracılığıyla bağlanırlar ve kablonun rezistansını düşürmemek için açıkta kalan iki ucuna sonlandırıcılar takılır. 10 mps hızda çalışır. Bir makinede veya kablonun herhangi bir noktasında oluşan arıza tüm sistemin çalışmasını engeller. Bu dezavantajına rağmen kurulumu en kolay yapı olduğu için tercih edilmektedir. Maksimum kapasitesi 10-12 makine olup, iki makine arası maksimum mesafe ince eş-eksenli (thin coaxial) kablo kullanıldığında 185 m, kalın eş-eksenli (thick coaxial) kablo kullanıldığında 500 metredir.



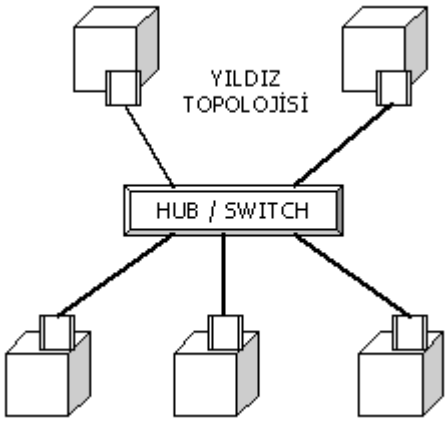
Zincir (Ring):

Kuyruk yapısındaki bir ağın sonlandırıcıların çıkarılarak iki ucunun birleştirilmesiyle oluşan ağ yapısıdır. En yaygın uygulaması IBM'e ait olan Token Ring topolojisidir. 4 mps veya 16 mps hızda çalışır. Kuyruk yapısının tüm özelliklerini taşımakla birlikte ağda bulunan düşük hızlı bir kart tüm sistemi yavaşlatır. Zincir yapısında ağda varolduğu düşünülen sanal bir jeton (token) tüm makineleri sırayla dolaşır ve bilgi alışverişi bu şekilde sağlanır.



Yıldız (Star)

Diğerlerinden farklı olarak, kablo,konnektör ve ağ kartına ek olarak hub,switch gibi diğer cihazlar kullanılarak oluşturulan ağ yapılarıdır. Genelde UTP (Unshielded Twisted Pair) korumasız çift dolanmış ya da STP (Shielded Twisted Pair) korumalı çift dolanmış kablo kullanılarak oluşturulur ve bilgisayarlarla bağlantı cihazının (hub gibi) maksimum mesafesi 100 metredir. Kullanılan çift dolanmış kablonun ve ağ kartının çeşitine göre farklı hızlarda çalışır. Her bilgisayarın bağlantısındaki problem yalnızca onun çalışmasını engellerken, ağdaki diğer cihazlar çalışmalarına devam ederler. Ancak bağlantı cihazlarındaki (hub, switch) problemler, o cihaza bağlanan tüm cihazların çalışmasını engeller. Diğerlerine göre daha güvenilir fakat pahalı çözümler sunar.



OSI Katmanları

Her teknojik üründe olduğu gibi ağlarda da standartları belirleyen bir kuruluş vardır. Bu kurum ISO (International Standards Organization) olarak bilinir ve ağ haberleşmesinde 7 katmandan oluşan OSI (Open System Interconnection) açık sistemler arası bağlantı kurallarını belirlemiştir. Bir ağ oluşturmak için fiziksel gereksinimlerin dışında, cihazların

haberleşebilmeleri için ortak bir anlaşma biçimine yani bir takım protokollere ihtiyaç duyulur. Her protokolün çalıştığı katman yaptığı işe göre değişmektedir. Bu bahsedilen katmanlar şu şekilde sıralanmaktadır:

7 Uygulama / Application
6 Sunum / Presentation
5 Oturum / Session
4 Taşıma / Transport
3 Ağ / Network
2 Veri iletim / Data Link
1 Fiziksel / Physical

Uygulama katmanı kullanıcıya en yakın olan ve programla iletişimini sağlayan katman, fiziksel katman ise en uzak olan ve kablodaki veri transferini içeren katmandır. Bir veri demeti, programın uygulama katmanından fiziksel katmana kadar çeşitli işlemlerden geçip (enkapsüle edilip), kablo üzerinden ağa ve oradan da diğer bilgisayarlara ulaşıp tam tersi işleme tabi tutularak, uygulama katmanına çıkarak diğer kullanıcılara iletilir. İnternette ve ağ uygulamalarında yaygın olarak kullanılan TCP/IP protokolünün uygulanmasında ise 6 ve 5 numaralı katmanlar uygulama katmanının içine dahil edilir ve sonuç olarak ortaya melez (hybrid) bir yapı ortaya çıkar.

TCP / IP Modeli:

7 Uygulama / Application

---
4 Taşıma / Transport
3 Ağ / Network
2 Veri iletim / Data Link
1 Fiziksel / Physical

Melez (Hybrid) Model (OSI & TCP/IP)

5 Uygulama / Application
4 Taşıma / Transport
3 Ağ / Network
2 Veri iletim / Data Link
1 Fiziksel / Physical

Ortaya çıkan bu melez model bundan sonraki anlatımların temelini oluşturacak ve her katman detaylarıyla ayrı başlıklar altında incelenecektir. Bu modele göre katmanlarda çalışan bazı protokol örnekleri ise şöyledir:

5 HTTP,TELNET,SMTP, IRC

4 TCP

3 IP

2 PPP

1 BNC

5 CNC

4 SPX

3 IPX

2 Ethernet

1 UTP

Fiziksel Katman

Bu katman tamamiyle fiziksel bağlantıdan sorumlu olup, kablo, konnektor gibi parçalardan meydana gelmektedir.
Ağ yapılarında kullanılan kablo türleri:

Eş-eksenli (coaxial / BNC): Televizyon kablosunun daha esnek ve ince olanıdır. Bakır tellerden ve üzerinde manyetik korumadan ibarettir. İnce ve kalın olmak üzere iki çeşittir. İnce olanının taşıma mesafesi 185m. Kalın olanının ki ise 500 metredir. Bu nedenler kalın eş-eksenli kablolar genelde omurga yapılarında kullanılır.

Çift dolanmış (twisted pair / UTP-STP): 8 tane çifte dolanmış telden ibarettir. 10 Mbit hızda çalışırken bunların yanlızca 4 tanesi kullanılır. 100 Mbit çalışabilmesi için bu 8 telin belirli bir sıra takip eder durumda bağlanması gerekmektedir. Korumalı (STP) ve korumasız (UTP) olarak iki çeşittir. STP genelde fabrikalar gibi manyetik alanların ya da fiziksel darbenin çok olabileceği yerlerde tercih edilir ve daha pahalıdır. Hıza göre şöyle ayrılır:

CAT3 10 mps.

CAT4 4-16 mps.

CAT5 100 mps.

CAT6 1000 mps.

CAT7 1000 mps.

Bunlar dışında fiber kablo, kablolu TV, telefon hatları veya kiralık hatlar (leased line) fiziksel katmana dahildir.

Yükseltici (Repeater): Kablonun kapasitesinden daha fazla mesafelere bağlantı kurulması gerektiğinde araya bir yükseltici konularak sinyalin güçlendirilmesini sağlayan cihazdır.

Hub: Yıldız yapısındaki ağlarda merkezi bağlantıyı sağlayan cihazdır. Üzerindeki port sayısıyla isimlendirilir ve bu portlara makineler takılır. Hub aslında içerisinde tüm portları birbirine bağlayan kablolardan oluşmuş bir cihazdır ve kablolardan taşınan bilgiyi anlama kapasitesine sahip değildir. Yanlızca bir porttan gelen paketleri diğer bütün portlara yayın (broadcast) şeklinde iletir. Bu yüzden fiziksel katmana dahildir.

Modem: Bilgisayarın dijital sinyallerini analoga çevirerek kablo üzerinden iletilmesini sağlayan cihazdır. 19600, 28800, 57600 Kb hızlarında çeşitli tipleri vardır. Kiralık hatlarda kullanılan modemlere senkron modem, çevirmeli bağlantılarda (dial-up) ise asenkron modem kullanılmalıdır.

Veri İletimi Katmanı (Data / Link)

Bu katman framelerle uğraşır. Giden veri akışının düzgün olmasını sağlar. Hata düzeltme yapar. Bütün bu işlemlerden sorumlu olan eleman ağ kartıdır. Ağlarda bulunabilen frame tipleri ise şöyledir:

802.2 Ethernet II

802.3 Ethernet

802.4 Token Bus

802.5 Token Ring

Mac (Media Access Control) Adresi: Ağ kartı olan her makinenin bir de MAC adresi vardır. Bu adres o ağ kartı üzerine, üretildiği firma tarafından ROM üzerine kaydedilir ve bir daha değiştirilemez. MAC adresi ait olduğu kartın bağlı olduğu makineyi bulunduğu LAN içerisinde ayırt etmekte, daha doğrusu haberleşmede kullanılır. Her üretici firmaya ait olan MAC adresi havuzu farklı olduğundan teorik olarak aynı MAC adresi iki farklı kart üzerinde bulunamaz. Bu olasılık gerçekleşse bile aynı ağ ortamı içerisinde çalışmadıkları sürece ağda bir problemle karşılaşılmaz.

Switch: MAC adresleri mertebesinde çalışan bir cihazdır. Portlarına bağlanan makinelerin MAC adreslerini kendi tablosuna kaydeder ve switch içerisindeki data transferi noktadan noktaya gerçekleşir. Switchler hublara göre daha akıllı ve pahalı cihazlardır ve kendi üzerlerinde işlemcileri ve hafızaları vardır. Switch ler yanlızca makinelerin direk olarak bağlanması için değil ayni zamanda ağların yükünü azaltmak için kullanılırlar. Diyelim ki birbirine bağlı 4 adet 16 portluk hub var. Bu ağdaki yayın trafiği ve paket çarpışmaları bayağı yüksek olacaktır. Bu durumlarda ağa bir merkezi switch koyup buradan hubları besleme yöntemine gidilmelidir. Böylece her bir hubda oluşan trafik diğer hublara yayın olarak yansımayacak ve lokal kalacak, hublar arası iletişm gerektiğinde ise noktadan noktaya gerçekleşecektir. İyi bir switch yüksek bir hafızaya, portlara aktarım ve portlar arası iletim hızına sahip olmalıdır. Eğer port başına düşen hafıza veya dinamik olarak paylaşılan hafıza düşük ise daha sonra gelen paketler o portun hafızasında tutulamıyacak ve tekrar yollanması istenecektir. Switchler bir ağı hızlandırır fakat ikiye bölmezler.


Catalyst 1900 Switch

Ağ (Network)Katmanı

Ağ katmanının tek görevi adreslemeyi sağlamaktır. Adresleme bir anlamda ağdaki paketin yolunu bulabilmesidir. İnternette adresleme için kullanılan protokole IP, bu protokolun kullandığı adreslere ise IP adresleri denir. IP adresleri her biri 8 bit yer kaplayan ve 0-255 arsında olan 4 oktetten oluşurlar. IP adresleri birinci oktetlerine göre 5'e ayrılırlar:

A grubu 0.0.0.0 - 127.255.255.255

B grubu 128.0.0.0 - 191.255.255.255

C grubu 192.0.0.0 - 223.255.255.255

D grubu 224.0.0.0 - 239.255.255.255

E grubu 240.0.0.0 - 255.255.255.255

Tüm ağlarda yanlızca A,B ve C grupları kullanılır. D grubu multicast adı verilen IP leri gruplayarak mesaj gönderen uygulamalarda (multimedya gibi) nadir olarak kullanılır. E grubu ise reserve edilmiştir ve kullanılmamaktadır.
IP adresleri Avrupada RIPE adı verilen bir kuruluş dağıtmaktadır. Herhangi bir IP yi kullanabilmek için RIPE e başvurup, onun size tahsis ettiği adresleri kullanmanız gerekmektedir. Aksi halde ciddi sorunlarla karşı karşıya kalmanız içten bile değildir. Fakat bu bahsedilen 5 grup içerisinde halkın kullanımına açılmış ve İnternet üzerinde kullanılmayan özel (private) IP adresleri vardır:

A grubu - 10.0.0.0

B grubu - 172.16.0.0

C grubu - 192.168.0.0

Yukarıda belirtilen özel IP lerin kullanımı herkese açıktır. Bunlar dışında bir de test amaçlı kullanılan ve her makinenin kendisini belirttiği kabul edilen bir başka IP adresi de 127.0.0.1 dir.
IP adresleri her zaman alt ağ maskesi (subnet mask) ile birlikte kullanılmaktadır. Subnet mask bir IP adresinin bağlı olduğu ağ adresini belirlemeye yarar. Standart subnet mask lar şu şekildedir.

A grubu - 255.0.0.0

B grubu - 255.255.0.0

C grubu - 255.255.255.0

Buna göre her gruptan birer IP adresi alıp, ilgili ağ adreslerini bulursak:

A grubu - 255.0.0.0 - 10.91.7.3 - 10.0.0.0

B grubu - 255.255.0.0 - 130.44.51.6 - 130.44.0.0

C grubu - 255.255.255.0 - 200.15.1.1 - 200.15.1.0

Yukarıdaki tablo bölünmemiş ağ adresleri, yani standart alt-ağ maskeleri ile geçerlidir. Bölünmemiş ağ adreslerinde bulunan IP adresleri sayıları ise şöyledir:

Grup	Ağ Adresi Sayısı	Adreslenebilir Makine Sayısı
A	126	(255*255*255)-2
B	63*255	(255*255)-2
C	31*255*255	255-2

Bir ağ adresindeki IP adreslerini ikinin üsleri şeklinde bölüp birden fazla ağ oluşturmak mümkündür. Buna alt-ağ oluşturmak (subnetting) denir. Bunu yapmak için bölümlenmiş alt-ağ maskeleri kullanmak lazımdır. Bu değerler aşağıdaki tablodaki gibidir:

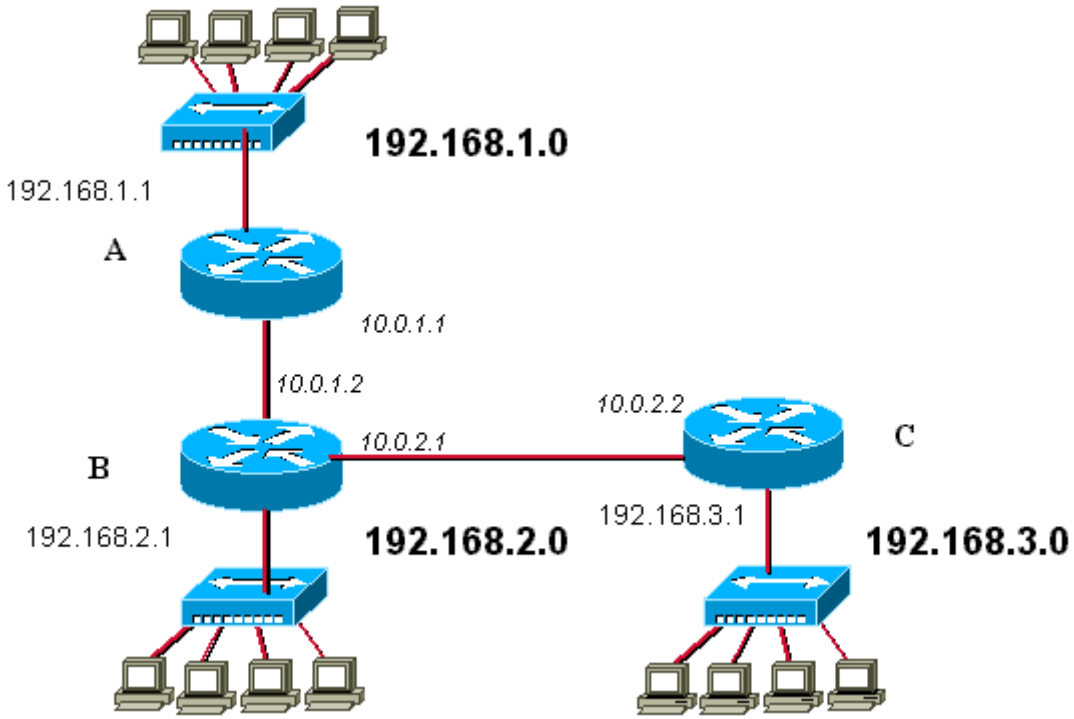
Alt-Ağ Sayısı	A Grubu Subnet Mask	B Grubu Subnet Mask	C Grubu Subnet Mask
2	255.128.0.0	255.255.128.0	255.255.255.128
4	255.192.0.0	255.255.192.0	255.255.255.192
8	255.224.0.0	255.255.224.0	255.255.255.224
16	255.240.0.0	255.255.240.0	255.255.255.240
32	255.248.0.0	255.255.248.0	255.255.255.248
64	255.252.0.0	255.255.252.0	255.255.255.252

Bu tablo ya göre 192.168.1.0 C grubu ağ adresini 4'e bölersek şu sonucu elde ederiz:

Ağ Numarası	Ağ Adresi	Yayın (Broadcast) Adresi	Alt Ağ Maskesi
1	192.168.1.0	192.168.1.63	255.255.255.192
2	192.168.1.64	192.168.1.127	255.255.255.192
3	192.168.1.128	192.168.1.191	255.255.255.192
4	192.168.1.192	192.168.1.255	255.255.255.192

Router (Yönlendirici): Networkler arası haberleşmenin yapılabilmesi için ara bağlantıyı sağlayacak cihazlara router denir. Routerin bir işlemcisi, epromu ve üzerinde bir işletim sistemi IOS (Internal Operating System) vardır. Routerlar IP paketlerinin yönlendirilmesinden sorumludur ve bu yüzden üzerlerinde routing tabloları tanımlanmıştır. Routing tabloları iki çeşittir: Statik ve dinamik.

Aşağıda şekli gözüken ağ için statik routing tabloları şöyledir:



Statik Routing - Router A

Hedef	Alt Ağ Maskesi	Interface	Gateway
192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.1
192.168.2.0	255.255.255.0	10.0.1.1	10.1.1.2
192.168.3.0	255.255.255.0	10.0.1.1	10.0.2.2

Statik Routing - Router B

Hedef	Alt Ağ Maskesi	Interface	Gateway
192.168.1.0	255.255.255.0	10.0.1.2	10.0.1.1
192.168.2.0	255.255.255.0	192.168.2.1	192.168.2.1
192.168.3.0	255.255.255.0	10.0.2.1	10.0.2.2

Dinamik routing tablolarında ise tabloya yanlızca router'ın direk olarak bağlı olduğu ağ adresleri eklenerek, RIP protokolü ile tabloların routerlar arasında paylaşılması sağlanır.

Dinamik Routing - Router A - Başlangıç

Hedef	Alt Ağ Maskesi	Interface	Gateway
192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.1
192.168.2.0	255.255.255.0	10.0.1.1	10.0.1.2

Dinamik Routing - Router B - Başlangıç

Hedef	Alt Ağ Maskesi	Interface	Gateway
192.168.1.0	255.255.255.0	192.168.1.2	192.168.1.1
192.168.2.0	255.255.255.0	192.168.2.1	192.168.2.1

192.168.3.0	255.255.255.0	10.0.2.1	10.0.2.2

Dinamik Routing - Router A - RIP sonrası

Hedef	Alt Ağ Maskesi	Interface	Gateway
192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.1
192.168.2.0	255.255.255.0	10.0.1.1	10.0.1.2
192.168.3.0	255.255.255.0	10.0.1.1	10.0.2.2

Dinamik Routing - Router B - RIP sonrası

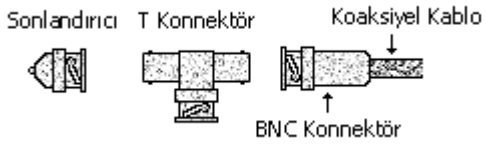
Hedef	Alt Ağ Maskesi	Interface	Gateway
192.168.1.0	255.255.255.0	10.0.1.2	10.0.1.1
192.168.2.0	255.255.255.0	192.168.2.1	192.168.2.1
192.168.3.0	255.255.255.0	10.0.2.1	10.0.2.2

Ağ Kurma

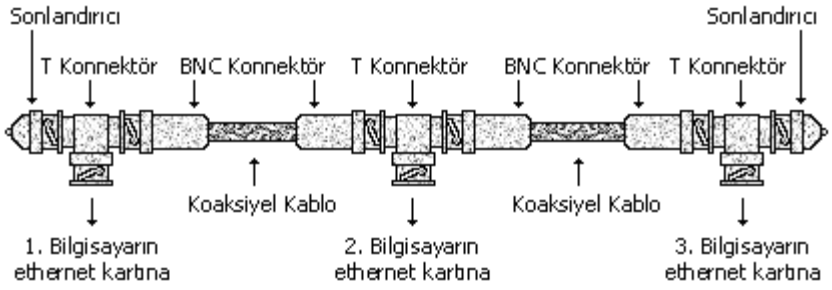
Ağ Bağlantıları

Ağımızı kurmak için önce bilgisayarların bağlantılarının nasıl yapıldığını anlatacağım. Bağlantı için değişik yöntemler kullanılabilir. İlk anlatacağım yöntem diğer bağlantı türlerine nazaran daha az masraflı bir yöntem. Fakat bazı dezavantajları olduğundan az sayıda bilgisayardan oluşan ağlarda tercih edilir.
Şimdi, bu yöntemle üç bilgisayardan oluşan bir ağ kuralım. İhtiyacımız olan şeyler: Dört tane BNC konnektör, üç tane T konnektör (genelde ethernet kartı ile birlikte verilir), iki tane sonlandırıcı ve yeterli uzunlukta koaksiyel kablo.

Parçalar hakkında biraz bilgi verirsek sanırım daha rahat anlaşılır. Koaksiyel kablo bildiğimiz anten kablosu. BNC konnektör de bu kabloyu ethernet kartına takabilmemiz için kablonun ucuna takacağımız parça. Sonlandırıcı ise ilk ve son bilgisayardaki T konnektörlerinin boş uçlarına takılan parça. Saydığım malzemeleri ŞEKİL 1'de görebilirsiniz.

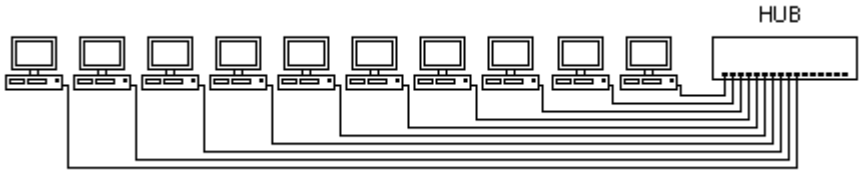


İlk olarak bilgisayarların arasına çekeceğimiz kabloların uçlarına birer BNC konnektör takalım. Sonra, bilgisayarların ethernet kartlarına T konnektörleri takalım ve ilk ve son bilgisayara takılı olan T konnektörlerin birer ucuna sonlandırıcı takalım. Sonlandırıcılar olmasza ağ kesinlikle çalışmaz. Son olarak, önce 1. ve 2. bilgisayarların arasına, sonra da 2. ve 3. bilgisayarların arasına koaksiyel kabloları takalım. Kablolar da takıldıktan sonra ağımız artık kullanıma hazırdır. Bilgisayarların ayarları yapıldıktan sonra ağı kullanılabilir. Bağlantıların nasıl yapıldığını ŞEKİL 2'den daha açık bir şekilde görebilirsiniz.



Bu bağlantı türü daha ucuz olmasına rağmen bazı dezavantajları vardır. Örneğin kabloların birinde kopma olduğu zaman ağ tamamen durur. Yani ağ "ya hep ya hiç" der. Bu durumda hatanın nerede olduğunu bulmak özellikle bilgisayar sayısı fazla ise oldukça zordur. Hata kontrolünü, kabloları ve sonlandırıcıları ölçü aleti ile deneyerek

yapabirsiniz. Ölçü aletinin kabloların iki ucu arasında sonsuz direnç göstermesi gerekir. Sonlandırıcının iki ucu arasındaki direnç değeri de 50 Ohm olmalıdır.
Anlatacağım ikinci bağlantı türü "ölen öldü, kalan sağlar bizimdir" görüşünde. Fakat ilkine göre daha pahalı. Şimdi de bu şekilde 10 bilgisayardan oluşan bir ağ kuralım. Bunun için ihtiyacımız olan şeyler: Bir 16'lı HUB, UTP bağlantı kablosu ve 20 tane RJ45 konnektör. Yine malzemeler hakkında biraz billgi vereyim. UTP bağlantı kablosu telefon kablosunun biraz daha kalını. İçinden 8 tane renkli kablo geçer. RJ45 konnektör de telefon kablosunun telefona takılan ucundaki parçanın biraz daha büyük hali. HUB'ın üzerinde, ethernet kartında olduğu gibi RJ45 konnektörlerin takılacağı yuvalar vardır ve adaptörle çalışır.
Konnektörleri kabloların ucuna takmak için penseye benzer özel bir alet vardır. Konnektörleri bu alet sayesinde kablolara takabilirsiniz. Konnektörleri takarken UTP kablosunun içindeki renkli kabloların sırasının iki uçta da aynı olmasına dikkat etmelisiniz. Aksi halde hatalı kablonun takıldığı bilgisayar ağı göremez. Kabloların uçlarına konnektörler takıldıktan sonra her bir kablonun bir ucu HUB'a diğer ucu bir bilgisayara takılır. Size tavsiyem, bir problem olması durumunda HUB'a takılan kablolardan hangisinin aradığınız kablo olduğunu daha rahat bulabilmek için kabloların uçlarına hangi bilgisayardan geldiği yazan küçük birer kağıt yapıştırmanız. Emin olun ihtiyacınız olduğunda çok işe yarıyor. HUB'ın adaptörü fişe takılıp bilgisayarların ayarları yapıldığı zaman bilgisayarlar ağı görebilirler. ŞEKİL 3'te bağlantılarının nasıl yapıldığı görülmektedir.

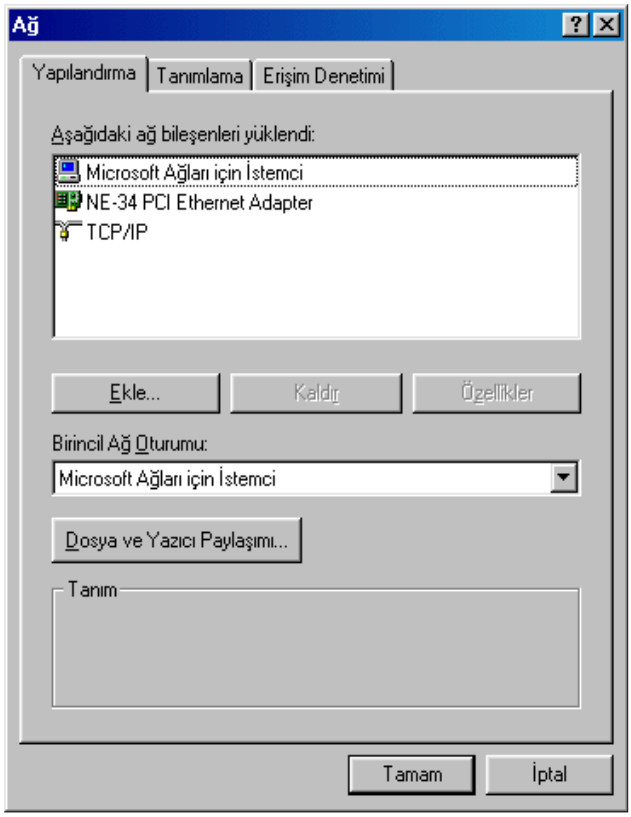


Şimdi anlatacağım yöntem sadece iki bilgisayarı birbirine bağlamak için kullanılır. İhtiyacımız olan malzemeler UTP bağlantı kablosu ve iki adet RJ45 konnektör. Cross-Cable dediğimiz bu yöntemle iki bilgisayarı HUB kullanmadan birbirine bağlayabiliriz. Hub'lı bağlantıdan farkı RJ45 konnektörün kabloya takılışında. Cross-Cable'da HUB'lı bağlantının aksine renkli kablolar konnektöre kablonun iki ucunda aynı sıra ile takılmaz. Cross-Cable hazırlanırken kullanılması gereken sıra aşağıdaki tabloda görülemktedir.

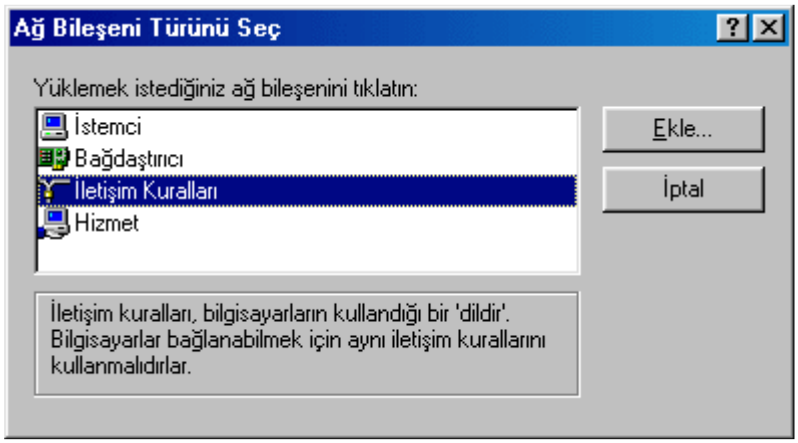
1 ==> 3
2 ==> 6
3 ==> 1
6 ==> 2
4 ==> 7
5 ==> 8
7 ==> 4
8 ==> 5

Ağ Ayarları

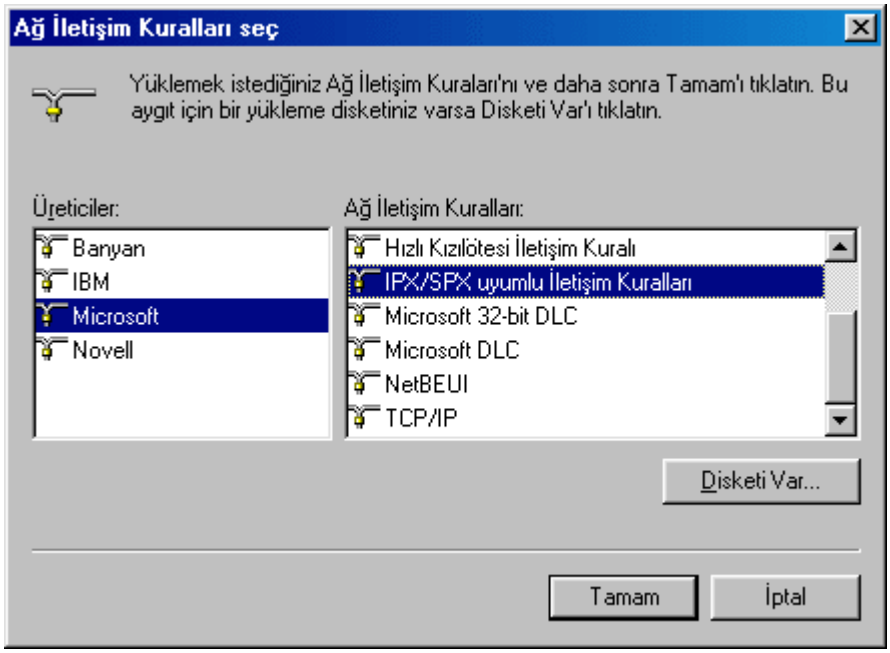
Bilgisayarınızın ağı görmesi için yapacağınız ayarlar yukarıda anlattığım bağlantı şekillerinin üçü için de aynıdır. Ethernet kartının bilgisayarınıza tanıtıldığını varsayarak ayarları anlatmaya başlıyorum. Eğer ethernet kartını bilgisayara tanıtmamışsanız Denetim Masası'nda **Yeni Donanım Ekle**'ye tıklayarak ethernet kartınızı tanıtın. Ethernet kartını bilgisayarınıza tanıttıktan sonra Denetim Masası'nda bulunan **Ağ** simgesine çift tıklayın. Karşınıza ŞEKİL 3'deki diyalog kutusu gelecektir.



Şimdi ağ için gerekli iletişim kurallarını kuralım. Bunun için **Ekle...** düğmesine tıklayın. Karşınıza ŞEKİL 4'teki diyalog kutusu gelecektir.

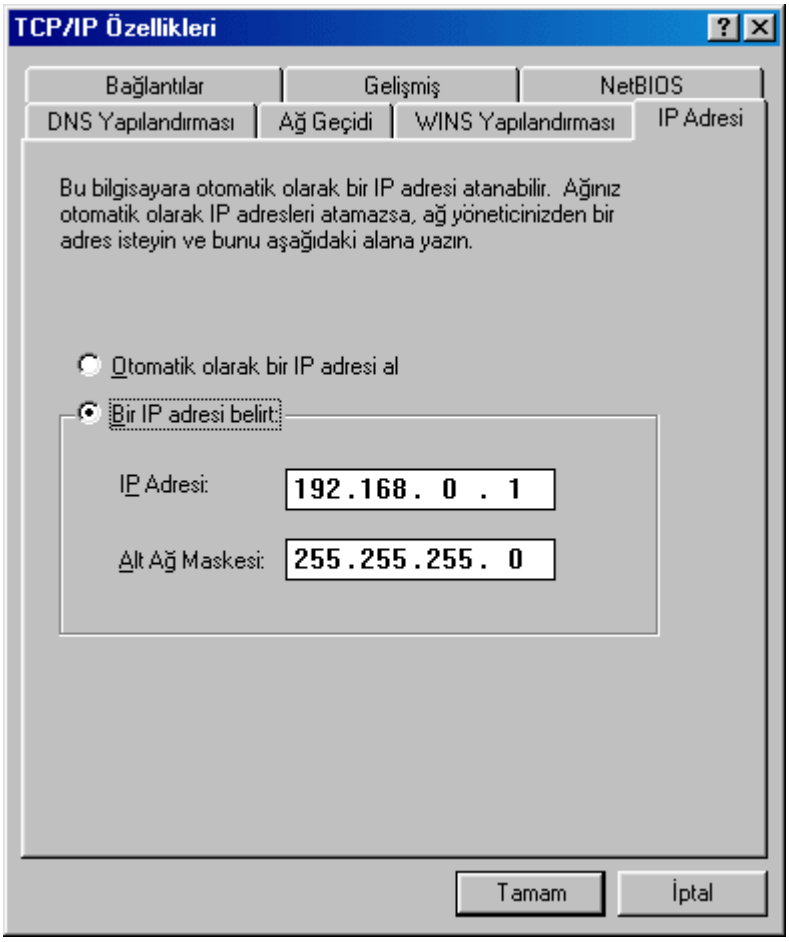


Bu diyalog kutusunda **İletişim Kuralları**'nı seçili duruma getirip **Ekle...** düğmesine tıklayın. Karşınıza ŞEKİL 5'teki diyalog kutusu gelecektir.

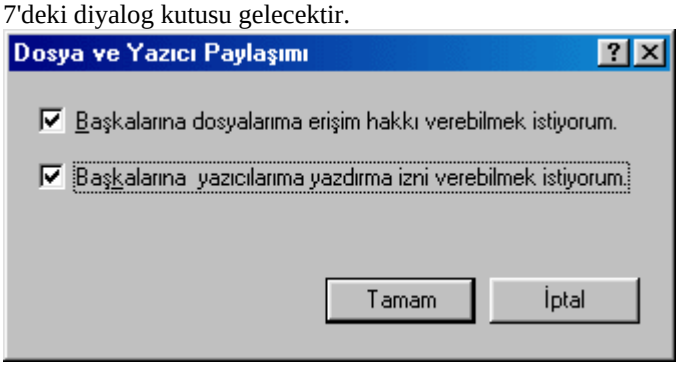


Önce sol tarafta bulunan **Üreticiler** kısmında **Microsoft**'u seçin, sonra sağ taraftaki **Ağ İletişim Kuralları** kısmında **IPX/SPX uyumlu İletişim Kuralları**'nı seçerek **Tamam**'a tıklayın. Sonra aynı işlemi tekrarlayarak **NetBEUI** iletişim kuralını kurun. (Ethernet kartını tanıttığınızda **TCP/IP** iletişim kuralı otomatik olarak kurulur. Eğer kurulu değilse aynı şekilde **TCP/IP** iletişim kuralını da kurmanız gerekir.)

Şimdi sıra **TCP/IP** ayarlarını yapmaya geldi. Bunun için **Ağ** diyalog kutusunda (ŞEKİL 3) **TCP/IP**'yi seçili duruma getirin ve **Özellikler** düğmesine tıklayın. Karşınıza ŞEKİL 6'daki diyalog kutusu gelecektir.

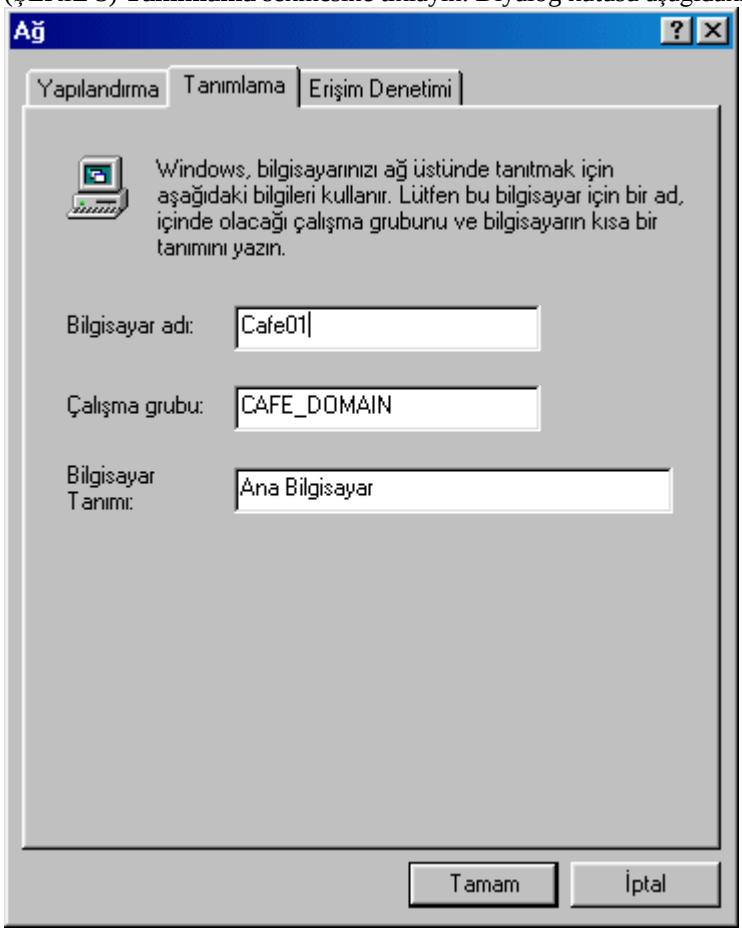


Bu diyalog kutusunda **Bir IP adresi belirt**'i seçin ve IP adresi olarak **192.168.0.1** yazın. Alt ağ maskesi olarak da **255.255.255.0** yazın ve **Tamam** düğmesine tıklayın. Diğer bilgisayarlara sırasıyla **192.168.0.2**, **192.168.0.3** ... adreslerini verin. Aslında bu adresleri vermeniz şart değildir. Eğer internete bağlanmayacaksanız bilgisayarınıza istediğiniz IP adresini verebilirsiniz. Fakat internete bağlanacaksanız mutlaka **192.168.0.*** şeklinde internette kullanılmayan ve sadece yerel ağlarda kullanılan bir IP adresi vermeniz gerekir. Her iki durumda da **192.168.0**'dan sonra istediğiniz sayıyı kullanabilirsiniz. Yalnız **0** ve **255** rakamlarını kullanmamalısınız. Çünkü **192.168.0.0** ve **192.168.0.255** adresleri özel adreslerdir. Dikkat etmeniz gereken bir husus ağdaki bütün bilgisayarların alt ağ maskesinin aynı olması gerektiğidir. Alt ağ maskesi farklı olan bilgisayarlar birbirini göremezler. TCP/IP ayarlarını da yaptıktan sonra **Ağ** diyalog kutusunda (ŞEKİL 3) **Dosya ve Yazıcı Paylaşımı...** düğmesine tıklayın. Karşınıza ŞEKİL 7'deki diyalog kutusu gelecektir.



Bu diyalog kutusunda bulunan onay kutularını işaretleyip **Tamam** düğmesine tıklayın. Eğer **Başkalarına dosyalarıma erişim hakkı verebilmek istiyorum** onay kutusunu işaretlemezseniz, bilgisayarınızın adı ağda görünmesine rağmen

diğer bilgisayarlar dosyalarınıza erişemezler. Aynı şekilde **Başkalarına yazıcılarıma yazdırma izni verebilmek istiyorum** onay kutusu işaretli değilse, diğer bilgisayarlar yazıcılarınızı kullanamazlar.
Şimdi sıra bilgisayarınızın ağ üzerinde hangi adla görüneceğini ayarlamaya geldi. Bunun için **Ağ** diyalog kutusunda (ŞEKİL 3) **Tanımlama** sekmesine tıklayın. Diyalog kutusu aşağıdaki görünümü alacaktır.



Bu diyalog kutusunda **Bilgisayar adı**, **Çalışma grubu** ve **Bilgisayar tanımı** olarak istediğiniz şeyi yazabilirsiniz. Fakat bütün bilgisayarların çalışma gruplarının aynı olmasına dikkat edin. Sizin çalışma grubunuzdaki bir bilgisayara **Ağ Komşuları** simgesine çift tıklayarak ulaşabilirsiniz. Eğer ulaşmak istediğiniz bilgisayar başka bir çalışma grubundaysa o zaman **Ağ Komşuları**'nda bulunan **Tüm Ağ** simgesine çift tıklayıp, ulaşmak istediğiniz bilgisayarın çalışma grubunu seçmelisiniz.
Eğer bilgisayarınızın her açılışında ağ parolası sormasını istemiyorsanız **Ağ** diyalog kutusunda (ŞEKİL 3) **Birincil ağ oturumu** olarak **Windows oturumu açma**'yı seçin.
Şimdi ayarlarımızın etkin olabilmesi için **Tamam** düğmesine tıklayalım. Windows kurulum CD'sinden gerekli dosyalar kopyalanacak ve bilgisayarınızı tekrar başlattığınızda ağdaki diğer bilgisayarlara erişebileceksiniz.
Son bir not: Bilgisayarınızı yeniden başlattığınız zaman **Ağ Komşuları**'nda diğer bilgisayarları hemen göremeyebilirsiniz. Bunun için birkeç defa F5 (yenile) düğmesine basmanız ya da bir müddet beklemeniz gerekebilir. İki bilgisayar arasında haberleşmenin mevcut olup olmadığını öğrenmek için `ping` komutundan faydalanabilirsiniz. Örneğin **192.168.0.2** IP'li bilgisayarla haberleşmeye çalışalım. Bunun için MS-DOS Komut İstemi'nde `ping 192.168.0.2` yazıp enter'a basın. Eğer karşı bilgisayardan `192.168.0.1 cevabı: bayt=32 süre<10ms TTL=128` gibi bir yanıt gelirse haberleşme mevcut demektir. Eğer `İstek zaman aşımına uğradı` gibi bir yanıtla karşılaşırsanız bağlantılarınızda ve ayarlarda bir hata var demektir.

İnternet Nasıl Çalışır?

İnternet'in yaygınlaşmasıyla birlikte TCP/IP kısaltmasını çok sık duymaya başladık. Bu kısaltmanın bir bilgisayar ağı protokolü olduğu, İnternet'in bu protokol üzerine kurulu olduğu hep tekrarlandı. Buraya kadar anladık. Ama hiç kimsede çıkıp bu TCP/IP'yi doğru düzgün anlatmadı. Internet'e bağlanırken girdiğimiz değerler (IP, Subnet Mask, Default Gateway vs. vs.) ne anlama geliyor. Bunları yanlış girince niye İnternet'e çıkış yapamıyoruz, kısacası nasıl oluyor da oluyor, hiç bilemedik. Ama artık yeter. Size bu yazıda TCP/IP'nin ne olduğunu bir bir anlatacağım. Artık gerçekler karanlıkta kalmayacak. TCP/IP, Transmission Control Protocol/Internet Protocol ifadesinin kısaltması. Türkçesi, İletim Kontrolü/İnternet Protokolü oluyor. Protokol belli bir işi düzenleyen kurallar dizisi demek.. Örneğin, devlet protokolü devlet erkanının nerede duracağını, nasıl oturup kalkacağını düzenler. Ağ protokolleri de bilgisayarlar arası bağlantıyı, iletişimi düzenliyor. TCP/IP'nin adına bakıp tek bir protokol olduğunu düşünmeyin. TCP/IP, bir protokoller kümesi. Herbiri değişik işler yapan bir yığın protokolden oluşuyor.
TCP/IP'nin kökleri, 1960'ların sonunda 1970'lerin başında Amerikan Savunma Bakanlığı'na bağlı İleri Araştırma Projeleri Ajansının (Advanced Research Projects Agecncy, ARPA) yürüttüğü paket anahtarlamalı ağ deneylerine kadar uzanır. TCP/IP'nin yaratılmasını sağlayan proje ABD'deki bilgisayarların bir felaket anında da ayakta kalabilmesini, birbirleriyle iletişimin devam etmesini amaçlıyordu. Şimdi baktığımız zaman projenin fazlasıyla amacına ulaştığını ve daha başka şeyleri de başardığını görüyoruz.
Bu projenin ilk aşamasında, 1970'de ARPANET bilgisayarları Network Control Protocol'ünü kullanmaya başladılar. 1972'de ilk telnet spesifikasyonu tanımlandı. 1973'de FTP (File Transfer Protocol) tanımlandı. 1974'te Transmission Control Program ayrıntılı bir şekilde tanımlandı. 1981'de IP standartı yayımlandı. 1982'de Defence Communications Agency (DCA) ve ARPA, TCP ile IP'yi TCP/IP Protokol suiti olarak tanımladı. 1983'de, ARPANET NCT'den TCP/IP'ye geçti. 1984'de Domain Name System (DNS) tanıtıldı.
Yukarıda kısaca verdiğimiz tarihçe aynı zamanda Internet'in tarihçesidir. Internet ile TCP/IP ayrılmaz kardeşlerdir. TCP/IP, İnternet'in temelidir.

Bu kısa tarihçeden sonra, bir yerel alan bilgisayar ağı üzerinde TCP/IP'yi anlatmaya geçelim. Burada anlatılanlar İnternet üzerinden de geçerlidir. TCP/IP ile kurulan bir bilgisayar ağında bir bilgisayarı üç parametre ile tanımlarız. Bu parametreler bilgisayarın adı, IP adresi ve MAC adresidir. TCP/IP protokoller kümesi bu 3 parametreyi kullanarak bilgisayarları birbirine bağlar.
Bilgisayar adı kullanıcı tarafından İşletim Sistemi yüklenirken bilgisayara verilen addır. (Bilgisayarlara MUHASEBE, SATIS, ye da AHMET gibi açıklayıcı ve kolay adlar verilmelidir.). MAC (Media Access Control, Ortama Erişim Kontrolü) adresi, bilgisayrların ağ kartının ya da benzer ağ cihazlarının içine değiştirilemez bir şekilde yerleştirilmiş bulunan bir adrestir. (0020AFF8E771 örneğinde olduğu gibi onaltılı düzende rakamlardan oluşur). MAC adresine donanım adresi de denir. IP adresi ise 131.107.2.101 örnek adresinde olduğu gibi, 4 bölümden oluşan bir adrestir. Nokta ile biri diğerinden ayrılan bu bölümlerin her biri 0 ile 255 arasında değer alabilir.

IP adresinin ilk bölümü adresinin gösterir. IP adresleri kabaca 3 sınıftır: Bu sınıflar A, B ve C olarak sınıflandırılır. A sınıfı adreslerin ilk bölümü 1 ile 126 arasında bir değer alabilir. B sınıfı adreslerin ilk bölümü ise 128 ile 191 arasında yer alır. C sınıfı adresler 192 ile 233 arasında bulunur. 223'ten sonrası ne oldu diye sorabilirsiniz. 223'ten sonrası bizi hiç ilgilendirmeyen işler için ayrılmıştır.
Dikkatli okuyucu arada 127 ile başlayan adreslerin kayıp olduğunu farketmiştir. 127 ile başlayan adresler özel işler için ayrılmıştır. Bu adreslerin bir tanesi bizi ilgilendirir ve sık sık kullanmamız gerekir. Bu adres 127.0.0.1'dir ve kendi bilgisayarımızı gösterir. İşlerin yolunda gidip gitmediğini öğrenmek için ilk önce bu adresi kullanırız.

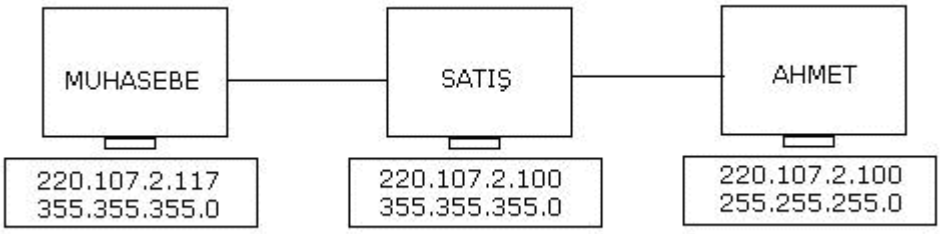
İnternette A sınıfı adresler çok değerli adreslerdir ve büyük ağlardaki bilgisayarlar için ayrılmıştır. Örneğin IBM'in adresleri A sınıfı adreslerdir. Şu anda İnternette A sınıfı adres tükenmiştir, kimseye verilmemektedir. A sınıfı adres alan bir işletme yaklaşık 16 milyon adres tanımlayabilir. İnternet'te B sınıfı adresler de şu anda tükenmiştir. Bir B sınıfı adreste yaklaşık 65000 bilgisayar tanımlanabilir. Örneğin, Microsoft'a bir B sınıfı adres alanı ayrılmıştır. C sınıfı adresler halen boldur, kullanılabilir. Ama C sınıfı bir adres alanı ile de ancak 250 küsür adres alanı tanımlanabilir. Bir yerel ağ kurarken İnternet'teki adres kısıtlamaları bizi bağlamaz. Kendi ağımız için her sınıftan bir adres verebiliriz. Burada verilen adreslerin İnternet ile bir bağlantısı yoktur. Bu noktaya dikkat ediniz. TCP/IP'yi anlamak için kendimizi bir yerel, daha sonra dageniş bir ağ ile kısıtlayacağız. Böyle bir ağın İnternet bağlantısı ise bambaşka bir konudur. Şimdi kendi bilgisayar ağımız için bir C sınıfı adres alanı tanımlayalım. Bilgisayarlarımıza vereceğimiz adresler 220.107.2.100 ile 220.107.2.200 arasında yer alsın. Örnek adresler:

Birinci bilgisayar için 220.107.2.100
İkinci bilgisayar için 220.107.2.101
Üçüncü bilgisayar için 220.107.2.102

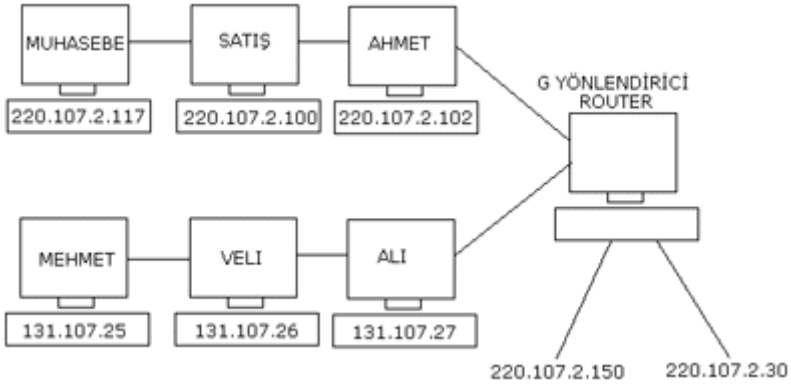
.....

Sonuncu bilgisayar için 220.107.2.200

Dikkat ederseniz, bütün bilgisayarların adreslerinin ilk üç hanesi sabit: 220.107.2. Bu adrese, tam olarak söylemek gerekirse 220.107.2.0 adresine, ağ tanımlayıcısı (Network ID) denir. Yani, sizin ağınızın adresi nedir derlerse 220.107.2.0 diyebiliriz. Buradan çıkaracağımız ilk sonuç şu: Hiç bir bilgisayara, sonu 0 ile biten bir adres veremeyiz. Sonu 0 ile biten adresler ağı tanımlar.
Bilgisayarımıza veremeyeceğimiz ikinci bir adres de, sonu 255 ile biten bir adrestir. Örnek ağımızdaki bilgisayarların adresleri araasında 220.107.2.255 yer alamaz. Sonu 255 ile biten adresler broadcast adresleridir. Broadcaast yayın demektir; Aynen radyo televizyon yayınlarındaki gibi. Yani, belli bir bilgisayara değil de tüm ağa mesaj göndereceğimiz zaman sonu 255'le biten bir adres kullanırız, böylece ağa yayın yaparız. Örnek ağımızda herkese gidecek mesajın hedef adresi 220.107.2.255 olur.
Şimdi biraz toplayalım. IP adresleri iki bölümden oluşur. İlk bölüm ağın adresidir. İkinci bölüm ağ içindeki bilgisayarların adresleridir. Örneğimizdeki adreslerde "220.107.2." ifadesini içeren bölüm, ağı tanımlar. Geri kalan kısım ise (100,101,...,200 gibi) ağdaki bilgisayarların her birini tanımlar. Başka bir ağda ağ adresleri 131.107.0.0 şeklinde, bir başkasında ise 90.0.0.0 şeklinde olabilir. Ağ adresleri seçtiğimiz sınıfa bağlıdır.
Bir bilgisayar, IP adresinin hangi bölümünün ağı tanımladığını, hangi bölümünün ise bilgisayarı tanımladığını bilmek zorundadır. Bunun için Subnet Mask bilgisini kullanır. Subnet Mask'i AĞ MASKESİ şeklinde çevirebiliriz. Subnet Mask'da bir IP adresidir; Dört bölümden oluşur ve ağ adresinin hangi bölüme kadar geldiğni göstermek için kullanılır. Örneğimizde Subnet Mask 255.255.255.0'dır. Yani örneğimizde ağ adresi IP adresinin ilk üç hanesi ile tanımlanmaktadır. Bilgisayarlar kendi ağ tanımlayıcılarını bulmak için Subnet Mask'i kullanırlar. Bu yüzden Subnet Mask'in doğru bir şekilde girilmesi ağımızın çalışması açısından önemlidir. Yanlış girilen subnet mask değeri, bilgisayarın diğer bilgisayarlarla iletişimini engeller.
Bilgisayarlar ağ tanımlayıcılarını bulmak için Subnet Mask'ı nasıl kullanırlar? Şimdi örnek bilgisayarımızdaki üç bilgisayarın adres bilgilerini Şekil-1' deki gibi girdiğimizi varsayalım:



Yukarıdaki şekilde MUHASEBE ve SATIŞ bilgisayarlarının Subnet Mask'i doğru, AHMET bilgisayarının Subnet Mask'i yanlış girilmiştir. Şimdi Ahmet adlı bilgisayarın MUHASEBE adlı bilgisayara bir bilgi iletmek istedigini varsayalım. AHMET bilgisayarı MUHASEBE'nin IP adresini kullanacaktır. AHMET, bilgi göndereceği bilgisayarın, yani MUHASEBE'nin, kendi ağında olup olmadığını anlamak için şu işlemleri yapar.
Önce kendi IP adresi ile Subnet Mask'ini AND işleminden geçirir; sonuç 220.107.2.96'dır. (inanmayan bu rakamları 0 ve 1 lerden oluşan ikili düzendeki rakamlara çevirip AND işlemini kontrol edebilir.) Bu rakam ona göre, içinde bulunduğu ağın tanımlayıcısıdır.
Sonra kendi Subnet Mask'i ile MUHASEBE'nin IP adresini AND işleminden geçirir; sonuç 220.107.2.112'dir. Bu iki adres ayni olmadığı için AHMET bilgisayarı, MUHASEBE bilgisayarının başka br ağda olduğunu varsayar. Bu da yanlış bir varsayım olduğu için MUHASEBE bilgisayarına bilgi gönderemez. Bu hatanın giderilmesi oldukça basittir. AHMET'in Subnet Mask değerini diğer bilgisayarlarla aynı yaparsanız, bütün bilgisayarlar aynı ağ üzerinde bulunduklarını hesaplayıp birbirlerine bilgi gönderebilirler. Bir bilgisayar ancak kendi ağı üzerindeki bir bilgisayara bilgi gönderebilirler. Bir bilgisayar ancak kendi ağı üzerindeki bir bilgisayara bilgi gönderebilir. Başka bir ağda bulunan bilgisayarlara bilgi göndermek gerekirse, yönlendirici (ROUTER) adı verilen cihazlar kullanılır. Cihaz dedik ama, üzerinde birden fazla ağ kartı bulunan bilgisayarlar da yönlendirici görevi görebilirler.



Şekil 2'de iki ayrı ağ, yönlendirici yardımıyla birbirlerine bağlanmış. SATIS bilgisayarı MEHMET bilgisayarına bilgi göndermek isterse, daha önce anlatılan işlemleri yaparak MEHMET bilgisayarının kendi ağında olmadığını anlar. ileteceği bilgiyi G bilgisayarına gönderir. G bilgisayarında iki adet ağ kartı (ethernet) bulunmaktadır. Kartların birisi 220.107.2.0 ağına, diğeri 131.107.2.0 ağına bağlıdır. G'de çalışmakta olan işletim sistemi (Windows NT ya da Novell Netware gibi) bu iki kart arasındaki bağlantıyı sağlar.

G bilgisayarında bulunan ağ kartlarının herbirinin ayrı bir IP adresi vardır. Şekil 1 'de bu adresler 220.107.2.150 ve 131.107.2.30 şeklindedir. Bilgisayarlar karşıdaki ağda bulunan bir bilgisayara bilgi gönderecekleri zaman bilgiyi, G'nin kendi taraflarında bulunan IP adreslerine gönderirler. G bilgisayarı bu adrese gelen bilgiyi alır ve 131.107.2.0 ağına geçirir.

Peki, 220.107.2.0 ağındaki bilgisayarlar kendi ağlarında bulunmayan bir bilgisayara bilgi gönderecekleri zaman yönlendiricinin adresini nereden buluyorlar ? Eğer bilgisayarınızda bulunan TCP/IP konfigürasyon bilgilerine bakarsanız, orada "Default Gateway" şeklinde bir adres alanı görürsünüz. Default Gateway varsayılan geçit demektir ve yönlendiricinin adresini gösterir. 220.107.2.0 adresi ile tanımlanan ağdaki bilgisayarlar Default Gateway olarak yönlendiricinin kendi taraflarındaki adresini, yani, 131.107.2.30 adresini verirler.

Yukarıda her şey IP adresleri ile oluyor bitiyor gibi görünüyor. Gerçekte ise iletişimden hemen önce, IP adreslerinin MAC adreslerine çevrilmesi gerekir. Ağ üzerinde iletişim aslında yalnızca MAC adresleri ile gerçekleşir. Çünkü IP adresleri TCP/IP protokolüne özeldir. Başka bir protokolde, örneğin, Novell'in kullandığı IPX/SPX protokolünde IP adresi diye birşey yoktur. Her protokol. kendine göre bir adresleme şeması kullanır ama, bu şemalarda yer alan adreslerin dönüp dolaşıp MAC adreslerine çevrilmesi gerekir ki, bilgisayarlar birbirleriyle iletişime geçebilsinler.

Bir bilgisayar bir başka bilgisayarın IP adresine sahip ama, MAC adresine sahip değilse Adres Çöümleme Protokolü (Adress Resolution Protocol, ARP) adı verilen bir protokol kullanarak IP adresini MAC adresine çevirir. TCP/IP'nin bir protokol kümesi olduğunu söylemiştik. İşte ARP bu kümenin üyesi.

İletişime geçeceği bilgisayarın IP adresini bilen bilgisayar, ARP protokolü ile "Bu IP adresi kiminse bana MAC adresini söylesin" şeklinde bir mesaj oluşturur ve bu mesajı broadcast yapar, yani ağdaki tüm bilgisayarlara gönderir. Ağdaki bilgisayarların tümü bu mesajları alırlar, eğer söz konusu IP adresi kendilerine ait değilse mesajı çöpe atarlar. Mesajdaki IP adresinin sahibi olan bilgisayar ise kendi IP adresini tanır ve hemen "Bu IP adresi bana ait, benim MAC adresim şu" şeklinde bir mesaj ile yanıt verir. İlk bilgisayar artık diğer bilgisayarın MAC adresini bildiği için asıl mesajını doğrudan (broadcast yapmadan) gönderebilir.

IP adresini bildiğimiz bilgisayarın MAC adresini öğrendik, ona bilgi gönderdik. Peki, o bilgisayara tekrar bilgi göndermek istesek ne olacak? Tekrar bir ARP broadcast mesajı mı yayınlanacak? Bu sorunun yanıtı hayır, çünkü ARP ile elde edilen bilgiler bir kaşe bellekte (ARP kaşe bellği) saklanır ve bir MAC adresi gerekli olduğu zaman, ilk önce bu tampon belleğe bakılır. Eğer IP adresine karşılık gelen MAC adresi bulunuyorsa, broadcast yapmadan bu adres kullanılarak iletişime geçilebilir. Ama TCP/IP'nin her bölümünde göreceğiniz gibi, bu ARP kaşesinde tutulan bilgilerin bir ömrü vardır. ARP kaşesine eklenen kayıtların ömrü en çok 10 dakikadır. Kaşeye kayıt eklenirken ekleme zamanı da belirtilir. ve eğer eklenen adres bilgisi 2 dakika içinde yeniden kullanılmazsa otomatik olarak silinir. Adres yeniden kullanılırsa yine silinir ama 10 dakika sonra. Ayrıca ARP kaşesine ayrılan yer kısıtlı olduğu için bu süreler dolmadan eski kayıtlar silinebilir.

IP adresi bilinen bir bilgisayarın MAC adresini bulmak için broadcast mesajı oluşturulur demiştik. Yani mesaj, ağ üzerindeki bütün bilgisayarlara gönderiliyor, yayın yapılıyor. Eğer Şekil 2'deki gibi birden fazla ağ söz konusu ise, yerel ağlarda kalması gereken broadcast mesajları ağdaki trafiği etkiler, ağ performansını düşürür. Çünkü yalnızca ağın bir

bölümünde anlamlı olan bir mesaj tüm ağa yayılarak bütün bilgisayarları meşgul eder. Bu durumu engellemek için yönlendiriciler, broadcast mesajlarını bir koldan bir kola aktarmazlar. Mantıklı, değil mi?

Broadcast mesajları gibi, herhangi bir şekilde yerine ulaşmayan ama serseri mayın gibi oradan oraya gidip gelen bir mesajı engelleme işini, yine yönlendiriciler yapar. Bir TCP/IP veri paketi oluşturulduğunda, pakete ilk değeri 128 olan bir yaşam süresi (ya da oyunlarda olduğu gibi "can". İngilizcesi Time-To-Live, TTL) verilir. Mesaj paketi herhangi bir yönlendiriciden geçerken "can" ı bir eksilir. Aynen oyunlarda olduğu gibi de, can değeri 0 olduğunda oyun sona erer; paket iletilemez, çöpe atılır.

Peki, bir bilgisayar IP adresini nasıl alır? Bunun iki yolu var: Ya siz bu adresi ele girersiniz ya da bir bilgisayar, belli bir adres havuzundan aldığı diğer bilgisayarlara dağıtır. Adresleri elle girmenin en büyük sakıncası adreslerin, Subnet Mask değerinin Default Gateway gibi diğer bazı bilgilerin yanlış girilmesidir. Eğer ağınızdaki bilgisayar sayısı onu aşıyorsa, adresleri elle girmek pek akıllıca değildir. Bu adresleri otomatik olarak dağıtmanın bir yolu vardır ve bu yolun adı Dinamik Bilgisayar Kontrolü (Dynamic Host Configuration Protocol, DHCP)'dür. Bu protokol ile bilgisayar DHCP sunucu (server) olarak tanımlanır ve IP adres dağıtımı bu sunucu üzerinden yapılır. DHCP'den alacağı belirtilmişse, açoldığında "Ben yeni açıldım, henüz bir IP adresim yok, eğer ortamda bir DHCP sunucu tanımlı varsa bana bir IP adresi göndersin" anlamında bir mesaj yayınlar. (broadcast eder). Eğer ortamda bir DHCP sunucu tanımlı ise bu mesajı alır "Ben bir DHCP sunucu olduğuma göre, bu mesaja yanıt vermek bana yakışır" şeklinde düşünüp kendisinde tanımlı olan IP adreslerinden boşta olanlardan birisini seçerek bilgisayara gönderir. IP adresi akan bilgisayarda artık diğer bilgisayarlar iletişim kurarken bu adresi kullanır.

DHCP sunucu ile IP adresi alan istemci bilgisayar arasındaki ilişki, bir sain alma işleminden kiralama işlemidir. İstemci bilgisayar, bir IP adresini DHCP sunucudan belli bir süretliğine "kiralar". Kira süresinin varsayılan süresi 72 saattir. Nası bir ev kiraladığınızda kira süresinin bitiminden önce kontrat tazeliyorsak, DHCP sunucudan alınan adresin de, bu süre bitmeden tazelenmesi gerekir.

Bütün DHCP istemcileri, kita sürelerinin %50'sine ulaştığında adreslerini tazelemek zorundadırlar. Kirasını tazelemek isteyen istemci, istediğini DHCP sunucusuna gönderir. Eğer DHCP sunucu ayakta ise kirayı tazeler ve bu durumu bir onay mesajı ile istemciye bildirir. İstemci onayı aldığında konfigürasyonunu günceller. Eğer istemci kirasını tazelemek istiyor da DHCP sunucusuna ulaşamıyorsa kiranın tazelenmediğine ilişkin bir mesaj alır ama, adresini kullanmaya da devam eder. Çünkü daha kira süresinin ancak yarısı geçmiştir. İstemci kira tazeleme isteğini kira süresinin yüzde %87.5'u tamalandığında tekrarlar. Eğer bu kez de yanıt alamaz ve süresi biterse istemci, IP adresini kullanmaya son verir ve yeni bir IP adres edinme sürecini başlatır.

Bir IP adresinin nasıl aldığını gördük, IP adresinin MAC adresine nasıl çevrildiğine de gördük. Şimdi "İyi ama, biz Windows 95'te ya da Windows NT'de Ağ komşuları (Network Neigborhood) 'na tıkladığımızda karşımıza IP adresleri ya da MAC adresleri gelmiyor ki, yalnızca bilgisayar adları geliyor" diyebilirsiniz, haklısınız. Başta söylediklerimizi anımsayalım:

TCP/IP dünyasında bir bilgisayarı 3 şey belirler:
Bilgisayarın adı, IP adresi, MAC adresi.

Bir bilgisayarın MAC adrsini ya da IP adresini değil de adını kullanmak daha kolay değil mi? Aksi takdirde, bilgisayarların IP adreslerini, daha da kötüsü MAC adreslerini ezberlemek zorunda kalabilirdik.

Bilgisayar adını kullanmak kolayımıza geliyor ama, ağ üzerinde iletişim gerçekte MAC adresleri üzerinden gerçekleştiriliyor. O zaman bilgisayar adını önce IP adresine çeviren sonra da MAC adresine çeviren mekanizmalar, protokoller olmalı değil mi? IP adresini MAC adresine çeviren protokolü görmüştük (belleği zayıf olanlara anımsatalım; bu protokolün adı ARP idi). Peki, bilgisayar adları IP adreslerine nasıl çeviriliyor? Burada çeşitli seçenekler var. Microsoft'un önerdiği şey WINS (Windows Internet Adlandırma Servisi, Windows Internet Naming Service). Bu servis ile bir makinayı WINS sunucusu olarak tanımlıyoruz, bütün bilgisayarlar girip adlarını ve IP adreslerini bu sunucuya bildiriyorlar. (aynen yeni eve taşındığımızda hane halkının mahallenin muhtarına kaydolması gibi). Bir bilgisayar, adını bildiği bir bilgisayarın IP adresini bulmak istediği zaman, broadcast yapmak yerine bu sunucuya gidiyor "Şu addaki bilgisayarın IP adresi ne olaki?" şeklinde bir soru soruyor. WINS sunucu da kendi veritabanına bakıp soruyu yanıtlıyor. Bu aşamadan sonrasını biliyoruz. (ARP ile IP adresi MAC adresine çeviriliyor).

İyi güzel de, bilgisayarlar ortamda bir WINS sunucunun var olup olmadığını ve varsa adresini nereden bilebiliyorlar? Yukarıda DHCP'yi anlatırken, DHCP sunucunun IP adreslerinin yanı sıra başka bilgileri gönderebileceğini söylemiştik. İşte bu bilgilerden birisi de WINS sunucunun adresi. Eğer biz tanımlarsak, DHCP sunucudan IP adresi alan

bilgisayarlar ortamdaki WINS sunucunun adresini de öğreniyorlar ve gidip kendilerini kaydettiriyorlar. Bu işlem otomatik olarak, el değmeden, son derece fenni yöntemlerle gerçekleşiyor.

Son cümleyi biraz abarttık değil mi? Ama bunun da bir nedeni var: WINS, Microsoft tarafından bulunan ve kullanılan bir yöntem. İnternet'te ad IP eşleştirmeleri başka bir yöntem kullanılıyor: DNS (Domain Name System). Bu sistemde bilgisayar adları ve IP adresleri DNS sunucu olarak konumlandırılan bilgisayarlara "elle" kaydediliyor. Bir bilgisayar, adını bildigi bir bilgisayarın IP adresini öğrenmek isterse DNS sunucuya gidiyor ve adresi soruyor.

DNS sisteminin kötülüğü, bilgilerin elle girilmesinde ve statik olmasında. Bilgisayar adlarının ve IP adreslerinin elle girilmesi ve değiştirilmesi gerekiyor.

Windows NT 4.0 versiyonuna kadar bir DNS sunucu fonksiyonu bulunmuyordu. 4.0 ile birlikte DNS sunucu fonksiyonu da eklendi. Üstelik Microsoft DNS'i WINS'e bağlamayı başardı. 4.0'da DNS sunucu bir kayıdı kendi veritabanında bulamazsa ortamdaki bir WINS sunucuya sorabilir ve ondan aldığı yanıtı iletebilir. Güzel bir olanak; hem Microsoft'un çözümünü koturyor hem de DNS sunucu isteklerini karşılıyor.