İLETİŞİM TEKNOLOJİLERİ

Veri iletimi, gönderici tarafından **iletim ortamına (KABLO - bakır, optik)** aktarılan bilginin alıcıya ulaştırılması olarak tanımlanabilir.
İletim olarak **kablo** veya **atmosfer** anlaşılmalıdır.
Veri iletimi **kısa** ve **uzun** mesafe olarak ikiye ayrılır.
Mesafe uzadıkça taşınan sinyal, iletim ortamının karakteristliğinden veya çevredeki gürültü faktörlerinden kaynaklanan bir takım kısıtlamalar ile karşı karşıya kalmaktadır.Bu kısıtlamaların üstünden gelmek için bir çok donanım ve yöntem geliştirilmiştir

ANALOG VE SAYISAL SINYALLER

SİNYAL

Bilginin ya da verinin bir uçtan diğer uca daşınması için kullanılan **elektriksel bir niceliktir**. Sinyalin üç bileşenden oluşur.

1) Genlik
2) Frekans
3) Faz

GENLİK

Sinyalin **"volt"** cinsinden elektriksel büyüklüğüdür.

FREKANS

Bir saniyede içersindeki sinyalin kendini **tekrarlama sayısıdır.**

FAZ

Belirli bir frekans açıya göre sinyalin **konumunu** ifade eder

Ağ sistemlerinde **"analog"** ve "**sayısal(dijital)"** olmak üzere iki tür sinyal vardır.
Analog sinyaller **doğal bir kaynak** tarafından üretiler.
Sayısal sinyaller ise **bilgisayar gibi cihazlar** tarafından doğrudan üretilir. Yada analog sinyalllerin örneklenmesiyle elde edilir.
Dolasıyla analog sinyallerden farklı olarak 1 ve 0 olmak üzere sayısal sembollerle ifade edilir."0 ve 1" ikiside bit olarak isimlendilir.

Bir iletim ortamında saniyede gönderilen **bit sayısı** ise alıcı ve verici donanımları arasındaki **"veri aktarım hızı"** olarak ifade edilir.

Verinin kendisi sayısal bir bilgi olduğu için doğrudan sinyaller kullanılarak iletilmesi birçok açıdan fonksiyoneldir. Bu nedenle tüm veri şebekelerinde sayısal sinyaller kullanılır.

SİNYAL İLETİMİNİ KISITLAYICI FAKTÖRLER

Sinyaller **gürültü, gecikme ve zayıflama** gibi faktörlerden ötürü bozulurlar. **Sinyalin bozulma oranı frekans ve genlik değerleri ile yakından ilişkilidir.**

Gürültü

Hava şartlarından, iletimin ortamındaki ısınmadan, kablo çiftlerinin birbirini etkilenmesinden, yakın çevredeki elektrik iletim hatlarından kaynaklanan faktördür.

Gecikme

Sinyalin farklı frekans bileşenlerinin alıcıya farklı zamanlarda ulaşması olarak tanımlanır. Karmaşık bir konudur. **En büyük faktör olarak bilinir.**

Zayıflama

Sinyalin genliğinin(elektirksel seviyesinin) düşmesi olarak tanımlanır. Sinyalin zayıflamasına, iletim ortamının direnci olarak tanımlanır. Zayıflamayı önlemek için alıcı ile gönderici arasına belli aralıklarla **güçlendirici ya da yineleyici** gibi donanım cihazları yerleştirilir. Ama bu donanım cihazları **gereğinden fazla** kullanılırsa alıcıya gelen birçok bitin hatalı olmasına sebep olur.
Çünkü güçlendiriciler sinyalin genliğini yükseltirken ağda var olan gürültüsünde genliğini yükseltir.

Bir hattın kalitesi sinyal/gürültü oranı ile ifade edilir

SNR (Signal to Noise Ratio)(Sinyal Gürültü Oranı) kısaltmasıyla bilinen bu oran ne kadar yüksek ise hat o kadar kalitelidir. Bu üç faktörden ötürü iletim kanallarından gelen bazı bitler hatalıdır. Hatalı gelen bitlerin tüm veri içerisindeki miktarını ifade etmek için **BER(bit error ratio)(bit hata oranı)** parametresi kullanılır. **BER ağ sisteminin kalite ve performansının bir göstergesidir.**

MODÜLASYON VE KODLAMA

Modülasyon sayısal ya da analog bir sinyalin iletim ortamından taşınabilmesi için başka bir sinyal üzerine bindirilmesi olarak tanımlanabilir.
İki kavram vardır;

1) Bilgi Sinyali
2) Taşıyıcı Sinyal

Bilgi sinyali insan sesi ya da bilgisayardan alınmış bir veri olabilir.
Taşıyıcı sinyal ise bilgi sinyaline göre yüksek sabit bir frekansa sahip bir sinyaldir.

Örneğin; İnsan sesi 400 Hertz - 3400 Hertz arasında değişir. Bu frekans değerine sahip bir sinyali iletim ortamında taşımak mümkün değildir. Bu yüzden böyle bir sinyali taşıyabilmek için yüksek frekans değerine sahip başka bir sinyal üzerine bindirilir. Modülasyonun bir avantajıda tek bir iletim kanalında birden fazla sinyal taşınmasına imkan vermesidir. Atmosferde aynı anda birden fazla radyo kanalının yayının yapılması ya da aynı kablo üzerinden birden fazla TV yayının alınmasıdır.

Her kanala ait bilgi sinyallerinin farklı taşıyıcı sinyaller kullanılarak iletilmesiyle mümkündür. Sinyallerin farklı taşıyıcı frekanslarla tek bir iletim ortamında aktarımı **FDM (frekans bölmeli çoklama) (frequency division multiplexing)** olarak bilinir.

Atmosfer ortamında sinyal iletimi için en çok kulllanılan modülasyon teknikleri şunlardır;
Amplitude Modulation (AM)
Frequency Modulation (FM)

Modülasyon normalde analog iletişim konusudur. Ancak veri iletişiminin ağ sistemleri yaygınlaşması ile birlikte sayısal sinyal taşıması içinde çeşitli modülasyon teknikleri geliştirilmiştir.

Ses Kodlama

Sesin sayısal olarak sinyalleşen ağ sistemi üzerinden iletilmesi için kullanılan kodlama teknikleridir. Günümüzde internet üzerinden ses taşımacılığı **VoIP (Voice IP)** olarak bilinir. Son derece popüler bir kullanımı vardır.

Veri Kodlama

Tıpkı modülasyon gibi sinyallerin iletim ortamında taşınabilmesi için kullanılır. Modülasyondan farkı iletim ortamındaki sinyalde sayısaldır. Bu nedenle kodlama da analog sayılsalda, sayısaldan analoga dönüşüm işlemi yapılmaz.

Bir iletim ortamında taşınabilecek maksimum veri oranı taşıyıcı sinyalin frekans değerine bağlıdır. Dolasıyla yüksek taşıyıcı frekans değerleriyle daha fazla veri taşımak mümkündür.

BANT GENİŞLİĞİ, TEMEL BANT VE GENİŞ BANT KAVRAMLARI

Bir haberleşme kanalının veya bir iletim ortamının kapasitesini ifade etmek için kullanılır. Analog sinyaller kullanılıyorsa birimi **Hertz'dir**. Sayısal sinyaller kullanılıyorsa birimi **bps'dir**.(bit per second) (her bir saniye başına bit)

Örneğin; radyo kanalının bant genişliği Hertz(Hz) internet kapasitesi bps cinsinden ifade edilir. Bir ağ sistemi gönderici donanımı, alıcı donanımı ve iletim ortamı olmak üzere en az 3 bileşenden oluşur. Bu üç bileşeni bant genişliği birbirinden farklı olabilir. Bu durumda ağ sisteminin kapasitesi minimum bant genişliğine sahip bileşeninki kadar olacaktır. Yani sistemin bant genişliğine minimum olan bant belirler. Veri ileşiminde sayısal

sinyaller kullanılır. Bant genişliği bps cinsinden ifade edilir. Başka bir ifadeyle saniyede aktarılabilecek maksimum bit oranı kanalın bant genişliğini verir. Verinin saklanabilme kapasitesi **Byte**, taşınabilme kapasitesi **bit** cinsindendir.

Byte 8 bitten oluşan ve anlam taşıyan bilgi birimidir. Klavyedeki her harfin sembolün veya rakamın ASCII kod sisteminde bir bytelı karşılığı vardır.

Veri bir yerden başka bir yere bit bit taşındığı için iletim ortamlarının kapasitesi için bps kullanılır.
Bant genişliği, bps, Kbps, Mbps, Gbps cinsinden verilebilir.

Örneğin; 240 MB büyüklüğündeki program 4 dakikada gönderiliyorsa bu iki bilgisayarın haberleşme kapasitesini Phpde gösteren programı yaz.

4 dk = 240 sn
240 MB = 240.000.000 byte = 1.920.000.000 bit
1 byte = 8 bit

1.920.000.000 / 240 = 8.000.000 bit/sn = 8 Mbps

Fiziksel bir iletim ortamında aynı anda birden çok haberleşme kanalı bulunabilir. Haberleşmenin tek bir kanaldan yapıldığı Base Band(temel bant), birden çok kanaldan yapıldığı Bread Band (geniş bant) denir.

TEMEL (BASE) BANT

İletim ortamında tek bir frekans bandı kullanılır. Bu durumda teorik olarak iletim ortamının kapasitesi tamamıyla tek bir kanal için kullanılır.
Örneğin; ethernet, temel bandı kullanan bir protokoldür.

GENİŞ BANT

İletim ortamında birden fazla frekans bandı kullanılır. Her frekans bandında farklı bir haberleşme kanalı bulunur. Bu durumda iletim ortamının kapasitesi, farklı kanallara paylaştırılmış olur. Örneğin; aynı anda hem internet hem de telefon bağlantısı yapılmasına imkan veren hem de telefon bağlantısı yapılmasına imkan veren **ADSL** teknolojisinde olduğu gibi. Burada hem “ses” hem de “internet” aynı iletim ortamında farklı bantlarda taşınmaktadır.
Bir frekans band filtresi sayesinde ses ve veri haberleşme kanalları birbirinden izole edilerek kullanılmaktadır. Aslında geniş band veri iletimi eskiden beri televizyon ve radyo iletişimi için kullanılan ve frekans bölmeli çoklama **(FDM)** olarak bilinen **RF** modülasyon prensiplerine göre yapılmaktadır.

Kanal Çoklama (Multi Plexing)

Temel anlamda FDM ve TDM olmak üzere iki tip çoklama tekniği kullanılır. Çoklama teknikleri bir iletim ortamında birden fazla iletişim kanalı oluşturmak için kullanılır.

FDM

İletim ortamının farklı frekans kanallarını kullanarak birden fazla haberleşme kanalı oluşturmaya yarayan çoklama tekniği kullanılır.
Örneğin; 2 telli telefon hatları üzerinden hem telefon hem de internet bağlantısının yapılması frekans çoklama tekniği sayesindedir.
FDM analog iletişimin konusu olmakla beraber artık geniş band veri iletişimde de kullanılmaktadır.

TDM

Farklı zamanlarda farklı uç sistemlere ait çerçeveleri taşıyarak tek bir fiziksel hat üzerinden birden fazla heberleşme kanalı oluşturan çoklama tekniğidir.
TDM yönteminde belli bir zaman diliminde birden fazla aboneye hizmet verilmektedir.
TDM temel band veri iletim yönetimidir.

PARALEL VE SERI İLETİMİ

Paralel İletişim

Bilgisayarın kendi içinde anakartın üzerinde veya yazıcı gibi yakın çevre cihazlarıyla yaptığı veri iletişimi için kullanılır. Paralel iletişimde karşı uçlar birbirleriyle byte düzeyinde iletişim kurarlar. Byte taki her bir bit aynı anda farklı bir tel üzerinden gönderilir. Yani aynı anda iki uç arasında 8 adet fiziksel iletim ortamı olmalıdır. Bu yüzden uzun mesafelerde paralel iletişim kurmak hem teknik hem de ekonomik açıdan uygun bir yöntem değildir.

Seri İletişim

Daha uzun mesafelerde verimli ve ekonomik veri aktarımı yapılmasını sağlar. Bilgisayar üzerindeki seri porttan veya modem üzerinden yapılan veri aktarımında seri iletişim kullanılır. Bitler göndericiden alıcıya doğru tek bir iletim ortamından birer birer gönderilir. Seri iletişimde veri sekron ve asekron olmak üzere 2 şekilde aktarılabilir. Asekron aktarımında herhangi bir zamanlama bilgisi kullanılmaz. Sekron iletişimde gönderici ve alıcı uçlar arasında ortak bir zamanlama kullanılır. Böylece gelen verinin nereden başlayıp nerede bittiği anlaşılabilir. Asekron iletişimde byte byte aktarılır. Her 8 bitin başına ve sonuna start ve stop ayraçları konulur.

Haberleşme Kanallarının Çalışma Modları

1) Simplex Kanal
2) Half Duplex
3) Full Duplex

Simplex Kanal

Yayının tek taraflı yapıldığı haberleşme kanalıdır.
Bu iletişim şeklinde alıcı pasif rol oynadığı için kanalın tamamı verici tarafından kullanılır.

Half Duplex

Haberleşme çift yönlü olarak yapılabilir. Ancak herhangi bir anda kanalı tek bir taraf kullanılabilir.

Full Duplex

Alıcıyla verici arasında 2 tane simplex kanal bulunur. Böylece her iki tarafta birbirine veri gönderilebilir.

İLETİM ORTAMLARI

Temelde atmosfer ve kablo olmak üzere 2 farklı iletim ortamı mevcuttur. Atmosfer ortamında RF (radyo frekans) kullanılarak iki uç arasında sinyal iletimi gerçekleştirilir. Günümüzde fiber optik teknolojisi sayısal bir sinyalin yüksek bant genişliği ve düşük gecikme değerleriyle uçtan uca aktarımına imkan tanımaktadır. Fiber optik iletişim giderek yaygınlaşmaktadır. Bakır kablo üzerinden veri taşımacılığı günümüzde halen vazgeçilmezdir.

Koaksiyel (Cooxial) Kablo

Elektiriksel gürültünün yoğun olduğu çevre şartlarında kullanımı en uygun olan bakır kablo tipidir. Koaksiyel kablonun **yapısı**;
Merkezdeki iletken üzerinde taşınan sinyalin elektriksel gürültülere karşı bağışıklığını arttırır.
Tipleri;
RG-6, RG-58, RG-8 olarak 3 çeşittir. Koaksiyel kabloları birbirinden ayıran en önemli özelliklerden biri kendilerine özgü empedans değerleridir.

*** RG-6 ses ve video iletiminde kullanılan koaksiyel kablo tipidir. 750hm RG-6 kablosunu sonlandırmak için yine 750hm luk konnektörler kullanılır.

*** RG-58 yerel ağlarda 180 metrelik mesafeye kadar 10Mbps hızında veri aktarımına imkan veren koaksiyel kablo çeşidi ve 10Base2 LAN (Local Area Network) standartlı olarak bilinir.

WAN= Wide Area Network- Geniş Alan Ağı (En Büyük Ağ)
WLAN= Wireless Local Network
MAN = Metropolitan Area Network (2. Küçük Ağ)
LAN = Local Area Network (En Küçük Ağ)

*** RG-6 daha kalın bakır iletkene sahip olduğundan yerel ağlarda 500 metrelik mesafelere kadar 10Mbps hızında veri aktarımına imkan tanır.
10Base2 LAN standartı olarak bilinir.

RG-58 ve RG-8 koaksiyel kabloları 500Ohm luk empedans değerine sahiptir. Her iki kabloyu da sonlandırmak için 500 Ohm luk BNC konnektör kullanılır.
Koaksiyel kablolar yerel ağlarda terk edilmiştir.

1) Çünkü 10Mbps yavaş hızda kalmaktadır.
2) İkinci sebebi ise maliyeti fazladır.

UTP KABLOLAR (Unshielded Twisted Pair)

Yapısı koaksiyel kabloya göre çok basit bakır kablodur. Bu kablolar belirli mesafeler, için üzerinden geçirebilecekleri veri miktarına göre kategorilere ayrılmışlardır. Bu kategoriler şunlardır;
CAT-1 > Telefon hatlarında kullanılır.
CAT-5 > Yerel ağ bağlantıları için kullanılır. Günümüzde neredeyse tüm yerel ağ bağlantıları CAT-5 UTP kablolarıyla yapılmaktadır. 100 metrelik mesafe asılmadığı müddetçe veri aktarımı çok net olmaktadır. 100Mbps hızını destekleyen ethernet kartı ile çalışabilecek en uyumlu kablodur.
CAT-6 > 1000Mbps hızında veri iletimine imkan sağlamaktadır. Gigabit ethernet kartlarıyla kullanılır.

UTP kabloları sonlandırmak için RJ-45 konnektörleri kullanılır. Kablo düzlü bir şekilde sonlandırılmazsa veri taşıma kapasitesi düşer dolasıyla sonlandırmalar standartlara uygun ve dikkatli yapılmalıdır. Ayrıca UTP kablo sonlandırılması 2 şekilde yapılabilir.

1) Düz Sonlandırma
2) Çapraz Sonlandırma

Örneğin; bir bilgisayarı başka bir bilgisayara bağlarken çapraz kablo kullanılır. Çünkü bir uçtaki bilgisayardan çıkan veri diğer bilgisayar için girdi olarak kullanılacaktır.

Port 1	Port2	Bağlantı Tipi
Pc	Pc	Çapraz UTP kabloyla
Pc	Hub/Anahtar(switch)	Düz UTP kabloyla
Hub/Anahtar	Hub/Anahtar	Çapraz UTP kabloyla
Hub/Anahtar	Yönlendirici(Router)	Düz UTP kabloyla
Pc	Yönlendirici	Çapraz UTP kabloyla

Çapraz bağlantının düz bağlantıdan farklı alıcı **(RX)** ve verici **(TX)** uçlarının birbirine karşılıklı olarak bağlanmasıdır. Günümüzde yeni nesil bazı anahtar cihazlar bağlantı

kablosunu düz mü yoksa çapraz mı olduğunu tayin edebilir ve o bağlantıya göre çalışabilir, yani kendisini ayarlayabilme yetkisi vardır.

FİBER OPTİK KABLOLAR

Fiber optik kablo yüksek maliyetine karşılık üstün bir iletim ortamı sağlamaktadır. Diğer fiziksel iletim ortamlarının aksine veri optik dalgalar aracılığıyla ışığın yansıma kurallarına göre iletilir. Dolasıyla sinyal bozucu elektromanyetik faktörlerden etkilenmez. Bunun dışında mesafeye göre sinyalin zayıflama oranıda çok daha düşüktür.
Bakır kablolarda olduğu gibi gerilim farkından kaynaklanan topraklama sorunuda bulunmamaktadır. Hatalı bir oranı **(ber)** bakırın binde biri kadardır.
Tüm bu nedenlerden ötürü fiber optik uzun mesafelerde yüksek band genişliğine ihtiyaç duyan ses ve veri aktarımı için çok ideal bir çözümdür.
Fiber optik kablo içerisinde sinyal yansıma kurallarına göre iletilmektedir. Bunun olabilmesi için veri fiber optik ortama verilmeden önce optik dalgalara çevrilmelidir. Verici tarafından ışık kaynağı olarak **LED (Light Emitting Diode)** yada **lazer diyot** kullanılır.
Benzer şekilde alıcıya ulaşan optik dalgalardan elektriksel sinyali elde edebilmek için foto diyot yada foto transistör kullanılmaktadır. Fiber optik kablolar **tek modlu (single mod), çok modlu (multi mod)** olmak üzere ikiye ayrılır.

Tek Modlu Fiber Kablolar (Single)

Uzun mesafelerde yüksek band genişliğine imkan verir. Uzak mesafe bağlantıları için tercih edilirler. Optik dalga üretmek için lazer diyotlar kullanılmaktadır. Dolasıyla verici ve alıcı donanımları daha pahalıdır.

Çok Modlu Fiber Kablolar (Multi)

Bina yada kampüs içi gibi tek modluya göre daha küçük mesafelerde kullanılır. Optik dalga üretmek için ledler kullanılmaktadır. Günümüzde fiber optik kablolar internetin omurgasını oluşturmaktadır.

YEREL AĞLAR

Günümüz yerel ağlarında ethernet haricinde bir bağlantı protokolü kullanılmamaktadır.

ETHERNET PROTOKOLÜ

İntel ve xerox firmaları tarafından geliştirilen bir protokoldür. Daha sonra IEEE tarafından standartırılmıştır. Bazı cihazlarda **802.03 koduyla** da yazılmaktadır.
Ethernet protokolü ikinci katmanda tanımlı bir bağlantı protokoldür. İkinci katman protokolleri ağ katmanlarından aldıkları paketleri kendilerine ait frame(çerçeve) biçimine dönüştürerek iletim ortamına göndermektedirler. Ethernet protokolünde yerel ağa bağlı herhangi bir bilgisayar bilgi çerçevesi gönderdiğinde diğerlerinin beklemesi gerekir. Eğer bekleme olmaz ise fiziksel hatta aynı anda birden fazla çerçeve olacağından çarpışma meydana gelir.

Yoğun kullanılan yerel ağlarda uygun donanımlar seçilir ve akılcı planlamalar yapılırsa çarpışma sorunu minimuma indirilir.

Ethernet Bağlantı Kapasiteleri

Ethernet protokolü aslında 10mbps bağlantı kapasitesine sahiptir. Günümüzde bu kapasite 1000Mbps ye kadar çıkmıştır. Dolasıyla ethernet kartları 10,100,1000Mbps olarak üretilmektedir. 100Mbps'lik portlar fast ethernet, 1000Mbps'lik portlar Gigabit ethernet olarak bilinir.

***Ethernet portlarının kapasitesi ve bu portlara ne tür kablo ve konnektör bağlanabileceği port üzerinde yazanlardan takip edilebilir.

10Mbps Ethernet Portları

1) 10Base2

Buradaki 10 rakamı portun kapasitesini 10Mbps olduğu gösterir. Base kelimesi iletim ortamının temel band kullanıldığını gösterir. 2 ifadesi fiziksel bağlantı için ince(rg58) koaksiyel kablo kullanılması gerektiğini anlatır.

2) 10Base5

Fiziksel bağlantı için (rg8) koaksiyel kablo kullanılması gerektirir.

3) 10BaseT

Ethernet base portuna UTP kablo bağlanır

100Mbps Ethernet Portları

1) 100BaseTX

Fiziksel bağlantı için UTP CAT5 kablo kullanılır.

2) 100BaseF

Fiziksel bağlantı için fiber kablo kullanılır.

1000Mbps Ethernet Portları

1) 1000BaseT

CAT5 ve CAT6 kablo kullanılır.

2) 1000BaseLX

Fiziksel bağlantı için tek modlu fiber yada çok modlu fiber kablo kullanılabilir. Çok modlu fiber ile yaklaşık 500metre, tek modlu fiber ile 3km ye kadar 1000Mbps kapasitesinde bağlantı sağlanabilir.

3) 1000BaseSX

Yalnızca çok modlu fiber kablo kullanılır. Dalga boyuna bağlı olarak mesafe 250-500metre arasındadır.

Çeşitli tanımlar FSk notlar (bunları internet programcılığı I derslerimde de yazdıracağım)

Client – Server Sunucu Kavramları / Mimarisi

İstemci – Sunucu mimarisinde, hizmet veren bir sunucu ve hizmet alan bir veya birden fazla istemci bulunur. İstemciler sunucuya bağlanarak vermiş olduğu hizmetlerden yararlanır. Doğal olarak sunucu bilgisayarların performansı istemcilerden daha iyi olmak zorundadır. Sunucu bilgisayar, dosya, e-posta, web hizmetleri gibi görevleri sunmak için görevlendirilmiş bilgisayarlardır. Bu bilgisayarlarda işletim sistemi, ağ işletim sistemi olmak zorundadır.

İnternet ve TCP/IP (Transfer Control Protocol / Internet Protocol)

İnternet nedir?

Dünyada TCP/IP protokolünü kullanarak birçok bilgisayarın birbiri ile bağlı olduğu, bilgisayar veya bilgisayar ağlarının meydana getirdiği sürekli büyüyen iletişim ağına internet ağı denir. Oluşturulan tüm ağ yapılarının (LAN, MAN, WAN) bağlanabildiği ortak bir ağdır. Bu ağda tüm işlemler ve bağlantılar TCP/IP protokol kümesine göre çalışır. Bu ağ üzerinde aynı protokolü kullanarak çok farklı cihazlar (kamera, bilgisayar, cep telefonu) ve sistemler (Linux, Windows, Unix, MacOs) ortak bir ağda TCP/IP üzerinden verilen hizmetlerden ve imkanlardan faydalanabilmektedir.

Verinin diğer tarafa gideceğinin garantisi vardır.

Intranet nedir?

Çoğunlukla TCP/IP protokolü kullanarak, bir şirket ya da kuruma ait tüm LAN veya WAN yapılarının içine alan bir ağdır. Temel amacı kuruluş içerisinde bilgi paylaşımı sağlamaktır.

TCP/IP nedir?

Internet üzerinde bilgisayarların haberleşmesine, veri iletimi ve paylaşımını belirleyen kurallara TCP/IP kuralları denir. TCP/IP içerisinde destekleyici veya başka başka fonksiyonlara sahip olan birçok protokol de bulunmaktadır. Örneğin dosya transferi için FTP, e-postalar için SMTP, internet üzerinde başka bilgisayarlara bağlantılar için TELNET.

Sunucu Tarafında Kullanılan Web Tabanlı Servisler

1) **HTTP**
2) **HTTPS**
3) **SMTP (Simple Mail Transfer Protocol)**
4) **DNS**
5) **FTP (File Transfer Protocol)**
6) **POP3 / IMAP**
7) **Proxy (Vekil Sunucu)**
8) **WWW (World Wide Web)**
9) **URL (Uniform Resource Locator) ** dahil olup olmadığı muallakta.**

HTTP – Hyper Text Transfer Protocol

İnternet üzerinde sunucu ve istemci arasında veri transferinin kurallarını ve yöntemlerini düzenler. Text ve grafik tabanlı bilgileri içerisinde barındıran, kullanıcı ile etkileşimde bulunan, nesne ve teknolojiye sahip HTML (Hyper Text Markup Language) dosyalarının transferinde kullanılır. Bir web sitesinin adresini yazarken başına HTTP konulmadığında tarayıcı otomatik olarak bunu ekler.

Çünkü sunucudan siteye ait bilgilerin alınabilmesi için isteğin (request)mutlaka HTTP ile yapılması gerekir. Bu protokolü kullanarak HTML tabanlı belgeleri görüntülemek için tarayıcılar kullanılır.

HTTPS (security)

İnternette sunucular ve istemci arasında veri transferinin 3. kişiler tarafından okunamayacak şekilde nasıl aktarılacağına dair kurallar ve yöntemleri düzenler. Özellikle internet bankacılığında veya e-ticaret sitelerinde adres çubuğundan HTTPS yazar.

SMTP (Simple Mail Transfer Protocol)

E-posta göndermek için sunucu – istemci arasındaki iletişim şeklini belirleyen protokoldür. Sadece e-posta göndermekte kullanılır. İstemci SMTP sunucuya bağlanır, kimlik kontrollerini yapar, postayı gönderir.

DNS (Domain Name Server)

İnternet üzerinde yer alan tüm sitelerin bir IP adresi vardır. Siteyi ziyaret etmek istediğimizde sitenin adresi kullanılır. Arka planda veri alışverişi IP numarası üzerinden gerçekleşir. Ancak her sitenin IP adresini akılda tutmak zor olduğundan siteler alan isimleriyle kullanılır. DNS adreslerin IP karşılığını verin sistemlerdir/sunuculardır. Bu karşılıklar veri tabanlarında tutulur. Bu veritabanlarına DNS sunucu da denir.

Alan adı: Domain Name
Alt alan adı: Sub Domain Name (Aynı alan adına bağlı birden fazla alt alanlar açılabilir ve bunlar birbirinden bağımsız kullanılabilir. Alt alan adı, alan adından önce nokta konularak kullanılır.)

FTP (File Transfer Protocol)

TCP/IP protokolünü kullanarak internet üzerinden dosya aktarımı ve paylaşımı sağlayan protokoldür. Dosyalar FTP sunucuda tutulur. FTP hizmetlerinden faydalanmak için FTP.exe isimli Windows içerisinde bir konsol uygulaması vardır. Bu program, çalıştır'dan ulaşılıp aktif hale getirilir. FTP amaçlı kullanılan CuteFTP, Filezilla, SmartFTP gibi programlar da vardır. Bu programlar kullanıldığında komut kullanmanıza gerek yoktur.

TELNET

Uzaktaki bir bilgisayara bağlanarak o bilgisayarın terminaliymiş gibi çalışılmasını sağlar. Bağlanılan bilgisayar tıpkı kendi bilgisayarımız gibi kullanabiliriz. TELNET gibi kullanılan başka programlar da vardır. TELNET'in birçok komutu vardır.

POP3

Bir kullanıcı e-postasını SMTP yoluyla alıcıya gönderir. Alıcının postaları çekmesi için SMTP kullanılamaz çünkü SMTP tek yönlüdür. Postaların alınabilmesi için POP3 ya da IMAP kullanılır. POP3 postaların alınmasını ve posta kutularının yönetilmesini sağlar. Postaları almak için kullanılır.

IMAP (Internet Messages Access Protocol)

POP3 gibi gelen postaları almak için kullanılır.
Aralarındaki fark:
- POP3 postaları sunucudan bilgisayara indirir. IMAP postaları bilgisayara indirmez.
- IMAP vasıtasıyla farklı bilgisayarlardan postaları okuyabilirsiniz, POP3 ile bu olmaz.

PROXY SERVER

İnternete erişim sırasında kullanılan ara sunucudur. Proxy kullanıldığında istek vekil sunucuya iletilir, vekil sunucu istenilen sayfaya bağlanır aldığı içeriği istekte bulunan tarayıcıya iletir. Tek bir bilgisayar için de kullanılabilir, komple bir ağ için de kullanılabilir. İnternete bağlanmak için Proxy server'a ihtiyaç zorunlu değildir.

Avantajları:
- Çok fazla ziyaret edilen sayfalar Proxy tarafından önbelleğe alındığından işlemlerde çabukluk sağlar.
- Güvenlik için erişim engellenebilir.
- Aynı sunucuyu kullanan birden fazla istemci varsa kimin nereyi ziyaret ettiği takip edilebilir.
- Virüs içeren sayfalar istemciye gönderilmeden Proxy tarafından temizlenme imkanı vardır.
- Yasaklanan sitelere erişim sağlanabilir.

WWW (World Wide Web)

Hyper-media (ses, görüntü, video…) tabanlı dosyalardan oluşan siteleri taramak amacıyla kullanılır. Temelde HTTP üzerinde çalışır.

URL (Uniform Resource Locator)

Web tarayıcı aracılığı ile ziyaret edilen sitenin adresine URL denir. URL'nin ilk bölümü transfer protokolünü (http, ftp…) ikinci bölüm alan adını (domain), diğer bölüm dizin ve sayfanın dosya adını gösterir. İnternet üzerinde yayınlanan sayfaların tamamı sunucu üzerinde bir dizinde depolanır. Tarayıcınızda www.websitem.com yazdığınızda sunucu üzerindeki websitem dizininin içeriği gösterilir. (C:\apache\htdocs\websitem)

Dijital Sertifikalar

Dijital sertifika günlük hayatta kullanılan ehliyet, pasaport gibi kimliklerin elektronik ortamdaki karşılığıdır. Ulaşılmak istenen bilgiye erişim hakkını ispatlamak için kullanılır. Dijital sertifikalar bilgilerin internet üzerinde güvenli bir şekilde iletilmesini ve veri bütünlüğünü sağlar. Verilerin şifrelenmesi ve şifresinin çözülmesi için kullanılır.

- cyber-cash / SET (e para transferi için)
- PGP / S-MIME (E-postalar için)
- IPSEC (Paket seviyesinde şifreleme)
- TLS / SSL (TCP/IP seviyesinde şifreleme)

SSL (Secure Socket Layer)

İnternet üzerinden şifrelenmiş veri iletişimi sağlar. Web tarayıcı ve web server arasındaki güvenliği sağlar. Veri gönderilirken şifrelenir. Sunucu tarafında deşifre edilerek alınır. İletilen veri sadece doğru alıcı tarafından açılabilir. Şifreleme yönteminin gücü şifre anahtarının uzunluğuna bağlıdır. 8 bitlik bir şifre 256 olasılık içeren değer alabildiğinden çözülmesi kolaydır. Günümüzde 128 bitlik şifreleme kullanılmaktadır. (2^128) kadar farklı değer olduğundan çözülmesi 67 yıl civarı sürmektedir. SSL protokolü sunucu ve istemci arasında şu nesneleri şifrelemektedir:

- Sunucudan istenen doküman içeriği ve bunun URL'si
- Kullanıcının doldurduğu ve gönderdiği form bilgileri şifrelenir
- HTTP başlık içeriği şifrelenir
- Her türlü çerez işlemleri şifrelenir.

Coaxial Cable

-

-

RG-8: Diğerlerine göre daha kalın bakır iletkene sahiptir. 500 mt mesafeye kadar 10 Mbps hızında veri aktarımına imkân tanır. Piyasada 10Base5 Lan standardı olarak bilinir. 50 ohm empedans değerine sahiptir. Sonlandırmak için 50 ohm empedans değerine sahip BNC konnektör kullanılır.

RG-58: 180 metreye kadar 10 Mbps veri hızına sahiptir. Piyasada 10Base2 Lan standardı olarak bilinir. 50 ohm empedans değerine sahiptir. 50 ohmluk empedans değerine sahip konnektör kullanılır.

10 Mbps'lik hız günümüzde düşük kalmaktadır. Yavaş yavaş UTP (Unshielded Twisted Pair Cable – bildiğimiz internet kablosu) kablolar koaksiyel kabloların yerini almaya başlamıştır.

CATEGORY 1,2,5,6 (CAT2, CAT1, CAT5, CAT6)

CAT1: Telefonlarda kullanılır.

CAT5: Yerel ağ bağlantıları için kullanılır. Neredeyse tüm yerel ağ bağlantıları CAT5 UTP kablolarıyla yapılmaktadır. 100 Mbps'lik veri aktarım aktarım kapasitesine sahiptir. Dolayısıyla 100 Mbps hızını destekleyen Ethernet kartı ile çalışırlar. En etkili alanı 100 mt'dir.

CAT6: Category 5 (CAT5) kablosuna göre daha üstün üretim tekniği ile üretildiğinden dolayı 1000 Mbps veri aktarım hızı kapasitesine sahiptir. Gigabit Ethernet kartları ile kullanılır. UTP kabloyu sonlandırmak için RJ45 konnektör kullanılır. Kablo düzgün bir şekilde sonlandırılma veri taşıma kapasitesi düşer. Dolayısıyla sonlandırma bağlantıları düzgün yapılmalıdır. Ayrıca UTP kablolarda sonlandırmalar **düz** ve **çapraz** olarak iki şekilde yapılabilir. Örneğin bir bilgisayarı başka bir bilgisayara bağlarken **çapraz** bağlanmış kablo kullanılır. Çünkü bir uçtaki bilgisayardan çıkan veri, diğer bilgisayar için girdi olacaktır.

PORT – 1	**PORT – 2**	**BAĞLANTI TİPİ**
PC	PC	Çapraz UTP Kabloyla
PC	Hup/Anahtar (Switch)	Düz UTP Kabloyla
Hup/Anahtar	Hup/Anahtar	Çapraz UTP Kabloyla
Hup/Anahtar	Yönlendirici (Router)	Düz UTP Kabloyla
PC	Yönlendirici (Router)	Çapraz UTP Kabloyla

Yeni nesil bazı anahtar cihazları bağlantı kablosunu düz mü çapraz mı bağlandığını sezer, ona göre çalışmasını ayarlamaktadır. Çapraz bağlantının düz bağlantıdan farkı; alıcı (RX) ve verici (TX) uçlarının birbirine karşılıklı (RX-TX – TX-RX) olarak bağlanmasıdır.

Fiber Optik Kablolar

- **SORU: FİBERİN ÇALIŞMA PRENSİBİ NEDİR?**
- **SORU: FİBER İLE BAKIR ARASINDAKİ FARKLAR?**
- ****'**

Fiber optik kablo yüksek maliyetine karşılık üstün bir iletim ortamı sağlar. Diğer fiziksel iletim ortamlarının aksine veri optik dalgalar aracılığıyla ışığın yansıma kurallarına göre iletilir. Bu nedenle bozucu elektromanyetik faktörlerden etkilenmez. Ayrıca elektriksel sinyallerle kıyaslandığında mesafeye göre sinyalin zayıflama oranı da daha azdır. Bakır kablolarda olduğu gibi gerilim farkından kaynaklanan topraklama problemi de yoktur. Hatalı bit oranı (BER – bit error rate) bakırın 1/1000 oranındadır. **Tüm bu nedenlerden ötürü fiber optik uzun mesafelerde yüksek band genişliğine ihtiyaç duyan ses ve veri aktarımı için ideal bir kablodur.

Ses ya da verinin fiber optik ortama verilmeden önce optik dalgalara çevrilmesi gerekir. Verici tarafında ışık kaynağı olarak LED ya da lazer diyot kullanılır. Alıcıya ulaşan optik dalgalardan elektriksel sinyalleri elde edebilmek için foto diyot ya da foto transistör kullanılır. Fiber optik kablolar tek modlu ya da çok modlu olarak iki çeşittir.

Tek Modlu Fiber Kablo (Single Mode): Uzun mesafelerde yüksek band genişliğine imkân verir. Dolayısıyla uzak mesafe bağlantıları için tercih edilir. Burada optik dalga üretmek için **lazer diyot** kullanılır. Dolayısıyla donanım maliyeti yüksektir.

Çok Modlu Fiber Kablo (Multi Mode): Bina ya da kampüs içi gibi daha küçük mesafelerde kullanılmaktadır. Optik dalga üretimi led ile yapılır.

Fiberden önce bölgeler ve ülkeler arası uzak mesafe için uydu bağlantıları kullanılıyordu. Günümüzde internetin omurgasını fiber optik kablolar oluşturmaktadır.

Yerel Ağ Protokolleri

Ethernet Protokolleri

İntel ve Xerox firmaları tarafından geliştirilmiş bir protokoldür. Daha sonra IEEE tarafından standartlaştırılmıştır. Piyasada birçok kaynaktan IEEE 802.3 adıyla da bilinir.

Ethernet protokolü ikinci katmanda tanımlı bir protokoldür. İkinci katman protokolleri ağ katmanından aldıkları veri paketlerini kendilerine çerçeve (frame) biçimine dönüştürerek iletim ortamına göndermektedirler. Ethernet protokolünde yerel ağa bağlı herhangi bir bilgisayar veri çerçevesi gönderdiğinde diğerlerinin beklemesi gerekir. Eğer beklemezlerse fiziksel hatta aynı anda birden fazla çerçeve olacağından çarpışma (collision) meydana gelir. Yoğun kullanılmayan ağlarda çarpışma olmayacağından fazla sorun çıkmaz. Yoğun kullanılan ağlarda mutlaka akılcı bir planlama yapılmalıdır. Bunun dışında uygun donanım birimleri seçilmelidir.

Ethernet Bağlantı Kapasiteleri

Ethernet protokolü en ilkel durumda 10 mbps bağlantı kapasitesine sahiptir. Günümüzde bu yetmemektedir. Kapasite 1000 mbps'a kadar arttırılmıştır. Ethernet kartları ya da ağ cihazlarının kapasiteleri 100 ve 1000 mbps olarak üretilmektedir. 100 mbps portlar, fast Ethernet, 1000 mbps giga port olarak bilinir. Ethernet portlarının kapasitesi ve bu portlara ne tür kablo ve konnektör bağlanabileceği port üzerinde yazan ifadelerden anlaşılabilir.

10 mbps'lık Ethernet portları

- 10 Base 2
- 10 Base 5
- 10 Base T

Olarak 3 çeşittir.

10 Base 2: 10 rakamı portun kapasitesinin 10 mbps olduğunu ifade eder. Base kelimesi iletim ortamının temel band (base band) kullanıldığını ifade eder. En sondaki 2 ise fiziksel bağlantı için ince (RG-58 coaxial cable) kullanıldığını ifade eder.

10 Base 5: ince değil de kalın kablo kullanılmıştır. (RG-8)

10 Base T: T ise Ethernet portuna UTP kablosu bağlanması gerektiğini ifade eder.

100 Base TX: Fiziksel bağlantı için UTP CAT5 kablo en çok kullanılan fast Ethernet budur.

100 Base FX: Fiziksel bağlantı için fiber kablo kullanılır.

1000 Base T: UTP CAT5 veya CAT6 kablolar kullanılabilir. Ancak CAT6 kablonun üretim tekniği daha üstün olduğundan tercih sebebinin. Haliyle maliyet artar.

1000 Base LX: Fiziksel bağlantı için tek modlu fiber kablolar ya da çok modlu fiber kablo kullanılabilir. SMF ile 3 km'ye kadar 1000 mbps kapasitesinde bağlantı sağlanır. MMF ile 500 metreye kadar 1000 mbps bağlantı kapasitesi sağlanır.

1000 Base SX: sadece çok modlu fiber kablo kullanılır. Desteklediği mesafe 500 m'dir.

Günümüzde 10 mbps portlar pek tercih edilmemektedir. 1000 mbps'lık portlar daha çok merkezi olarak konumlandırılmış yerlerde tercih edilir. Giderek yaygınlaşmaktadır. En çok 100 mpbs'lık portlar kullanılmaktadır.

Mac Adresi ve Adres Çözümleme

Yerel ağdaki bir bilgisayarla haberleşmeyi sağlayan Ethernet çerçevesinde 48 bitlik bir adres kullanılır. Bu adres Mac adresi olarak bilinir. Yerel ağ için de IP 3. Katmanda tanımlı bir adrestir. Mac adresi, ikinci katmanda tanımlıdır ve Mac adresiyle veri aktarımı karşılıklı olarak daha kolay ve daha hızlıdır. Yerel ağdaki bilgisayar ve ağ cihazları birbirlerine doğrudan ya da dolaylı olarak Ethernet kartları vasıtasıyla bağlanırlar yani Ethernet kartı, Ethernet protokolünü kullanan ağ bağlantı ara yüzleridir. Unique'tir, üretici tarafından üretim esnasında verilir. Mac adresi 48 bitlik bir adres olup ilk 24 biti kartın üretici kodunu son 24 bit ise kartın üretimde atanan seri numarasını verir. Bir üretici daha önce kullandığı seri numarasını ikinci bir defa kullanamaz. Eğer aynı Mac adresini kullanan iki Ethernet kartı aynı yerel ağda bulunursa karışıklık çıkar, hatalar meydana gelir.

Yerel ağdaki bilgisayar ve ağ cihazlarının birbirleriyle haberleşebilmeleri için birbirlerinin Mac adreslerini bilmeleri gerekir. Başlangıçta hiçbiri diğerinin Mac adresini bilmez. Bunun için ARP (address resolution protocol) denilen bir protokol kullanılır.

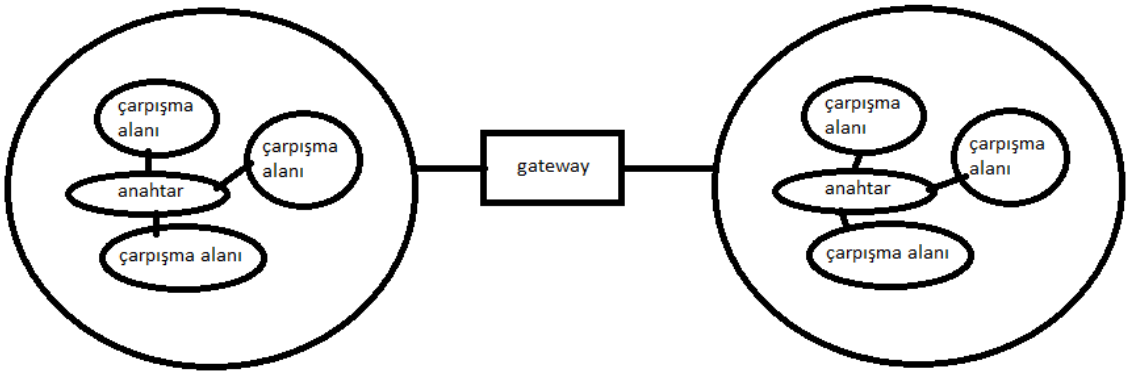
Yayın Adresi (Broadcast Adress): Tüm yerel ağı temsil eden bir IP adresidir. Bu adrese gönderilen bir paket tüm yerel ağ elemanları tarafından alınır.

Yayın Paketi (Broadcast Package): Yerel ağın yayın adresine gönderilen paketlere yayın paketleri denir. Yayın paketi, ağ elemanlarının Mac ve IP adreslerini öğrenmek için kullanılır. Yerel ağdaki herhangi bir bilgisayar açıldığı zaman ağa bir yayın paketi gönderir. Bu paketle kendi Mac ve IP adreslerini verir; bu yayın paketini alan bilgisayarlar kendi IP ve Mac adreslerini gönderirler. Her bilgisayar üzerinde diğerlerinin IP ve Mac adreslerini tutan bir tablo oluşturur.

Yayın Alanları ve Çarpışmalar

Yayın alanı: Bilgisayarların doğrudan MAC adresleriyle haberleşebildikleri alandır. Bir bilgisayar yayın paketini gönderdiğinde onu alabilen tüm bilgisayarlar aynı yayın alanındadır. Bir bilgisayar kendi yayın alanında olmayan başka bilgisayarlarla iletişim kurabilmek için ağ geçidini (gateway) kullanmak zorundadır.

Çarpışma alanı: Bir yayın alanı içinde bir ya da birden fazla çarpışma alanı bulunabilir. Aynı çarpışma alanındaki bilgisayarlar birbirlerine gelen her paketi görürler. Ancak sadece kendi MAC adreslerine gelen paketleri kabul ederler. Çarpışma alanı aynı anda sadece tek bir bilgisayar tarafından kullanılabilir, iki bilgisayar aynı anda paket göndermek isterse çarpışma olur. Yayın ve çarpışma alanları ağ tasarımında dikkat edilmesi gereken konulardandır. Özellikle trafik yoğunluğu fazla olan ağlarda bu alanlar daraltılıp bölünerek çarpışma önlenmeye çalışılır. Bir yandan da, ağın performansının artması hedeflenir.



Yerel Ağ Bağlantı Donanımları

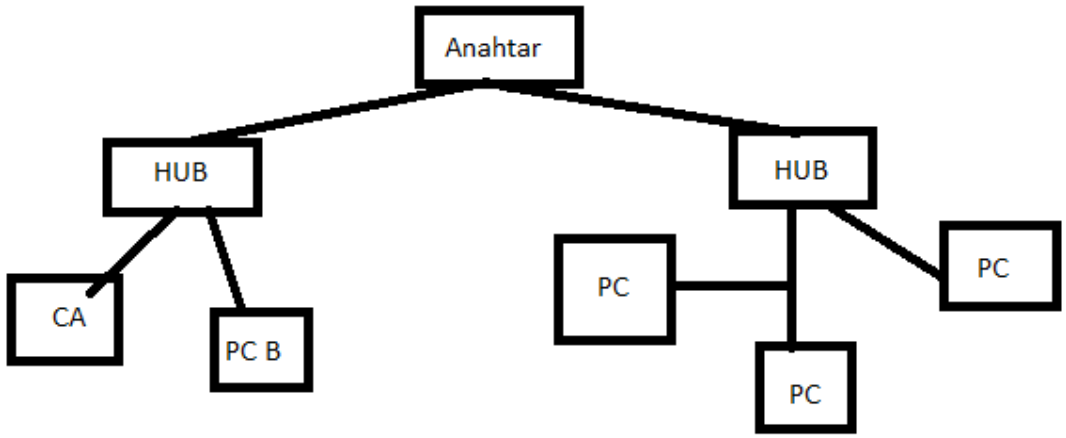
1. **Hub**
2. **Anahtar (Switch)**

HUB: Birinci katmanda çalışan LAN donanımıdır. HUB kendi portundan aldığı sinyalin genliğini yükselterek diğer tüm portlarından gönderen bir donanımdır. Böylece bir porttan gelen veri paketini HUB'ın diğer portlarına bağlı birçok bilgisayar alabilir. Diğer bir ifadeyle aynı HUB'a bağlı bilgisayarlar aynı çarpışma alanında bulunurlar. HUB'lar bilgisayarları birbirine bağlayabilmek amacıyla kullanılırlar. Port sayısını arttırabilmek için birkaç HUB arka arkaya bağlanabilir. Bu durumda birçok bilgisayar birbirine doğrudan ya da dolaylı olarak HUB ile bağlanacağından çarpışma alanı genişleyecektir. Bunun aksi tarafı da var. Sinyal defalarca yükseltileceğinden hata oranı da yükselir. İkincisi çarpışma alanı da aşırı büyüyeceğinden veri akışında tıkanmalar da yaşanır. O halde en fazla 3 tane HUB'ı art arda bağlamak bu gibi hataları azaltır. Trafiğin yoğun olduğu noktalarda. HUB yerine anahtar tercih edilmelidir.

Anahtar(Switch): İkinci katmanda çalışan donanım birimidir. Ayrıca anahtarlar akıllı cihaz grubundandır. HUB'lara karşı açık bir teknolojik üstünlüğü vardır. Anahtarlar, ağdaki yayın paketini dinlerler ve kendi portlarına bağlı tüm bilgisayarların MAC adresini bünyelerinde bir tabloda tutarlar. Dolayısıyla gelen paketi hangi portundan nereye göndereceğini tahin edebilir. Anahtarın bir portundan aldığı paketi başka bir portuna göndermesi işlemi "**forwarding"** olarak bilinir. Bu işlemi kavramsal olarak yönlendirme (routing) kavramı ile karıştırmamak gerekir. Çünkü iletme işlemi MAC adreslerine göre yapılmaktadır ama yönlendirme işlemi IP adreslerine göre yapılmaktadır. Dolayısıyla yönlendiriciler ve anahtarlar farklı donanım birimleridir.

Anahtarlar bir yayın alanı içerisinde birçok çarpışma alanı oluşturmak için kullanılır. Anahtarın her bir portu ayrı bir çarpışma alanıdır.

Örneğin, 10 portlu bir anahtarın kullanıldığı yayın alanında 10 tane çarpışma alanı bulunur. Böylece yerel ağın performansı artar. Aynı olayda HUB kullanılırsa, HUB'ın port sayısı ne olursa olsun, bir tane çarpışma alanı var demektir.

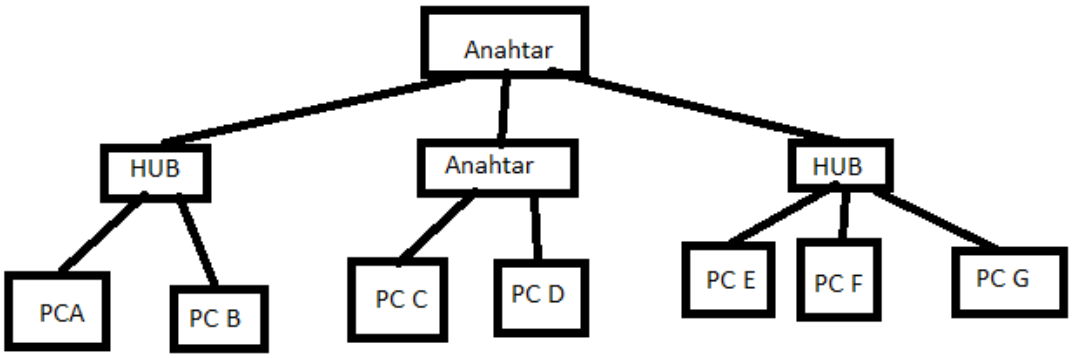


Soru 1) Kaç çarpışma alanı vardır?

- Anahtara bağlı her porta bakacak olursak 2 adet çarpışma alanı vardır.

Soru 2)

- Birinci çarpışma alanında CA ve PC B olarak 2 bilgisayar, ikinci çarpışma alanında PC, PC, PC olmak üzere 3 adet bilgisayar vardır.



- PCA ve PC B bilgisayarları HUB ile birbirlerine bağlı olduklarından aynı anda paket göndermeye çalıştıklarında çarpışma olur. Bu yüzden her ikisinin de paketi boşa gider. Bu nedenle A ve B aynı anda paket gönderemez.
- Buradaki herhangi bir bilgisayar yayını paketi gönderdiğinde diğerlerinin hepsi alabilir. Ancak fiziksel bağlantının yanı sıra IP yapılandırılması da önemlidir. Tüm bilgisayarların aynı yayın adresine sahip olması gerekir.

- C ve D bilgisayarları anahtar ile birbirlerine bağlanmıştır. Bu nedenle aynı çarpışma alanı içerisinde değillerdir. Dolayısıyla C ve D bilgisayarlarının aynı anda paket göndermesinde sakınca yoktur.
- A ile C arasındaki bağlantı, merkezi anahtar üzerinden gerçekleşir. Bu nedenle ikisinin de aynı anda başka bir yere paket göndermesinde bir sakınca yoktur.
- E, F ve G HUB ile birbirlerine bağlıdır. Bu nedenle herhangi biri diğerine gelen paketi görür.
- Bir anahtarın her portunun farklı bir çarpışma alanı olduğunu söylemiştik. C ve D bilgisayarlarının birbirinden bağımsız birer çarpışma alanı vardır. Diğer yandan merkez anahtara bağlı HUB'lar da birer çarpışma alanına sahiptir. Böylece toplamda dört tane çarpışma alanı olur.

Anahtarların üzerindeki portlara başka anahtarlar, HUB'lar ya da doğrudan bilgisayarlar bağlanabilir. Bu portlar giriş portu olarak adlandırılır. Diğer yandan anahtar üzerinde çıkış (uplink) adı verilen tek bir port ile ağ geçidine ya da VLAN anahtarlarına bağlantı yapılan bir port bulunur. Genelde çıkış portunun kapasitesi diğerlerinden fazladır. Anahtarın giriş portları 10 ya da 100 Mbps kapasitesine sahiptir. Çıkış portu ise genelde daha yüksek bir kapasiteye sahiptir.

Bir anahtarın üzerinde 9'u giriş 1'i çıkış olmak üzere 10 port olduğunu düşünelim. Giriş portlarının kapasitesi 100 Mbps, çıkış portununki ise 1000 Mbps olsun. Bu durumda giriş portlarının tümü tam kapasiteyle ağ geçidi üzerinden internete çıkabilirler. Ancak gerçekte durum her zaman böyle değildir. Her anahtarın, üzerindeki trafiği çevirebilme kapasitesi (switchfabric / throughput) farklıdır. Örneğin; bir anahtarın çevirme kapasitesi 4000 Mbps olarak verilmişse bu, aynı anda tüm portların yaratabileceği trafik 4000 Mbps değeri geçemez anlamına gelir. Trafik çevirme kapasitesi bir anahtar cihazında aranması gereken en önemli kalite parametresidir. Özellikle trafiğin yoğun olduğu ağlarda merkezi olarak konumlandırılmış anahtarlar için çevirme kapasitesi oldukça önemlidir.

Ağ Geçitleri (Gateway)

Klasik LAN tasarımında bilgisayarlar bir HUB veya anahtar kullanılarak birleştirilir. Anahtarlar çarpışma (collision) trafiğini geçirmedikleri için performans açısından HUB'lara tercih edilirler. Ancak anahtarlar çarpışma trafiğini geçirmemelerine rağmen yayın (broadcast) trafiğini geçirirler. Bünyesinde çok fazla bilgisayar bulunan yerel ağda yayın paketlerinin çokluğu ağı hantallaştırır. Bu nedenle LAN'ları birden çok LAN'a bölmek, yani sanal LAN'lar oluşturmak performansı arttıracaktır.

Bir yerel ağı birden çok yayın alanına bölmeden önce farklı çalışma grupları (sanal LAN) belirlenir. Örneğin; bir binanın her bir katı farklı bir çalışma grubu olarak ele alınabilir. Eğer temel kriter güvenlikse, şirketin farklı departmanları birer çalışma grubu olarak düşünülebilir. Kısaca çalışma gruplarının nasıl seçileceği ihtiyaca ve şartlara bağlıdır. Daha sonra her bir çalışma grubu ayrı ayrı anahtarlar üzerinde birleştirilir. Bu anahtarlar ağ geçidi üzerindeki farklı ağ arayüzlerine (Ethernet kartlarına) bağlanır. Her bir çalışma grubunun yayın adresi farklı olacağından LAN'da birçok yayın alanı oluşturulmuş olur. Bu yayın alanları arasındaki irtibat, ağ geçidi üzerinden yapılır.

"Ağ geçidi" adı, yönlendirme ve yerine göre protokol çevirme işlemini yapan tüm cihazları kapsar. Bu, bir bilgisayar, yönlendirici (router) ya da özel üretilmiş bir cihaz olabilir. Kısacası ağ geçidi bir kavramdır ve yönlendirme, protokol çevirme, sinyal dönüştürme gibi işlemleri yapan her türlü donanıma verilen genel bir addır.

Tekrarlayıcılar (Repeater): Bakır kablolar verileri 100-150 m kadar taşıyabilir. Sonrasında taşınan sinyal zayıflar. Sinyalin zayıflaması bozulma anlamına gelir. Bunun için tekrarlayıcı denilen cihaz kullanılır. Bu sayede veri bozulmadan tekrarlanmış olur. Tekrarlayıcılar verileri elektrik uzatma kablosunda olduğu gibi elektriksel sinyal olarak algılar. **Verinin kim tarafından gönderildiği, kime gönderildiği gibi çözümlemeler yapılmaz**. Tekrarlayıcı 4.5V'luk bilgisayar ağı sinyalini uzak mesafeye taşır.

Ağ Sistemleri FSK notlar

Ağ Cihazları ve Protokollerin Sınıflandırılması

- **OSI Model (Open System Interconnection)**

Bir bilgisayardan gönderilen verinin ağ ortamı üzerinden başka bir bilgisayara nasıl ulaştığını anlatmak için tasarlanmıştır. OSI bu iletişimi yedi katmanlı bir yapıyla tanımlar. Her katmanın fonksiyonu diğer katmanlardan bağımsız olarak teker teker tanımlanır. OSI, ISO tarafından tasarlanmıştır. OSI modeli bilgisayar ağlarında ortak bir dil konuşulmasını sağlamak amacıyla geliştirilmiş katmanlı bir modeldir. Bir katman görevini tamamlamadan diğer katmana geçiş gerçekleşmez. Her katman bir üst katmana hizmet eder ya da bir alt katmanın sunduğu hizmetten yararlanır. Yani işlemler iki taraflı gerçekleşir. Kullanıcı bilgisayar başında kullanmış olduğu program aracılığı ile ağa veri aktarmak isterse en üstteki katman olan uygulama katmanından en alttaki katman olan fiziksel katmana doğru bir düzenleme yapılır. Tersine ağdan kullanıcıya doğru veri aktarılacaksa en alttaki katman olan fiziksel katmandan en üstteki katman olan uygulama katmanına doğru akış gerçekleşir.

- 7 → Uygulama Katmanı – Application Layer
- 6 → Sunum Katmanı – Presentation Layer
- 5 → Oturum Katmanı – Session Layer
- 4 → Taşıma/Aktarım Katmanı – Transport Layer
- 3 → Ağ Katmanı – Network Layer
- 2 → Veri Bağlantı Katmanı – Data Link Layer
- 1 → Fiziksel Katman – Physical Layer

1 → Fiziksel Katman

Fiziksel katman bakır kablo, fiber optik kablo ve kablosuz bağlantılar aracılığıyla bilgisayar ağına aktarılan sinyallerin düzenlenmesinden taşınmasından ve hedef birim tarafından alınması işlerinden sorumludur. Yani, kablolu ve kablosuz ortam üzerinden taşınan sinyallerin veri aktarım mantığına uygun duruma getirilmesi fiziksel katman kontrolünde gerçekleştirilir. Sayısal haberleşme sistemlerinde iletilebilen en küçük bilgi bit olarak adlandırılır. Dolayısıyla fiziksel hattın bağlantı hızı bit/saniye olarak (bps) ifade edilir. Bu katmanda çalışan donanımlar şunlardır;

1) UTP, Koaksiyel, Cat, Fiber optik gibi kablolar
2) RF sinyal göndericileri ve alıcıları
3) Kabloların mekanik olarak sonlandırmaya yarayan konnektörler
4) Sinyalin elektriksel sinyalini yükselten ve aynı sinyalin birden fazla noktaya iletilmesini sağlayan HUB'lar
5) Tekrarlayıcılar (Repeater)

6) Sinyalin uzak mesafeleri taşınabilmesini sağlayan modemler, ayrıca daha yüksek hızlar için kullanılan PDH, SDH modemler
7) TDM anahtarları
8) Ethernet kartları (NIC → Network Interface Card)

2 → Veri Bağlantı Katmanı

Fiziksel katmanda kullanıcı verilerinin elektriksel sinyallere dönüşümü gerçekleştirilir. Bu verilerin herhangi bir değişime uğramadan fiziksel katmana iletilmesi gerekir. Bu iletim aşamasındaki basamaklardan birisi veri bağlantı katmanıdır. Veri bağlantı katmanı OSI üçüncü katmandan gelen veri akışının kontrolünü sağlayan ve kontrol edilmiş veriyi elektriksel sinyallere dönüştürmesi için fiziksel katmana gönderen bir katmandır. Başka bir anlatımla veri bağlantı katmanı fiziksel katmandan alınan bilgilerin gönderilen bitlerle aynı olup olmadığını test eder. Bunun için hata sezme yöntemleri vardır. Birincisi; eşlik sınaması (parity check), ikincisi; CRC (cyclic redundancy check).

Veri bağlantı katmanı fiziksel katmandan bitleri veya bir üstündeki ağ katmanından aldığı veri paketlerini çerçeve (frame) formatına dönüştürür. Çerçeveleme işlemi aynı zamanda kapsülleme (encapsulation) olarak da bilinir. Birbirine doğrudan bağlı ağ donanımlarının aynı çerçeve formatını (kapsülleme) yöntemini kullanıyor olması gerekir. Günümüzde en çok kullanılan ikinci ksatman protokolleri yerel alan ağları için Ethernet ve MAC adres, uzak alan ağ bağlantıları için PPP, Frame Relay ve ATM'dir. MAC (Media Access Control – Fiziksel Bağlantı Kontrolü) adres OSI 2 katmanında kullanılmaktadır. Ethernet kartı üzerinde bulunur. Fiziksel bir adrestir. Bilgisayar ağı uzmanı MAC adresi yapısını ve çalışma mantığını ayrıntılı bilmek zorundadır. İkinci katmanda çalışan protokoller veriyi kendilerine özgü fiziksel veya yerel adreslerle iletirler. Örneğin, Ethernet protokolü MAC adresini kullanır, Frame Relay protokolü DLCI adresini kullanır. Yerel ağ ya da veri şebekesi içerisinde sınırlı sayıda donanım olacağından bu donanımlar aralarında kendi fiziksel veya yerel adresleriyle haberleşebilirler.

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.
2

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.

Avantajları :

♣ 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:

3

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.
4

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.

5

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.

6

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.
7
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.
8
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.

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 bölmek gerekir

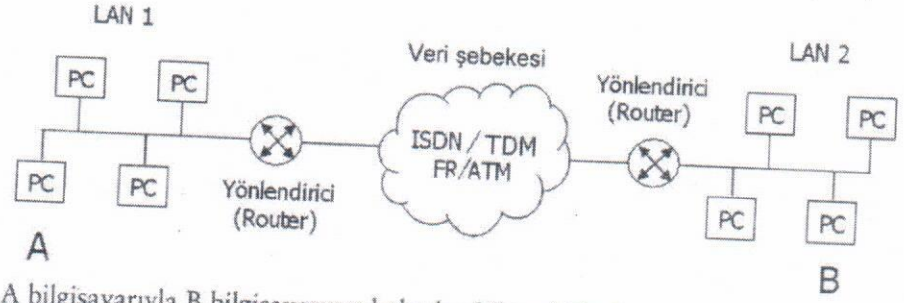
Mevcut network yapısı genişleyince Broadcast etki alanı da büyüyecek ve tüm networkdeki bilgisayarlar yoğun bir Broadcast trafiğinin ortasında sıkışıp kalacaklardır. Bu da ağ performansını negatif yönde etkileyecektir.
IP adreslerini de yine aynı şekilde ortamda gürültü (Broadcast trafiği) olmaması ve 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;

Ağ Katmanı (Network Layer)

Veri paketlerinin bir uçtan diğer uca birbirinden farklı haberleşme kanallarından (1. katman) ve veri şebekeleri (2. katman) üzerinden taşınmasına imkân veren katmandır. İşte interneti dünyanın farklı yerlerindeki farklı şebekeler üzerinden erişilebilir kılan katman budur. Aynı zamanda IP katmanı olarak da adlandırılır.

IP, mantıksal ve yönlendirilebilir bir adresleme protokolü olduğu için her türlü haberleşme kanalı ve veri şebekesi üzerinden haberleşmeye imkân tanır.

2. katman protokolleri, kendi fiziksel ya da yerel adreslerini kullandıklarından kısıtlı bir alanda iletişim imkânı tanırlar. Aşağıdaki örnekte görüldüğü gibi, birbirlerinden bağımsız yerel ağlarda bulunan bilgisayarlar, birbirlerinin Ethernet adreslerini bilemezler. Ancak her iki bilgisayarlara birer mantıksal adres verilir ve bu adreslere nasıl ulaşılacağı bilgisi bilinirse, iki bilgisayar farklı ağlarda olsa da haberleşme imkânına kavuşurlar.



A bilgisayarıyla B bilgisayarının haberleşebilmesi için 2 temel şartın sağlanması gerekir.

1. Her iki bilgisayar da birbirlerinin adresini bilmelidir. A ve B birbirlerinin yerel/fiziksel adreslerini bilemeyeceklerine göre her iki bilgisayara da mantıksal bir adres atanmalıdır.
2. Her iki bilgisayar da karşı adrese nasıl gideceğini bilmelidir. Bunun için gerekli yönlendirmelerin yapılması gerekir.

Ağ katmanının en önemli görevi, adresleri yönlendirme işlemidir. Bu işlem, birden fazla ağ arayüzüne (*network interface*) sahip bilgisayarlar ve yönlendirici (Router) adı verilen cihazlar tarafından yapılır. Yönlendiriciler 3. katman fonksiyonları çok güçlü olan ve internet'in omurgasını oluşturan cihazlardır. Yönlendirme işleminin ayrıntılarına ilerleyen bölümlerde girilecektir.

Aktarım Katmanı (Transport Layer)

MS Outlook, Internet Explorer, ICQ gibi uygulama programları için sanal iletişim kanalları kuran katmandır. Bu iletişim kanalları, port adı verilen servis numaraları kullanılarak kurulur. Aktarım katmanı, bu sanal iletişim kanallarının kurulmasından, yönetilmesinden ve sonlandırılmasından sorumludur. Ayrıca, iletişimin ne şekilde kurulacağı da bu katmanın görevidir. İki bilgisayar arasında sanal iletişim kanalı bağlantı temelli (connection oriented) ve bağlantısız (connectionless) olmak üzere iki şekilde kurulabilir. TCP ve UDP olmak üzere IP ağları üzerinde kullanılan iki farklı iletişim protokolü vardır.

TCP, bağlantı temelli bir protokoldür. Yani iki bilgisayar arasında veri aktarımı başlamadan önce karşılıklı görüşme yapılır. İstekte bulunan bilgisayar karşıdaki bilgisayara, ilgili servisinin müsait olup olmadığını sorar. Bu yönüyle TCP protokolünü, telefon görüşmesine benzetebiliriz. Görüşme başlamadan, karşıda biri varsa ve meşgul değilse bağlantı kurulur. Daha sonra konuşma başlar. Bu yönüyle güvenilir bir iletişim sağlar.

UDP, bağlantı temelli değildir. İki bilgisayar arasında önceden kurulmuş bir bağlantı olmadığından paketin iletimini garanti etmez. Yani gönderilen bilginin kaybolması durumunda gönderenin haberi dahi olmaz. Bu durum başlangıçta her yönüyle dezavantajlı gibi görünse de internet üzerinden yapılan video-konferans vs. gibi gerçek zamanlı uygulamalar için daha elverişlidir. (UDP protokolünü mektupla haberleşmeye benzetebiliriz. Siz mektubu posta kutusuna bırakırsınız, postacı alıcının adresine götürüp bırakır. Siz mektubun ulaşıp ulaşmadığından haberdar olmazsınız.)

Transport katmanının diğer bir görevi de uygulama katmanından aldığı bilgiyi **bölümleyerek** (segmentation), daha küçük parçalara ayırmaktır. Bölümlenmiş bu veriye segment adı verilir. Ağ katmanından alınan veri paketlerini de **birleştirerek** (desegmentation) uygulama katmanına iletir.

Uygulama Seviyesi (Application, Presentation, Session Layers)

OSI modelinin 5, 6 ve 7. katmanlarını uygulama seviyesi adı altında toplamamızda bir sakınca yoktur. Çünkü bu üç katmanın fonksiyonları da uygulama programları tarafından yönetilir. Bu üç katman arasındaki fark, ağ yöneticilerinden çok sistem programcılarının ilgilenmesi gereken bir konudur.

Ağ ortamında kullandığımız uygulama programlarını istemci (client) ve sunucu (server) olmak üzere iki başlık altında toplayabiliriz. Ms Outlook, Internet Explorer, CuteFTP, Msn Messenger vb. gibi programlar internet üzerinden servis aldığımız istemci programlarıdır. Bu istemci programların servis aldığı programlara ise sunucu programları denir. Örneğin; e-posta almak için MS Outlook'un bir e-posta sunucuya (POP3 ya da IMAP sunucusu) bağlanması gerekir. İstemci programlarının sunucu programlarına bağlanması (login) ve aralarındaki diyalogun yürütülmesi (dialogue control) oturum katmanı tarafından yürütülür.

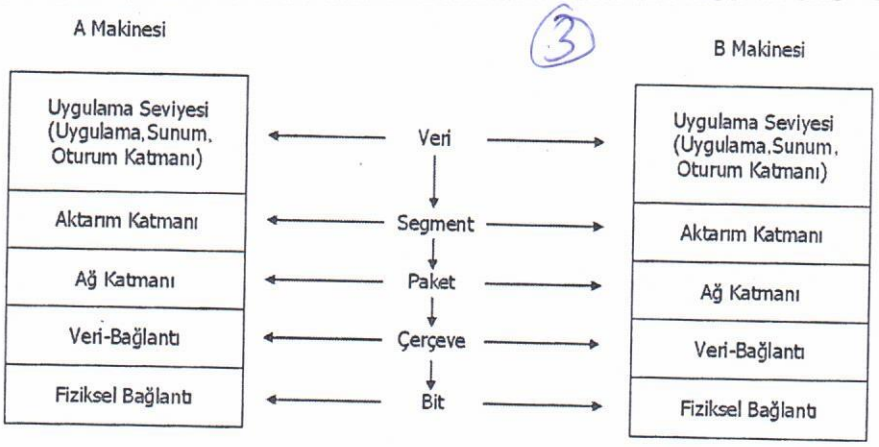
Bu uygulama programları arasındaki veri aktarımı ise daha alt seviyedeki aktarım katmanının sağladığı sanal iletim kanalları (portlar) üzerinden sağlanır. Bu nedenle farklı uygulamalar farklı port numaraları kullanırlar. Bilgisayarında

Verinin Gönderim Süreci

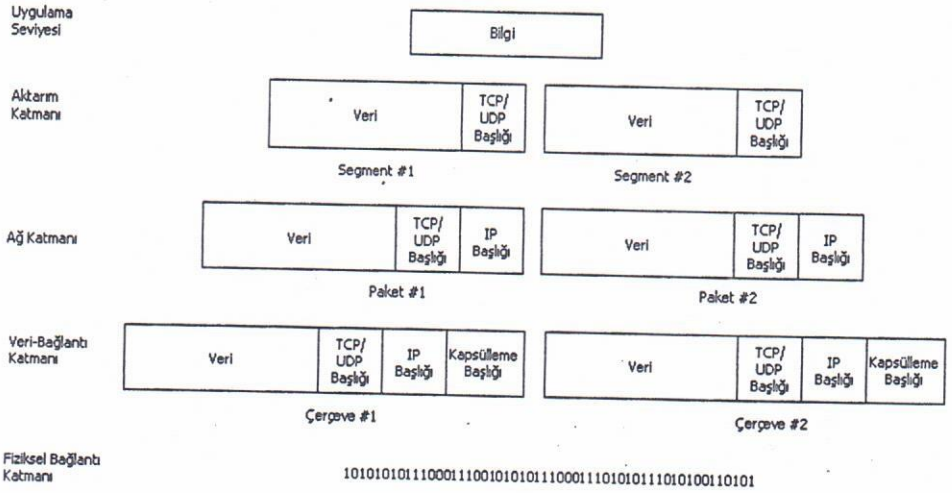
Burada, bir uygulama programından gönderilen bilginin fiziksel iletim ortamına verilene kadarki süreç anlatılacaktır. Fiziksel iletim ortamından alınan bitlerin, uygulama seviyesindeki programın anlayabileceği şekle getirilmesi süreci de diğerinin tam tersidir.

Şu ana kadar farklı katmanları anlatırken bilgi, segment, paket, çerçeve ve bit kavramlarını kullandık. Bunların farklı katmanlarda farklı isimlendirilen veri birimleridir. Aşağıdaki tabloda hangi katmanda hangi veri biriminin kullanıldığını görebilirsiniz.

	Katman Adı	Veri Birimi (Data Unit)
7, 6, 5	Uygulama Seviyesi (Application, Presentation, Session Layers)	Bilgi (Information)
4	Aktarım Katmanı (Transport Layer)	Segment
3	Ağ Katmanı (Network Layer)	Paket ya da Datagram
2	Veri-bağlantı Katmanı (Data-Link Layer)	Çerçeve (Frame)
1	Fiziksel Katman (Physical Layer)	Bit



Uygulama seviyesinden fiziksel katmana gelene kadar, verinin önüne her katman kendi başlık bilgisini ekler. Aşağıda da görüldüğü gibi veri, iletim ortamına varana kadar başlıklardan ötürü boyutu sürekli büyür.



Yukarıda görüldüğü gibi uygulama seviyesinden alınan bilgi, fiziksel iletim katmanına gelene kadar çeşitli işlemlere tabi tutuluyor. Bu işlemler:

1. Bilgi uygulama seviyesinden, aktarım katmanına gönderiliyor.
2. Aktarım katmanı bilgiyi bölümleyerek birden fazla segment haline getiriyor. Daha sonra her bir segmentin başına TCP ya da UDP başlık bilgilerini ekleyerek ağ katmanına gönderiyor.
3. Ağ katmanı segmenti alıp başına alıcı ve gönderici adreslerini içeren başlıkları (IP başlığı) ekleyerek paket haline getiriyor.

4. Veri-bağlantı katmanında çerçevenin formatı, kullanılan 2. katman protokolüne göre değişmektedir. Burada paket, çıkacağı ağ arayüzüne bağlı olarak, Ethernet (Arpa), Frame-Relay, PPP gibi 2. katman protokollerinden biriyle kapsüllenerek iletim ortamına gönderilir.
5. Çerçeve elektriksel sinyallere dönüştürülerek sıralı olarak taşıma ortamına verilir.

Burada üzerinde durulması gereken bir konu da verinin boyutudur. Zira verinin boyutu, doğrudan iki uç arasındaki iletişimin performansını belirleyici bir etkendir.

Veri/(Veri+TCP/UDP başlığı+IP Başlığı+Kapsülleme başlığı)

Yukarıdaki ifade bize bilginin aktarım verimliliğini verir. Bu ifadeden de anlaşıldığı gibi, verinin boyutu ne kadar büyürse aktarım verimliliği de o kadar büyüyecektir. Ancak, çok büyük olması da fiziksel ortam üzerindeki taşınabilirliğini kısıtlar. Bu nedenle, her iki kriteri de göz önünde bulundurarak optimum bir değer kullanmak gerekir.

İletim ortamına, tek bir çerçevede gönderilecek maksimum veri miktarına MTU (Maximum Transmission Unit) adı verilir. MTU değeri, bilgisayardaki ya da yönlendiricideki ağ arayüzüne göre değişir. Kullanılan 2.katman protokolüne göre optimum MTU değerleri yanda verilmiştir.

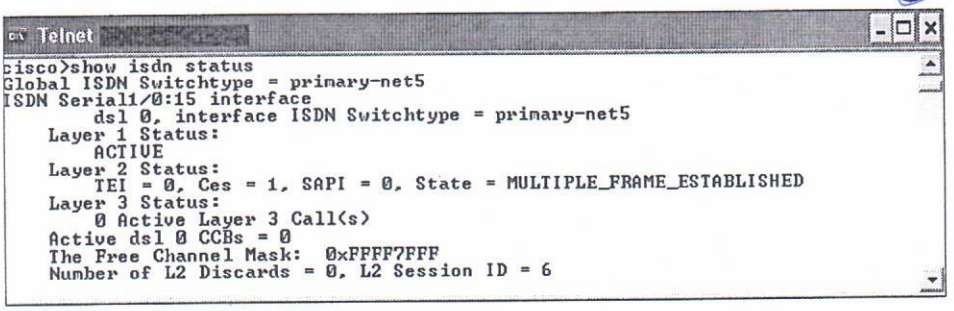
MTU Büyüklüğü (Byte Cinsinden)	
576	PPP (Dial-UP modem ile)
1500	PPP (Default)
1500	ARPA (Ethernet)
1492	PPPOE (DSL)

OSI Modelin Sağladığı Avantajlar Nelerdir?

1. Üretici firmaların, ağ tasarımcılarının ve ağ yöneticilerinin birbirlerini anlamak için kullandıkları ortak bir dil gibidir. Örneğin; bir üretici firma size yeni çıkan ürünlerinin hangi katmanda çalıştığını söylediğinde, siz bu cihazı nerelerde kullanabileceğinizi kolayca anlarsınız.
2. Farklı üretici firmaların geliştirdikleri cihaz ve yazılımların birbirleriyle uyumlu çalışmasına katkıda bulunur.
3. Bilgisayardan bilgisayara yapılan iletişimin (host-to-host networking) kolay anlaşılmasını sağlar. Katmanlı model, kullandığımız cihazların ve protokollerin benzerliklerini ve birbirlerinden farkını anlamamıza yardımcı olur. Böylece ağ cihazlarının ve protokollerinin sınıflandırmasını kolayca yapabiliriz.

4. Cihaz veya yazılımların hangi katmanlarda çalıştığını bilmek, ağ tasarımı kolaylaştıracaktır. Ayrıca, tasarımın basitleşmesi, ağ kurulum maliyetlerini de düşürecektir.
5. Ağda yaşanan sorunun hangi seviyede (kaçıncı katmanda) olduğu bilinirse nereden kaynaklandığı daha kolay bulunabilir. Böylece ağ yönetimi kolaylaşacaktır. Örneğin; bilgisayarınızın karşıdaki sunucuya bağlanamama sebebinin 1. katmandan mı (fiziksel bağlantı seviyesinde), 3. katmandan mı (IP seviyesinde) yoksa 7. katmandan mı (uygulama seviyesinde) olduğunu bazı komutlar (`ping`, `trace`, `nslookup`, `telnet` vs gibi) kullanarak anlayabilirsiniz. Böylece sorunu nerede aramanız gerektiğini bulursunuz.

Aşağıda Cisco marka yönlendirici cihazına kurulu ISDN PRI bağlantısının ne durumda olduğunu görmek için `show isdn status` komutu girilmiştir. Gördüğünüz gibi ISDN PRI bağlantısının durumu katman katman gösterilmiştir.



Yukarıdaki komut çıktısından ilk üç katmanın problemsiz çalıştığı görülmektedir. Şayet problem olsaydı bu problemin hangi katmanda olduğunu görecektik. Böylece problemi nerede aramamız gerektiği hakkında fikir sahibi olacaktık.

Örneğin; birinci katman aktif durumda değil deseydi, problemi fiziksel düzeyde arayacaktık.

Kısaca aslında OSI model teorik bir modelleme olsa da, ağ yöneticilerinin bir cihazın ya da protokolün kaçıncı OSI katmanında çalıştığını bilmesinde oldukça yarar vardır.