Ders teorik gidecek, uygulama kısmı AWS ye girince uygulayacak, diğer arkadaşlarda fiziksel bir uygulaması olmayacak bir genel kültür dersi gibi olacak, neyin ne olduğunu bileceksiniz, sistemi anlayacaksınız.

Bugün ne yapacağız;

Network ün tanımını yapacağız

Local area network nedir (LAN)

Ağ kavramı içerisinde geçen terminolojilerden bahsedeceğiz

WAN nedir, bu iki kavramdan bahsetmiş olacağız

Topolojilerden bahsedeceğiz, fiziksel bazı topolojileri konuşacağız

Network Nedir ?

En az iki cihaz (bilgisayar değil, günümüzde bir sürü cihaz ortaya çıktı…), bilgi paylaşımı için birbiri ile bağlantı kurmasına denir. Kablolu olur, kablosuz olur bağlantı türü önemli değil önemli olan bilgi paylaşımı için bir bağlantı olsun.

Transmission medium, elektrik veya ışık demetlerinin iletildiği veya radyo frekanslarının iletildiği ortam. ( storage medium dediğimizide ise verilerin depolandığı ortam, cd, flash bellek gibi cihazlar aklınıza gelsin.

Tarihçesi

İlk network, 1970 yıllarında Amerika savunma bakanlığı tarafından Arpa net adı altında Askeri birlikler arasında dosya paylaşımı için kuruldu.

Daha sonra üniversitelerin erişimine açıldı.

Daha şirketlerin erişimine açılması ile giderek büyüdü. Çok kısa bir sürede 80 lerde evrilmeye ("Evrilmek" terimi, "dönüşmek" veya "değişmek" anlamına gelir.) başladı

İlk çıkış noktasından itibaren tarihsel olarak baktığımızda;

* Networkler paylaşılan dosya klasörlere erişim hizmetleri vermek,
* Yazıcılara ve tarayıcılara erişim sağlıyor
* E-mail
* Database
* Web
* Voice over IP - internet üzerinden telefonla görüşme görüşme
* Multimedia -- zom üzerinden görüşme

Arpa netten günümüze…..

\*\*\*Bir network bu yansıda gördüğünüz bir veya daha fazla özelliği olmalı, (telefonu bilgisayarda şarja takmak bir network değil, birbirine dosya transferinde bulunmak network dür)

Bilgisayar ağlarının bazı özellikleri olması lazım, biz ağ kurunca bu yetmez, belli başlı özelliklerinin de olması lazım. Belli başlı hizmetleri vermesi lazım.

1. Ağın performansının yüksek olmasını bekleriz. ( dosya transferi için hızlı olması lazım). Daha önce bu şekilde değildi, dosyalar text boyutundaydı. Boyutları küçük ve resim azdı, telefonlarda bile o zamanlar 3G bile yoktu. Şu anki Web sitelerini o zaman açmaya kalsak 15 dk falan beklememiz gerekirdi.

Performansı nasıl ölçüyoruz, respons time ile ölçüyoruz, nedir response time, talebin karşıya gidip cevabın gelmesi arasında geçen süre. Çift taraflı. Genellikle milisaniye olarak ölçülür. Oyunlarda ping değerine karşılık gelir bu response time. 100 mili saniyenin altında olanlar hızlı olarak kabul edilir.

1. Data sharing, information sharing yani mutlaka bir paylaşım olması lazım, (dosya ve benzeri gibi)

Veri Paylaşımı: Bilgisayar ağını kullanmamızın nedenlerinden biri de, bir iletim ortamı aracılığıyla birbirine bağlı farklı sistemler arasında veri paylaşımıdır.

1. Backup, her networkün mutlaka backup ının alınması lazım, her paylaşılan bilginin ve dosyanın mutlaka bir yedeğinin alınması lazım. Network mükemmel çalışan sistemler değil, bağlantı koptuğunda bilgilerin backup ının alınması lazım.

Yedekleme: Bir bilgisayar ağının, bir arıza durumunda verileri daha hızlı kurtarabilmesi için, ağ üzerinden paylaşılacak tüm verilerin yedeğini tutan merkezi bir sunucuya sahip olması gerekir.

1. Relayblitiy, Güvenilirlik: Ağda herhangi bir arıza olmamalı veya arıza durumunda kurtarma hızlı olmalıdır.

Her zaman erişilebilir olmak, ulaşılabilir olmak, bir networkün sürekli ayakta olması lazım. Tabi bu her zaman maalesef mümkün olmuyor. Minumum sürede bir çökme olması lazım, bunu sağlamalıyız. Olursa da backup ı alınmalı ki bu arada bilgi kayıpları olmaması lazım ve bu backup ı da tekrar ayağa kaldırmak önemli.

1. Security, günümüzün en popüler konularından biri malum. Her türlü bilginin internet ortamında bu denli dolaşması biz son kullanıcılar için önemli hale geldi. Bu yüzden network içerisinde çeşitli algoritmaların kullanılması lazım. ( günümüzde kriptolanmadan şifrelenmeden bilgi paylaşan kalmadı. Google de yine öyle çok az şifresiz sayfa mevcut.

Güvenlik: Bir bilgisayar ağı güvenli olmalı, böylece ağ üzerinden iletilen veriler yetkisiz erişime karşı korunmalıdır. Ayrıca gönderilen verinin alıcı düğümde olduğu gibi alınması yani iletim sırasında herhangi bir veri kaybı yaşanmaması gerekmektedir.

Biz bir kere ağa gönderdikten sonra bu dosyam karşıya ulaşana kadar benim bir dahlim yok. Arada veriler çalınmasın diye şifreleyip göndermeliyiz.

Biz bunlar için sertifika almalıyız,( bunlarında belirli aralıklarla yenilenmesi gerekecek---3 ay mesela) tabi bu algoritmaları çözmek imkansız değil (kırılamaz çözülemez değil ) zaman kazanmak önemli onlar şifreleri kırıp içine girene kadar biz ara ara şifrelerimizi değiştirmemiz lazım ki onlar kıramadan yeni bir engel ile karşılaşsınlar.

Bankacılık işlemlerinde kesinlikle buradaki bağlantının secure olduğunu görmeden işlem yapmamalıyız.

\*\*\*Oltalama yöntemi ( phishing ) deniyor,

Domain name e dikkat etmek lazım, bir harf bile değişik olmamalı (amazonda 200 tl lik alışveriş kuponunuz var buraya tıklayıp giriş yapabilirsiniz diyor) siz buraya giriş yaptığınızda aynı arayüzü getiriyor sizin bilgilerinizi ele geçirebilir, bazı mailler scripler içeriyor ve arka planda bunlar çalışıyor ve bilgileriniz kayıt altına alınıyor. Bunlara kesinlikle dikkat etmek gerekiyor.

1. Scalabilitiy, ( bunun Türkçe karşılığı ölçeklenebilirlik) ; (teknik terimleri kullanmak önemli, pre clası da ing okuyalım).

Ölçeklenebilirlik: Bir bilgisayar ağı ölçeklenebilir olmalıdır; bu, mevcut bilgisayar ağına her zaman yeni bilgisayarların (veya düğümlerin) eklenmesine izin vermesi gerektiği anlamına gelir. Örneğin bir şirket, 100 çalışanı için bir bilgisayar ağı üzerinden 100 bilgisayar çalıştırıyor, diyelim ki 100 çalışan daha işe alıyor ve mevcut LAN'a 100 yeni bilgisayar eklemek istiyor, bu durumda yerel alan bilgisayar ağının buna izin vermesi gerekir.

Ağa istediğimiz zaman yeni cihazlar ekleyebilmek ve istediğimiz zaman çıkarabilmek. (scale up, scale down ). Evinize misafir geliyor ve networke bağlanabiliyor.

1. Günümüzde şu an en önemli konu yazılım ve donanım uyumluluğu, günümüzde şu an 100 ün üzerinde işletim sistemi var, ağda kullanılan. ( en yaygın olanlar, Windows, Mac, Linux, IOS ve Android) ve bunun dışında onlarca farklı donanım üreticisi var. Onların da onlarca farklı modeli var.

Hepimiz farklı bilgisayarlar kullanıyoruz, bunların farklı ethernet kartları var, farklı modemler kullanıyoruz ama hepimiz şu an ortak bir zeminde iletişim kurabiliyoruz.

İşte network ağının bu şekilde farklı donanım ve yazılımları destekliyor olabilmesi lazım. (daha sonra ayrıntısını göreceğiz) ( bunun için OSI model ve TCP IP modeli geliştirilmiş. ) bunları konuşacağız.

Gelelim şimdi LAN kavramına;

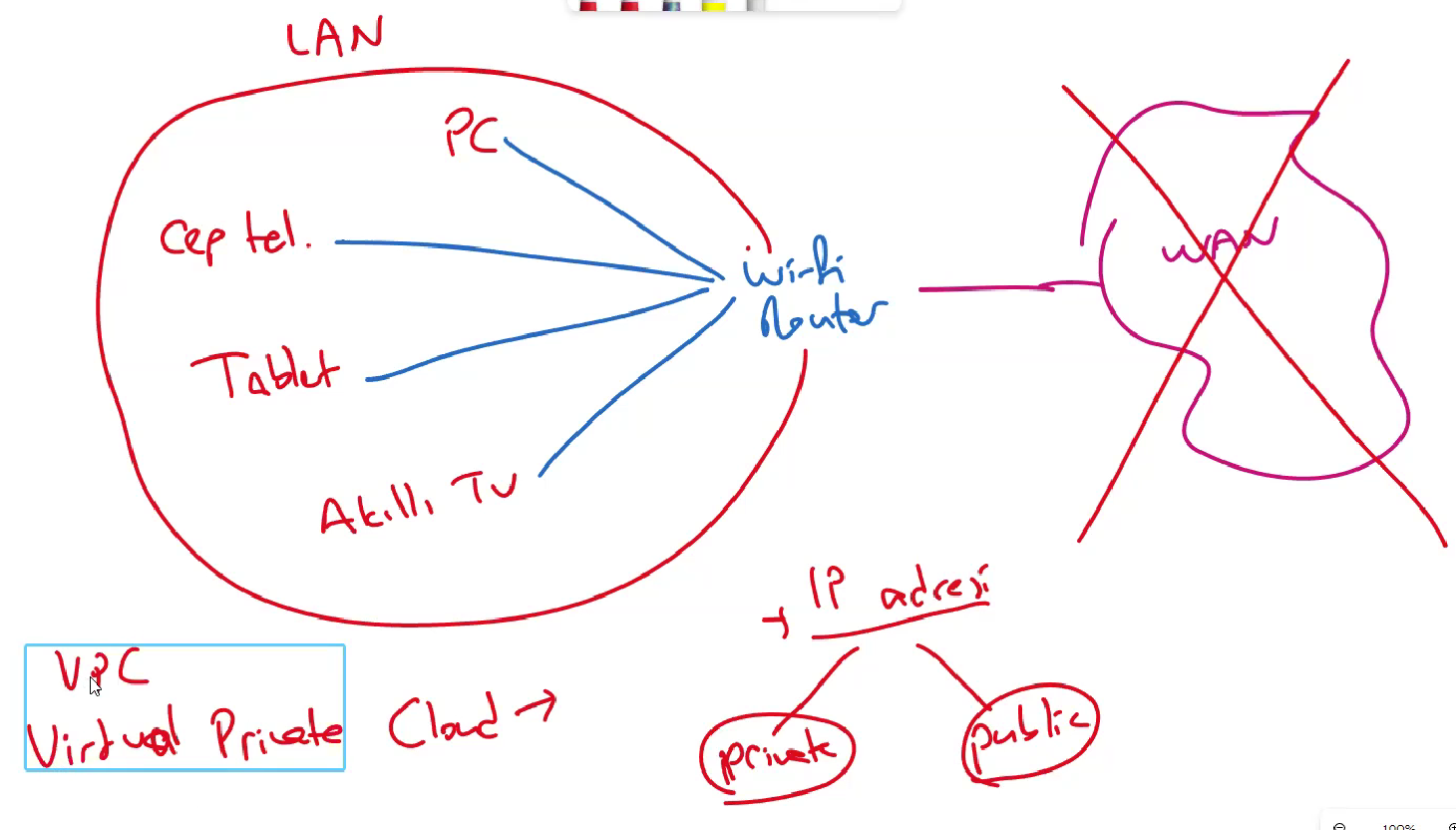
Adı üzerinde local, yerel bir ağ demek.

İki bilgisayardan da oluşabilir, 100 lerce 1000 lerce bilgisayardan da oluşabilir.

\*\*\*Bir binanın bir katı, üniversitenin bir kampüsü, bir iş yeri ofisi, bir site veya en fazla bir site. Sarılı bir alana yayılmış ağ olarak tanımlanıyor. Günümüzde şu şekilde kullanıyoruz, internete doğrudan çıkış yapmayan bilgisayarların (cihazların) bulunduğu bir ağ. (wifi router---modem)

(Cep telefonlarının kendilerinde bir router işlevi gören cihazlar olmasa da, çoğu akıllı telefon Wi-Fi hotspot (Wi-Fi paylaşım) özelliği sunar. Bu özellik sayesinde, cep telefonunuzun mobil veri bağlantısını kullanarak kablosuz bir Wi-Fi ağı oluşturabilirsiniz.)

Evinizdeki cihazlar doğrudan internetten çıkış yapılamıyor, arada bir wifi router tarafından iletişim sağlanıyor. Dolayısıyla bizim evlerimizdeki ağ bir local ağdır.



Local olunca private ip üzerinden iletişim sağlanır

Public -----google yaz----what is my ip

Private ----- ipconfig yaz

Soru:

\*\*Tek bir binadaki bir şirket LAN olarak kabul edilir

\*\*Aynı bölgede birden fazla binadan oluşan bir şirket LAN olarak kabul edilir

Bir binadaki şirketin 3 katı bir lan olabilir, bir site bir lan olabilir dedik ama böl yönet network de çok mantıklı bir yöntem. Ağı ne kadar küçük parçalara ayırırsanız yönetimi o derece kolay olur.

VPC kurarken de bu böyle…. Büyük ölçekli bir vpc yerine bu daha zor olsa da küçük ölçekli vpc kurmak daha sonra yönetmede kolaylıklar sağlar.

Slayt 12:

LAN'ın boyutu ve bir LAN'ın yayabileceği mesafe sınırlı değildir

Ancak yönetimi kolaylaştırmak için büyük bir LAN'ı **Workgroups**  olarak bilinen daha küçük mantıksal bölgelere bölmek en iyisidir.

Bu tanımlama karşınıza çıkmaz çok önemli değil, Microsoft, Windows 95 veya 98 de hayatımıza soktuğu bir kavram.

Burada bir şirketin 3 ayrı departmanı var, her biri kendi içerisinde bir local ağ, bir workgroup, workgroup daha çok mantıksal bir tanımlama Windows da siz gidiyorsunuz workgroup ismi belirliyorsunuz, o isme ait cihazlar aynı workgroup a dahil olmuş oluyor, lojikıl bir kurulum.

Tipik bir iş ortamında, LAN'ınızın çalışma gruplarını departman bölümleriyle birlikte düzenlemek iyi bir fikirdir; örneğin, Muhasebe için bir çalışma grubu, Satış için başka bir çalışma grubu ve belki de Pazarlama veya yazdırma işleri için başka bir çalışma grubu oluşturabilirsiniz.

Şekilde her biri kendi çalışma grubu olan 3 ayrı LAN gösterilmektedir.

Resimde 3 LAN var çünkü çalışma gruplarının hiçbiri birbirine bağlı değil. Bu sorunun üstesinden gelmek için, 3 LAN'ı 3 çalışma grubuyla tek bir LAN'a bağlamak için bir yönlendirici kullanabiliriz.

Common network Companents

Node, aslında bir bağlantı noktası demek ama ağlarda ağa bağlanan her hangi bir cihaz anlama gelir. (laptop, server, router….)

Station , kablosuz ağlarda her bir cihaza (düğüme genellikle istasyon) diyoruz.

Node, ağ üzerinde bir veya daha fazla ağ arayüzü aracılığıyla iletişim kurabilen herhangi bir cihazdır. Düğüm terimi bilgisayarlar, dizüstü bilgisayarlar, sunucular, IP telefonları, akıllı telefonlar veya yazıcılar gibi uç nokta cihazlarını ve switch ve router gibi bağlantı veya iletme cihazlarını tanımlamak için kullanılabilir.

---bir cihazın birden fazla rolü olabilir, örneğin host,

Host, ip adresi olan tüm cihazlara denir, aynı zamanda bir node dır veya stationdur.

Peki her node bir host mudur, değildir ama her host bir node dur. Hostların bir ip adresi vardır. Bazı cihazlar ip adresi olmadan internete bağlanırlar, kapalı çevrim güvenlik kameraları. Bunlar node olarak isimlendirilir ama host olarak isimlendirilemez.

Şu an bizim kullandığımız bilgisayarlar bir hosttur ip adresi olduğu için, host olduğu için ve internete bağlı olduğu için aynı zamanda bir node dur.

\*\*Buradaki terimlere çok takılmayın, bizim burada çok kullanacağımız clint, server ve host olacak.

\*\*\*Workstation, bunu aslında bir genel kültür olarak bilseniz yeterli, güçlü bir bilgisayar, genelde masaüstü olarak üretilir ama laptop versiyonları da günümüzde var. Geçen yıllarda çıkmış apple nin rende (kasa tipi), hp nin de var. Genetik biliminde (üniversitelerde, güçlü hesaplamalarda bu bilgisayarlar kullanılır. Datasaince de ihtiyaç duyulur.

Bu cihazlar genelde ağ üzerinden erişilebilir oluyor. Aynı anda bir kişi kullanıyor çoğunlukta. Biri girip oturum açıyor kullanıyor çıkınca diğeri oturum açıp girebiliyor. Peki normal bilgisayarlardan farkı ne, bunlar farklı mimaride işlemci ve ram kullanıyorlar.

Google dan bak apple rende………………………

Gelelim en çok kullanacağımız iki kelimeye; server ve clint

Server;

Server larda bir Workstation kadar hatta bazı Workstation dan daha güçlü bir donanıma sahiptir. Bunlar bize belli başlı hizmetleri veren çok güçlü bilgisayarlar.

Günümüzde bir server bir amaç için kullanılabileceği gibi bir çok amaç için de kullanılabilir. En çok duyacağınız server lar, Proxy server, web server……..

Şu an mesela Google bağlansak bir servere bağlanmış oluyoruz.

Clint ne, server dan hizmet talebinde bulunan host. Hem clint hem server bunlar aynı zamanda birer hosttur. Bunlar ip adresi almak zorunda. (clint----bizim bilgisayarlarımız)

Segment, segmentler bir ağın belli bir bölümünü ifade eden bir kavram. 10 bilgisayarlı bir local ağ düşünün bunu daha küçük parçalara bölmek daha iyidir dedik, 3 bilgisayarlı segmentlere böler o şekilde yönetebiliriz ağı. Burada bridge kullanırsınız. Bu ifade çok karşınıza çıkmaz.

Backbone, bu bakır bir kablodur. Serçe parmağı kalınlığında, ilk çıktığı zamanlar için hızlı (tabi şu an daha hızlı teknolojiler var) 100 mbit e kadar çıkan hızda backbone var.

Bir networkdeki segmentler arasındaki fast link dir, bağlantı türüdür, bir kablodur..

Transmission media

elektrik sinyalleri veya ışık demetlerinin iletildiği veya radyo frekanslarının iletildiği ortam.

Veri transferi, bilgiyi iletim şekli. Verinin iletildiği ortam.

İletim ortamı, bilgiyi göndericiden alıcıya taşıyan düğümler arasındaki bir iletişim kanalıdır. Veriler elektromanyetik sinyaller aracılığıyla iletilir.

İletim ortamının temel işlevi, bilgiyi bitler halinde LAN üzerinden taşımaktır.

Bakır bazlı bir ağda bitler elektrik sinyalleri şeklinde gönderilir.

Fiber tabanlı bir ağda bitler ışık darbeleri şeklinde gönderilir.

Kablosuz ağda bitler radyo dalgaları şeklinde gönderilir.

İkiye ayrılır genel olarak

Guided (yönlendirilebilir) ve unguided (yönlendirilemez)

Kablolu bağlantılar kablosuz bağlantılar

Koaksiyel, baseband telefon santrallerinde, tv lerimizde hala kullanılıyor.

Broadband

Fiber

Twisted, Ethernet kablo,

ethernet aslında bir standart dökümanı, farklı cihazların birbiriyle iletişim kurabilmesi için bazı standartlar belirlenip bir doküman hazırlanmış. Bu dökümanda ne var, kullanılacak bakır kablonun bir standardı var, özellikleri, kablo drenci ne olmalı mühendislik seviyesinde bir doküman.

Onun haricinde ağ kartlarımız var bilgisayarlarımızda kullanılan, ethernet kartları bunların nasıl tasarlanması gerektiğini, nasıl üretilmesi gerektiğini bildiren bir standardizasyon dökümanının adı.

Biz bunlara ethernet kablosu diyoruz ama bunların dökümandaki adı twisted pair, neden twisted pair onlar çiftler halinde bükülmüş olduğu için twisted pair.

Unguided

Radiowaves, radyo dalgaları, evimizdeki wifi routerler radio dalgası kullanıyor.

Microdalgalar, bu genellikle askeri cihazlarda, donanımlarda kullanılıyor.

İnfrared, 20 veya 30 cm menzili olan mause için veya kumandalar için kullanılıyor. Kızılötesi ışınlar yayarak iletirler.

Cable Properties kablo özellikleri

Her türlü cominikasyonlar ( iletişim) için kullanılan standart kavramlar.

Simplex, tek yönlü iletişim radyo gibi.

Half-duplex, iki yönlü fakat aynı anda olmuyor, biri bitirince konuşmayı diğerine geçiyor.

Full-duplex, çift yönlü ve aynı anda iletim olunca. Cep telefonu gibi.

WAN ( Wide Area Network )

Geniş, çok daha büyük alana yayılmış network olarak isimlendirilirken, şimdi internet WAN olarak isimlendiriliyor. Aslında internet WAN lardan oluşan çok daha büyük largest WAN olarak isimlendiriliyor.

İnternet olduğu için de artık ip adresleri de public olarak kullanılması gerekiyor.

Rauding işlemi, public ip adresine göre işlem yapar. Biz bir istekte bulunduğumuzda bunu bir pakete koyup alıcıya iletmekle sorumludur. Bu da evlerimizde bulunan routerler sayesinde oluyor.

Gelelim Topology lere

Topology, dizilim, yerleşim gibi bir anlamı vardır.

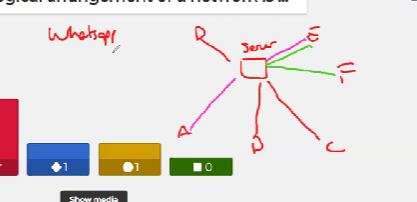
Ağ topolojileri, cihazların birbirine nasıl bağlandığını ve verilerin bir düğümden diğerine nasıl aktarıldığını ana hatlarıyla belirtir.

Network de nasıl kullanıyoruz. Network de iki türli topology var; Fiziksel ve mantıksal.

Fiziksel topl, ağın içinde bilgisayarların yerleşimi, ağdaki cihazların birbirleriyle bağlantısı

Logical topl, Yazılım tarafında bir programın çalışma mantığı, veri iletim mantığı diyebiliriz.

Verinin nasıl iletileceğinin kararlaştırılması.



Fiziksel topology, genelde çok duyacağınız topology ler çok kullanılanlar değil çünkü bunların çoğu kullanılmıyor. Günümüzde hep star topology kullanılıyor.

Fiziksel topolojiler;

Bir ağın fiziksel topolojisi, ağ erişim cihazlarının ve ortamının yetenekleri, istenen kontrol düzeyi veya hata toleransı ve kablolama veya telekomünikasyon devreleriyle ilgili maliyet ile belirlenir.

Ağınız için seçeceğiniz fiziksel topoloji şunlara bağlıdır:

* Ofis Düzeni, kurulumu
* Sorun Giderme Teknikleri, Kullanacağınız trabulşuting teknikleri
* Kurulum Maliyeti
* Kullanacağınız kablolara göre değişiyor.

Bunlara göre kullanacağınız topolojiyi belirleyebilirsiniz.

Logical topoloji; bunlar daha çok full stack bölümünde kurs alacak arkadaşları ilgilendiriyor.

Mantıksal topoloji, ağın yönlendirme ve iletişim protokollerini belirlemek için kullanılır. Bir ağdaki cihazların birbirleriyle nasıl iletişim kuracaklarını ve veri paketlerinin nasıl iletilip yönlendirileceğini tanımlar. Mantıksal topoloji, ağdaki veri trafiğinin organizasyonunu sağlamak için kullanılır.

Fiziksel topolojiler;

Bus teknoloji:

Backbone kablo, parmağınız kalınlığında bakır kablo ortada, diğer bilgisayarlar bir jak yardımıyla (tv ye takılan ) burada bunları birbirine bağlayacak hub, switch, router gibi bir cihaz yok. Uçlarında sınırlayıcı var tıpa gibi. Aralarda bilgisayarların takılacağı jaklar üretilirken ayarlanmış yerleri.

Avantajı nedir, kurulumu, düzeni çok basit ve maliyeti çok basit.

Dezavantajları, ağın üstüne kurulduğu sistem çökünce tüm ağ çöküyor. Kablo kırılsa kopsa tüm ağ çöküyor.

Networkün performansı düşük, çünkü bu half-duplex bir kablo, aynı anda sadece bir bilgisayar gönderme yapabilir. Çünkü tüm sinyaller tek bir kablo üzerinden iletildiği için çakışmaması adına aynı anda tek bir bilgisayar paket gönderebilir.

Not sceylibıl, ölçeklenebilir değil çünkü kablo üzerindeki jack sayıları belli

\*\*\*Günümüzde backbone ağırlıklı olarak askeri sistemlerde kullanılıyor, sağlamlığı ve basitliği için. Yedek olarak iki backbone kullanılır. Birinde bağlantı gittiğinde diğeri kullanılır.

Star topoloji;

Günümüzde en çok kullanılan topoloji, ortada swich, hub gibi cihazlar var diğer bütün cihazlar, node lar bu ortadaki cihaza bağlı. Bizim evimizde de şu an kullandığımız topoloji bir star topoloji. Ortada bir router var diğer bütün cihazlar bu router e bağlı.

* Yönetimi kolay
* Çok daha az kablo gerektiriyor

Dezavantaja gelince ortadaki cihaz çökünce tüm ağ çöküyor.

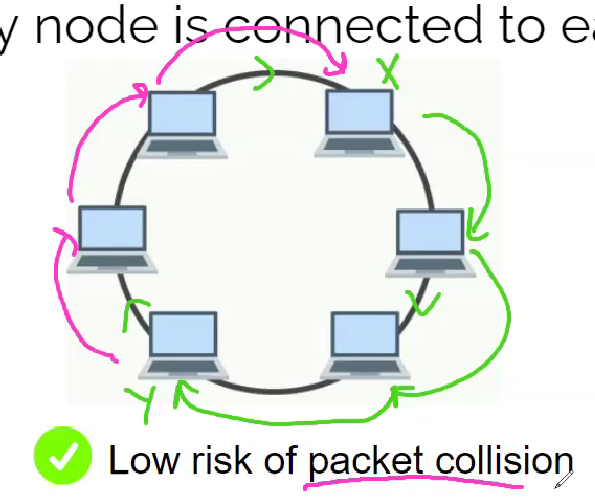
Ve performans ortadaki cihazın performansıyla doğru orantılı. Buradaki bütün node lar 1 Gbit bağlantıyı destekliyor. (hız olarak). Ortadaki cihaz 100 mbit i destekliyorsa hızı buradaki tüm cihazların hızı da 100 mb olur. Donanımlar en düşük hıza göre çalışıyor.

Maliyet açısından da çok uygun değildir.

Ring Toploloji;

Ring topl IBM tarafından çıkarılmış 1960-70 lerde. Günümüzde pek yeri yok. Telefon santrallerinde, swichlerin birbiri ile bağlantısında kullanılıyor ama onun haricinde ağlarda çok göreceğiniz bir topoloji değil.

Burada tüm cihazlar birbiri ile tek bir kablo ile bağlı ama bus topolojiden farklı. Burada backbone yok, her bir bilgisayar diğerine bağlı ve veri tek yönlü gidiyor.



Burada collisin olma ihtimali çok düşük paketler hep saat yönünde ilerlediği için.

Kurulumu basit

Dezavantajı, bu node lardan herhangi biri çöktüğünde tüm ağ çöküyor.

Ne kadar fazla cihaz olursa iletişim o kadar yavaşlıyor çünkü elden ele gönderiyorsunuz paketi, performansı düşük bir topoloji.

Sceylibıl, ( ölçeklenebilir) ağa bir node ekleyip çıkarabilirsiniz ama bunun için tüm ağı kapatmanız gerekiyor.

Performansı arttırmak için çift yönlü bir ring kurulmuş. Bu hızı arttırmış ama bu şekilde bağlamak her node için 4 port gerektirmiş oluyor, bağlantı noktası olması lazım.

Mesh topoloji

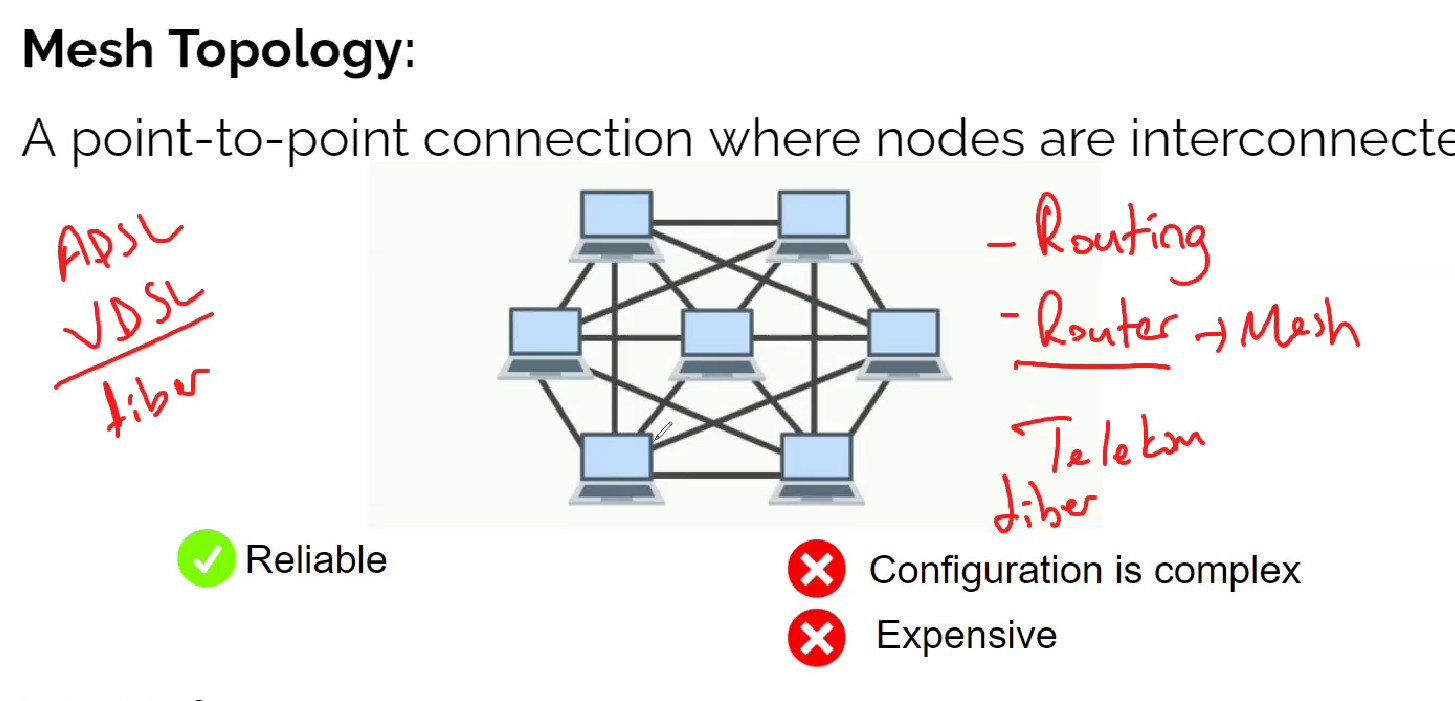
Bu topolojideki tüm node lar birbiri ile bağlantılı. Arada bir bağlantı kopsa dahi tüm ağın iletişimi devam ediyor.

Reliable (güvenilir) buradaki node lardan biri çökse tüm ağ yine işler.

Ama konbinasyonu biraz karışık, tüm cihazları birbirine bağlayıp kontrol etmek zordur.

Ve pahalıdır, bu topolojiyi yapmak için çok fazla kabloya ve çok fazla porta ihtiyacınız var.

\*\*\*Günümüzde mesh topoloji nerede kullanılıyor, internette kullanılıyor.



Bunun en büyük avantajı bir router çöktüğünde internet erişiminde herhangi bir aksama yaşanmaması.

Mesh topoloji genellikle büyük ölçekli ağlarda kullanılır, özellikle kritik sistemlerde veya özel ağlarda yüksek güvenilirlik ve performans gerektiren durumlarda tercih edilir. Örneğin, bankalar, telekomünikasyon altyapıları veya askeri ağlar gibi alanlarda mesh topolojisi yaygın olarak kullanılabilir.

Tree (Heirarchy ) hiyerarşi topoloji;

(Eskiden üniversitelerde kullanılıyordu, şimdi kullanılıyor mu bilmiyoruz.)

Ortada bir node var, root dediğimiz bir node bu node dan swich, hub gibi diğer node lar ile bağlantı sağlanarak bir ağaç görünümünde oluşturulan bir ağ topolojisi.

Avantajları;

Scaleable, istediğiniz kadar yeni cihaz ekleyebilirsiniz.

Managibıl, çünkü alt dallara ayırıp, guruplayıp yönetimi kolaylaştırabiliyorsunuz.

metin, diyagram, ekran görüntüsü, çizgi içeren bir resim

Açıklama otomatik olarak oluşturuldu

Anlaması, algılaması mesh den daha komplex ve zor

Bir de root gittiği zaman tüm ağ çöküyor. Alt parçalardan biri gidince pek problem olmaz ama root gidince hepsi gider.

Hybrid Topoloji;

Çok formlu, çok yönlü demektir.

Birden fazla topolojiyi aynı network de kullanıyorsanız bu hybrid dir. Hybrid araba gibi.

Flexibil dir. İstediğiniz kadar node ekleyebilirsiniz.

Çok komplextir yapısı. Oldukça maliyetli olabilir

OSI Model ----- Open System Interconnection

Açık Sistem Bağlantısı (OSI) Özellikleri (standartları)

Bir networkün farklı donanım ve yazılımları destekleyebilmesi lazım. (Linux, Windows…)

Benim kullandığım wifi kartının anakartın modeli farklı, sizin kullandığınız ethernet kartınızın wifi routerinizin marka modeli farklı ama hiçbir problem olmadan hepimiz iletişim kurabiliyoruz.

İşte bunu OSI spesifikasyonlarına, OSI standatlarına borçluyuz.

Şimdi bu internet ilk savunma bakanlığı tarafından Arpa netten daha sonra internet evrilmeye başlayınca her marka kendi özel donanımlarını çıkarıyordu, siz bir ağ kurmak için o markaya özel ağ kuruyor olmanız lazım. Mesela ethernet kartı, hepiniz aynı marka ethernet kartı almak zorundasınız.

Bu sıkıntıyı ön gören Uluslararası standardizasyon Organizasyonu (ISO) , 1984 de OSI modelini tanımlıyor.

Bu sorunu çözmek için Uluslararası Standardizasyon Örgütü (ISO) farklı ağ modellerini araştırdı ve sonuç 1984'te piyasaya sürülen OSI modeli oldu. Günümüzde çoğu satıcı OSI modeline dayalı ağlar oluşturuyor ve farklı satıcıların donanımları bu sayede uyumlu olmuş oluyor.

Bu tavsiye edilen bir standart, zorunlu değil.

Bu standart diyor ki, siz bir yazılım işletim sistemi veya bir donanım, hub, switch, router, ethernet kartı, kablo bu tarz yazılım ve donanımlar üretecekseniz şu standartları sağladığından emin olun ki farklı farklı modeller birbirleri ile iletişim kurabilsin.

Günümüzde İki tane model var, biri OSI model birisi de son ders göreceğimiz TCP/IP model. Bu modeller farklı marka ve model tüm yazılım ve donanım cihazlarının birbiriyle haberleşmesini sağlayan bir standardizasyon.

Peki neden hala ikisini birden kullanıyoruz ??????

OSI model günümüzde artık daha çok donanımları tanımlamak için kullanılıyor. Donanım üreticilerinin dikkate aldığı bir model.

TCP/IP ise, günümüzde internetin üzerinde çalıştığı model.

TCP/IP modeli, Transmission Control Protocol (TCP) ve Internet Protocol (IP) gibi protokollerin temelinde yer alır. Bu model, internetin temelini oluşturan protokollerin organizasyonunu ve işlevlerini tanımlamak için kullanılır.

TCP/IP model OSI nin biraz daha sadeleştirilmiş bir modeldir.

Gelelim OSI modele en üstten başlayalım.

Nedir en üstte zoom var, Google crome var. Uygulama programlarından işletim sistemine geliyoruz, işletim sisteminden Kernel a geçiyoruz, Kernel dan artık donanım seviyesine geçiyoruz. Ethernet kartıdır, switch dir, hub dır, ondan sonra neler var, kablolar var ve radyo frekansları var.

İşte bu çeşitli yelpazedeki farklı farklı unsurları daha iyi tanımlayabilmek için OSI model 7 katmana bölünmüş.

Dolayısıyla siz bir yazılım geliştiricisiyseniz, en üstteki 2 veya 3 katmanı bilmeniz yeterli.

Bir işletim sistemi yazıyorsanız en üstteki 4 katmanı bilmeniz gerekli.

Bir kablo üretiyorsanız katman 1 (layer 1) veya bir wifi router üretiyorsanız fizikıl katmanına göre üretiyor olmalısınız.

Ethernet kartı üretiyorsanız datalink layer deki standartlara göre bir kart üretmeniz lazım. Bu standartlara göre çalışan bir kart üretmeniz lazım.

Transport Layer, genelde Kernel in gündemde olduğu bir katman

Upper Layers --- yazılım ve işletim sistemi katmanı.

Lower Layers, Network , alttaki 3 katman donanım kısmı, burada artık yazılımdan bahsedemiyoruz.

Sıralama alttan yukarı doğru çıkar. Layer 1 deyince ne olduğunu bilmek gerekir. Router Layer 3 de switch ve hub lar layer 2 de çalışır. Mac adresi burada ortaya çıkıyor.

Bunları anlamak öyle hemen kolay olmayacak, ders sonunda bazı şeyler oturmaya başlayacak.

Bu katmanlar ne işe yarıyor tek tek bakalım.

Layer 7;

En son katman Appilication katmanı, kullanıcıyla OSI modelin etkileşime girdiği tek katman burası. Şu an benim kullandığım zoom, browser bunlar şu an layer 7 de çalışırlar.

Burası işte kullanıcıdan veriyi aldığı ve kullanıcıya veriyi sergilediği katman. Bu katmandan sonraki kısımlarda benim bir etkileşimim yok kullanıcı olarak. Bundan sonraki artık işletim sisteminin ve donanımın kontrolünde.

Dolayısıyla burada bizim için önemli kısım kullanıcıyla yazılımın veya işletim sisteminin etkileşime girdiği ( Google da clarusway yazalım bunu yazdığımızda bir etkileşim başlatmış oluyoruz), ağ haberleşmesi kapsamında (network kapsamında etkileşime girdiği tek katman aplication layerdir)

Bu, kullanıcıdan gelen verilerle doğrudan etkileşime giren tek katmandır. Web tarayıcıları ve e-posta istemcileri gibi yazılım uygulamaları, iletişimi başlatmak için uygulama katmanına güvenir. Ancak istemci yazılım uygulamalarının uygulama katmanının parçası olmadığı açıkça belirtilmelidir; bunun yerine uygulama katmanı, yazılımın kullanıcıya anlamlı veriler sunmak için kullandığı protokollerden ve veri manipülasyonundan sorumludur. Uygulama katmanı protokolleri HTTP'nin yanı sıra SMTP'yi de içerir (Basit Posta Aktarım Protokolü, e-posta iletişimini sağlayan protokollerden biridir).

Layer 6;

Transleşin yapıyor. Layer 7 den aldığı talebi alttaki katmanın anlayacağı formata çeviriyor. Encript ediyor, şifreliyor ve compres ediyor sıkıştırıyor. Neden sıkıştırıyor, internet trafiğini yani network trafiğini mümkün mertebe azaltmak için.

İnternet üzerinde haberleşmeler paketler üzerinden yapılıyor. Bu paketlerin her birinin max boyutu 1,5 kbayt ki bu 1,5 kb ın içinde veri çok daha az yer kaplıyor. Dolayısıyla siz 10 mbaytlık bir resim karşı tarafa göndermek istediğiniz zaman en az 1000 tane paket gidiyor karşı tarafa. (uzun iş) bunları daha sonra birleştiriliyor.

İşta siz bu verileri kompres etmezseniz ağ da bir sürü paketle trafiği arttırır, ağ performansını düşürür. Onun için bu kompreşın önemli.

\*\*\*Neden bu jpeg formatı çıktı, mp3 formatı çıktı. Eskiden internet çok yavaştı, bir audi formatının boyutu 50 mb civarında idi. Mp3 çıktı boyutunu 2, 2,5 mb ta düşürdü. Eskiden bmp formatındaki resimlerin boyutu 10 mb iken jpeg ile yarım mb a kadar düştü.

O yüzden internet üzerinden ağ bağlantıları ve donanımlar o zamanlar yavaş olduğu için siz veriyi 10 bin tane 100 bin tane paket yerine 1000 tane pakete bölüp hızı arttırmaya çalışıyordunuz.

İşte böyle jpeg, mp3 gibi formatların aslında çıkış noktası bu. Sonuçta siz bu veriyi kompres ediyorsunuz ama bir zip kadar yüksek oranda sıkıştırma sağlayamıyorsunuz, siz burada veriyi göndermeden önce de veriyi sıkıştırırsanız daha sonra bu katmanda onlarda biraz daha sıkıştırılır dolayısıyla 1000 tane paket yerine 700 tane paket üreterek ağ trafiğini biraz rahatlatırsınız.

O yüzden compreşın burada önemli.

Burada benim yazdığım clarusway yazdığım talebi web browser aldı ve layer 6 ya gönderdi.

Layer 6 burada bir sonraki katman için translete etti, enkript etti ve sonra sıkıştırdı ve session 5 e gönderdi.

Session Layer 5;

Siz karşı tarafla bir haberleşme başlatmak istediğiniz zaman sizin ve karşı tarafın bilgisayarına bir session bilgisi oluşturulur, session datası. Bu bir yere kaydedilmez, memory de oluşturulan bir datadır.

Bu ne işe yarar, haberleşmenin başlangıç ve bitiş zamanlarını tutar. Senkronizasyonu sağlar. Çünkü binlerce paket gönderip alıyoruz ya, bu paketlerin gidiş geliş senkronizasyonunu sağlamak için bir session bilgisi üretilir. Karşı tarafla cominikeşinda kaldığımız sürece bu session bilgisi aktif olur, karşı tarafla iletişim koptuğunda(browseri kapattığımızda) session bilgisi silinir. Bu hem server tarafından hem clint tarafından tutulan bir bilgi.

Bu ne işe yarar, karşı taraftan paket geldi ama siz session bilgisine bakıyorsunuz ben karşı tarafla cominikeşinimi bitirmiştim diyorsunuz. O zaman bu paket kötü niyetli bir paket olabilir. Karşı tarafı taklit eden bir kötü niyetli kişi karşı tararfta girdiğim server gibi davranıp bana kötü amaçlı bir paket gönderiyor olabilir.

Firewallar genellikle bu gelen giden paketlerin session bilgisine bakarak gelen giden paketleri de kontrol ederler. Bir paket geliyor kimden geldiği belli (kimlik bilgisi, gerçek yada sahte olabilir onu bilemez), session bilgisi belli bu paket doğru değil deyip bu paketi çöpe atar. Firewoll tarafından bu şekilde kullanılıyor.

Web de nasıl olur, bir oturum açıyorsunuz, session bilgisi oluştu, oturum kapatınca session bilgisi kapanıyor. Siz tekrar bağlanmak istediğinizde credenşıl bilgileri tekrar giriş yapmak istersek tekrar şifreyi sorar.

\*\*\*

Bu, iki cihaz arasındaki iletişimi açıp kapatmaktan sorumlu olan katmandır. İletişimin açılıp kapanması arasındaki süreye oturum denir. Oturum katmanı, oturumun, alınıp verilen tüm verileri aktaracak kadar uzun süre açık kalmasını sağlar ve ardından kaynak israfını önlemek için oturumu hemen kapatır.

\*\*\*

Oturum katmanı ayrıca veri aktarımını kontrol noktalarıyla senkronize eder. Örneğin, 100 megabaytlık bir dosya aktarılıyorsa, oturum katmanı her 5 megabaytta bir kontrol noktası ayarlayabilir. 52 megabayt aktarıldıktan sonra bağlantının kesilmesi veya çökme durumunda oturum son kontrol noktasından devam ettirilebilir; bu da yalnızca 50 megabaytlık verinin daha aktarılması gerektiği anlamına gelir. Kontrol noktaları olmasaydı tüm transferin sıfırdan başlaması gerekecekti.

Layer 4;

İlk 3 katmanı bitirdik, burada artık Kernel seviyesinde benden aldığın request i al clarusway.com a git, ağdan iletilmesi için artık segmentlere bölünüyor.

Buradaki kavramlar önemli, segment, paket, frame, bit streem e…

Layer 4 de artık veri segmentlere ayrılarak gönderilmeye hazırlanıyor. Biz veriyi son haline getirdik. Benden talebi aldı, bu katmana kadar diğer işlemlerden geçti, bu katmana kadar son haline geldi, şimdi burada ağ üzerinden göndermek için fizikıl olarak veriyi hazırlamaya başlıyoruz. O datayı alıyoruz segmentlere parçalıyoruz.

Daha sonra Layer 3 de o segmentlerin her birini İP paketlerine çeviriyoruz.

metin, yazı tipi, ekran görüntüsü, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu metin, yazı tipi, ekran görüntüsü, el yazısı içeren bir resim

Açıklama otomatik olarak oluşturuldu

Bu segmentlerin her birinin başına İP bilgilerini ekliyoruz, İP paketi oluyor. Layer 3 de artık bunları İP Paketine çeviriyoruz.

Layer 2 de, bu yukarıdan gelen paketleri başına ve sonuna minik paketler ekliyerek frame lere çeviriyoruz. Artık verinin son hali bu oluyor. Tabi bundan onlarca oluşuyor, ne kadar çok segment varsa o kadar çok paket ve aynı sayıda da frame oluşturuyorsunuz.

Karşı tarafa gitti yani servera, clinttan yukarıdan aşağı inerken server da aşağıdan yukarı çıkarak ilerleyerek ağdan gönderecek.

Yani önce frame mi açacak, sonra paketi açacak…….

En son Layer 1 fizikıl layer, burası kablonun olduğu kısım. Fizikıl layer de kablonun haricinde birkaç tane ilkel cihaz var;

Tranciver var(alıcı-vericiler), media converter(çeviriciler) var, repeater lar var (tekrarlayıcılar), modem ve hub lar var. Bunlar layer 1 de geçen ilkel cihazlar.

Layer 1 ne yapıyor, yukarıdan gelen frema leri elektrik sinyallerine, radyo frekanslarına çevirip ağa salıyor. Ağa verdikten sonrada karşı aradaki routerlar tarafla bu verileri alıp elden ele elden ele karşıdaki alıcıya ulaştırıyorlar.

Peki modem, reperter, converter bunlar bir cihaz ve neden layer 1 de çalışıyorlar, çünkü bunlar kendilerine gelen elektrik sinyallerini okumaktan acizler. Şimdi o elektrik sinyallerinin içerisinde frame var, ip paketi var, data var. Bu layer 1 deki cihazlar ve kablolar elektrik sinyallerinin içini açıp okuyamadığı için kendisine gelen sinyali aynı şekilde iletiyorlar.

Layer 1, 2 ve 3 cihazları işte buradan ayırt ediyor olacağız.

Router----layer 3 ip paketlerini okur.

Bir ethernet kartı, bir swich layer 2 de çalışır. Bunlar mac adreslerini okuyabilir ama ip adreslerini okuyamaz. Frame mi görür içindeki bilgileri okur ama ip paketini okuyamaz.

Layer 3 de çalışan bir cihaz layer 1 ve layer 2 standartlarını yerine getirir. Yani bir router elektrik sinyallerini alıp oradan frame i okuyabilir. Frame in içini açıp ip paketini okuyabilir. Ama ip paketinin içini açtıktan sonra datayı okuyamaz. Çünkü layer 4,5,6,7 standartlarını sağlamıyor.

TCP/İP model ve protokollerle birlikte bu konu biraz daha kafanızda oturacak.

Data Encapsulation

Şimdi ne dedik en yukarıdan itibaren benden veriyi aldı, sıkıştırdı, translate etti, encript etti sonra segmentlere böldü, sonra ip paketlerine çevirdi, sonra frame lere çevirdi gönderdi.

İşte bu her bir değişim encapsulation olarak adlandırılıyor. Verinin yeniden üretilmesi yani şekillendirilmesi, kapsüllendirilmesi.

* İki düğümün iletişim kurabilmesi için aynı protokolü kullanmaları gerekir
* Her katman (OSI veya DoD), modelin alt katmanları aracılığıyla diğer düğümdeki eşdeğer katmanıyla iletişim kurar.
* Her katman bir üstteki katmana hizmet sağlar ve alttaki katmanın hizmetlerinden yararlanır.

Slayt 16 hareketli görüntü;

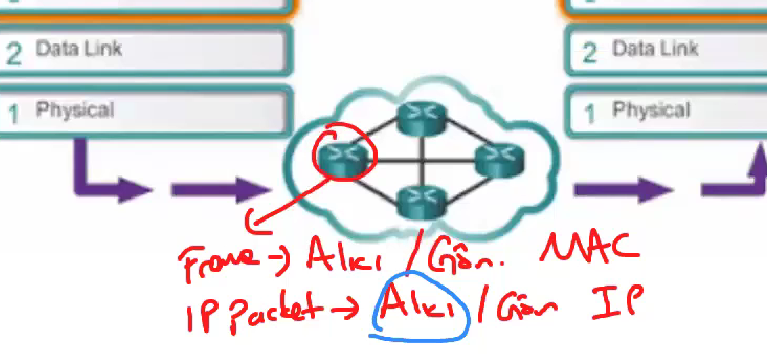
Buradan datayı alıyoruz…

Frame----alıcı mac adresi ve gönderen mac adresi bulunur

metin, diyagram, ekran görüntüsü, çizgi içeren bir resim

Açıklama otomatik olarak oluşturuldu

Packet-----alıcı ip ve gön ip yer alır



Kargo örneği verebiliriz.

metin, el yazısı, diyagram, çocukların yaptığı resimler içeren bir resim

Açıklama otomatik olarak oluşturuldu

metin, ekran görüntüsü, diyagram, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu

KAHOOT

1. Bilgisayar ağı nedir?
2. Hangisi bir ağın beklenen özelliklerinden değildir?
3. LAN açılımı nedir
4. Hangisi bir transmission, iletim ortamı DEĞİLDİR (datanın iletildiği ortam) ?
5. Fiziksel ve logical tasarımı yerleşimli bir network ne olarak adlandırılıyor.
6. Resimde gördüğünüz hangi topolojiye aittir
7. Hangi network topolojisi hub veya switch e ihtiyaç duyar
8. OSI modelin amacı nedir
9. OSI modelde kaç katman vardır
10. Veriyi bit strem e (elektrik sinyallerine ve radyo frekanslarına ) çeviren katman hangisidir
11. Yazılımlar, web browserları, e-mail istemcileri gibi uygulamalar cominication başlatmak için hangi katmanı kullannıyorlar---- Burada kullanıcı ile etkileşime girilen katman hangisidir