Önceki dersimizde topolojilerden bahsettik ve OSI modelden bahsettik.

Bugün 1. Ve 2. Layer deki ethernet standardizasyonundan bahsedeceğim.

Ethernet kartı diyoruz, ethernet kablosu diyoruz bu aslında bir standardizasyon.

Ethernet kısacası cihazların bir ağa bağlanması için uymaları gereken standart.

Aytırıpıl i diye okunuyor. IEEE diye bir kurum var Amerikada, bu kurumun yayınladığı bir doküman var. 1985 civarında çıkarılmış bir doküman. Bu dökümanın adı Ethernet.

IEEE 802.3 yayınlanan dökümanın resmi numarası. Kablolu bağlantıyı tanımlamak için hazırlanmış.

IEEE 802.11 ise kablosuz bağlantıyı tanımlamak için hazırlanmış bir doküman.

Peki bu dokümanda neler anlatılmış, neler belirlenmiş, layer 1 ve layer 2 de kablolar ve layer 2 deki hardware ile ilgili standartlar nedir onlardan biraz bahsedelim.

Her ne kadar layer 1, 2 desek, ip adresi ile bir ilgili olmasa da ethernetin ip tarafındaki standart tcp/ip standardı ile belirlenmiş durumda.

Fiziksel katman, layer 1 yani en alttaki katman. Ağırlıklı olarak kabloları ve konnektörleri tanımlamakla birlikte onların standartlarını belirliyor. Ve birkaç tane daha dami dediğimiz cihaz, repertır, convertır, hub lar var, bunları göreceğiz.

Fizikıl layer bu cihazların özellikleri tanımlanmışken data layerda da Mac adresi gibi bir kavramı tanımlamış ethernet. Mac in açılımı Medya acces control

Burada layer 2 de hatırlayın frame ler vardı.(segment, paket, frame) Data her zaman frame ler içerisinde karşıya gönderiliyor.

Gelelim layer 1 deki ethernet standartlarına.

Bant genişliği, Soldaki kablonun hızını belirleyen standartlar

İnformal name, bunlar resmi olmayan isimleri , base band----aynı anda kablodan tek sinyal geçen

Broad band, tek kobladan aynı birden fazla sinyal gönderebilen kablolar.

T-----twisted pair olduğunu gösterir. LX fiber olabilir.

IEEE name, 802.3 numaralı dökümanda bu kablonun standardı belirlenmiş.

U z ab an bu dökümana yapılan ekler demek.

Burada sadece bakır kablolar yok fiber kabloların da standardı vardır, tabi bu çok sonra çıktığı için z ekiyle eklenmiştir.

An ye kadar gelişmiş. Çünkü donanımlar gelişiyor, donanımlar geliştikçe mevcut kabloların hızı donanımların hızına yetmiyor. Yetmeyince yeni daha hızlı kablolar geliştirmek gerekiyor. Bunun standardını belirlemek gerekiyor. Dolayısıyla bu 802.3 nolu dökümanı teknolojinin gelişmesiyle birlikte ekler yapılarak daha hızlı kabloların hayatımıza girmesi sağlanıyor.

Bunları ezberlemenize gerek yok.

Burada şuna dikkat ederseniz bakın ethernet kablolarında max mesafe genelde 100 metre hızı ne olursa olsun. Ethernet kablolarının böyle bir kısıtlaması var, yani kullanılan sinyalin gücü, elektrik akımının gücü max 100 metreye kadar sinyalin taşınmasını mümkün kılıyor.

Eğer 100 metreden daha uzağa bir bağlantı kuracaksanız araya repetırlar koymanız gerekecek, yükselticiler… repeterlar da yine bahsedeceğiz, layer 1 cihazlardan. İçerisinden geçen elektrik akımını tekrar güçlendirip tekrar gönderiyor. O elektrik akımı içerisinde frame, data paketini ve segmanti okumaktan aciz. Sadece gelen elektrik sinyalini güçlendirip gönderdiği için layer 1 de çalışıyor ve bunun için ethernet standartlarında üretilmesi gerekiyor.

Tabi bu zorunluluk değil bir tavsiye ama şu an sadece ethernet standardı var ve herkes buna göre üretim yapıyor. Layer 1 ve 2 için tek standart bu günümüzde.

Dolayısıyla siz bir internete bağlanmak istiyorsanız ethernet standardında üretilen bir kart ve kablo edinmeniz gerekiyor.

Ethernet dökümanında tabi kablolar tanımlanmışken jack larda tanımlanıyor. Ne tür jacklar kullanacaklarını.

RJ45 dediğimiz telefon jacklarından biraz geniş 8 pimli bir kablo. Bunun 4 pimlisi sabit telefonda.

Ethernet kablosu bu şekilde, twisted pair dediğimiz, 8 ayrı bakır kablo, her biri bükülmüş. Gürültünün ve dış etkenlerin çok olduğu ortamlarda bu kablolar etkilenecek ve bozulacaktır. Dikkat etmeli.

Fiber optik, içerisinde cam elyaf veya plastik dediğimiz saç telinden daha ince bir madde var. En pahalı ve en hızlı. Elektrik sinyalleri değil de ışık demetleri kullandığı içinde ışık hızına yakın bir kablo teoride. Günümüzde de fiber optik in hızına yaklaşan bir kablo yok.

Günümüzde hiçbir donanım da fiber kadar hızlı değil.

Şimdi bu ethernet kablolarının gelişimi hızların artması donanımla doğru orantılı olarak ilerliyor. İşlemci hızları arttı, harddisk, ram hızları arttı, veriyi işleme hızı arttı ama ağdan aldığımız verinin hızı yavaş kaldığı için sistemi yavaşlatıyor. Hatırlayın bir bilgisayar sisteminde tüm bilgisayar sisteminin hızı en yavaş kompanentin hızı kadardır. Dolayısıyla ağ kabloları bu sistemde yavaş kalıyordu.

Bununla birlikte işte 10 mbit, 100 mbit, 10gbit, 1 gbit bu hızlarda kablolar geliştirdiler ve donanıma yaklaştı hızları.

Fiber kablolar tabi çok çok daha hızlı günümüzdeki donanımlara göre. Uzun süre de bu kullanımda kalacağı tahmin ediliyor.

Kablolardaki bu base kelimesi ne anlama geliyor bakalım;

Bakır veya fiber kablo kullanın fark etmez, iki tür kablonuz vardır.

Baseband, broadband

Baseband, Tek bir kablodan tek bir frekans gönderebildiğiniz kablolar. Yani bizim evde kullandığımız kablolar, ethernet kablolar baseband kablolar, yani bir internet kablosunun içerisinde 8 ayrı hat, kablo var demiştik ya o kanalın 4 ü gönderim 4 ü alım için kullanılıyor.

Baseband kablolar half-duplex kablolardır.

Broadband kablolar da genellikle (ISP) internet servis sağlayıcısı tarafından kullanılan kablolar, bunlar tek bir kablodan birden fazla frekans, birden fazla sinyal göndermeye izin veren kablolar.

Full-duplex kablolardır.

\*\*

Evlerimizde, apartmanlarda, binalarda kullandığımız kablolar baseband

Binadaki kutudan ISP santraline giden kablolar çoğunlukta broadband

\*\*\*

Layer 1 deki ethernet standartları bu şekilde, jackları, kabloları, radyo frekanslarına ışık demetlerini elektrik sinyallerine, işte bunun nasıl olacağını, layer 1 deki bit stream lerin, datanın elektrik sinyali veya ışık demeti ve radyo frekansı olarak nasıl iletileceğini 802.3 dökümanında bunları belirlemiş.

Bu dökümanda aynı zamanda layer 2 yi de belirlemiş. Ethernet layer 1 ve layer 2 nin ortak dökümanı diyebiliriz.

Daha önceden ethernet kartları ayrı satılıyordu, ayrıca getirip takıyor sonra internete bağlanıyorduk.4 tane ayrı ethernet kartı olabiliyor. ( blutut, wifi, kablolu ) her türlü internete bağlanabiliriz.

Şimdi gelelim Layer 2 deki standartlara;

Bizi layer 2 daha çok ilgilendiriyor. Çünkü burada hem frame lerden konuşacağız hem de MAC adreslerinden konuşacağız. Mac adresi bizim için önemli. Yani önemli derken veri bir ağda nasıl iletilir onu anlamak adına önemli. (detaylarını bilmeye gerek yok)

Ağa bağlı olan her cihazın, host olarak düşündüğümüz her cihazın mutlaka ve mutlaka uniq bir ip adresine ve uniq bir mac adresine ihtiyaç var. Mac adresi fiziksel adres olarak da geçer, donanımsal olarak da geçer.

Ethernet kartı, Network İnterface Card (NIC)

Biz hep ethetnet kartı diyoruz ama bunun adı NIC dır.

Her NIC, içerisine gömülü bir Mac adresiyle gelir, uniq dir ve bu interface dediğimiz kısım bir çip, bu çipin içerisinde bir mac adresi var. Mac adresleri donanımsal adresler, her bir donanımı birbirinden ayırt etmek için kullanılıyor. Bunlar değiştirilemezler, fabrika çıkışında gömülü olarak geliyor ve buna müdahale edemiyoruz. (hekırlar özel prog yazılımlar geliştirip değiştirebiliyor.)

Layer 2 deki ethernet standardı ağırlıklı olarak bu mac adreslerinin adreslemesinden sorumlu. Mac adresinin tanımını yapmak ve bu mac adresinin nasıl kullanılacağını belirlemektir, layer 2 deki ethernet standardı.

İp adreslerini genelde onluk olarak kullanıyoruz ama mac adresleri 16 lık sistemde gösteriliyor.

\*\*\*

Bilgisayarda gösterelim, komut istemci ile

cat /sys/class/net/eth0/address

arp -a

\*\*Broadcom kartın üreticisi, 802.11 wifi standardı,

Mac değişmez ama ip adresimi değiştirebilirim. Ama ne olursa olsun bu numaralar uniq olmak zorunda yoksa çakışma olur ve çünkü siz frame i hazırlarken, ip paketinin içerisinde ne var demiştik, gönderici ve alıcı ip adresleri var, frame de ne var, alıcı ve gönderici mac adresleri var. Dolayısıyla burada mac adresleri gündemde olduğu için ağda aynı mac adresine sahip iki tane istasyon varsa bu paketi tabi ki nereye göndereceğini sistem çözemez, çakışma olur.

\*\*\*\*Yeni çizim yapıp tekrar anlatalım kargo örneğinde olduğu gibi

metin, diyagram, el yazısı, daire içeren bir resim

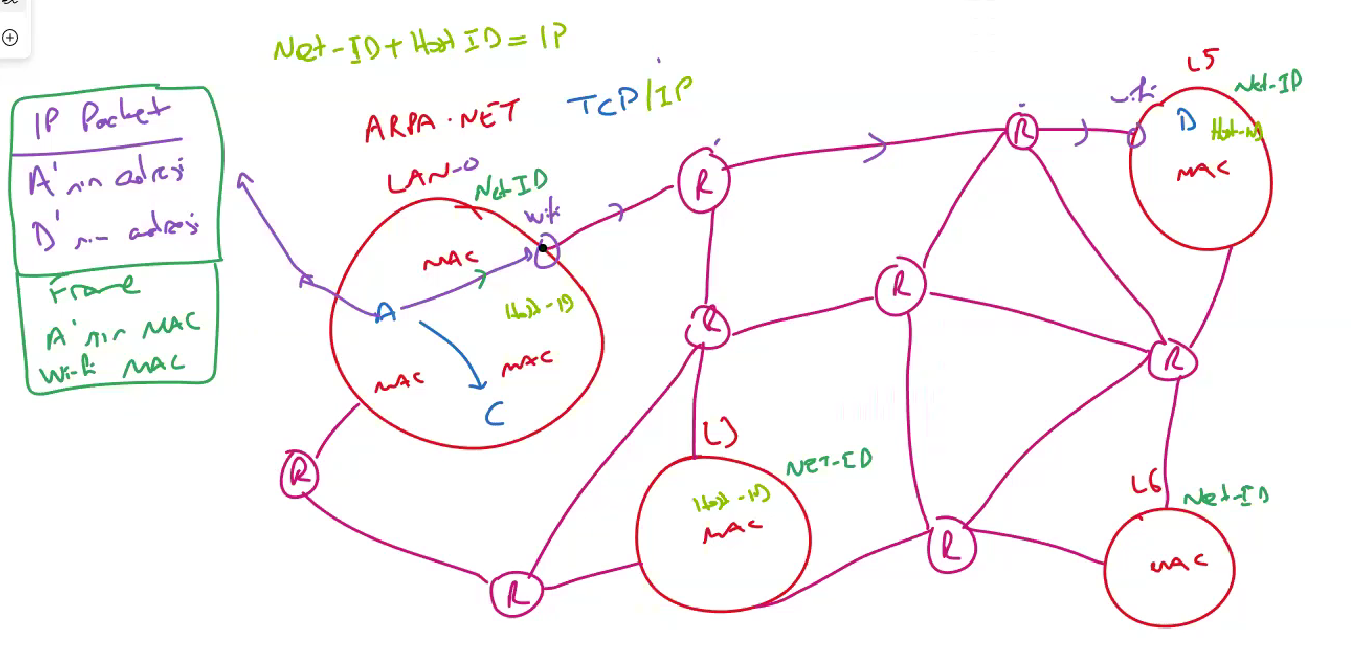
Açıklama otomatik olarak oluşturuldu diyagram, çocukların yaptığı resimler, çizgi, daire içeren bir resim

Açıklama otomatik olarak oluşturuldu

Router in görevi, en düşük maliyetli ve en hızlı yolu seçmek. ( yolda yoğun olan veya arızalı olanları seçmez)

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

Açıklama otomatik olarak oluşturuldu



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

Açıklama otomatik olarak oluşturuldu el yazısı, çizim, çocukların yaptığı resimler, metin içeren bir resim

Açıklama otomatik olarak oluşturuldu burada ip paketi değişmez ama her istasyonda frame açılır ve değiştirilir.

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

Açıklama otomatik olarak oluşturuldu



\*\*\*\*İkili çevirilere bakalım

metin, ekran görüntüsü, yazı tipi, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu



Şimdi hexedecimal çevirilere bakalım;

Bir rakamın önünde 0x görüyorsanız veya sonunda küçük h görüyorsanız buradaki rakam onaltılık demektir.

Şimdi burada E harfi olduğu için bunu anlıyorsunuz ama önümüze 27 rakamı çıktığında nasıl anlarız 10 luk mu 16 lık mı diye, işte bu şekilde başına 0x veya sonuna h harfi konur ki anlaşılsın.

metin, yazı tipi, el yazısı, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu çok fazla kullanmayacağız, gerekirse hesap makinası ile hesaplayabiliriz. Windows un hesap makinasında soldaki işarete tıklayıp programer den çıkıyor solda, hexe, dec, 8 lik ve 2 lik hesaplamalar.

Mac adresleri nasıl sağlanıyor yani nasıl belirleniyor ???

Merkezi numara veren bir kurum var, sol 24 bit üreticinin kimliğidir, kalan yarısı da üretici tarafından verilen rastgele rakamlardır.

Firma ücret ödeyerek bu yetkili kurumdan mac adres bloğu satın alıyor. Bu alınırken sadece üretici numarası veriliyor. Bir üreticinin birden fazla mac adres bloğu vardır. Soldaki rakamları internette arasak hangi firmanın diye bulabiliriz.

Şimdi gelelim adres tiplerine. Ne dedik, bir paketin gönderilebilmesi için alıcı ve gönderici adreslerinin olması lazım. Burada 3 çeşit alıcı adresimiz var, networklerde kullandığımız.

1. Unicast ; tek bir alıcının olduğu adresleme tipi.
2. Multicast; bu birden fazla alıcının olduğu adres tipi, genelde abonelik sistemi üzerine çalışır. Slack te kanallar olarak düşünebilirsiniz, bir gurup olarak düşünebilirsiniz. Peki bunu nasıl anlıyor router, burada multicast adreslerde alıcı adresi 01:00:5E ile başlaması lazım. Frame i açıp bakınca ve bu numaraları görünce bunun bir guruba gönderildiğini anlıyor router. Bu bizi çok ilgilendirmiyor, çok karşınıza çıkmayacak, büyük firmalar kurumsal firmalar tarafından kullanılıyor. ( netfilx veya youtube aboneliklerine giden mesaj)
3. Broadcast; bu en çok kullandığımız ve arka tarafta da çok yapılan bir adres. Bazen bir mesajın herkese ulaştırılması gerekebilir. Yani tüm ağa bir duyuru yapmanız gerekebilir. Bu durumda herkesi tek tek adreslemek yerine alıcı adresine FF:FF:FF:FF:FF:FF yazıyoruz. Bütün bitleri turn all yapıyorsunuz önünüze bir broadcast adresi çıkıyor.

Bu adres hiçbir cihaza tanımlanamaz, bu reselv (rezerve edilmiş) bir adrestir. Hiçbir ethernet kartında böyle bir adres göremezsiniz.

Herkesin adresini bilmeniz mümkün değil onun için bu yöntem kullanılır.

Bu broadcast adresi ağların çalışma dizaynının bir parçası. Broadcast adresi arka planda sürekli yapılır. Sebeplerinden TCP/İP kısmına gelince bahsedeceğiz.

CSMA/CD

Bu konu detay bir konu, sadece ne olduğundan bahsedelim yeterli.

Ağlarda özellikle Bus topoloji dedik veya normal ağlarda da bu geçerli, simplex ve hulf duplex ağlarda çatışma olabilir. Aynı anda iki veya daha fazla bilgisayar aynı anda mesajını göndermek isteyince ağda bir çakışma olacaktır, frekanslar birbirine girecektir, kimse mesajını gönderemeyecektir. Buna collission denir. Bunu engellemek için çeşitli algoritmalar geliştirilmiş, bunlardan birisi Carrier Sense Multiple Access / collision Detection. Bunlar işletim sistemi tarafından yapılan algoritmalar.

Bir veri göndermek isteyince karşıya bir carrier sinyali (sabit telefonun dıt sesi gibi) gönderiyor, ağı kontrol etti ve veriyi ağdan gönderdi. İkisi aynı anda carrier e baktı müsait diye veriyi gönderdi o anda çakışma olur, böyle olunca ne yapıyor rastgele bir zaman bekleyip veriyi tekrar gönderiyorlar. Ta ki mesajlarını gönderene kadar.

Collision

Bu kavram a da bakalım, collision domain ağlarda kaçınılmaz bir durum.

Bizim telefon hatlarımızda, ethernet kablolarımızda sürekli bir elektrik sinyali var, bu sinyal olmazsa ağ bağlantısı kurulamaz. Bu sinyali modüle ederek, normal giden durumun şeklini değiştiriyoruz.

yazı tipi, metin, çizgi içeren bir resim

Açıklama otomatik olarak oluşturuldu

Böyle şeklini değiştirerek veriyi iletiyoruz.

Bunun 3 tane yöntemi var, dalganın frekansıyla oynadığınızda FM yapmış oluyorsunuz, genliğiyle oynadığınızda AM bandı oluyor, dalganın artı eksi yönüyle oynadığınızda PM oluyor. PM günümüzde çok kullanılmıyor ama radyolarda hala FM ve AM kullanılıyor. (FM—kısa mesafeler, AM uzun mesafeler)

Ağlarda da siz frekans modülasyonu yaparak biz bu carrier sinyalinin şeklini değiştirerek veriyi iletiyor.

Buradaki carrier sense dediği bu , önce frekansa bakıyor olması gerektiği gibi mi eğer bir farklılık yok ise gönderimini yapıyor, veya tam tersi olunca bekliyor.

Broadcast Domain

Braoadcast adresi herkese gönderiyor. Peki bu broadcast adresi giderken başka bilgisayarlar gönderme işlemi yapabiliyor mu, yapamıyor. Genel olarak ağı meşgul ediyorsunuz, ağın performansını düşürüyorsunuz ve brcast mesajları siz istemeseniz de network tasarımının bir gereği olarak arka planda sürekli olarak kullanılan bir method. Çünkü sürekli olarak ağı güncel tutmanız lazım, onların mac adresleriin, ip adreslerini bir yerde toplamanız lazım bir tablonuz var, o tabloyu güncel tutmak adına…

Broadcast domain ne, bir ağda broadcast mesajının ulaşabildiği en son uçtaki bilgisayarların toplamı bize bir domain oluşturuyor. Bu domain in boyutu bizim için neden önemli, siz broadcast mesajı yaptıkça ağda sürekli trafik oluyor (performans kaybı), yani sizin göndermeniz gereken mesaj gecikebilir. Ve ağ da 300-3000 tane bilgisayar olduğunu düşünün bu durumda trafik oldukça fazla olacaktır. Dolayısıyla biz bir ağ tasarlarken b\_domain i mümkün mertebe küçük tutmamız lazım. Ağın performansını yüksek tutmak adına, çünkü broadcast lerden kaçınamıyoruz, bunlar mutlaka olacak. Bu b\_domain in boyutunu ne kadar küçültürsek o kadar trafiği azaltmış oluruz.

Peki nasıl küçültebiliriz.

Bunlar switc ler, bunlar layer 2 de çalışıyorlar. Switcler kendilerini ilgilendiren bir mesajsa hem cevap verirler hem de bu mesajı tüm portlarından yayınlarlar. Biz switclerin olduğu bir ağda b\_domain i küçültemeyiz.

Bunu küçültmek için bir router lazım. Router ne yapar kendilerini ilgilendiren mesaja cevap verirler ama kendi diğer portlara göndermezler.

metin, ekran görüntüsü, diyagram, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu

\*\*\*

3 ayrı domain ve 3 ayrı yer oldu ve birbirlerinin performansını etkilememiş oldular.

Frame nedir, içerisinde ne var bunlara bakalım.

Şimdi biz bir ip paketi hazırladığımızda başına header ve sonuna trailer konulur. Elektrik sinyali iletilirken nerede bittiği belli olmalı. Bu paketinde elektrik sinyalini iletim şekli bu frame olduğu için böyle olması gerekiyor.

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

Açıklama otomatik olarak oluşturuldu

Preamble ----- ikaz kısmı veri gelecek , dıdıdıdıdıt diye sinyal gönderip haber veriyor.

Start of frame----analog, dijital

FCS ---- frame check secınd, gelen frame in doğruluğunu kontrol edeceğimiz bir hash kodu, veri bozulmuş mu diye bakıyor.

NETWORKİNG DİVİCESES

Cihazlardan konuştuk, router, hub, …. Bu cihazlardan bahsedelim. Şimdi önce genel cihazlardan sonra bazı özel cihazlardan bahsedeceğim.

Ethernet Kartı, NIC, LAN adapter, Fizikıl Network İnterface gibi çeşitli isimleri var.

Bu temel seviyede bir cihazın ağa bağlanması için gerekli olan kart. Eskiden ayrı satılır takılırdı, hala var ama günümüzde bu kartlar anakartla beraber geliyor.

Çip de analoğu dijitale çevirip sinyali gönderiyor alırken de tam tersi.

HUB

En ilkel cihazlardan biri, eskiden çok kullanılırdı. Hub layer 1 de çalışan bir cihaz. Layer 1 de çalıştığı için frame leri okuyamıyor, o yüzden gelen mesajı tüm cihazlara gönderiyor. Mac adresini okuyamaz.

Ağın performansını ciddi oranda düşüren bir cihaz.

Güvenli değil, paket herkese gittiği için.

Bir collision domain oluşturuyor, çakışma oluyor ve tüm ağda trafik duracak.

Hulf-duplex

Buna damin cihaz da deniyor, gelen paketin kime geldiğini okuyamadığı için.

Küçük ağlarda evlerde kullanılabilir.

100 megabit hızı.

SWİTCH

Eskiden hep HUB kullanıyorduk çünkü switch e göre daha uygundu fiyatları. Artık fiyatları daha uygun.

Birden fazla hostu ağa bağlamak için kullanılıyor. Layer 2 de çalışıyor. Frame leri okuyabiliyor. Mac adreslerini okuyabildiği için paketleri sadece ilgili node gönderiyor.

Full-duplex, hem gönderim hem alım yapabiliyor.

iki veri aynı anda gidebiliyor.

Günümüzde de artık şirketlerde de bu kullanılıyor.

BRİDGE

Çok sık görmezsiniz bunu, Bridge, Hub ı segmentlere ayırmak için kullanılıyor.

Şimdi hub a dedik ya tüm portlara gönderiyor paketi, diyelim ki sizin büyük bir ağınız var ama switch pahalı olduğu için alamıyorsunuz, onun için bridge alıyorsunuz. Bridge de layer 2 de çalışan bir cihaz switch e benzer bir şekilde çalışıyor ama özellikleri düşük bir cihaz. Üzerinde 2 veya 4 tane port olur.

Bridge nin tek mantığı tek bir ağı iki veya 4 e bölmek için kullanılır.

Switclerde collision u küçültmek için router kullanıyorduk, hubda da performansı arttırmak için bu şekilde bölüyoruz.

ROUTER

Gelelim router e internet için en önemli cihaz. İnternet trafiği bu router denen cihazlar üzerinden yapılıyor. Router ler en gelişmiş ağ cihazlarından biri. Aslında bir router bildiğimiz anlamda bir bilgisayar, kendi işletim sistemi, kendi donanımı olan bağımsız bir cihaz, yani rami, işlemcisi ve harddiski olan klavye, mause takarak kontrol edeceğiniz bir cihaz. Çok gelişmiş olmakla birlikte çok pahalı da cir cihaz.

Router, asıl görevi routing yapmak, rauting yapmak ne, ip paketlerini internet üzerinde istenen yere göndermek ki biz internet üzerinde ip paketleriyle iletişim sağlıyoruz.

Layer 3 de çalışıyor, frame okur ve ip paketindeki ip yi okuyor.

Son derece akıllı cihazlar, tüm dünyadaki routerler birbirlerini tanıyor, diyoruz ama bölgesel olarak birbirlerini tanıyorlar. Konumlarını biliyorlar, bunları güncel olarak takip ettikleri bir tabloları var kendi içlerinde. Bu tablolar broadcast mesajlarıyla, L3 de yapılan broadcast mesajlarıyla güncel tutuyorlar. Ve bu sayede istenen paketi istenen yere en hızlı şekilde gönderebiliyor.

FİREWALL

Firewall iki türlü hem yazılımsal hem donanımsal versiyonları var. Bunun yazılım kısmı zaten işletim sistemlerimizde hemen hepimiz kullanıyoruz.

Donanımsal versiyonları black box da deniyor.

Firewall ın görevini biliyorsunuz, ağı dışardan gelebilecek kötü amaçlı saldırılara karşı korumak.

FW lar genelde L3 de çalışır, Net cenereşın firewall dediğimiz L7 de çalışan bu en gelişmiş FW. Bu L7 de çalışması sebebiyle hem ağ trafiğini fiziksel olarak takip ediyor, oradan analizler yapıyor, hem de arka planda çalışan yazılımlar, uygulamalar onların da talebini kontrol ederek gelen paketlerle uygulamaların taleplerini eşleştirip kötü niyetli biri var mı…. ( layer 2 de değil layer 7 de çalıştığı için aradaki kötü niyetli kişilerin girmesine engel olabiliyor. Session bilgisi başlatılmış mı, kim talep etmiş bu Google isteğini, ne zaman başlatılmış bunlara bakar)

Gördüğünüz gibi ne kadar yukarı üst katmanlara çıkarsanız paketin içerisinde o kadar çok veriyi okuyabiliyorsunuz. Ne kadar çok veriyi okursanız o derece analiz yapabiliyorsunuz.

IDS/IPS

Gelelim bir diğer cihaz, sibercilerin kullandığı, konfigüre ettiği cihazlar genellikle.

Intrusion Detection System (IDS), Intrusion Prevention System (IPS) bu ikisi ayrı cihaz ama genelde bir arada kullanılır.

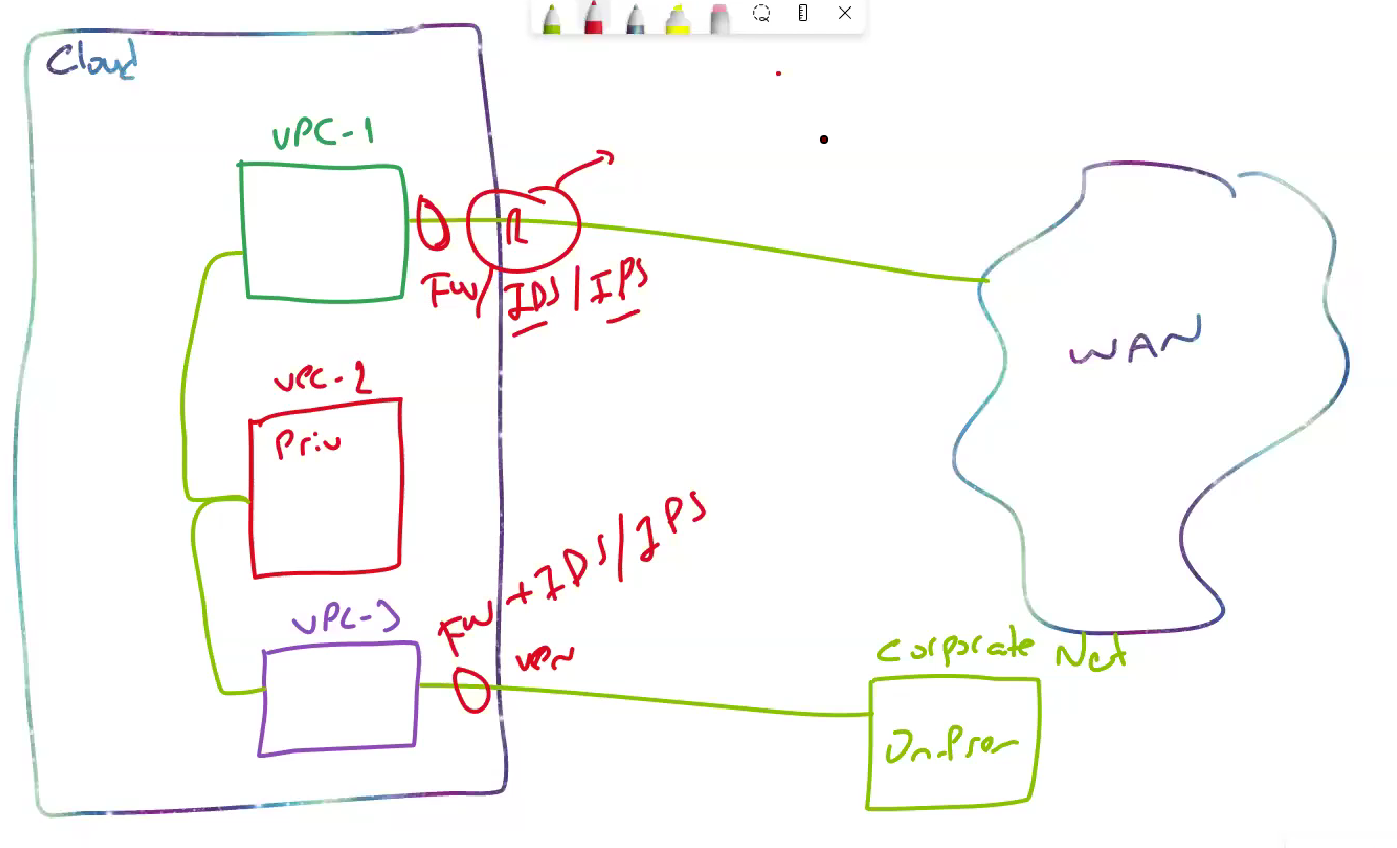
Farkı ne, bunlar firewall mantığıyla çalışıyor. Kötü amaçlı trafikleri analiz edip bunların ağa ulaşmasını engelliyor.

IDS tespit ediyor, IPS engelliyor.

IDS, internet trafiğine paralel koyuyorsunuz, sizin networkünüze yaklaşmak isteyenler firewall ı geçebilir, burada IDS giden trafiği sürekli analiz ediyor, şüpheli bir şey gördüğünde burada administreytıra, yöneticiye ikaz veriyor ama o trafiği engellemiyor.

IPS, gördüğünüz gibi trafiğin tam üzerinde oturuyor, firewall dan gelen trafiği analiz ediyor, eğer şüpheli gördüğü bir şey varsa izin vermiyor.

Genelde beraber kullanılır. Tek bir katman olarak yazılımın üçünü birden yükleyebiliriz ama 3 ayrı kompanend olursa geçmesi daha zor oluyor bu yüzden 3 ayrı cihaz olarak tercih ediliyor.



Şimdi gelelim biraz özel amaçlı kullanılan cihazlardan.

Load Balalncer

AWS de çok kullanacağınız bir service.

Load balancer ne işe yarıyor, mesela amazon.com alış-veriş sitesi arka planda 10 tane birbirinin tıpatıp aynısı olan serverlar, tabi bu serverların max kapasitesi var, bu kapasiteleri aştıkça gelen trafiği serverlar arasında dağıtan bir cihaz. yazılımsal da olabilir, donanımsal da olabilir. AWS dekiler tabi sanal makineler…

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

Açıklama otomatik olarak oluşturuldu zoom server da öyle.

Kullandığın hizmet kadar para ödemek istiyorsak Autoscaling kurup ihtiyaç kadar server kalkıyor gerekmedikçe kapanıyor serverlar.

<https://inframetrics.trendyol.com/d/gP0c_Sc7z/inframetrics?orgId=1&kiosk>

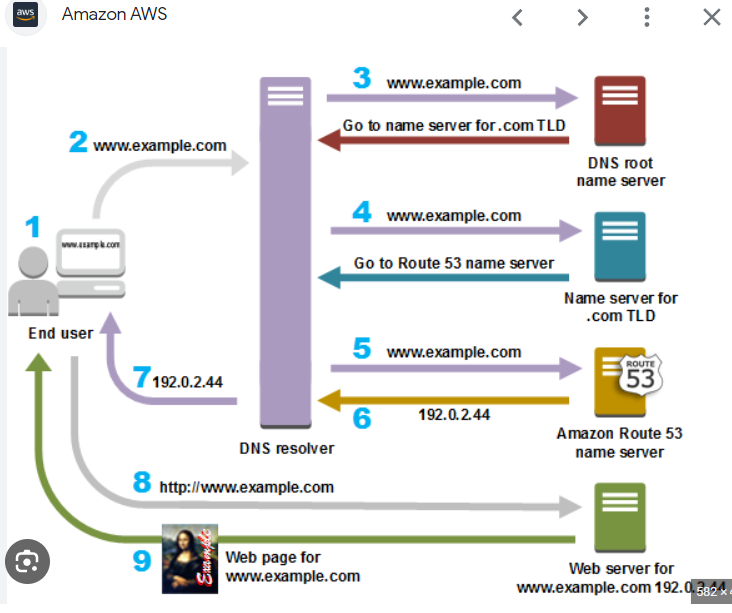
bulut sistemi bu tür şirketler için her zaman daha mantıklı.

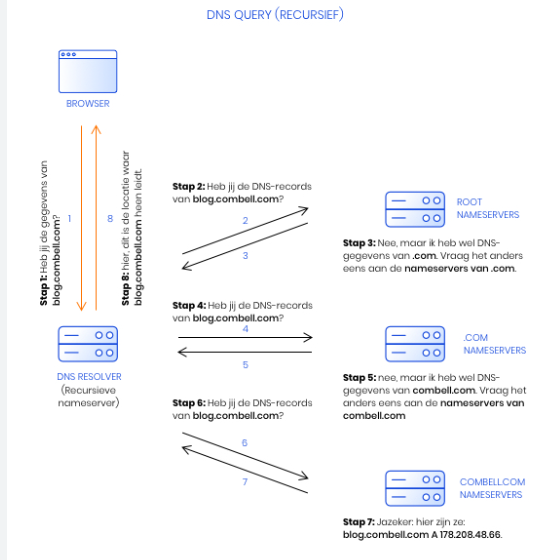
Domain Name Server

En önemli serverlar diyebiliriz. Bunlar olmasa internet kullanımı bizim için işkenceye dönüşebilirdi.

DNS nedir önce ondan bahsedelim, tüm routing işlemi ip adresine göre işlem yapıyor. Ama biz kullanıcılar için ip adresini ezberlemek çok zor. Router ler de bizim yazdığımızı okuyamıyorlar.

DNS server ---- bir telefon rehberi gibi





DNS serverlar daha doğrusu Top level dns serverlar IANA tarafından kontrol ediliyor, onların yetkisinde.

İana.org stesinden bakabiliriz, .com, .tr her biri için farklı server var.

Mesela DNS server lardaki isimli adres hiç değişmiyor ama arka planda makinalar ve ip ler değişiyor kullanıcılar için problem olmuyor.

Proxy Server

Proxy server bir nevi firewall görevi de görüyor, bir nevi cache görevi de görüyor. İnternet ile comprer ağ arasına kuruyoruz bunu.

Ne işe yarıyor bu, en büyük amacı, bir şirket içerisinden dışarı çıkarken istenmeyen web sitelerine erişimi engelliyor. Mesela çalışanların mesai saatleri içerisinde sosyal medya hesaplarına girmesi istenmiyorsa bu Proxy server da istenmeyen şeyleri kısıtlıyorsunuz buradan artık bağlanamıyorsunuz.

Bu en çok kullanılan amaçlarından biri.

Bir diğer amacı, dışardan şirket ağına sadece yetkili kişilerin erişmesini sağlıyor. Siz Proxy server ayarı yapıyorsunuz bilgisayarınızda kullanıcı adı ve şifre ile şirket ağına bağlanabiliyorsunuz.

Üçüncü kullanım amacı cache bellek, en sık kullanılan web sitelerini burada depoluyor. Dolayısıyla her seferinde internete çıkmadan doğrudan bu Proxy server üzerinden bu web sitelerine erişim sağlayabiliyoruz. Bunun da amacı hem internete çok sık çıkılmamasını sağlamak hem de hızı arttırmak.

Bir firewall gibi işlem görüyor.

Encription Devices

Encription, şifrele cihazları. Bunlar yazılımsal olabildiği gibi böyle donanımsal da kullanılabiliyor. Bunlar gelen verileri şifrelemek, kriptolamak için kullanılan cihazlar.

Packet shaping

Bunlar da ISP lerin en çok kullandığı cihazlar, şirketlerde de kullanılıyor.

Trafik polisi gibi düşünebilirsiniz.

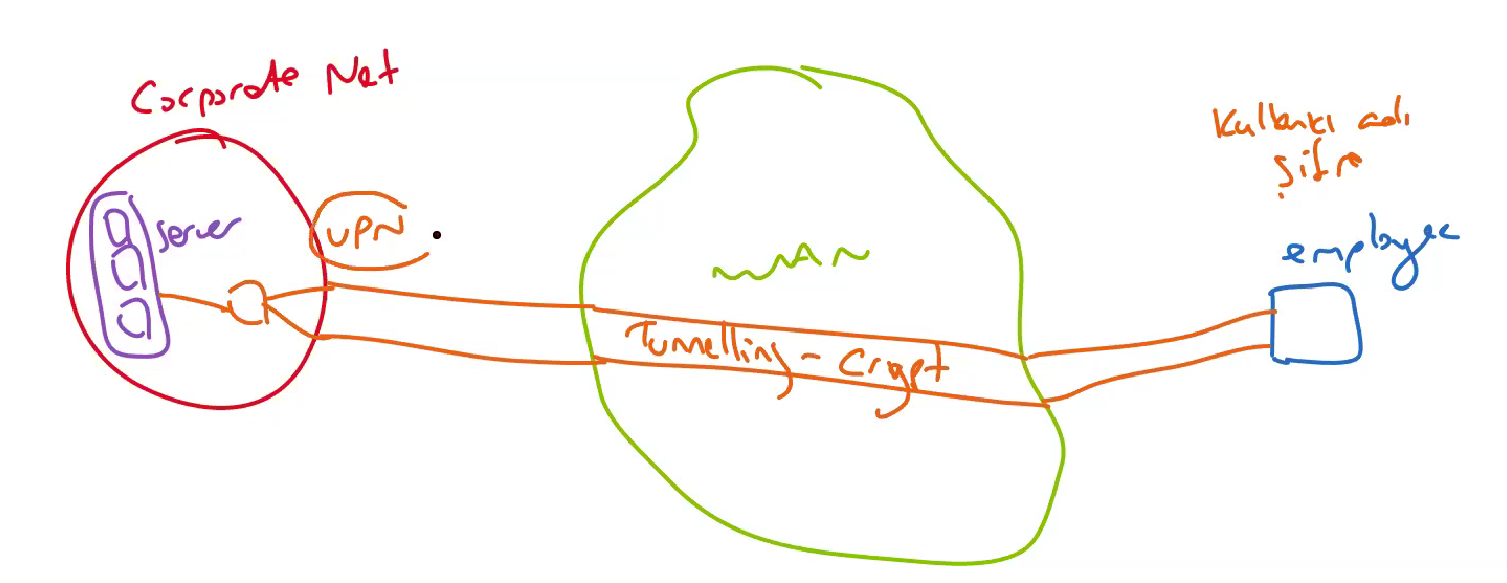
ISP ler tarafından nasıl kullanılıyor, sizin internetlerde kota var değil mi, kota dolunca internet yavaşlıyor veya kesiliyor. İşte bu hızı düşüren cihazlar. Gündüz ayrı gece ayrı hız kullanımları veya gb kullanım farklılıkları olabiliyor.

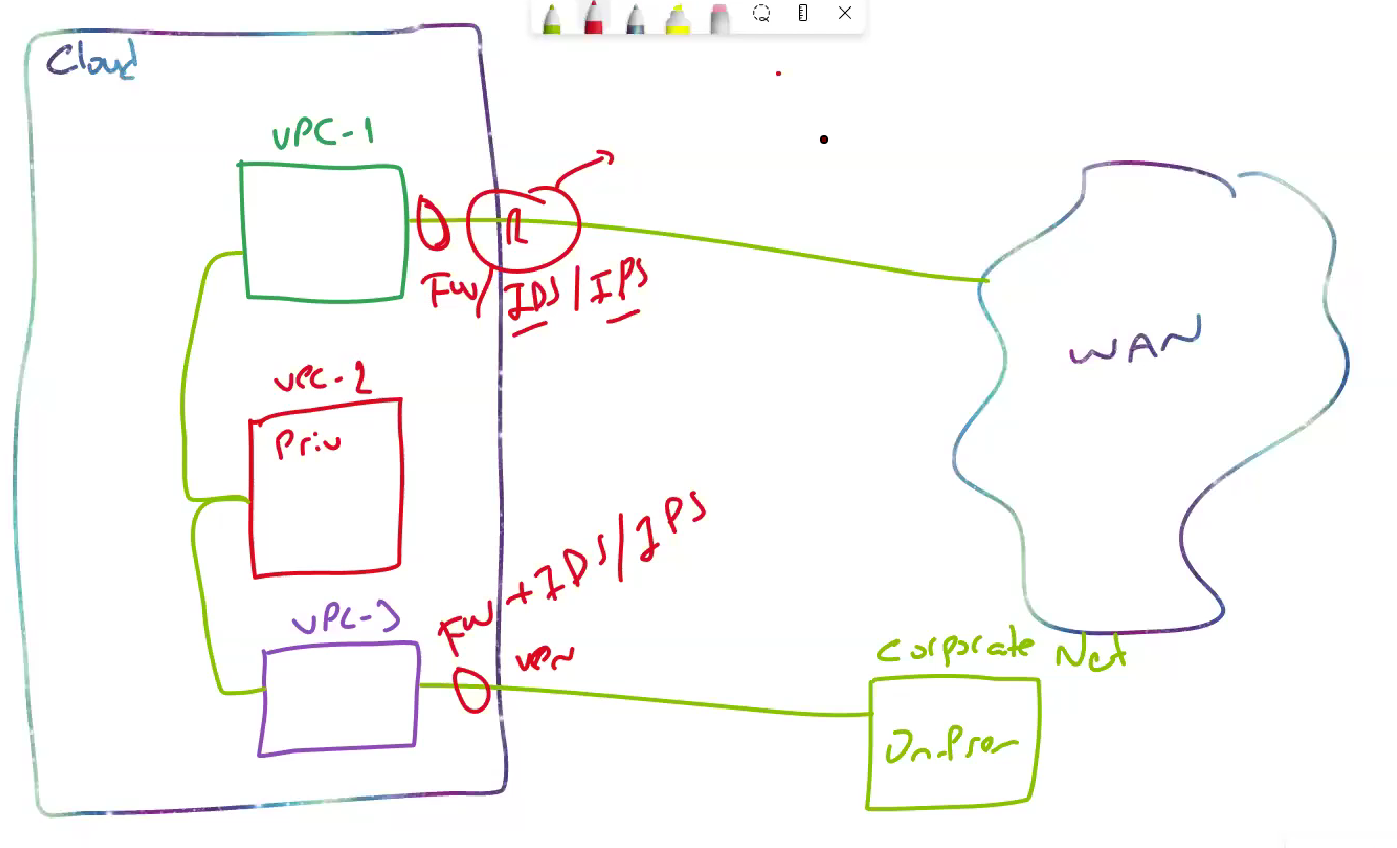
Şirketler için nasıl oluyor, belli bir kısmı patron için önemli bir toplantı için ona ayrı band ayrılıyor görüşmesi kesilmesin diye, sonra istenirse değiştirilebiliyor.

VPN

Vpn ne işe yarıyor,

Remote çalışma sistemi ortaya çıkınca böyle bir hizmet çok yararlı olacaktır.





KAHOOT ( ethernet spesification and network divicese)

1. Hem verinin gönderimi hem de bu teknolojiyi kullanan cihazlar için kullanılan standardın adı nedir
2. Ethernetin kullandığı dökümanın numarası (wifi değil)
3. Router u kullanmadan bağlı cihazların ayrı ayrı…..??????

Bir router in her bir portu bir broadcast domain dir

1. Bu kablolardaki BASE ne anlama geliyor.
2. NIC nedir
3. Switch ile hub arasındaki fark nedir
4. Gelen paketi analiz edip ilgili networke ileten cihazın adı nedir
5. Firewall nedir
6. DNS server ın amacı nedir
7. WAN internet ile LAN arasındaki trafiği filtreleyen cihaz veya server nedir