OSI model ve TCP/IP modell var, OSI model daha çok donanım seviyesinde standartlar belirlenirken, internet TCP/IP üzerine kurulmuştur. (1984 yıllarında)

Bugün TCP yi biraz daha hızlı geçeceğiz çünkü ip kısmı daha önemli…

TCP modeli biraz tanıyıp daha sonra protokollerden bahsedeceğiz.

Önce TCP/IP nin geçmişinden bahsedelim;

Açılımı, *Transmission Control Protocol/Internet Protocol,* ip dediğimiz kısım işte bu internet protokol kısmı. İnternet protokollerinin belirlendiği kısım bu ip, lojikıl adresleme dediğimiz kısım internet protokol ile belirlenmiş. O yüzden ip adresi diyoruz.

Bir TCP İP bir protokol süiti, işletim sistemlerinde yüklü olarak gelir. Bazı belki küçük distrolarda olmaz ama genelde tüm işletim sistemlerinde yüklüdür. Çünkü bir http protokolü olmadığı için internete bağlanamazsınız.

1974 de ilk TCP Arpa netle ortaya çıktı. Biliyorsunuz o zaman tek bir lokal ağ vardı, mac adreslerini kullanarak birbirleri ile iletişim kuruyorlardı.

Ancak önce üniversitelerde daha sonra da umuma açılması ile birlikte, internete evrilmesi ile birlikte local ağların sayısı inanılmaz derecede arttı. Local ağ sayısı artınca TCP protokolü yeterli gelmedi. Çünkü tüm internete beğlı cihazların mac adreslerini bilmeniz lazım bu mümkün değil.

Tabi bu internet mühendisleri o zamanlar bu gidişatı öngörüp, mevcut zaten çalışan bir protokol var TCP protokolü local ağlar içerisinde çalışıyor. Şimdi biz local ağlar arası bir cominication kurarsak ne kadar çok local ağ olursa olsun internet üzerinden bu local ağlara erişimde bir problem yaşamayız diyorlar. Ve internet protokolü geliştiriyorlar 1978 de ve artık TCP/İP adını alıyor.

İlk önce savunma bakanlığı bünyesinde geliştirilen bir protokol, daha sonra internetin evrilmesiyle herkesin erişimine açılmış bir protokol ve şu an günümüzde herkes TCP/İP protokolü üzerinde çalışıyor.

Kalifornia Berkeley(börkliy) ünv ağırlıklı olarak İP kısmı ağırlıklı olarak çalışılmış.

TCP/İP modelin bir diğer adı DOD model. ( savunma bakanlığı modeli, Arpa nette öyle)

TCP/İP model aslında tamamen OSI modelin sıkıştırılmış hali, tamamen konseptler aynı. OSI modelde 3 katman bu modeldi daha düzenli tek bir katman olarak alınmış. Diğerlerinin tamamını kapsıyor ve Biraz daha anlaşılır kılmak için tek bir katmana düşürmüşler ama yapılan işlem tamamen aynısı, session, presentesion…..aynı.

OSI modelde protokoller belirlenmemiş, nasıl haberleşileceğinin standartları belirlenmiş, nasıl enkripşın yapılacağı, compres yapılacağı belli ama bunların çeşitleri yok.

İşte TCP ip model buradaki kavramları protokollere bölmüş. Mesela internet sitesine bağlanmak istiyorsanız http kullanacaksınız. Bir file server a bağlanmak istiyorsanız FTP protokol kullanacaksınız. Mail servera bağlanacaksanız IMAP veya POP3 protokolünü kullanacaksınız….. yüzlerce hatta binlerce protokol var, tabiki en çok kullanılan protokoller 15 – 20 tane herkesin duyduğu bildiği veya ihtiyaç duyacağı. O yüzden TCP ip ye protokol süit deniliyor. Çünkü tamamen protokollerden oluşuyor. Protokol neydi ortak bir dil, farklı donanımlar ve yazılımlar arasında ortak bir dil konuşmak için geliştirilmiş bir standart.

Transport Layer burada da tamamen aynı, burada da belli başlı iki tane protokol var. Günümüzdeki trafiğin % 95 den daha fazlası UDP ve TCP protokolü üzerinden yapılıyor.

İnternet Layer OSI model ile tamamen aynı, İP adreslerinin gündemde olduğu kısım. İnternet layerda da bazı protokoller var bunlar en çok routerler tarafından kullanılan protokoller. Hani dedik ya routerler birbiriyle haberleşip en kısa yolu, en hızlı yolu ve en sağlıklı yolları bulup bunların (cost) hesabını yapıyor. Bunları da bazı protokollerle yapıyorlar. Bunlar bizim kontrolümüz dışında internet layerda gerçekleşiyor.

Daha sonra network interface, burası OSI modelde datalink ve fizikıl layer la tamamen aynı. Bunu ikiye bölmüştü OSİ, hatırlayın bunların günümüzde kullanılan standardı ethernetti. Hem L1 ve L2 standartları ethernet dökümanıyla belirlenmiş. Aynısı TCP ip de de düşünün ethernet deyince Network interface olarak düşünün.

Ethernet deyince ne aklımıza gelecek, MAC adresleri aklımıza gelecek. Dolayısıyla network interface dediğimizde de mac adresleri gündemde olacak.

Şimdi en alttan yukarı doğru bir iki cümleyle katmanları tanıtalım, sonra katmanların detayına ineceğiz.

Network acces layer aynı OSI modeldeki gibi verinin fiziksel olarak nasıl iletileceği, fizikselden kasıt OSI model L2 de frame lere ayrılıyordu paketler, ip paketlerini frame lere koyuyorduk, bu frame lerde daha sonra kablolar üzerinde wifi üzerinden radyo freakansları veya elektrik sinyalleri veya fiber üzerinden ışık demetleri olarak gönderiyoruz. Fiziksel olarak veriyi ilettiğimiz kısım.

Main protokol kullanan esas kısım tcp ip modelde kullanılan protokoller), ethernet, token ring, ethernet haricinde diğerlerini duymanız çok zor, onlar eski protokoller. Günümüzde FDDI bunu bazı Telekom şirketleri kullanıyor. Token ring IBM tarafından geliştirilmiş, X.25 beş büyük şirketin geliştirdiği protokol ama günümüzde ethernetin yaygınlaşmasıyla pek kullanım yeri kalmadı.

O yüzden TCP ip modelde Network acses layer dediğinizde ethernet protokolü aklınıza gelsin diğerlerini bilmenize ezberlemenize gerek yok, diğerlerinin karşınıza çıkacağını düşünmüyorum.

Gelelim bir üst katmana, internet layer, işte internet trafiğinin şekillendiği katman burası. Neydi OSI modelde veri segmentlere bölünüyor, segmentlerden ip paketlerine ayrılıyordu. Burada paket yerine datagram çevrisi daha çok kullanılıyor ama kavram şu şekilde, UDP kullanılan paketler için datagram (çünkü UDP nin açılımı User datagram protokol), TCP olanlar paket olarak adlandırılıyor. Paket ya da datagram olarak duyarsanız bunun farklı şeyler olduğunu bilin.

Üst katmandan opereting sistem tarafından hazırlanan veriyi ağda göndermek üzere internet layere veriyor, internet layerde de artık bunlar datagramlara veya paketlere çevriliyor. OSI modeldeki ip paketinin aynısı.

Bu katman ip paketlerinin internet üzerinde iletilmesinden yani alıcı adresinin almasından sorumlu. Rauterlerin çalıştığı katman bu. OSI---layer 3, TCP ip ye göre internet katmanı ( yine aynı şekilde).

En çok kullanılan protokoller tabi ki internet protokolü ip adresi, ICMP bu özellikle ciber sec ler için önemli bir protokol, ARP, RARP, AGMP, bunlardan teker teker bahsedeceğiz. Bunlar en çok kullanılan protokoller. Bunlar haricinde birkaç tane daha protokol var ama çoğunun kullanım yeri kalmamış veya çok özel maksatla kullanılıyorlar.

Bu katmanda karşınıza çıkacak protokoller bunlar, ICMP iki katmanda birlikte çalışıyor, hem network hem de internet layerde. Özel bir protokol. Kullanıcı olarak bizi ilgilendiren protokol, ip protokolü. Diğerleri arka tarafta işletim sistemi tarafından kullanılan protokoller. İp bizzat bizim muhatap olduğumuz protokol, işte ip adresini ip protokolü sayesinde belirliyoruz.

Gelelim bir diğer katmana, Host-to-Host olarak da görebilirsiniz, transport layer olarak da görebilirsiniz. (Kernel seviyesinde bir katmandı OSI modelde, burada da).

Host to host artık hostların iki tarafta da karşılıklı olarak muhatap olduğu katman. Veri network, internet layer da şekillenip karşı tarafa gönderiliyor ya karşı tarafta artık host veriyi transport layerde artık veriyi işlemeye başlıyor. İp paketini artık açıyor içinden datayı çıkarıyor. Datayı içinden çıkardığı kısım bu transport layer.

Burada da en çok kullanılan belki internetin % 95 den fazlası TCP ve UDP protokollerini kullanıyor. Burada biraz kafa karışıklığı olabilir, bir TCP model diyoruz ve TCP protokol diyoruz, bu tabiki TCP modelin ismini aldığı bir protokol ama siz şimdi Appilication layerde de protokoller var http mesela, http protokolü kullanırken verileri yine TCP veya UDP protokolüyle paketleyip gönderiyorsunuz karşıya. Bunları bir zarf olarak düşünebilirsiniz. Yukardan nasıl gelirse gelsin bunlardan birinin içine koyup öyle internete yolluyorsunuz. (http, FTP veya Pop da kullansanız bunları mutlaka TCP veya UDP paketleriyle karşı tarafa gönderiyorsunuz.

Ve en üstteki katman, proses veya appilication layer olarak geçiyor. Kullanıcıyla interakşına(etkileşim) girdiğimiz tek katman burası. Burada artık uygulamaların birbiriyle haberleştiği kısım. Aynı zamanda alt layer la, transport layerla ve internet layerla cominicationu (iletişimi) sağlanan katman. Çünkü burada kullanıcıdan alınan bilgiler burada hazırlanıp alt katmana iletiliyor, alt katmanda transport layerda TCP veya UDP paketinin içine konuluyor ondan sonra network layerdan fiziksel olarak gönderiliyor. İnternet layerda ip paketlerine koyuyoruz tabi daha sonra network layerden gönderiyoruz.

Datanın hazırlandığı kısım, appilication layer. Burada bir dünya protokol var hatta 1000 in üzerinde protokol var ama bir çoğu çok özel amaçlar için yazılmış ya da kullanım yeri kalmamış protokol. Günümüzde DNS (domain nema server), HTTPS secur versiyonu, Telnet artık çok kullanım yeri yok, SSH ciber ve diğer pedlerde çok kullanılıyor, FTP dosya paylaşım için kullanılan protokol, ftp…. Başa yazılarak kullanılır.

Burada katmanlardan kısaca bahsettik şimdi protokollerden bahsedelim ama hepsinden tabi ki bahsedemeyiz, belli başlı karşınıza çıkacak protokollerden bahsedeceğiz. Burada bilinmesi gereken şey şu, her amaç için bir protokol var. Dosya mı göndereceksiniz onun ayrı bir protokolü var, e-mail mi göndereceksiniz, müzik mi, video mu hepsinin ayrı protokolü var.

AWS de firewall ayarları yapacaksınız sanal makineye bağlanırken o sanal makine üzerinde bazı protokolleri, portları açıp kapayacaksınız. Hangi portları (protokolleri) açmanız gerektiğini buradan bileceksiniz. Bir web uygulamasını çalıştıracaksanız bu sanal makinede bu makinenin http protokolünün ilgili portunu da açmanız gerekecek.

Transport Layer Protokol (3. Katman)

En önemli protokollerden biri, Kernel seviyesinde bir katman.

Burada belli başlı iki tane protokol var TCP ve UDP.

Yukarda appilication da hazırlanan tüm paketler hangi protokolü kullanırsa kullansın mutlaka TCP ve UDP protokolü kullanılarak karşı tarafa gönderilir.

TCP full-duplex bir protokol, aynı anda iki tarafa birden gönderme ve alma yapabiliyor.

Connection-oriented, gönderme yapmadan önce mutlaka bağlantı yapmak gerekiyor.

Reliable karşıdan hazırım mesajı almadan paketi göndermiyor.

accurut, (kesin) karşı taraf paketi almadığı sürece göndermeye devam ediyor. Böylece tüm paketlerin iletildiğinden emin olan bir protokol.

TCP yi cep telefonu araması gibi düşünebilirsiniz. Karşı taraf açana kadar siz konuşmuyorsunuz, sonra karşı traf açıyor ama sizin konuşmak istediğiniz kişi mi diye soruyoruz sonra konuşuyoruz.

Tcp de böyle karşı taraf cevap veriyor, kimliğini doğruluyor ondan sonra paketleri göndermeye başlıyoruz. Ve her paketten sonra karşı taraf tamam paketini aldım diyor ondan sonra yenisini gönderiyoruz. Bu sayede TCP protokolü güvenilir bir protokol göndermek istediğimiz paketlerin hepsinin karşıya gittiğinden emin olabiliriz.

Hatırlayın frame lerin boyutu 1,5 kb onun içine giren dataların boyutu daha az, biz çok basit bir dosya gönderirken bile binlerce frame hazırlayıp öyle gönderiyoruz. Bu frame lerin bazıları kaybolabilir ve bu çok sık karşılaşılan bir durum, siz tüm paketlerin karşı tarafa gittiğinde emin olmak istiyorsanız tcp protokolünü kullanacaksınız.

\*\*\*Belli başlı protokollerin bu tcp mi udp mi kullanacağı baştan bellidir.

Tcp aynı cep telefonu gibi connection-oriented bir protokol.

Tcp aynı OSI modeldeki gibi segmentlere ayırıyor paketi (datagram).

Tcp binlerce paketi sırayla gönderiyor, 1000 tane paket gönderiyor ve her birisi için ben bu paketi aldım cevabını bekliyor. Bu tcp nin yavaş olmasına neden oluyor. Her paketi bekliyor ve her paket sonunda bir egnoliçd , alındı bilgisi bekliyor.

UDP

Şimdi tcp güvenli bir protokol, güvenli derken verinin karşıya tam olarak gittiğini ve sırayla gittiğini biliyoruz. Bu aslında bizi yavaşlatan bir protokol.

Öyle oluyor ki bazı paketler karşı tarafta kaybolsa bile önemsemeyiz, hız daha önemlidir bizim için. Mesela şu an zoom yapıyoruz…

Şu an tcp üzerinden zoom ile görüşseydik sesler bile kesik kesik olacak ….

Udp nin de tabi hızı var ama bazı eksikleri var,

* udp tcp den hızlı olmasının sebebi nedir, tcp nin üçte biri kadar bant genişliği kullanıyor, tcp de paket boyutu udp nin neredeyse 3 katı.

daha hızlı bir protokol çünkü paket boyutu daha küçük

* sırayı önemsemiyor, herhangi bir sırayla gönderiyor. Zoom da oluyor bazen önce ses gelmiyor ama daha sonra hızlı çekimle konuşuyor gibi olur. Udp her ne kadar sırasız gönderse de karşı taraf bunu bir sıraya koyar.
* Udp karşı taraf paketi alıp almadığıyla ilgilenmez, elindeki tüm paketleri bir anda gönderir. Karşı taraf hazır mı bununla bile ilgilenmez (mektup gibi) connections değil

TCP bant genişliği, ağ bağlantısının veya iletişim kanalının ne kadar hızlı veri iletebileceğini belirler. Daha geniş bant genişliği, daha fazla veri iletim hızı anlamına gelirken, daha dar bant genişliği ise daha yavaş veri iletimine neden olabilir. Bu nedenle, TCP bant genişliği, ağ performansını etkileyen önemli bir faktördür. Çoğu zaman, kullanıcılar daha hızlı veri iletimi için daha geniş bant genişliği talep ederler.



\*\*\*\*\*Çizim yapalım

Karşılaştıralım (udp ve tcp)

Tcp udp

Secure

Bağlantı bekler siz talebi yaptıktan sonra…….

Yavaştır

Her paketten sonra ulaştı mesajı

Paketler sırayla gider

Karşıya iletildiğinden emindir

Sanal bir tünel oluşur ve tüm paketler o tüneli izler

Alındı bilgisi bekleniyor

Header 20 byte UDP 8 BYTE

2. katman

İnternet Layer Protokol

Şimdi bu protokol ve portlardan bahsedelim.

Buradaki esas protokol ip, arp, ıcmp.

İP

İp nin ne olduğunu biliyoruz, ama ip nin tam olarak ne olduğunu bir sonraki derste öğreneceğiz.

İp adresi internet üzerinden routerlerin paketleri alıcılarına ulaştırabildiği bir sistem. İnternet üzerinde ağa bağlanan herhangi bir node, mutlaka ve mutlaka bir ip adresine sahip olmalı ve bu ip adresi uniq olmalı. Local ağlar için private, internete çıktığınız public adresi ikisi de mutlaka uniq olacak. Olmazsa çakışma olur. Bu adresleri kim sağlıyordu, IANA dediğimiz bir kuruluş sağlıyordu.

Şimdi internette önce bir paketi birisine göndermek için şunları bilmemiz lazım, öncelikle karşıdaki alıcının hangi network de olduğunu bilmek lazım ve onun id sini bilmeniz lazım. Çünkü o network de 10 larca yüzlerce host olabilir, pc olabilir. Hem hangi network hem de id sini bilmem lazım. Network kısmı software adres veya diğer adıyla logical adres veya ip adres orada saklı, is si de mac adres ve ip adres içerisinde saklı.

İp adresi iki kısımdır, biri network id networkü tanımlar, ikinci kısmı da o network içerisindeki hostu tanımlar. Dolayısıyla bir bilgisayarın hem mac adresi hem de ip adresinin olmasının gerekçesi bu (daha sonra bunu daha iyi anlayacaksınız)

ICMP (internet control message protokol)

İnternet üzerinde cihazların birbiriyle haberleşmesini sağlayan protokol. Yani siz şimdi bir server a bağlanmaya çalışıyorsunuz server down olmuş, normalde ICMP protokolü olmazsa hiçbirimizin server in down olmasından haberimiz olamaz, bağlanmaya çalışırız sayfa açılmaz. Ama bu ICMP sayesinde biz server a gidiyoruz server diyor ki şu an ben off line ım veya server tamamen cevap veremeyecek durumda server ın önündeki router cevap veriyor, ben server a şu an ulaşamıyorum, server erişilmez durumda diye bize bir ICMP hata mesajı gönderiyor. Ben bu mesajı açarak hatamın ne olduğunu biliyorum ve ona göre hareket ediyorum.

Hatalar ne olabilir,

Destineşin anriçıbıl, aradığınız server a ulaşılamıyor. Bunun sebebi ya server down olmuştur ya da server ın içindeki web stesi down olmuştur. Web sitesinde bakım vardır bu yüzden bağlanamıyorsunuzdur. Burada işte browser de http kodları alıyorsunuz ya 404 sayfa bulunamadı, 500 de sunucu tarafındaki yazılım hatasında verir gibi. İşte o kodları bu ıcmp sayesinde çözüyoruz.

Aynı şekilde internet üzerindeki routerler birbirleriyle bu şekilde haberleşiyorlar.

Ping ve traceroute bir iki tane tool (commend line tool) var bunlar ıcmp protokolünü kullanıyor.

Ping neydi karşıdaki server ayakta mı cevap verip vermiyor mu bunu görüyoruz.

ping google.com

tracert google.com

Cevabını nasıl alıyoruz bize bir ıcmp paketi gönderiyor karşı taraf, ben de ping ile bir ıcmp paketi gönderiyorum o da bana durumunu ıcmp paketiyle gönderiyor.

Olmayan bir adresi atarsam bana time out cevabını gönderecektir.

Cihazların birbirleriyle durumlarını paylaştığı, birbirlerine durumlarını raporladığı protokol olduğunu bilin, giden gelen paketlerin yolda başına bir şey gelirse yine ıcmp ile geri bildirimde bulunuyor. (ciber ve aws için mülakatta sorabilir)

ARP (adress resulation protokol)

Bu arka tarafta gerçekleşen bir protokol, (arp -a)

Ne demiştik her bilgisayarın bir mac adresi bir de ip adresi var. Ben biriyle haberleşmek, istiyorsam onunla eğer aynı ağdaysam ip adresine gerek yok mac adresimi kullanırım paketimi gönderirim.

Ama farklı network deysem onun mutlaka ip adresini bilmem lazım.

Bu zorunluluktan dolayı cihazlar kendi bünyelerinde bir arp tablosu tutarlar, burada ağa bağlı her cihazın ip adresi ve mac adresleri bulunuyor.

Peki bu arp tabloları nasıl oluşturuluyor, hani broadcast mesajları demiştik ya işte biz ip adresi bilip mac adresi bilmezsek bir FFFFFF mesajı ile ip yi gönderiyoruz kimin ise o cevap veriyor ve bu tablo doluyor.

Arka planda işletim sistemi bu broadcast mesajlarıyla arp protokolü kullanarak bu tabloyu sürekli güncel tutar.

RARP ( reverse arp---- arp ın tersi)

Ben mac adresi biliyorum diyelim, ama bana bir ip adresi daha atanmadı ya da haberi yok burada benim ip mi bilen bana cevap versin diyorum ve bir bilgisayar (bu genellikle DHCP server oluyor, o atıyor ip adreslerini) cevap veriyor ve bildiriyor ip adresini. .8 broadcast mesajıyla)

Gelelim en üst katmandaki protokollere;

Burada her amaç için bir protokol olduğu için ve her protokolün bir port numarası kullandığını bahsetmiştik.

FTP, dosya transferi için kullanılan bir protokoldür. FTP serverlar vardır, o ftp server lara ftp protokolü üzerinden bağlanılır.

ftp bir tool, ftp ye bağlandıktan sonra buraya bağlanacağınız server ın adresini yazarsınız.

User da iken ftp [ftp.gunu.com](ftp://ftp.gunu.com) şifresi Anonymous

Buradakileri read only olduğu için değiştiremem ama bilgisayarıma indirebilirim.

Genelde ne işe yarar büyük firmalarda bir ftp sunucu kurarsınız, çok sık kullanılan klasörleri ve uygulamaları buraya kopyalarsınız. İnsanlar buraya bağlanıp buradan alırlar.

İşte bu FTP protokolünü kullanıyor.

Bunları bilmenize gerek yok.

Bu protokolün 3 tane tipi var

* Bir tanesi FTPS secur bir protokol TCP
* TFTP bu biraz daha light bir protokol hız önemli burada biraz, ftp de olan tüm komutlar burada çalışmaz. Burada dosya gönderme alma işlemleri yapılabiliyor. UDP
* SFTP bu da secure ama buradaki secure Shell işlemi kullanılıyor, ssh ile bağlanılıyor. TCP

Bunların kullndığı portlar var, hangisi karşınıza çıkar bunlardan bahsedeceğiz, hepsini bilmenize gerek yok (zaten Google dan aradığınızda hepsi çıkar karşınıza)

SSH protokol

Bu en çok kullanılacak protokol. Uzaktaki sanal makinalara bağlanıp o makinaların ayarlamaları yapılıyor. Dosya kurulumu, ayarların kurulumu, sistemin güncellenmesi gibi işlemleri yapılır. Bunun için de SSH protokolü kullanılıyor. SSH protokolü TCP kullanıyor ve port 22 den bağlanılıyor.

SSH secure bir protokol, bütün cominication criptolanıyor öyle gönderiliyor.

TELNET, SSH dan önce TELNET vardı, aynı mantıkla ama telnet güvenli bir protokol değil, tüm bilgiler clear text olarak karşı tarafa iletiliyor buna şifre bilgileri de dahil.

RDP, remote desktop protokol bu Microsoft un geliştirmiş olduğu bir protokol. SSH ile terminal üzerinden bağlanıyorsunuz, grafiksel arayüzden bağlanmayı sağlar, karşı tarafın desktop unu görerek kullanıyorsunuz.

Port numaraları neden önemli;

Şimdi bilgisayarlarda 2 üzeri 16 tane port vardır. Yani 65 535 tane. Her uygulama farklı bir portu kullanarak haberleşmek için internete çıkar.

Kaynak izleyicisi ( resource monitör) task manager den den bakalım bilgisayarımızın

İşletim sistemi hangi paketin hangi uygulamaya ait olduğunu port numaralarından ayırt ediyor.

Reselve portlar var kimse bunları kullanamaz ( ssh ve http gibi , değiştirilemez)

Velnome portlar, bazı kullanılmayan portları mesela watshap ın kullandığı portlar eğer o anda kullanılmıyor ise bilgisayar tarafından siz istediğinizde kullanabilirsiniz.

Bir de sizin uygulamalarınız için seçecek olduğunuz port numaralarıdır. Bu da genellikle 32000 ve üstü port numaraları kullanabilirsiniz. Normalde siz port listesine baktığınız zaman 65535 portun 55000 tanesi zaten başka uygulamalar için kullanılıyor. Ama bunlardan velnome portlar eğer bilgisayarınızda o uygulama yoksa bir sıkıntı olmaz, çakışma olmaz. Ama reselve portları kesinlikle kullanamazsınız işletim sistemi kesinlikle buna izin vermez. Genelde de 32 000 üzeri bir port numarası verirseniz bir problemle karşılaşmazsınız.

http ve HTTPS

Biz internete secure olarak bağlanıyoruz. 74

http de web sitelerine bağlanmak için kullandığımız bir protokol. 80, reselvedir.

https secure versiyonu. Certifica verilir. Google aradımdaki tüm trafiği criptolamış oluyorum.

Günümüzde şuan SSL fazla kullanılmıyor, TLS sertifikası kullanılıyor, transport layer securty. TCP modelde bir katman. Alttan 3. Katmanda haberleşmeyi kriptolamaya yarayan bir katman bu.

Port 443 , reselve dir.

Email protokolleri

POP u duymuşsunuzdur belki. E mail serverlara bağlanacağınız zaman bu protokolü kullanırsınız. Güncel versiyonu POP3.

IMAP, bu da bir e mail protokolü ama çalışmaları biraz daha farklı. Birisinde servera bağlanıp orada ilgili mailleri indiriyorsunuz, diğerinde tüm mailleri indiriyorsunuz. Buralar çok detay ayrıntıya gerek yok.

Burada önemli olan email için farklı protokoller kullanıldığı.

Multimedia Protokol

İsimlerinin açıklamalarını okuyalım.

H323---4 , internet üzerinden ses dosyası ve video izlerken bu protokol kullanılıyor.

Diğerleri, zoom gibi veya VoIP gibi protokoller maltimedia konferanslarda kullanılan protokoller.

(Google dan bakılabilir)

Utility Protokol

SNMP, bu network hakkında bilgi toplamak için (siber ve network adminler kullanılır). Daha çok network üzerindeki veri trafiğini kontrol etmek için, cihazların durumunu sorgulamak için kullanılan bir protokol.

NTP, internete bağlanan tüm cihazların saat senkronizasyonunun aynı olması lazım. Cep telefonları da aynı şekilde. Bu nasıl sağlanıyor, internet üzerinde saat senkronizasyonu için kullanılan yüzlerce server var, bu serverlara NTP protokolü üzerinden bağlanıp cihazlarınızın saatini senkronize ediyorsunuz. Bunu siz değil arka planda işletim sistemi otomatik yapıyor.

DHCP

Bu çok önemli bir protokol, hani demiştik ya bir ağda ip adresinin uniq olması önemli. Şimdi internet üzerinde network id lerini dağıtan bir firma var, IANA. Bu tüm dünyada network id lerin uniq olmasını sağlıyor. Peki local ağlarda hostların farklı id olmasını nasıl sağlıyoruz.

Her ağda bir tane server vardır. DHCP. Bu ağa bağlanan her cihaza bir ip adresi tahsis eder. Evlerimizdeki bu cihaz hangisi, bizim wifi router imiz aynı zamanda bizim DHCP serverımızdır. İşte bu server DHCP protokolünü kullanarak ip adresinin tahsisini yapar.

LDAP (TCP 389)

Microsoftun geliştirdiği bir protokol. Belli başlı standart ayarları, folderları ortak bir yere koyup internet üzerinde tüm bilgisayarların buraya bağlanıp ayarları ve dosyaları çekmesini sağlar, ağa bir bilgisayar bağlandığında o bilgisayarın hangi ayarları kurulacak bu LDAP teki ayar dosyalarını otomatikmen çekiyor o ayarları uyguluyor. Onları çekip bilgisayara yüklüyor.

Otomatik kombinasyonlar için kullanılan bir protokol.

Encription protokol

Az önce bahsettiğimiz TLS, SSL. SSl eski bir protokol, TLS yeni version. Bu bir sertifika. Burada gördüğünüz kilit işareti ( browser da). Bu sertifika dediğimiz şey aslında bir criptolama algoritması (anahtarı).

Bir siteye girişte kullanıcı adı ve şifre bilgisi girerken bunların kriptolayarak gitmesini sağlama için bu tarz sertifikalar kullanıyoruz. Bu sertifikaların kullanıldığı protokollere de SSL ve TLS diyoruz.

\*\*\*

Her uygulama için kullanılan ayrı ayrı kullanılan protokoller var, her protokolün bir portu var. Buradakiler en çok karşınıza çıkacak olanlar.

Googlden aratalım

Tcp protocol

Tcp udp port numaraları

\*\*\*

IP ADRESİ

İp adresinin ne olduğunu biliyorsunuz aslında ama ip adresi düşündüğünüzden çok karışık bir konu.

İp adresi decimal olarak gösterilir, ve her byte ına octed deniyor, soldan sağa 1. , 2. Octed gibi.

İp adresi iki kısımdan oluşur demiştik, önceki bir kısmı network id yi verir, o network içerisindeki tüm hostlar bu numaralar ile başlar. Geri kalan kısmı da host id dir., o ağ içerisindeki tüm hostlar her biri uniq olmak üzere bu sıradaki numaralardan birer tane alırlar.

Broadcast adres, tüm herkese gönderilen, local de nasıl ihtiyaç duyuyorsak, ihtiyaç layer 3 de de ip adreslerine de biz broadcast mesajlarına ihtiyaç duyuyoruz.

Şimdi ip adresleri sıralı gitmiyor, bir hiyerarşik yapısı var (sistematik).

İp dediğimiz zaman ip v 4 den bahsediyoruz demektir.

İp 32 bit, 4 byte, 4 octed.

Onluk, binary ve hexedecimal olarak gösterilebilir.

İp flat değil ( 00001, 00002, 00003 diye gitmiyor.), hiyerarşik bir yapısı var. Nasıl bir hiyerarşi var bahsedeceğiz.

Network id ---- ilk kısımda yer alan octed

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

Açıklama otomatik olarak oluşturuldu

Evdeki bilgisayarlarımızın network id sine bakalım. Her cihazımızın ki aynı gelir.

Peki hangi kısım bize network id hangi kısım bize host id yi veriyor, işte bu kısım bize hiyerarşik yapıyı geliyor.

İp adresi 5 clas tan oluşuyor.

D ve E bizi ilgilendirmiyor ( kısaca bahsedeceğim)

Peki bunların farkı ne;

A, B ve C nin yapısına bakalım.

Class A ip adresi;

Bir ip adresi 0 ile 127 arasında bir değer ile başlıyorsa bu class A bir ip adresidir.

0 ve 127 reserve adreslerdir. Bunu hiçbir networke veremezsiniz. ( AWS için çok önemli)

127.0.0.1 local host tur, bu özel bir adres, internette sitemiz nasıl gözükür buradan bakıyoruz ( internet üzerinden trafik oluşturmadan testlerinizi yapabiliyorsunuz). Bu numaraları kimseye veremezler reserve bir adrestir.

İlk biti sabit olduğu için 7 biti değiştirebilirim. Bu da 2 üzeri 7 den 128 farklı adres eder. Yani siz dünya üzerinde sadece 128 farklı class A network oluşturabilirsiniz. ( LAN ağı düşünelim)

Peki her bir network içerisine kaç tane host koyabilirsiniz, 2 üzeri 24 den, 16 milyondan biraz fazla host sığdırabilirsiniz.

Günümüzde hangi ağda bu kadar bilgisayar var. Çok fazla ip adresi israf oluyor, büyük firmalar bu adresleri aldılar.

Class B;

10 ile başlar, bu rakamlar ile oluşturulabilecek max değer 128 ile 191 arasındaki değerlerdir. Bu numaraları görünce bu class olduğunu bileceksiniz.

İlk iki biti sabit olduğu için 2 üzeri 14 den dünya üzerinde 16 bin class B network oluşturabiliriz.

Her bir network içerisine de 2 üzeri 16 dan 65 bin üzerinde host tanımlayabilirsiniz, daha fazla tanımlayamazsınız.

Class C;

İlk 3 bit sabittir. 192 ile 223 arasında değerlerei alan ip adresleridir. İlk 3 octed networkü gösterir.

2 üzeri 21 network

2 üzeri 8 host

Her iş yeri kendine göre ip ağı alıyor.

Class D ve Class E;

Class E zaten IANA tarafından deneysel amaçlar için kullanılan bir ip adresi, bunu hiçbir yerde göremezsiniz.

Class D de, abonalik sistemi üzerine çalışan bir multicast adres. Mesela Netflix gibi abonelik servisi veren firmalar tarafından kullanılıyor, bireysel kullanımlara açık değil. Global olarak kullanabilmek için IANA den ayrıca onay almanız gerekiyor.

Bu çok karşınıza çıkmaz ama

224 - 239 a kadar class D

240 – 255 e kadar class E olarak geçiyor. Bunları bilmenize gerek yok.

\*\*\*

Özet olarak biz A, B, C ye tekrar bakalım.

A 1-127 ilk biti 0 NHHH ……

B 128-191

C 192-223

32 bit var ve 2 üzeri 32 den toplam 4 milyar ip adresi demek, peki bu yeterli mi Dünya üzerindeki cihazlar için (fırın, buzdolabı, süpürge).

İsraf olan bir sürü ip lerde var.

Bu sıkıtıyı gören mühendisler buna bir çözüm arayışına girmişler.

Dünya üzerindeki network id sayıları yetiyor aslında ama her bir host için yeterli ip adresi yok.

Onlarda demişler ki bu 32 bit in bir kısmını ayıralım bunada private ip adresi diyelim. Bu adresleri local ağlar içerisinde kullanalım. Local ağlar birbirinden bağımsız olduğu için bir çakışma olmaz.

Bir kısmı bu şekilde private yapalım geri kalanı da public yapalım demişler.

İnternete çıkıyorsak mutlaka bir public ip ye bağlanmalıyım. Bir ip ile tüm cihazlarımla internete çıkış yapabiliyorum. Böylece ne oluyor ip adreslerini biraz daha iktisatlı kullanmış oluyoruz.

Peki bu private adresler hangileri;

A, B ve C deki bazı bloklar ip adresi olarak atanmıştır. Bunları public ip adresi olarak kullanamazsınız, router bu adresleri gördüğü zaman bunları drop eder, internete çıkarmaz bile.

Bunları sadece local ağlar içerisinde kullanabilirsiniz.

Router aynı zamanda DHCP server da olduğu için zaten ip adreslerini kendisi dağıtıyor onun için ilk private ip adresini router kendisine alır ( 192.168.1.1)

Peki benim evimde 10 tane cihaz var hepsi aynı public ip adresiyle nasıl çıkıyor.

Nat denilen mantık var burada, (mühendisler oturmuşlar bunu da çözmüşler), Nat Network adress translation.

Bu ne iş yapıyor,

Evimizdeki wifi router hem bir router hem bir DHCP server hem de bir Nat server. 3 ana fonksiyonu var.

Nat translate işlemi yapıyor, public i private ye, private yi de public e çeviriyor.

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

Açıklama otomatik olarak oluşturuldu

Her cihaz aynı anda internete bağlanmak isterse ne olacak, ayrı ayrı mı public alacaklar. Bu nat sistemi de yeterli gelmeyecek.

ISP firmalarında yeterince public adresi yok, public adreslerinin çoğunluğu amazon un elinde, sanal makinalar için.

Nat ın nasıl çalıştığına bakalım, birkaç tane nat çeşidi var, bizi ilgilendiren ve günümüzde en çok kullanılan nat çeşidi PAT diye geçen sistem.

Az önce dedik ya evimizde bir sürü cihaz var ve aynı anda hepsi internete bağlanmak isterse ne olacak, hepsi public ip adresine ihtiyaç duyacak. Nat için ISP nin elinde o kadar public ip adresi yok. Düşünün ISP nin 1 milyon kullanıcısı var her evde 5 cihaz olsa bu 5 milyon public ip adresi eder, bu da mümkün değil.

Burada işlem nasıl çalışıyor, cihazlar public ip ile çıkmak isteyince hepsine aynı ip yi verip sonuna bir port numarası ekliyor, private ip de ekliyor bunu aynısını gelip public ip de de ekliyor ve bunu nat a kaydediyor.

Buradaki port numaralarıyla protokollerdeki port numaraları ile tamamen farklı, karıştırmayalım. Burada da 2 üzeri 16 tane port numarası var. Nat bu taleplere göre birer port numarası vererek aynı ip adresini kullanarak tüm cihazların internete çıkış yapmasını sağlıyor.

Bunun avantajı da çok bariz, tek bir ip adresi ile sayısız cihazı internete bağlayabiliyorsunuz.

İp adresi yetmediği için bu çözümler geliştirilmiş.

Bunun avantajı ne, local ağın ip yapısını gizliyorsunuz dışardan birisi bilgisayarların ip adreslerini gözlemleyemiyor, anlayamıyor, çözemiyor. Sibercilerin zorlanacağı bir durum. Bu güvenlik anlamında bir artı.

Eksisi ne, legal durumlarda, mesela bir cihazdan yasa dışı bir talep gitti, o cihazı tespit etmek biraz daha zor. Burada bütün senkronizasyonu sağlamak için bu ağdaki tüm cihazların modemin, ISP nin ve santralin hepsinin aynı saati kullanması lazım. Çünkü bir milisaniyede onlarca talep oluyor. Hepsinin saati denk olursa ancak bir ilişki kurabilirsiniz. Ancak saatte bir farklılık varsa burada kimlik tespiti çok zor oluyor.

O yüzden NAT lardan ip adresi tespit edip birini zan altında bırakmak kesin olmadığı için doğru bir hareket olmaz. Ki günümüzde herkes nat kullanıyor. Bir de benim routerimde Nat var ama ISP de de Nat var ve ben oraya gidip oradan internete çıkıyorum. Üç ISP den geçeceksem 3 ayrı nattan geçmiş olacağım. Dolayısıyla kimlik tespiti çok zor. Ve doğruya yakın bir bilgi için de bütün bu nat cihazlarının ve bilgisayarın saatlerinin ayarının tam olması lazım, başka türlü kimlik tespiti çok zor.

Layer 2 broadcast

Layer 2 de ne vardı, siz tüm ağdaki bilgisayarlara bir mesaj gönderecekseniz frame de alıcı mac adresine şunu ( FF:FF:FF:FF:FF:FF) yazdığınız zaman swich bu adresi görünce diyor ki tamam bu mesajı tüm ağdaki herkese göndereceğim diyor ve gönderiyor.

Layer 3 de de broadcast var, broadcast ler internetin ve ağların vazgeçilmezi.

Broadcast mesajları nasıl oluyor. Bir ağ içerisinde bir broadcast adresi mutlaka vardır.

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

Açıklama otomatik olarak oluşturuldu

Host için ayrılan bitlerin tamamını turn on yaparsanız, hani iki tane adresi hiç kimseye veremezsiniz demiştik ya bunlar reserve adresti.

Host bitlerin tamamını torn off yaptınız ya da torn on yaptınız bunlar reserve adrestir. Turn on yaptığınız adreslerde broadcast adrestir.

Mesela benim ağımda;

İpconfig/all

Benim ağımda ip adresim class C, ilk iki octedim network iidyi, diğerleri host idyi gösterir. Network id değişmez.

Yani ben bir paket hazırladığımda alıcı kısmına adresi ( 192.168.255.255) yazarsam, router bunun bir broadcast mesajı olduğunu anlayacak çünkü tüm host bitlerini turn on yapmışım 255 olmuş. Bunun broadcast adresi olduğunu anlayıp ağdaki tüm cihazlara gönderecek.

Broadcast ler ağın vazgeçilmez unsurlarından biri, bundan kaçış yok. Ağın performansını düşürse de şu an günümüz network teknolojisi bunun üzerine kurulmuş.

İPv6 de bu kısmen giderilmiş.

Burada bilmeniz gereken bu, sonu 255 le biten (host kısmın) broadcast adresidir.

Nerede kullanıyoruz, ARP ve DHCP protokolde kullanıyoruz.

Unicast Adres, Aynı mac adreslerinde olduğu gibi tek bir alıcısı olan adres.

Multicast de var da burada değinmeye gerek yok, multicast ne idi sadece abonelere gider.

\*\*\*\*

IPv6 adres

İpv6 e neden ihtiyaç duyduğumuzu anlamışsınızdır.

2010 Kasım itibariyle İPv4 adreslerinin doluluk oranı. Peki nasıl oldu da bitti bu kadar ip adresi bu kısa sürede.

İPv4 de demiştik, Dünya üzerinde 4 milyardan biraz fazla ip adresi üretebiliyoruz 32 bitle ama bunların hepsi kullanılabilir değil.

Class A dan kaç tane network üretebiliyorduk 126 tane. Host olarak 16 milyon tane üretebiliyoruz ama siz bir ip alırken host olarak almazsınız, network id olarak satın alırsınız. Ben şimdi IANA ye gitsem bana bir class C ip adresi ver dedim, IANA bana şunu verir;

200.28.14.0

Buradaki class C olduğu için ilk 3 octed i değiştiremem, geri kalan bir octedi kafama göre verebilirim.

Büyük firmalar bu ilk çıktığında class A aldığı için onlarda bir çok host için adres çöp olmuş oldu.

Bu adreslerin yetmeyeceğini öngördüler ve yeni bir IPv yapısına geçtiler. IPv5 bu deneysel aşamada kaldı, kullanıma girmedi IPv6 e geçtiler ama IPv6 e geçiş, bir ip adresi sistemini değiştirmek uzun yani maliyet ve zaman isteyen bir şey. Bütün cihazları, işletim sistemlerini, yazılımları, routerleri buna göre güncellemeniz, yenilemeniz lazım. Hatta bazı elektronik cihazları komple değiştirmeniz lazım.

Bunlar çok büyük maliyet olduğu için IPv6 ya geçiş çok yavaş. Bu sürede de internetten yoksun kalmamak için IPv4 ü biraz daha uzatmak için çeşitli yöntemler geliştirmişler, birisi işte bu public ve private ip adresi ayrımı. Diğer ayrım subneting kısmı onu AWS e devam edecek arkadaşlar görecek.

Peki IPv6 nasıl bir ip adresi;

IPv4 ün tam 4 katı, 128 bit uzunluğunda toplam bu kadar sayıda farklı ip adresi oluşturabiliyorsunuz. Tüm bu sayı emin olun tüm galaksiye yetecek sayı. Yani okumak isterseniz şu şekilde okumanız lazım(slayttaki gibi)

Dolayısıyla IPv6 ip adresinin yetmeme ihtimalini ortadan kaldırdı. Şu an ben 1 milyon tane ip adresi alsam yine tüm Dünyaya yeter. Dünyada 7 milyar tane insan olduğunu düşünün , herkes 1 milyon tan ip adresi alsa bu sayının 10 da birine bile yetişmiyor.

Peki sadece ip adresinin sayısı mı artmış, belli başlı geliştirmelerde yapmışlar.

* Routing daha efektif daha hızlı
* Paket headerler biraz daha sadeleştirildiği için daha hızlı.
* Broadcast artık IPv6 de yok, broadcast a yakın anicast denen bir consept var. (anicast te sadece komşulara yayın yapıyorsunuz, bu routerler tarafından kullanılan bir adres çeşidi.
* Network kombinasyonu daha sadeleşti, çünkü artık private ip ve public ip ye gerek yok, bunlara gerek olmadığı için NAT a da gerek yok.
* İp security kısmını doğrudan inclement ettiği (sert) için daha güvenli, paketler daha güvenli.

Herkese IPv6 statik ip adresi verilebilir .

IPv6 2000 lerin sonunda nihayete erdi ve 2003 veya 2006 yıllarında kullanılmaya başlandı. Ama ne kadarı geçti bu sisteme derseniz % 35-40 civarlarında. Geçiş yavaş oluyor çünkü biraz masraflı.

IPv4 10 sistemde gösterilir ve 4 octeddir

IPv6 16 lık sistemde göst ve 8 hexdect den oluşur

IPv4 ip adresini doğrudan bilgisayarınıza yazıp kullanabilirsiniz ama IPv6 yı kullanamazsınız ( köşeli parantezle yazmanız lazım)

Bazı kısaltmalar yapıyorsunuz, bunlar çok önemli değil;

* Arka arkaya gelen sıfırları atabiliyorsunuz, ama bunu bir kez yapabiliyorsunuz. İki kere yaparsanız karışır nerede kaç tane sıfır yazacağınız.
* Baştaki sıfırları atabiliyorsunuz, 0001 1 yapmak gibi.

Unicast adres

Multicast

Anycast

IPv6 da reserve problem olmadığı için burada bir sürü adres reserve edilmiş.

Burada bilmeniz gereken husus local hostun adresi, 0:0:0:0:0:0:0:1 dir.

Şu an günümüzde hem IPv6 ve IPv4 kullanıyorsak bu nasıl oluyor,

Benim bilgisayarımda ikisi de var ama bazılarında IPv6 olmayacak. Bende IPv4 var ve karşıdaki de IPv6 kullanıyor. Bu geçiş tamamlanana kadar birkaç tane algoritma var; Dual stacking ve 6to4 tunelling diye iki tane algoritma var. Bu algoritmalar sayesinde IPv4 ve IPv6 nın arasındaki iletişim sağlanabiliyor.

KAHOOT (IP & IP adresing)

1. TCP/IP modelde kaç tane layer var
2. Hangi sistemle private networkten public ip ye bağlanı yapabiliyoruz
3. Kullanıcılara hizmet sunan layer hangisiydi
4. TCP protokolü neden relayble bir protokol, verinin sağlam bir şekilde karşıya ulaştığını teyit etmek için hangi sistemi kullanıyor. Acnolic gelmezse göndermiyor paketi
5. TCP de ilk cominicationu başlatmak için sistemin adı nedir (three-way handcheking)

3 aşamalı işleme deniyor.

1. Aşağıdakilerden hangisi UDP için yanlış bir seçenek
2. Aşağıdakilerden hangisi bir appilication protokol değildir
3. Arp ın birinci amacı ne, ne amaçla kullanılıyor.
4. İpv6 adresinin boyutu ne kadar 128 bit
5. Clas A adresinin bloku hangisi
6. En çok kulllanılan NAT türü
7. Hangi cihaz nat işlemini yapar
8. IPv4 den IPv6 ya geçmemizin amacı nedir