



Network

Veri aktarımı olan her bağlantı bir network oluşturur.

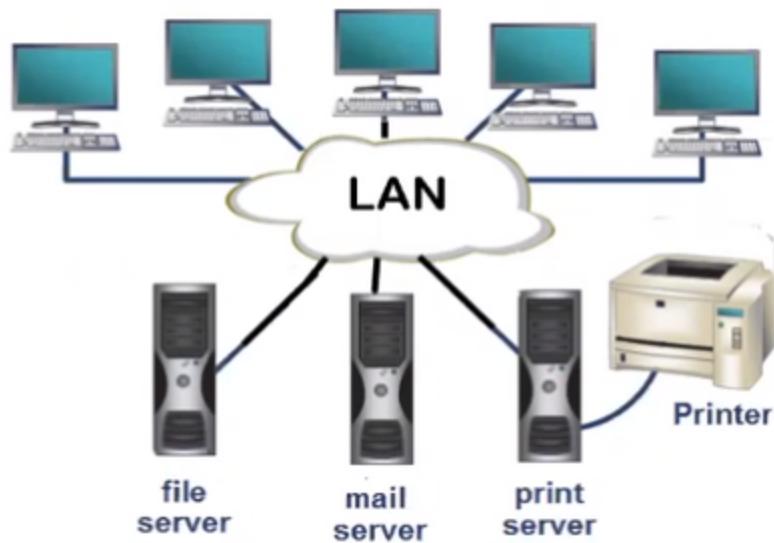
Networklerin Özellikleri

- Performance (Response Time) Verinin gidiş geliş süresine RRT (Round Trip Time) denir ve yüksek olmasını isteriz
- Data Sharing Dosya paylaşımına uygun olması
- Backup Yedeklenebilirlik
- Reliability Sürekli aktif olmalı (Mümkün olduğunda)
- Security
- Scalability Ölçeklenebilirlik. İstenildiği zaman sisteme yeni cihaz ekleyip çıkarmak. Evdeki modem çok rahat bir şekilde cihaz eklenebiliyor.
- Software and hardware compatibility: Farklı cihazlarla uyumluluk

LAN (Local Area Network)

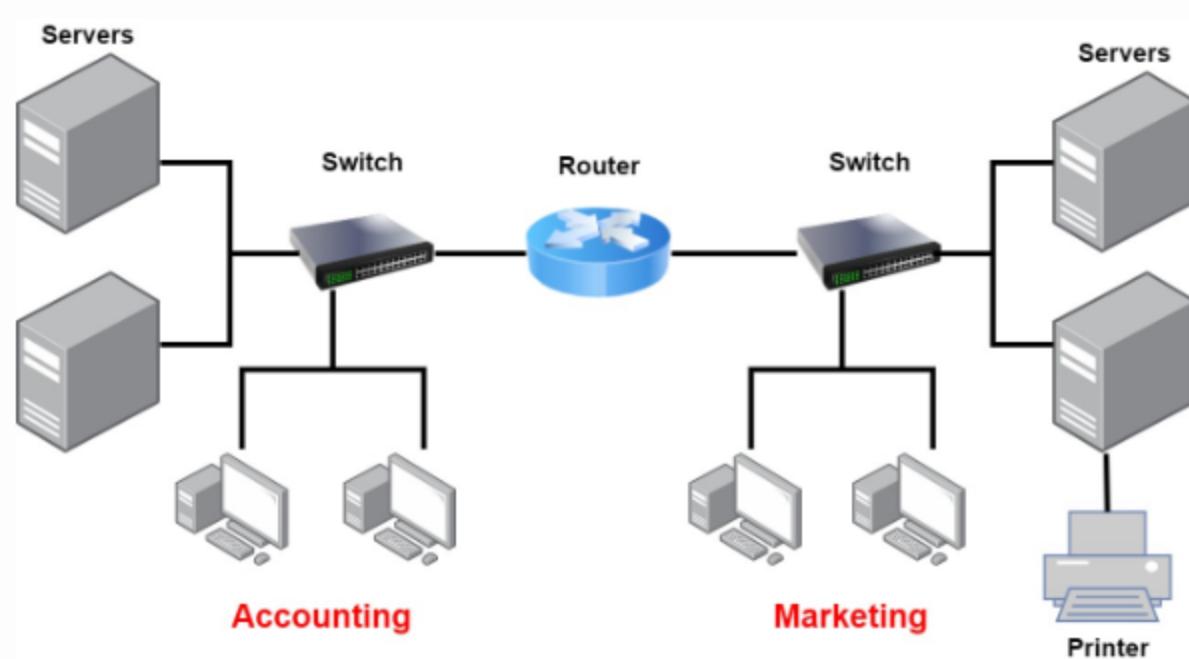
Bir router'a (gateway) bağlı cihazlardan oluşan sisteme LAN denir. LAN'daki hiç bir cihaz tek başına internete bağlanamaz. Bu işlem için router yani Wi-Fi lere ihtiyaçları var.

2 bilgisayardan oluşan bir LAN'da olabilir. Yüzlerce bilgisayardan oluşan tek bir LAN'da olabilir. Ancak çok makinalı LAN mantıklı değil. Küçük LAN'lara bölerek yönetmek daha kolay



Şehirler arası/Ülkeler arası da LAN'lar kurulabilir ancak mantıklı değil.

LAN'lar tek başına bir biri ile bağlanamazlar. Bu bağlantıyi sağlamak için yine bir router'a ihtiyaç var.



A network with two LANs

WAN (Wide Area Network): Çok sayıda LAN'ın oluşturduğu ağlardır. Günümüzde internet bunun en güzel örneği.

VPC: Virtual Private Cloud. Biz AWS'de kaldıracağımız makineler için bir VPC kuracağız. Bu VPC'lerle bir LAN oluşturmuş oluyoruz.

Host: Ağa bağlanabilen cihazlardır. IP Adresi alması gereklidir

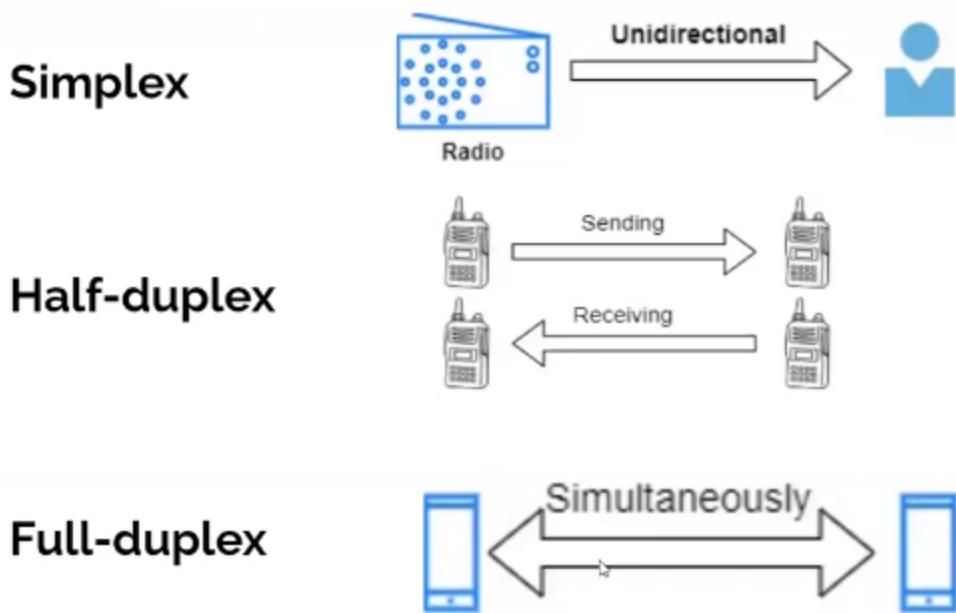
Server: Güçlü bilgisayarlar

Bağlantı Özellikleri:

Simplex, tek yönlü bağlantı

Half-duplex, biri gönderim yaparken diğerleri bekler. Telsiz gibi

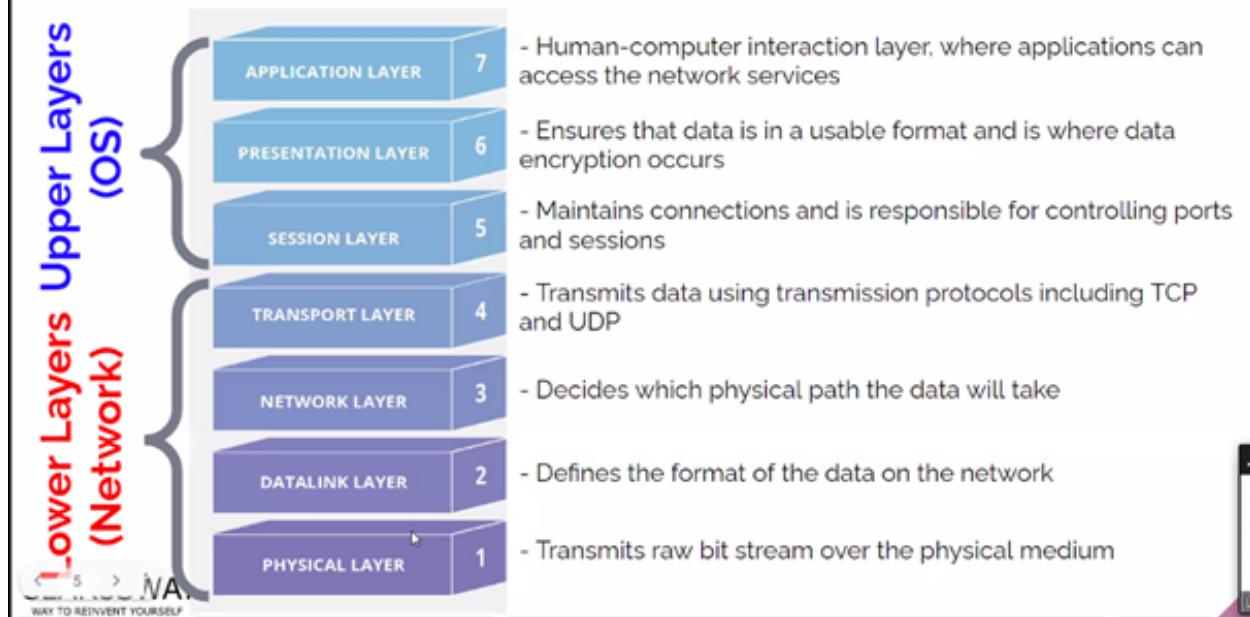
Full-duplex, aynı anda hem gönderim hem veri alımı yapılabilir. Telefon sistemi



OSI (Open Systems Interconnection) Model

Farklı yazılım ve donanımları aynı internet ağına bağlanması sağlanan kriter listesi. Tavsiye niteliğinde. 7 katman var. Donanımlar genellikle bu standartlara göre üretiliyor.

What is OSI Reference Model?



7.Katman (Application):

Kullanıcı ile etkileşime geçilen katmandır. Örneğin chrome da yaptığımız bir bağlantı isteği. Chrome bu isteği alır ve bir alt katmana iletir.

6.Katman (Presentation):

Genel olarak datanın hazırlanmasından sorumludur. İlk olarak L7'den gelen veriyi şifreler. Sonra sıkıştırır. Çünkü ağ üzerinde çok yoğun bir trafik var. Sonra bunu alt katmanın anlayacağı dile çevirir.

5.Katman (Session):

Burada kendi işletim sistemiyle koordineli olarak ki taraf arasında iletişimini başlatır. Yani benim PC ile chrome server arasında bir session başlatır. Bağlanılan bazı sitelerde (bankacılık, clarusway lms vs.) bu sessionları süreli yapar. Belli bir süre işlem yapılmazsa oturum sona erer.

4.Katman (Transport):

Bu katmandan sonra kernel devreye girer. Çünkü artık donanım üzerinde çalışmaya geçirilir. Hiç bir uygulamanın (google vs.) bilgisayarın donanımına doğrudan erişim yetkisi yok. İsteğini kernel'a bildirir. Kernel donanıma emir verir.

Üst katmandan gelen tek parça halindeki veriyi segmentlere yani daha küçük parçalara böler. İlk parçalama burada yapılır ve veri ağ kartına gönderilir.

3.Katman (Network):

Segmentler halindeki veriyi paketlere koyar. İçine alıcı ve gönderici IP bilgilerini, MAC adresini girer. Router L3 bir cihaz

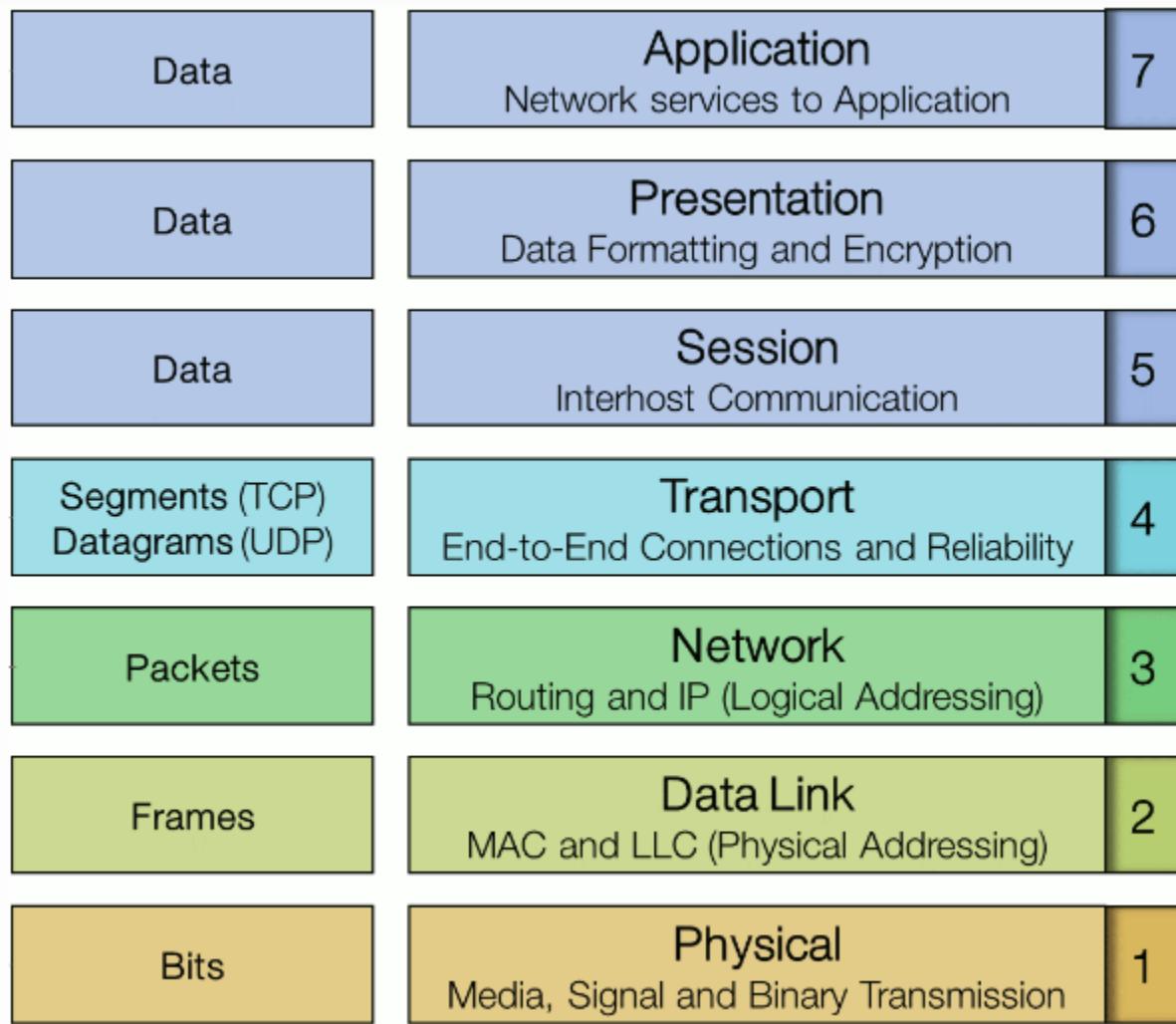
2.Katman (DataLink):

Yukarıdan gelen paketleri frame'lere koyar. Veri akışının yönetilmesinden ve hata kontrolünden sorumludur.

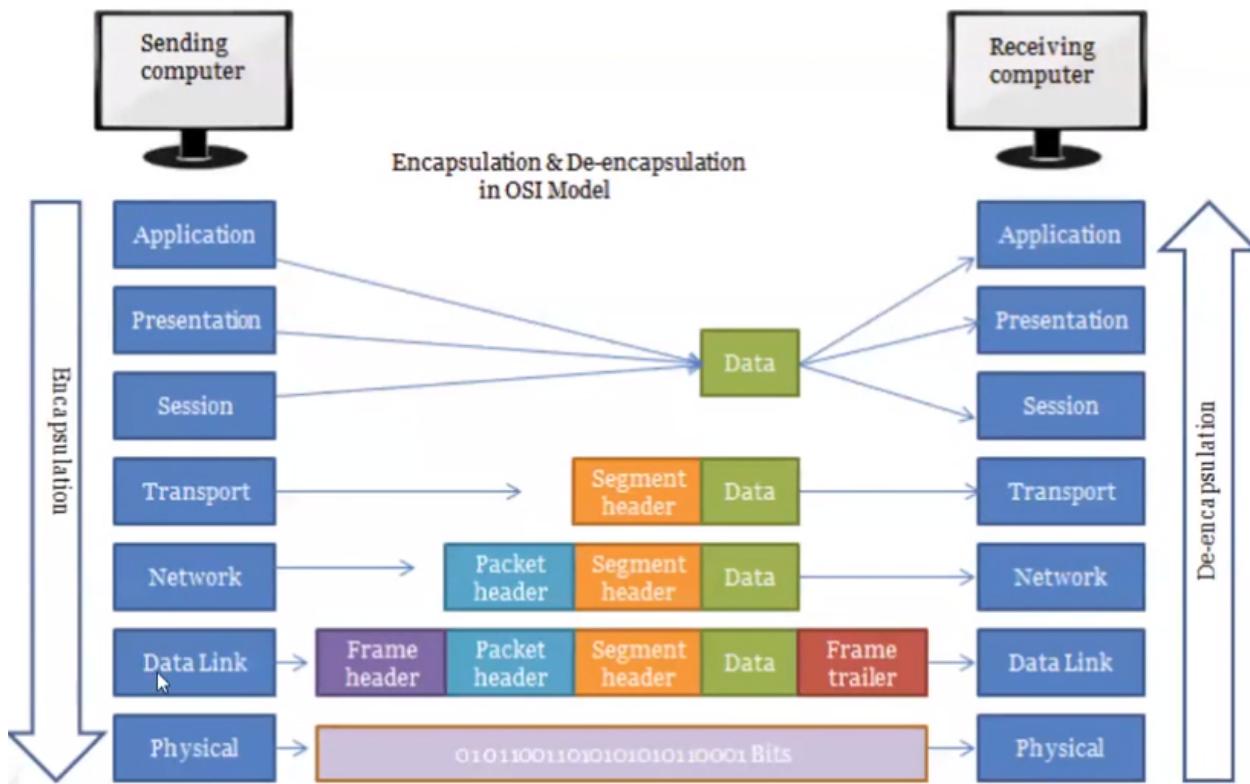
Ethernet kartı, L1den gelen elektrik sinyalini anlamlandıırıp üst katmana gönderir. Switch L2 bir cihaz

1.Katman (Physical):

Frame halindeki verinin fiziksel yollarla (kablo vs.) iletiliği kısımdır. Bitler halinde iletilir. Bir kere veriyi ağa verdikten sonra veriye herhangi bir müdahalede bulunamıyoruz. Hub L1 bir cihaz



Data Encapsulation



5,6 ve 7 basamaklarda oluşan bir veri layer 4 te segmentlere bölünür ve her bir segmentin başına Segment Header eklenir. 3'te alıcı gönderici adreslerini de ekleyip bir pakete konur. 2'de Frame header ve tailer eklenir.

Bir Frame'in Yapısı (Lazım olmayacak bir bilgi)

Field Length, in Bytes		IEEE 802.3						
7	1	6	6	2	46-1500	4		
Preamble	SOF	Destination Address	Source Address	Length	802.2 Header and Data	FCS		

Preamble: Alıcıya uyarı mesajı

SOF: Start of frame

Destination ve Source Adress MAC Adresleridir.

FCS:Mesajın bozulup bozulmadığını gösteren kısım

ETHERNET

IEEE 802.3 standartına göre üretilen kartlar Ethernet kartıdır. Standartına göre üretilen kablolar Ethernet kablosudur. IEEE=> Electonic Engineerintopluluğu.

Layer 1 standartı kablo ,ile ilgili diyebiliriz

Bir bakır kablonun iletebi

Ieceği max mesafe 100m.dir. Bu yüzden her 100 m.de bir amplifier ya da repeater lazım.

MAC adresi Layer 2 yani Frame leri okuyabilir.

Network interface Card (NIC):Ethernet kartı.

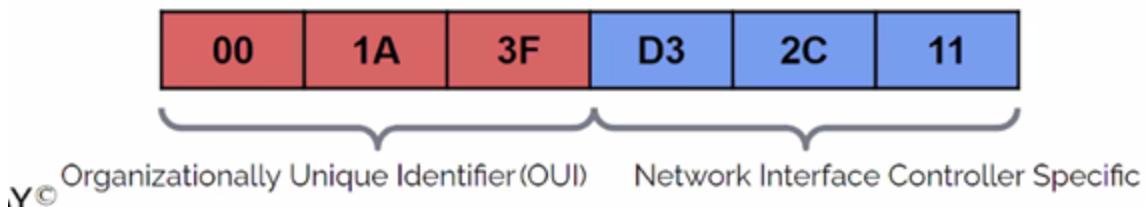


Bir bilgisayar ağa bağlanmak için iki değere ihtiyaç duyar. Bunlardan biri IP adresi diğeri MAC (Physical Address)adresidir. MAC, Ethernet kartına gömülüdür. Ayrıca o local ağ içerisinde başka kimsedef aynı MAC ya da IP adresinin olmaması gerekiyor.

MAC (Media Access Control) ADRESİ (Fiziksel Adres)



MAC Adresi 48 bit yani 6 bytes dan oluşur. İlk üçü üretici kodu. Onun ürettiği ethernet kartlarında bu 3 byte aynı. Diğer üçü eşsiz, başka hiçbir cihazda olmayan sayılardır. MAC adresi ile IP yi eşlestiren yer ARP tablosu. Eğer router da ... IP li routerın MAC adresi kayıtlıdır. Eğer değilse arp broadcast mesajı çekiyor çevre routelara. İlgili router cevap veriyor.



İki şekilde gösterilir:

00:1A:3F:D3:2C:11 or 00-1A-3F-D3-2C-11

MAC Adres Tipleri

Unicast Adres: Bir alıcı bir gönderici olan iletişim modeli

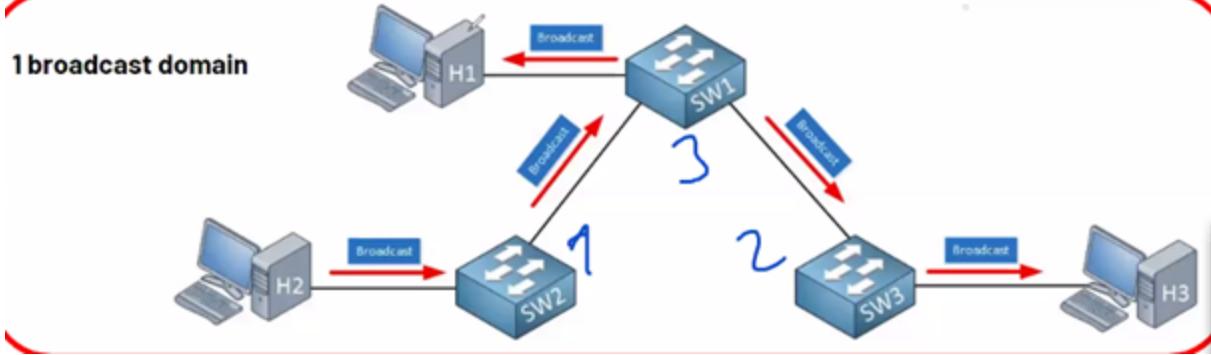
Multicast Adres: Bizim için önemli değil

Broadcast Adres: Ağdaki herkese gönderir. Alıcı olarak FF:FF:FF:FF:FF:FF adresi yazılması gereklidir. Bu broadcast adresi ağdaki hiç bir cihaza verilmemeli. Aynı şekilde 00:00:00:00:00:00 adresi de hiç bir cihaza verilmemeli

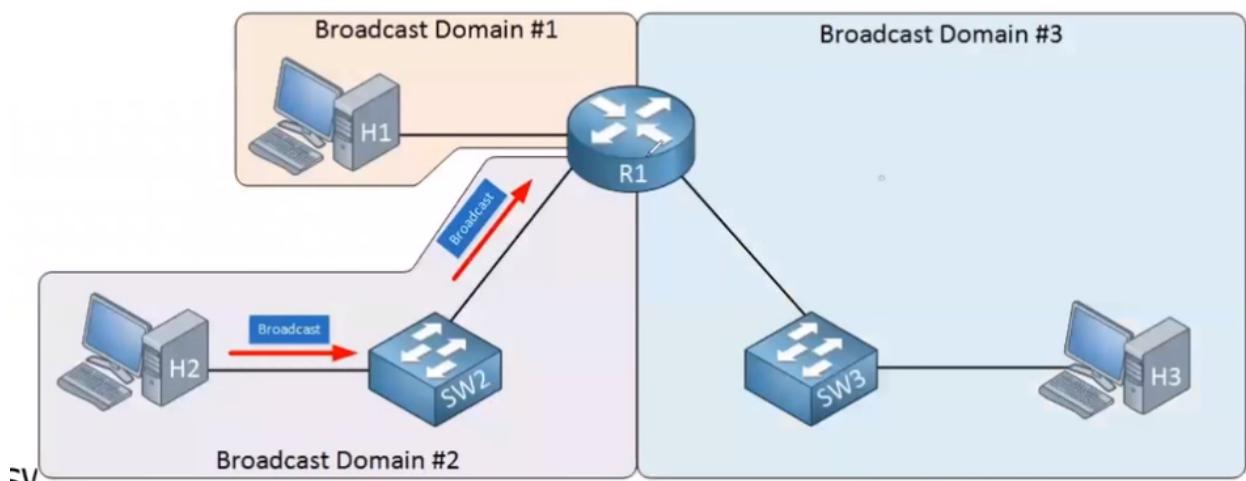
CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Çakışma

Carrier sinyali telefon düt sesi. Bu ses hatta bir elektrik sinyali olduğunu gösterir. Biz veri gönderirken bu sinyali ekip bükerek gönderiyoruz. Bir hattaki bir cihazın ethernet kartı önce hattı dinler ve hattın boş olduğunu duyar ardından mesajını gönderir. O sırada başka bir cihaz da veri gönderirse çakışma olur. Bu durumda iki cihaz da rastgele bir süre bekler ve kendi mesajlarını gönderir. Bu işlem mesaj önderilene kadar devam eder.

Broadcast Domain: Broadcast mesajı kaçınılmaz bir şey. Mutlaka gönderilir. 1 broadcast mesajının gidebileceği tüm cihazları bir araya toplarsak bu sisteme broadcast domain diyoruz.



Broadcast Domainini kaldırıramayız ancak boyut küçültülebiliriz. Yukarıdaki domainde switchler kullanılmış. Switch layer 2 cihaz ve alıcı adreslerini okuyamazlar. Bu yüzden gelen broadcast mesajlarını tüm portlarından yayar. Bu da ağda gereksiz bir trafiğe neden olur.



Ancak Switch1 yerine router kullanırsak sistemi daha küçük ve yönetilmesi kolay broadcastlere bölebiliriz. Çünkü Router, Layer 3 bir cihaz ve alıcı adreslerini okuyabilir. Gelen broadcast mesajında kendisine gelen bir soru varsa buna cevap verir ancak başkasına iletmez. Bu da ağdaki gereksiz yükü azaltır.

NETWORK CİHAZLARI

Ethernet Kartı (NIC): Özel bir MAC adresi var içinde. Bu iki cihazla iki bilgisayar birbirine bağlanır. Ancak 3 ve daha fazla PC olursa HUB/Switch kullanılır.



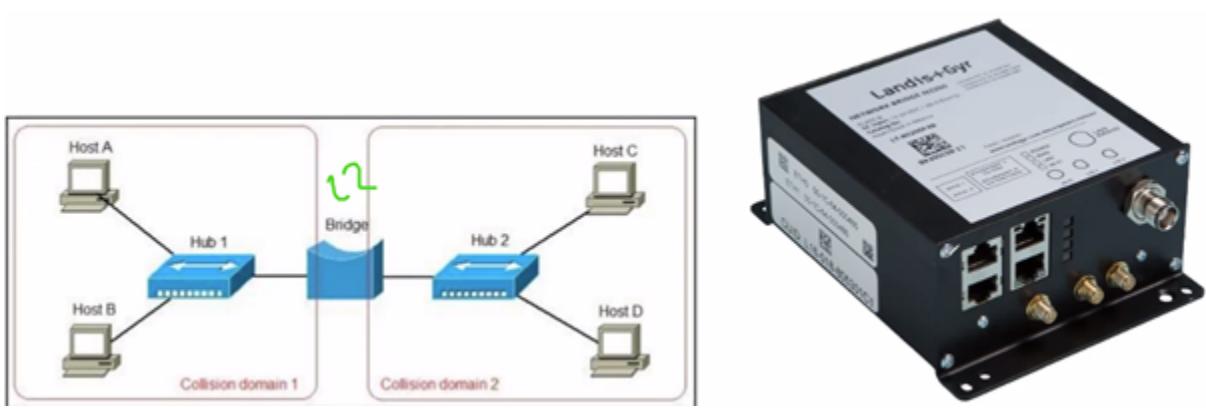
HUB: Layer 1 de çalışır. Sadece elektrik sinyali,ni okur. Alıcı adresini okuyamaz bu yüzden ağdaki herkese gönderir. Aptal Switch de denir. Artık HUB kullanmak ciddi bir güvenlik ihlali. Çünkü ağdaki herkes ilgili mesajı görebilir.



SWITCH: Layer 2 de çalışır. Yani Frame leri görür ve alıcı MAC adresini okur. Buna göre ilgili portundan alıcı PC ye gönderir.

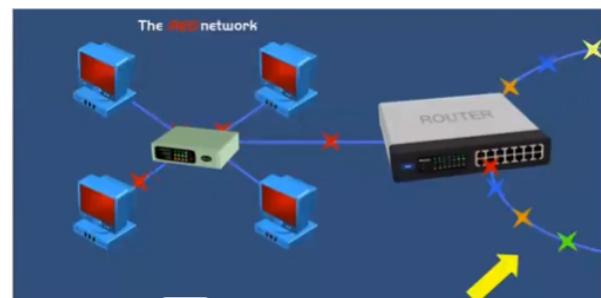


BRIDGE: Layer 2 cihazı. Hublardan oluşmuş networkü bölmeye ya da birleştirmeye yarar.



ROUTER:

L3 bir cihaz. IP adreslerini okuyabiliyor. Kendine has işlemcisi vs olan akıllı bir cihaz. Internet trafiğini kontrol ediyor. Her bir portunun ayrı interface i var. Yani 4 ayrı MAC adresi ve IP adresi vardır. Switchler ağ içerisindeki trafiği MAC adresleri sayesinde ayarlayabilirken, LAN'lar arasındaki trafik için IP adreslerine ihtiyaç vardır. Routerlar bu yönlendirme işlemini sağlar. Router in her bir portundan bir Network kurabiliriz. Çünkü her birinin ayrı ethernet kartı mevcut.



FIREWALL: Hem yazılımsal hem de Black box denilen donanımsal koruma var.

LOAD BALANCER: Gelen trafiğin bir server a yüklenmesini engeller. Tüm serverlar arası yükü paylaştırır.

DOMAIN NAME SERVICE (DNS) SERVER: Bir çeşit telefon rehberi. Siteni adı ile IP adresini eşleştiriyor. Kullanıcı youtube yazınca DNS youtube un IP adresine gitmeyi sağlıyor.

www.clarusway.com than 13.35.253.82

Bilgisayar ilk kez gireceği bir sitenin IP adresini bilmiyor. Bunu DNS serverlara sorar. Kendisinde kayıtlısa DNS Server adresi bize gönderir, eğer yoksa bir üst server'a sorar. En nihayetinde Root (Top level) DNS Server'a sorar. Orada kesinlikle var. Bunların kontrolü IANA isimli bir grup apar. Sitesinde .com/.org gibi uzantılara göre IP adreslerini tasniflemişler. Buradan biz de görebiliriz.

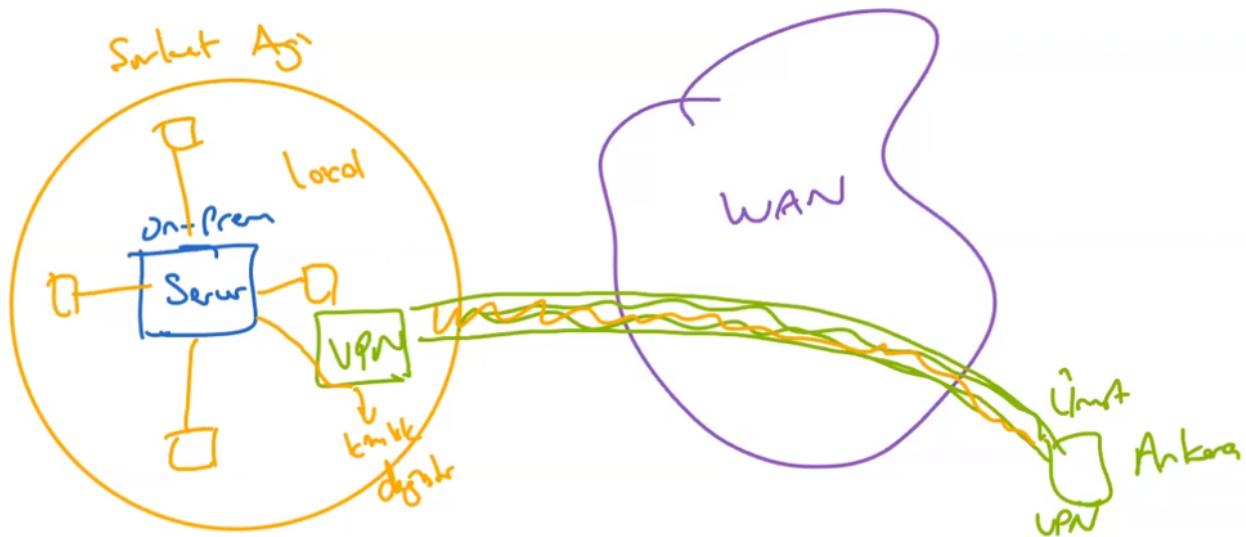


Bizim .tr uzantılı serverların kontrolünü BTK (Bilgi Teknolojileri Kurumu) sağlar.

PROXY SERVER: Bir çeşit bilgisayar. Sistemin internete çıkışına konulur. İnternete çıkışları düzenler. Örneğin bir iş yerinde çalışanların instagrama girmelerini engellemek için proxy server'a yasaklı bir kural konur ve şirket bilgisayarlarından Instagrama erişim engeli gelir. Aynı zamanda cache'leme işlemi yapar. Yani çok kullanılan siteleri hafızasına alır ve daha hızlı bağlanmaya yarar. Ayrıca dışarıdan gelen tehditlere karşı bir firewall gibi de çalışır.



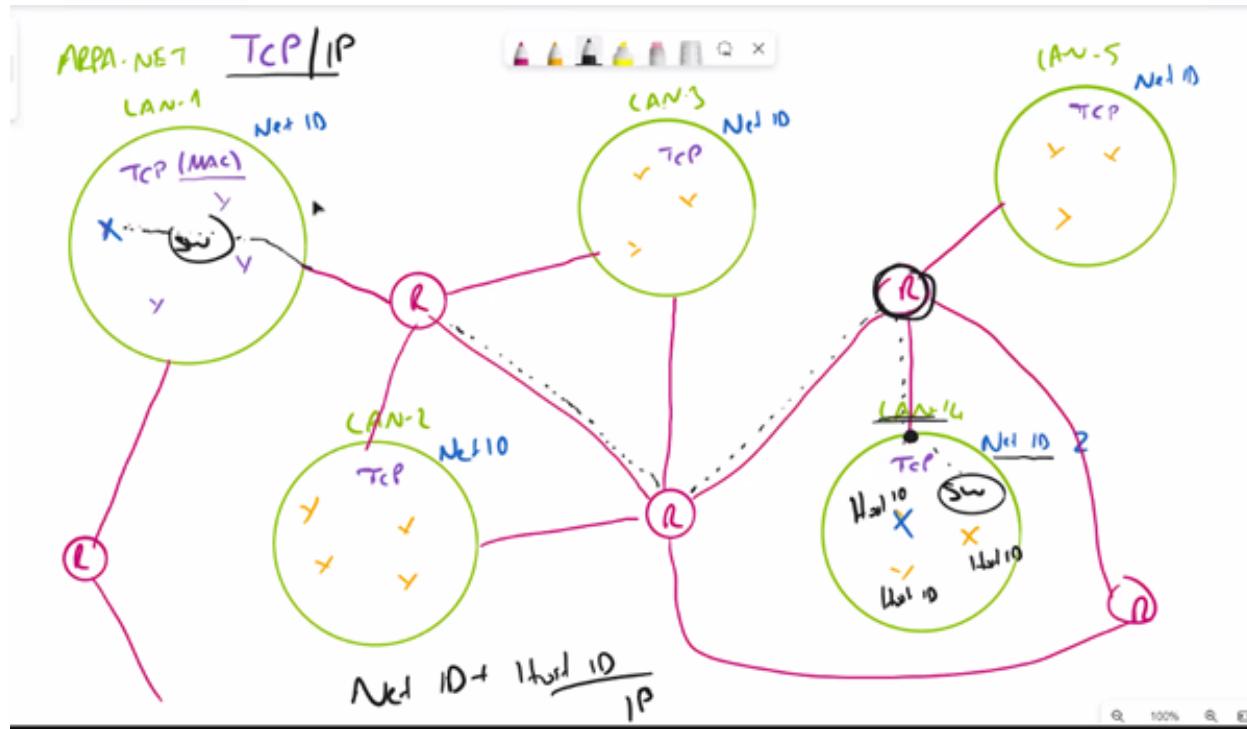
VPN Concentrator Cihazı: Her ne kadar Türkiye'de yasaklı sitelere girmek için kullanılsa da normalde kapalı sistemlere bağlanmak için kullanılır.



Örneğin bizim şirketin serverları on-premise şekilde çalışıyor. Ve buraya sadece şirket binasından erişebiliyoruz. Dışarıdan internet üzerinden bağlantıyi engelleyecek şekilde programlanmış. Ancak pandemi ile birlikte evden çalışanların da bu ağa erişmesi gerek. Mecburen internet üzerinden şirket ağlarına girmem gerek. Burada VPN cihazı devreye giriyor. Benim adresim ile şirket server'ı arasında bir tünel açar. Bu tünel şifrelidir ve sabit bir rotayı izler. (Normalde internette data trafiği en hızlı yolu izler. Buna göre bağlanacağı router'ları seçer). Bu tünel sayesinde VPN sanki ben local ağdaydım gibi benim kimliğimi değiştiriyor ve bağlantı sağlıyorum.

TCP/IP Modeli

(Transmission Control Protocol/Internet Protocol) Donanımdan ziyade daha çok yazılımsal bir protokol. Donanımlar genellikle OSI protokolüne göre yapılıyor. Diğer adı DoD Model (Department of Defence) 4 katmanlıdır.



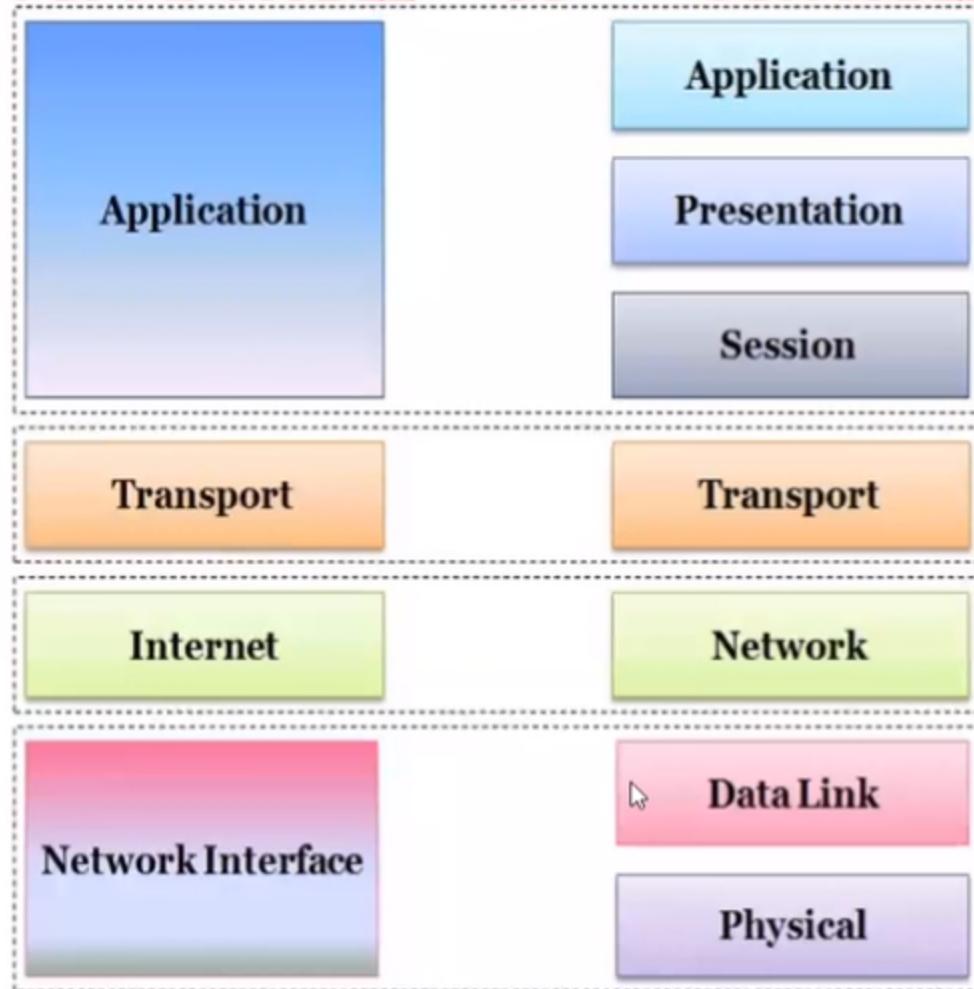
İlk kullanılan LAN (network) ARPA.nettir Bu networkler içinde TCP model kullanılarak haberleşme yapılır. Yani ağ içindeki tüm cihazların MAC adresini bilirsek konuşabiliyoruz. Zamanında çok az sayıda ağ vardı ancak şimdi milyonlarca LAN (Network) var. Bu LAN'lardaki tüm cihazları bilmemiz imkansız. Bu yüzden bu LAN'lara bir Network ID verilir. Örneğin LAN-1 den LAN-4 e mesaj göndereceksek önce LAN-1deki switch bizi router'a yönlendirir. Bu router'da hedef Network ID'ye ulaşmak üzere routerları kullanarak bir yol belirler.

IP Address = Network ID + Host ID

LAN-4 ün dışındaki routerlar Network ID'ye bakarak LAN-4 ü buldu ancak ağıın içindelerin MAC adresi ya da Host ID'lerini bilmiyor. Bunu da kapıldığı router (yani evimizdeki Wi-Fi cihazı) biliyor. Buna göre evimizdeki router (Wi-Fi Modem) ilgili mesajı LAN içindeki ilgili adrese teslim ediyor.

Sonuç olarak networkler içinde kullanılan bir TCP modelimiz vardı. Daha sonra buna networkler arası iletişimini sağlamak için IP modeli eklendi ve TCP/IP modeli oluştu.

TCP/IP MODEL Vs OSİ MODEL



Network Access Layer: TCP/IP modelin L1'idir. Datanın fiziksel olarak nasıl gösterileceğini belirler.

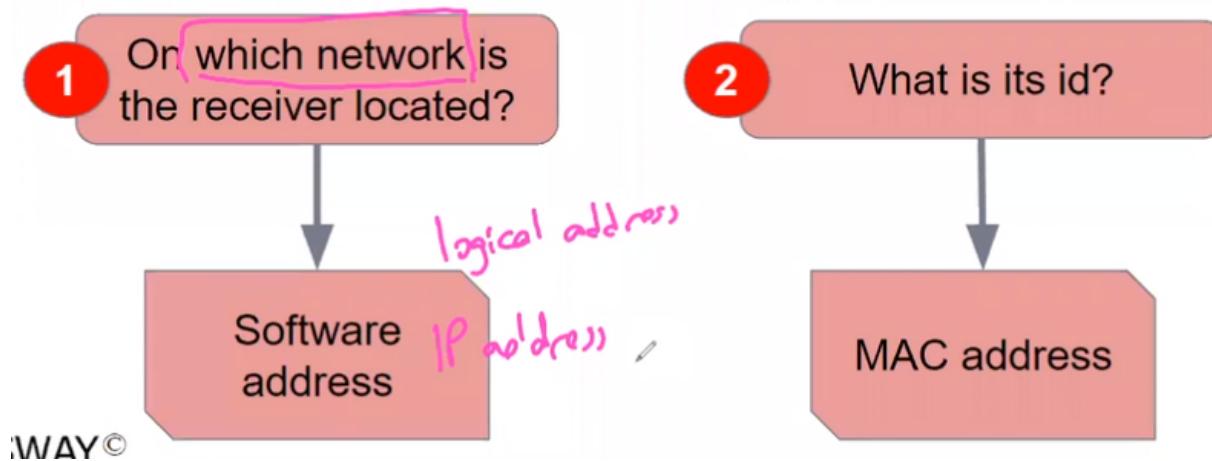
Internet Layer: Paketlerin (ya da datagramların) yönlendirmesinden sorumlu. OSİ modelde L3, burada L2'ye karşılık geliyor.

Temel kullanılan protokoller

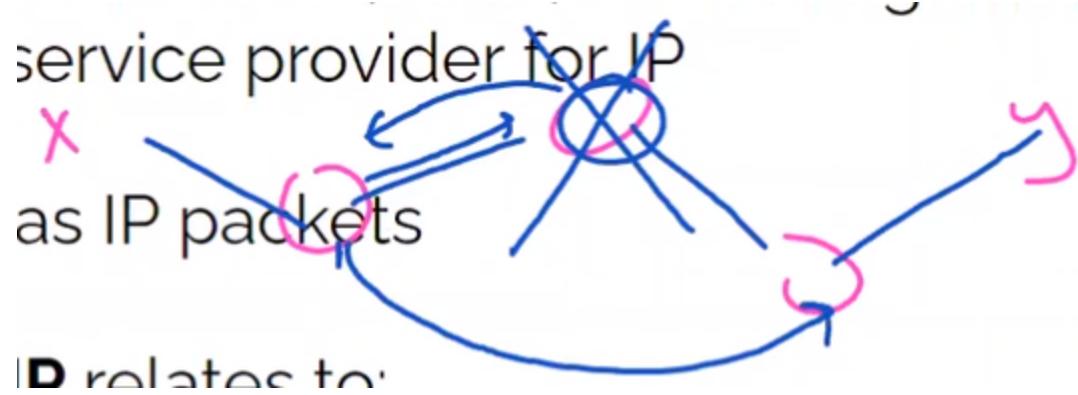
- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)

Internet Protokolü (IP) kullanılıp biri ile haberleşmek için şu sorgulamalar yapılır: alıcı hangi networkte? (dunu da IP adresinin içindeki Network ID'ye bakarak anlar) Eğer aynı Networkteysek alıcının MAC adresini bilmem gereklidir.

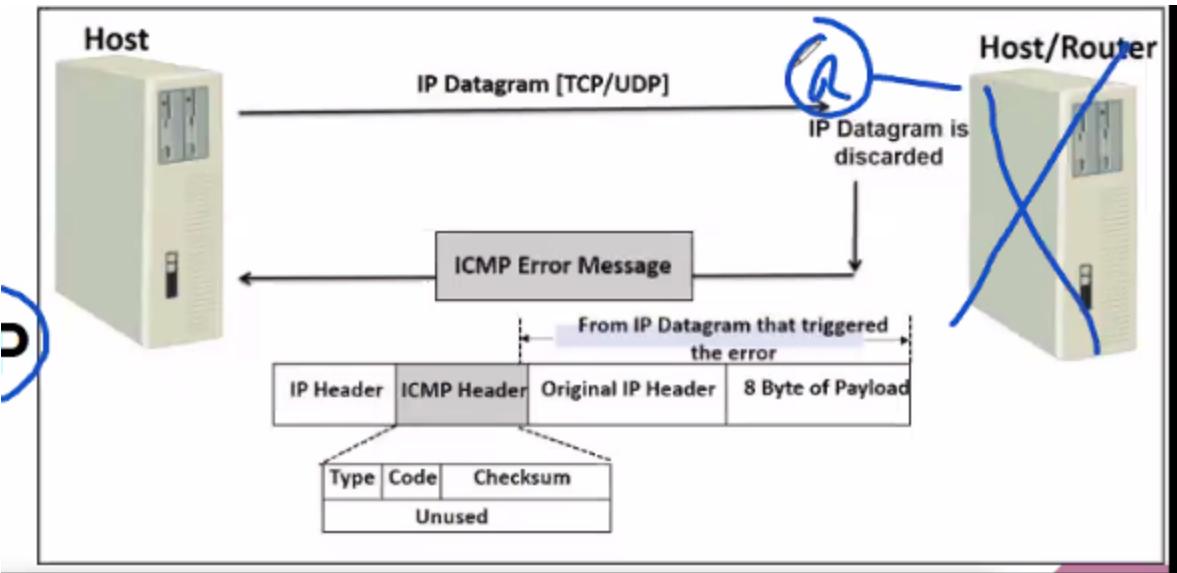
Farklı networkteysek IP Adresin içindeki Host ID ve yine MAC adresi bana lazımdır.



Kullanılan bir diğer protokol ICMP'dir. Bu protokol özetle paket gönderdikten sonra networklerin birbirine durumlarını haber vermesidir. Aksi takdirde bir paket yolladığımızda onun durumunu bilemeyeziz. Gitti mi bir sıkıntı mı oldu nerede kaldı vs. Örneğin bir router çöktü ya da arızalandı. Geriye ICMP mesajı gönderir.



Bir önceki router da farklı bir yol kullanarak veriyi iletir. TCP/IP ye göre L2 de çalışır.



ARP table: Ağa bağlı tüm cihazlarda buna routerlar da dahil bir ARP tablosu bulunur. Bu tabloda agdaki tüm cihazların MAC adresleri ile Host ID'leri eşleştirilir. ARP Tablosu sürekli güncell tutulur. Yukarıda LAN-1den veriyi LAN-4'e gönderirken pakete IP adresini yazar. LAN-4ün routerı agdaki cihazların MAC adreslerine ARP tablosundan bakar ve ilgili bilgisayara veriyi gönderir. Eğer tablodaki değer güncel değilse ağa B/C mesajı çeker. İlgili Host bu IP benim, benim de MAC adresim bu şeklärde bir cevap verir.

Command Prompt		
Internet Address	Physical Address	Type
169.254.255.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

RARP: Reverse ARP. Burada cihaz kendi IP'sini bilmediği zaman bu mesajı agdaki diğer cihazlara çeker.

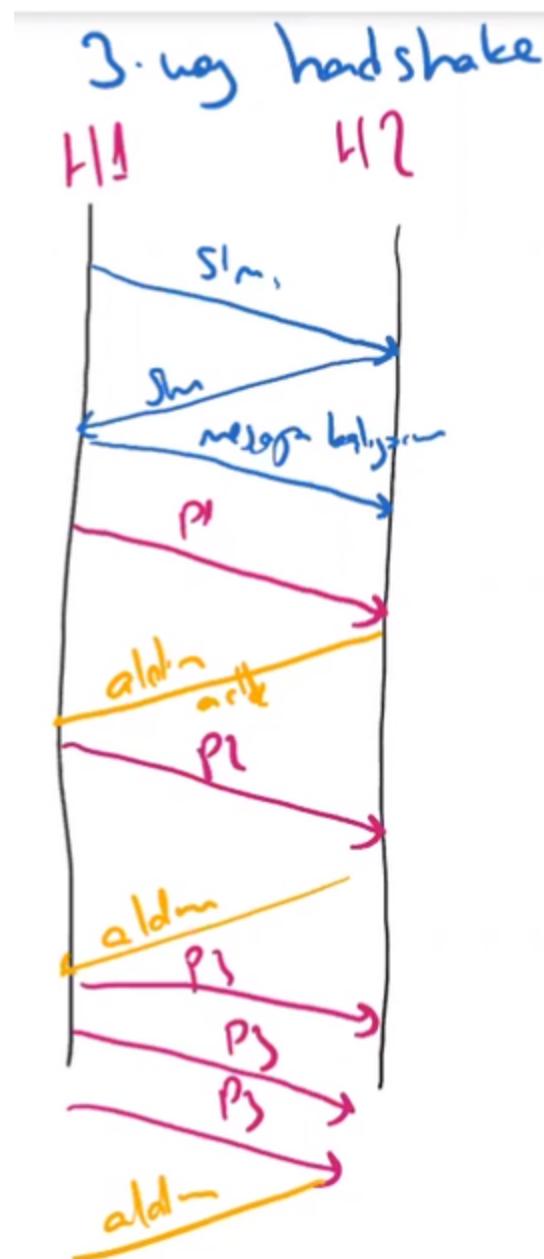
LAN içinde olduğu gibi LAN dışında da Routerlar arasında da ARP tablosu tutulur ve birbirlerinin IP ve MAC adreslerini bilirler.

Transport Layer(Host-to-Host Layer): Burası kernel'ın devrede olduğu bir katman. Üst katmandan gelen paketleri TCP ya da UDP paketleri ile karşı tarafa gönderilir.

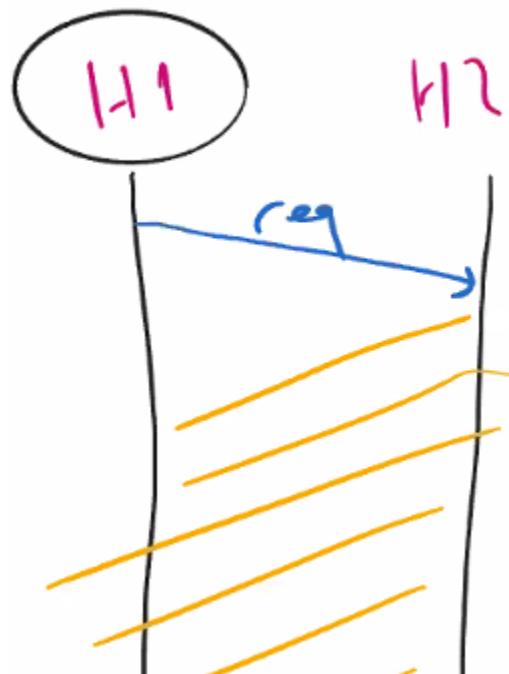
Transport Layer Protocols

- TCP Protokol: 3-way Handshake yöntemi var.

Öncelikle kimlik kontrolü ve cevabı. Ardından gönderiyorum diyoruz ve mesajı iletmeye başlıyoruz. Her paketten sonra alındı mesajı (acknowledge) bekliyorum. Yavaş, güvenilir, bağlantı şartı var, veriler sıralı gönderilir. Full-Duplextir.



- UDP protokol: Güvenilir değil veri kaybı olabilir, bağlantı şart değil, segmentler sırasız gönderilir, hızlı. Ör: zoom görüşmesi. Buradaki önemli olan şey hız. Görüntüde, seste ufak kopmalar olsa da sıkıntı yok



TCP	UDP
Secure	Unsecure
Connection-oriented	Connectionless
Slow	Fast
Guaranteed transmission	No guarantee
Flow control	No flow control
Reliable	Unreliable
Virtual circuit	No virtual circuit
Acknowledgement	No acknowledgement
20 bytes header	8 bytes header

Process/Access Layer: Uygulamalar arasında iletişimini sağlayan binlerce protokol var. Onlar burada çalışır. DNS, HTTP, SSH, FTP, DHCP bu protokollerden bazıları. Örneğin bir DNS server'ından bir sitenin adresini soracağım. Bu sorgulamayı da DNS protokolü üzerinden konuşmam gereklidir yani DNS'ce. Yaptığımız bu sorguyu DNS server'a L3'teki TCP ya da UDP protokollerile iletiyoruz.

PORT Numarası: 2 byte lik bir değer. İşletim sistemi üzerinde 1 portu 2 program kullanamaz. Hatta bir programda örneğin Chrome daki her bir sekmeye farklı port numarası atanır. Bunun gibi atanmış olanlar var. 2^6 yaklaşık 64000 farklı port olabilir. Kullanılmayan portlar kapalı kalır güvenlik için.

Yaklaşık olarak ilk 1000 porta Well-known ports denir. Hemen hemen herkesin bildiği işlevler için bu portlar ayrılmıştır. Başka programlara atanmaz. Örn: 80 portu http içindir. 22 portu ssh içindir. Genelde 1000-30000 arası portlara da registered ports denir. Bunları da kullanmamız tavsiye edilmez ama kullanıldığı olur. Sık kullanılan programlara ait portlardır. Bilgisayarda o program yüklü ise sistem otomatik olarak o

portu o programa verir. Eğer yüklü değilse portu kullanabiliriz. 30000 üzeri ise diğer portlardır. Boşta olanları kullanabiliriz.

The Process/Application Layer Protocols

- FTP Protocol: File transfer Protocol iki bilgisayara arası. 20 ve 21 nolu portları kullanır.



Name	TCP/UDP	Port	Description
FTPS	TCP	20/21	FTP Secure is an extension of FTP that adds support for TLS encryption.
TFTP	UDP	69	Trivial FTP is the stripped-down, stock version of FTP. TFTP is fast and so easy to use. It can only send and receive files.
SFTP	TCP	22	Same as FTP but Secure FTP uses an encrypted connection through an SSH session, which encrypts the connection

- SSH protocol: Port 22 yi kullanıyor.
- Telnet: 23 porttan gider. Ancak şifrelenmeden gider.
- RDP: Anydesk gibi grafik arayüzüne kullanarak bağlanır
- HTTPS: 443 nolu portu kullanır. WEB serverlarla konuşmak için
- POP ve IMAP: Mail uygulamalarının kullandığı protocoller
- SNMP (Simple Network Management Protocol) Ağda bir sıkıntı olduğu zaman kontrol etmemizi sağlayan bir protokol

- NTP (Network Time Protocol): Saat ayarı için
- DHCP (UDP 67/68) Her LAN/WAN'da Host lara IP atayan bir protocol bulunur. (Dynamic Host Configuration Prot.) Bu protokol sayesinde ağdaki tüm cihazlara aşağıdaki bilgileri birbirinden farklı olacak şekilde atar
 - IP Address
 - Subnet Mask
 - Domain Name
 - Default Gateways
 - DNS Server Address

Evdeki LAN'da da bu işlemi Wi-Fi Router yapar.

- LDAP (TCP 389) Ağdaki tüm pclere program yüklemek için. Ör. İnternet kafelerde tüm masalara pro yükleme gibi
- TLS/SSL: Kriptolama protokolü. Yetkili bir merci var. Ör. Google bu sertifikayı almak istiyor. Bu merciye başvuruyor. Özel olarak Google a private key iletiliyor. Google Asimetrik bir public key üretip müşterilerine dağıtıyor. Ben evden Google a girerken bendeki public key ile google serverdaki private key eşleşiyorsa benim bilgisayarım Google'ın güvenli bir site olduğunu anlıyor. Yok eşleşmezse ya da sertifika süresi dolmuşsa bağlanmak Güvenli değil/ isterSEN devam edelim uyarısı çıkardı.

IP ADDRESS (Logical Adress/ Software Adress/ Internet Adress)

Genellikle 10luk tabanda yazılır. 32 bitlik 4 byte ya da 4 octet ten oluşur. Bu Adresin bir kısmı Network ID'yi bir kısmı Host ID'yi gösterir. Ne kadarının Network ne kadarının Host olduğu IP sınıflarına bağlı olarak değişir.

192.168.10.0
/ 2 3 4

NETWORK CLASSES

Class A'nın ilk biti 0 ile başlar.

Class B'nin ilk biti 10 ile başlar

Class C'nin ilk biti 110 ile başlar

Class D ve E pek karşılaşmayacağımız.

Network addresses are divided into 5 classes:

	Octet 1	Octet 2	Octet 3	Octet 4
Class A	0	Network ID		Host ID
Class B	1 0	Network ID		Host ID
Class C	1 1 0		Network ID	Host ID
Class D	1 1 1 0		Multicast Address	
Class E	1 1 1 1		Reserved	

5 farklı IP sınıfı var. Bizim için önemli olan ilk 3ü.

A Sınıfı



İlk oktetin ilk biti 0 ile başlar. İlk oktet Network ID'yi verir. Son üç oktet Host ID'yi verir

00000000 = 0 ile

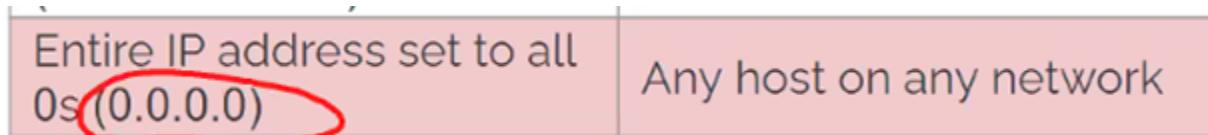
01111111 = 127 arasında olan IP'lerdir.

Maksimum $2^7 = 128$ adet Class A Network kurulabilir.

Bir Network içinde maksimum $2^{24} = 16.777.214$ adet Host oluşturulabilir.

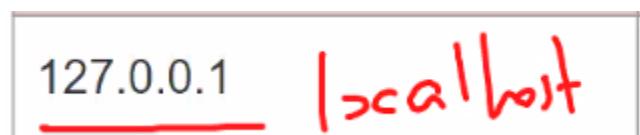
0 ve 127 ile başlayanlar rezerve edilmiş bunları kullanamayız ağıda. Yani Class A da 1-126 arasını kullanabiliyoruz.

X.255.255.255 \Rightarrow Broadcast adresidir.



Bu şekilde yazarak herhangi bir kısıtlama yapmıyoruz yani her pc bağlanabilir.

local host 127 ile başlar. Kendi kullandığım bilgisayarın test adresi. Örneğin bir developer olarak yazdığımız kodun test edilmesi gereklidir. Ancak bunun için para verip bir host adresi almam gereklidir. Bunun yerine sanki herkese yayın yapıyormuş gibi bir sayfa oluşur. Testlerimizi burada yaparız.



B Sınıfı



İlk oktetin ilk 2 biti 10 ile başlar. İlk iki oktet Network ID'yi verir. Son iki oktet Host ID'yi verir

10000000 = 128 ile

10111111 = 191 arasında olan IP'lerdir.

Maksimum $2^{14} = 16.384$ adet Class B Network kurulabilir.

Bir Network içinde maksimum $2^{16} = 65.534$ (-2 rezerve IP) adet Host oluşturulabilir.

X.X.255.255 \Rightarrow Broadcast adresidir.

C Sınıfı

network network network host

İlk oktetin ilk 3 biti 110 ile başlar. İlk üç oktet Network ID'yi verir. Son oktet Host ID'yi verir

11000000 =192 ile

11011111 = 223 arasında olan IP'lerdir.

Maksimum $2^{21} = 2,097,152$ adet Class C Network kurulabilir.

Bir Network içinde maksimum $2^8 = 254$ (-2 rezerve IP) adet Host oluşturulabilir.

X.X.X.255 ⇒ Broadcast adresidir.

GENEL TABLO

Address Class	1st Octet Range	1st Octet Bits	Network & Host Parts	# of Possible Networks # of Hosts per Network
A	<u>1-127</u>	00000000 - 01111111	N.H.H.H	128 nets (2^7) 16,777,214 hosts per net (2^{24})-2
B	128-191	10000000 - 10111111	N.N.H.H	16,384 nets (2^{14}) 65,534 hosts per net (2^{16})-2
C	192-223	11000000 - 11011111	N.N.N.H	2,097,150 nets (2^{21}) 254 hosts per net (2^8)-2

PRIVATE IP ADDRESS

Artık IP sayıları yeterli olmadığı için Private IP diye bir şey çıktı. Lokal ağlarda bu Private IP adresleri kullanılıyor. Her classta aşağıda verilen IP adresleri Private olarak belirlenmiş. Private IP'Ler non-Routabledır. Yani Routerlar bu adresleri tanımaz. Kendisine böyle bir adrese iletmek üzere bir paket gelirse adresi tanımadığından bu paketi çöpe atar.

A'da 10 ile başlayan

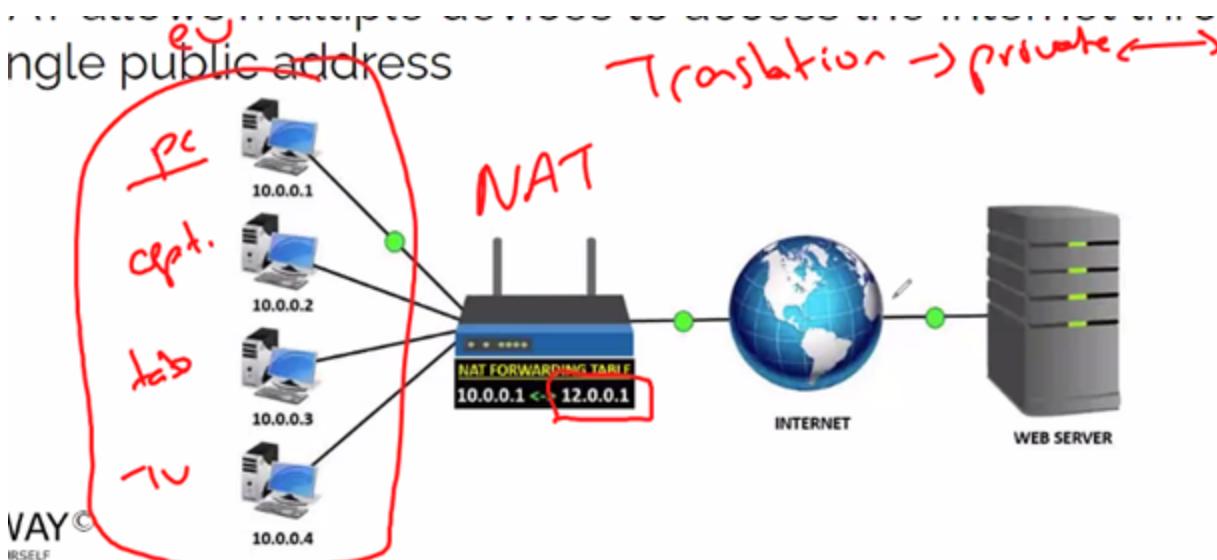
B'de 172.16-172.31

C'de 192.168 ile başlayan. C'de normalde 3 oktet ayrılrken private IP'de 2 oktet ayrılmış

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 172.16.0.0 to 172.31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

Benim evdeki PC nin private IP si ile Ankaradaki birinin evindeki PC nin private IPsi aynı olabilir. Nasıl olsa local ağıda olduğu için bir çakışma olmayacak. Ancak internete çıkışken Public IP ile çıkılıyor. Bunu sağlayan cihazın ismi NAT

NAT Network Address Translator: Yerel ağimdaki Private IPyi public e çevirip internete çıkış yapıyor.



255:255:255:255 Broadcast IP adresidir. Yani tüm adreslere gönderir.

IPv6 Internet Protocol Version 6:

IPv4 ün yetersiz kaldığını görünce private IP çıktı daha sonra subnetting konusu ortaya konuluyor. Hala IPv4 kullanamı oranı %50 den biraz fazla. IPv4 32 bitlikti IPv6 128 bit. Daha fazla IP adresi var. IPv4 browser a yazınca siteye gidebiliriz. Ancak v6 da [] içine yazarak browsera bağlanmamız gereklidir.

Original : 2001:0001:0002:0003:0004:0005:0006:0007

Her birine hextet denir.

Her cihazda (PC vs.) hem v6 hem de v4 IP vardır. Bunun nedeni Hala dünyada hem v4 hem de v6 kullanan siteler var bizim cihazda bu IPler olmazsa bağlanamayız.

Kısaltma için 3 kural var.

- Arka arkaya gelen sıfırları silebiliyoruz. Yerine :: koyarız bilgisayar tüm adresi 8 hextet yapacak şekilde bu arayı 0 ile doldurur. Ancak bu işlemi sadece bir yerde yapabiliriz. Yani atacağımız sıfırlar yan yana olmalı

Original : 2041:0000:140F:0000:0000:0000:875B:131B 
Short : 2041:0000:140F:0:875B:131B

Original : 2001:0000:0000:0012:0000:0000:1234:56ab 
Wrong! : 2001:0012:1234:56AB

- Tekrar eden :0000: yerine sadece :0: yazabiliriz

Original : 2041:0000:140F:0000:0000:0000:875B:131B
Short : 2041:0:140F:0:875B:131B

- Soldaki sıfırlar silinebilir

Original : 2001:0001:0002:0003:0004:0005:0006:0007
Short : 2001:1:2:3:4:5:6:7



İnternete bağlanan cihazların IP adresleri sabit değil sürekli değişiyor. Eğer değişim istersek ekstra ücret ödeyerek statik IP almamız gerekiyor. Genelde evden yayın yapanlar IP'lerinin değişimini istemezler. Çünkü Başkaları onun server'ına kolay bir şekilde bağlanamaz. Eğer Amazon üzerindeki EC2ların IP adreslerinin değişimmemesini istersek Amazon'dan Elastic IP Adres almamız gerekiyor.

SUBNETTING

7 ayrı network ihtiyacım var ancak sadece 1 tane alabildim

COMPANY

7 offices in different countries
500 hosts/office

At least 7 network

I
133.86.0.0

10000101.01010110.00000000.00000000

Bu yüzden Host ID'min bir kısmını Subnet olarak ayıriyorum.

10000101.01010110.00000000.00000000 133.86.0.0
10000101.01010110.01000000.00000000 I 133.86.64.0
10000101.01010110.10000000.00000000
10000101.01010110.11000000.00000000

Bir alttaki 0 ve 255 lik IPler reserve yani kullanılamaz. 0 loopback(test), 255 B/C Adresi Loopback adresine aynı zamanda Network Adresi de denir.

```
10000101.01010110.00000000.00000000 -> loopback  
10000101.01010110.11111111.11111111 -> b/c
```

```
1 x Network 2^16 - 2 = 65534
```

```
10000101.01010110.00000000.00000000  
10000101.01010110.00000000.00000000  
10000101.01010110.00000000.00000000
```

Örneğin 7 farklı ülkede çalışan bir şirketim var. Herbirinde 500 tane Host olacak. Toplamda 7 ayrı network lazım bana ancak bunun için sadece 1 IP adresi alabildim. Bu yüzden 3 tane biti subnet olarak ayıriyorum

```
1 x Network 2^16 - 2 = 65534
```

```
10000101.01010110.00000000.00000000 133.86.0.0  
10000101.01010110.00100000.00000000 133.86.32.0  
10000101.01010110.01000000.00000000 133.86.64.0  
10000101.01010110.01100000.00000000 133.86.96.0  
  
10000101.01010110.10000000.00000000 133.86.128.0  
10000101.01010110.10100000.00000000 133.86.160.0  
10000101.01010110.11000000.00000000 133.86.192.0  
10000101.01010110.11100000.00000000 133.86.224.0
```

Genel bir kural/ bir tavsiye Subnetler için ayrılan bitlerin tamamının 0 yada tamamının 1 olduğunu kullanmamız tavsiye edilmez. Çünkü bazı sistemler bunları Host adresi olarak tanımlar.

tanımlamaz bunlara yayın yapmaz/mesaj iletmeyez. Ancak AWS'de bu kural geçerli değil 000 ve 111 için AWS'de Host adresi atayabiliriz..

LAN-1

```
10000101.01010110.00000000.00000000 133.86.0.0 reserved
10000101.01010110.00000000.00000001 133.86.0.1
10000101.01010110.00000000.00000010 133.86.0.2
10000101.01010110.00000000.00000011 133.86.0.3
10000101.01010110.00000000.00000100 133.86.0.4
.
.
10000101.01010110.00000000.11111110 133.86.0.254
10000101.01010110.00000000.11111111 133.86.0.255
10000101.01010110.00000001.00000000 133.86.1.0 I
10000101.01010110.00000001.00000001 133.86.1.1
10000101.01010110.00000001.00000010 133.86.1.2
I
```

LAN-2

```
10000101.01010110.00100000.00000000 133.86.32.0 loopback
10000101.01010110.00100000.00000001 133.86.32.1
10000101.01010110.00100000.00000010 133.86.32.2
10000101.01010110.00100000.00000011 133.86.32.3
.
.
.
10000101.01010110.00100000.11111111 133.86.32.255
10000101.01010110.00100001.00000000 133.86.33.0
10000101.01010110.00100001.00000001 133.86.33.1
10000101.01010110.00100001.00000010 133.86.33.2
```

Subnet Mask: Eğer subnet yaptığımız sistem kaç biti subnet yaptığımızı bilinemez sadece IP adresine bakarak bu yüzden Subnet Mask i de iletmemiz gerek. Subnet Mask

oluşturulurken Network ve Subnet bitleri ON Host bitleri OFF yapılır

11111111.11111111.11100000.00000000 : subnet mask

Network ID bulunurken IP ile Subnet Mask AND işlemine tabi tutulur. Sonuç Network ID dir

10000101.01010110.10100101.00110111	133.86.165.55
11111111.11111111.11100000.00000000	255.255.224.0
<hr/>	
----- AND	
10000101.01010110.10100000.00000000	133.86.160.0

T T : T

T F : F

F T : F

F F : F

CIDR – Classless Interdomain Routing

ID ve Subnet Mask i yan yana yazınca uzun bir sayı oluyor bunu kısaltmak için böyle bir kısaltma yapılıyor

133.86.165.55 – 255.255.224.0

Yukardaki adresin CIDR'ı => 133.86.165.55 /19 Subnet Maskte kaç tane 1 varsa o rakamı yazıyoruz.

11111111.11111111.11100000.00000000

Burada 19 tane 1 olduğu için 19 yazdık. İlk 16 digit zaten network rakamı ve oraya dokunamıyoruz. Doğal olarak 3 tane digit Subnet olarak kullandığımızı anlıyoruz.

Default Gateway: Bir Hosta gönderim yaparken ilk baktımız gereken onunla aynı Networkte olup olmadığımdır. Buna baktmak için Network ID'leri buluruz

- Source host : **192.168.123.72**
- Subnet mask : **255.255.255.192**
- Destination host : **192.168.123.109**

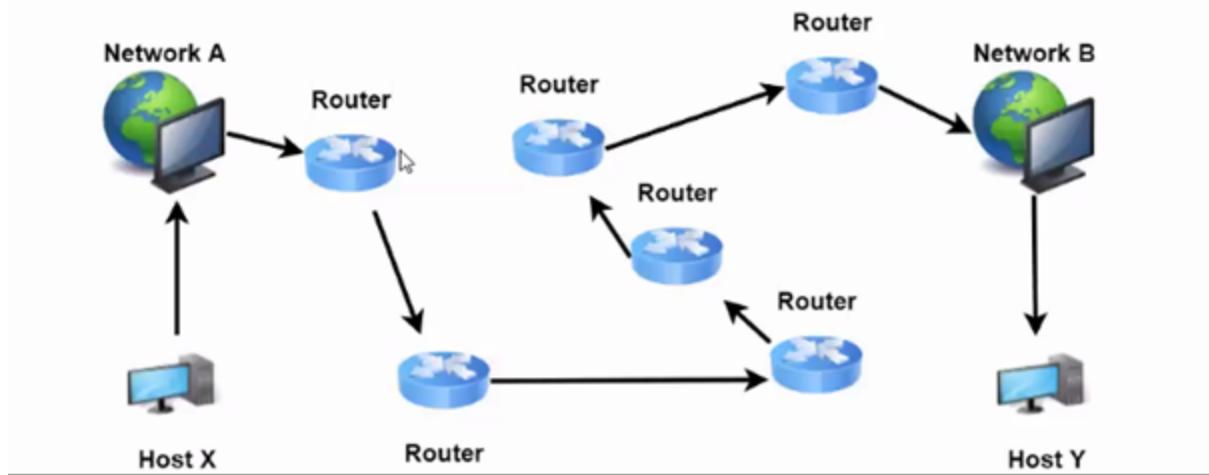
Source IP : **11000000.10101000.01111011.01001000** Logical AND
Subnet mask : **11111111.11111111.11111111.11000000**
Network ID **11000000.10101000.01111011.01000000**(192.168.123.64)

Destination IP : **11000000.10101000.01111011.01101101** Logical AND
Subnet mask : **11111111.11111111.11111111.11000000**
Network ID **11000000.10101000.01111011.01000000**(192.168.123.64)

Same result! Two hosts are on the same network.

Eğer Network IDler farklı çıkarsa farklı networklerde olduğumuz anlaşılır. O zaman da paketi dışarıya göndermek üzere gateway'e göndeririz. Evdeki gateway Wi-Fi router oluyor.

BİR PAKETİN GÖNDERİM AŞAMASI



Alicı hostun networkünü bilmesi gerek

Etraftaki routerları da bilmesi gerek.

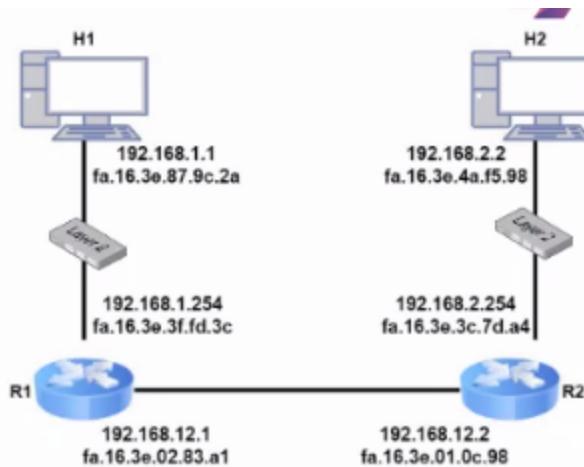
Hedef networke gönderecek en hızlı yolu bilmesi gerek. Bunu kendi hesaplıyor. Bunun için bir aşağıdaki gibi bir routing table oluşturuyor. Hedef adresi, gönderim protokolü,

gidiş süresi yani cost, bir sonraki router IPsi port numarası gibi bilgiler var.

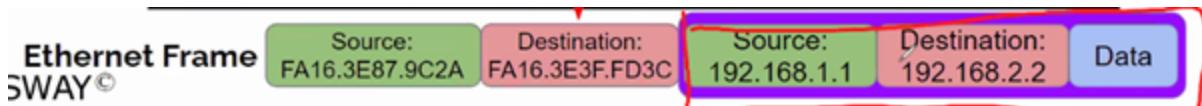
```
[Comware] display ip routing-table
Routing Tables: Public
Destinations : 7 Routes : 7

Destination/Mask Proto Pre Cost NextHop Interface
10.2.0.0/18 OSPF 10 110 10.1.1.5 Vlan3
10.2.64.0/18 OSPF 10 130 10.1.1.13 Vlan5
10.2.128.0/17 OSPF 10 30 10.1.1.5 Vlan3
10.2.192.0/17 OSPF 10 40 10.1.1.13 Vlan5
<-output omitted->
```

Paket internetten farklı bir adrese gönderilirken ilk önce aynı networkte olup olmadığına bakıyor sistem. Bunu da Network IPlerini kıyaslayarak yapıyor. Bunun için ARP tablosuna bakıyor. Aynıysa Alıcı adresine Host ID yazabilirdik.



IP paketini Layer 3 te bir frame içine koyuyor. Daha sonra Layer 2 de Ethernet frame i oluşuyor



Time to Live (TTL): Bir paketin ömrü. Her router da 1 azalıyor. 0 larnırsa paket çöpe atılır.

TROUBLESHOOTING

Ping : Karşındaki hostun ayakta olup olmadığını sorguladığımız komut. Cevap gelirse karşı bilgisayar açık ancak gelmezse kesinlikle çökmüş diyemeyiz.



SUBNET SORU ÇÖZÜMÜ

Firewall kuralları belirlerken dikkat!

Üstteki kural alttakini ezer. Yani sıra ile bakmak lazım