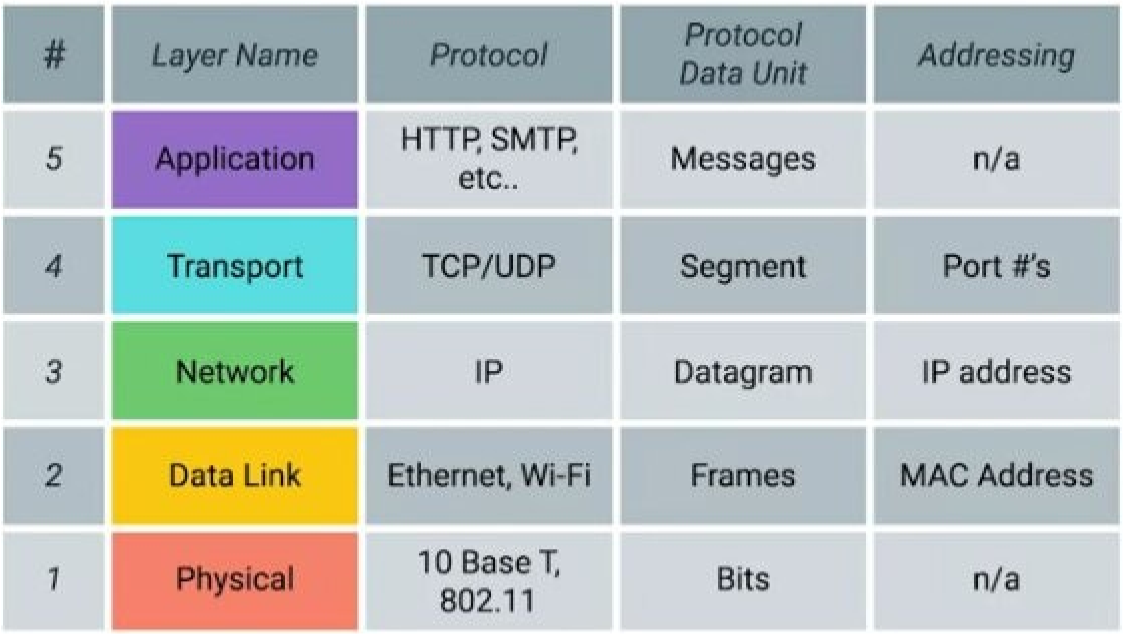
TCP IP FIVE LAYER NETWORK MODEL

To really understand networking we need to know all the thing that is involved from cable to the protocols there are a lot of models thats describes how a computer communicates with other like

1)OSI model
2)DOD model
3)TCP/IP model

we are going to talk about the TCP/IP model



#	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc..	Messages	n/a
4	Transport	TCP/UDP	Segment	Port #'s
3	Network	IP	Datagram	IP address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

lets start with the physical layer.
Its just like it sounds when we talk about the physical layer we ment the hardware that connects the computer it can be the different cable and their specifications and their connectors.

Then comes the data link layer in the data link layer we apply our strict protocols. actually the data link layer is responsible for interpreting this signal in a common way that every network devices can communicate with each other.Lots of protocols are exists in this layer .But the most common on is the **ethernet.**Although the wireless become more and more popular.The ethernet standerds also define a protocol responsible for getting data to node on the same network

Then comes the network Layer.It allow multiple /different network to communicate with each other through the devices known as router.one of the most popular example is the internet

[remember data link layer responsible for a single link on the other hand the network is responsible for a bunch of network. If you think about the Client and Server Its the network layer that helps to do that]
but what protocol is used in the network layer??

IP [internet protocol] ip protocol is not a connection oriented protoccol like TCP because it dot give us the confirmation for the data receive.IP is the heart of the internet and most smaller networks around the world

Then comes the transport layer.Ever wonder that you are on the same router wifi using you devices and even so your mail comes to your mail client and if you run a server it data will go to the server (even you are on the single node) Thats because of the transport layer.

Network layer gives the data to the node The transport layer figure out which client and server supposed to get the data.the protocol that is used in the Transport layer is the TCP protocol.

[other transport protocol also use the IP like udp too.but TCP is the protocol that ensure that the data is sent correctly on the other hand the udp dont]

then come the application layer.they are the applicatoion like firefox like different software

NETWORKING DEVICES AND NETWORKING CABLES

.

Lot of different cables and network deviecs are used to communicate with different network

lets talk about different network components of a wired network
1)cables: cables connect different devices to each other allowing the data to be transmitted over them. Most of the network cable are divided into two categories copper and fiber.copper cable are the most common for the networkig cables.They are made up wuth multiple copper cable inside the plastic wrapper/ insulators.you already know that computer communicate in binary form in the cable the binary data is sent by changing the voltages.the system at the receving end can interpret the voltage change as binary ones and zeros.the most common cable are the cat5,cat5e and the cat6 cables

this cat is known as category this category is separated by different categories also like the transfer rate and the different twisted.the cat5 is old tech and mostly replaced by the cat5e.and cat5e is replaced by the cat6.They maybe look like the same but for the data sending speed are very different .

Cat5 had a problem in its cable which is called CROSSTALK

WHAT IS CROSSTALK

when an electric pulse in one wire is accidentally detected by another wire .so the receiving end cant understand whats the data is because of the network error.Higher lavel protocol have functionality for detecting the missing data and asking a request for them but this process takes more time but the CAT5e does this thing very less thats why more data can be transferred win CAT5e is a given time

CAT6 cable are more strict to crosstalk .Cross talk is very very less in the CAT6 cable thats make it more expensive They can transform more reliably and in more speed BUT there is a problem too.because of the internal structure of the CAT6 cable it has a shorter maximum distance when data is sending on max speed

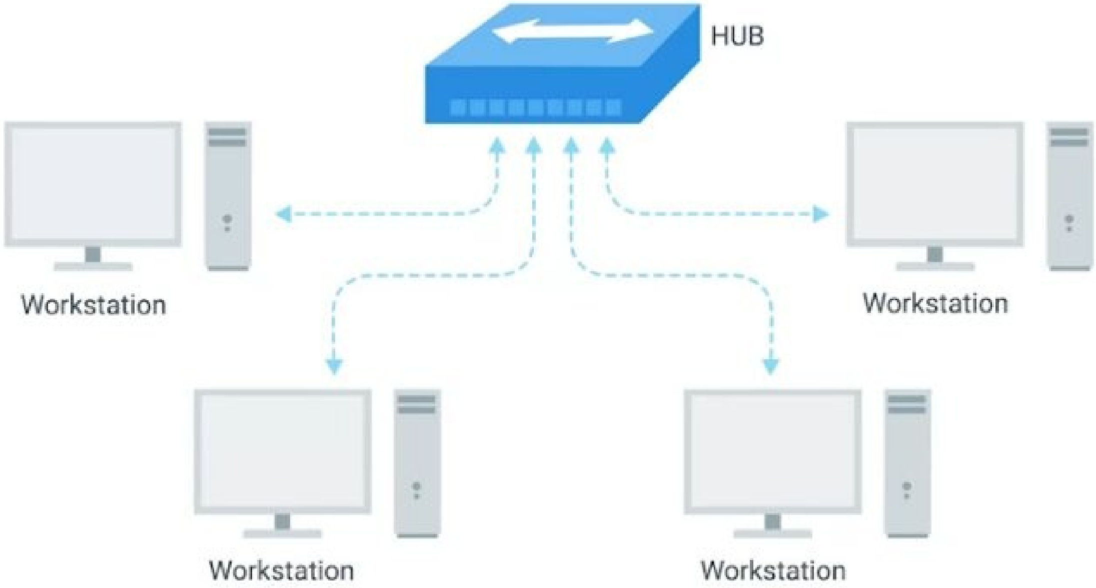
THEN COMES THE FIBER which isn a short form of the fiber optic cable

Fiber cables contain individual optical fibers which are tiny tubes made out of glass about the size width of a human hair.

Copper cable uses voltage change and the fiber use the pulse of the light to transfer the data. fiber is preferable in a place where there is a lot of electrical and magnetic interference fiber cable can transport more speed and more distance but they are expensive and fragile

HUBS AND SWITCHES

cable allow you to make a point to point networks but it works on a single devices on each side .it is not very useful when a lot of computer try to reach each other. There are network devices that allow multiple node to connect with each other .one of the simpliest devices is the HUB.HUN is a physical devices that allow a computer to communicate with multiples computer at once



all the devices connected to the hub is end up talking with all the computer at once.But the node have to check every single time that the data that is broadcasting by another computer is ment for it or other .if meant for it then accept other wise reject.This cause a lot of problem and make a collision domain.

WHATS A COLLISION DOMAIN:

remember in a network segment only one devices can communicate at a time but if the multiple system try sending data at the same time.the electrical pulses sent across the cable can interfere with each other. Because of this situation the computer have to wait until they gat a chance to send the data.it casuse a lot of time and slow down the data communication process.thts why the HUB are not used

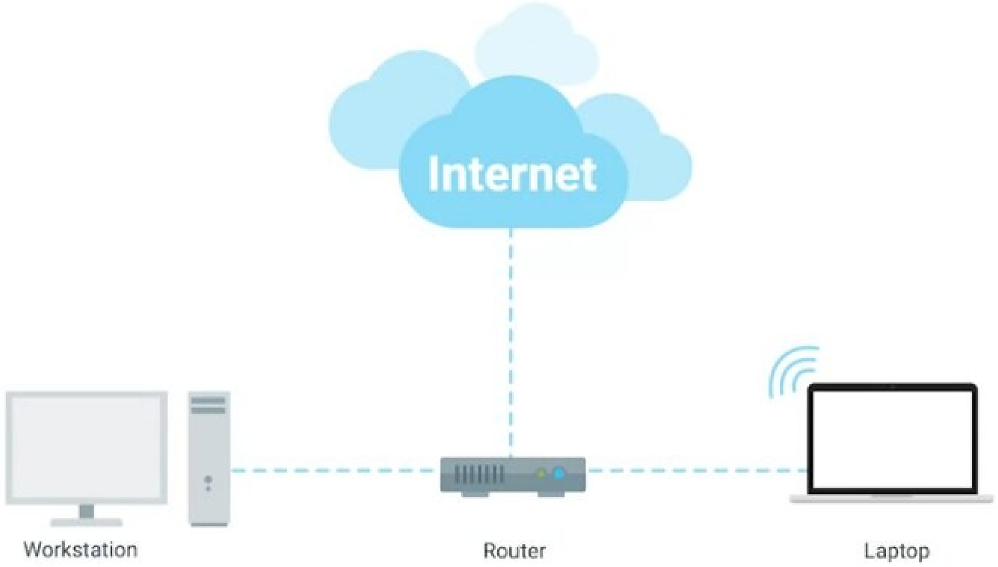
[REMEMBER HUB IS A PHYSICAL LAYER DEVICES]

on the other hand the Switchs are a little bit different than the hubs [SWITCHES ARE IN THE DATA LINK LAYER] and for that the switch can aactually inspect the data and determine which computer it has to send and then only send to that computer .that reduces the collision domain and the size of the data that is sending

ROUTERS

HUBS and SWITCHES are used to connect computers on a single network usually referred to the LAN or LOCAL area network.but sometimes we need to send data on other independent network.thats where the routers come .
Routers are the devices that knows how to forward data between independent networks

HUB is a layer 1 devices
SWITCHS are layer 2 devices
and the
ROUTER is the layer3 (network layer) devices



like a switch A router can inspect IP data to find where to send this data.Router store Routing table with different network address find out where to send the data

Most common are the home use or small office.these kinds of routers dont have a very detailed routing table.Their main target is to take data from home/office and send them to the ISP(internet service provider).once its in ISP then more sophisticated router takes over .These core routers form the backbone of the internet.and these router are responsible for how we send and receive data every single day.These are the core routers and they have to connect to many other routers and they have to make a decision in which router that have to send the data in a particular time

Router Share data between the each other with a protocol name BGP (Border Gateway Proticol) this protocol allows the router to find the most optimal path to forward traffic.

When you open a browser and visit a website the data have to pass a lot of routers to get to your computer. Routers are the guide to find the right place in the complicated internet

SERVER AND CLIENT

we used the word server and client very often but it has a larger meaning in the network.
We are calling these in one word is node.
What is a server:
server is some that provides data to someone who is requesting this
and client is simply who is requesting this or reciving the data
so why we use the term node. because individual application inside a computer can act like a server or a node at the same time .In the communication system most devices are not exactly a client or a server they can be both at the same time depending on their

purpose.for example suppose you are running a email server so this is a server no doubt but this can be a client of Other DNS server. To make this distinction that is it a server or a client you have to understand what is its primary purpose.we use the word server and client to identify the primary purpose of that node.when a node can be a server and a client depending on different point of view for example for serving email that email sevrer is server but fro the DNS server point of view that email server is actually a client

A physical layer is responsible for sending bit from one computer to another computer

whats a bit?
A bit is the smallest representation of data that a computer can understand. its either one or zero.it does not matter what are you sending or receiving .you can send a email but in the lowest level you are just sending ones and zeros.a standerd copper cable when connected between two devices are carrried constant electrical charges and by changing the volteage across the cable they send the data

MODULATION

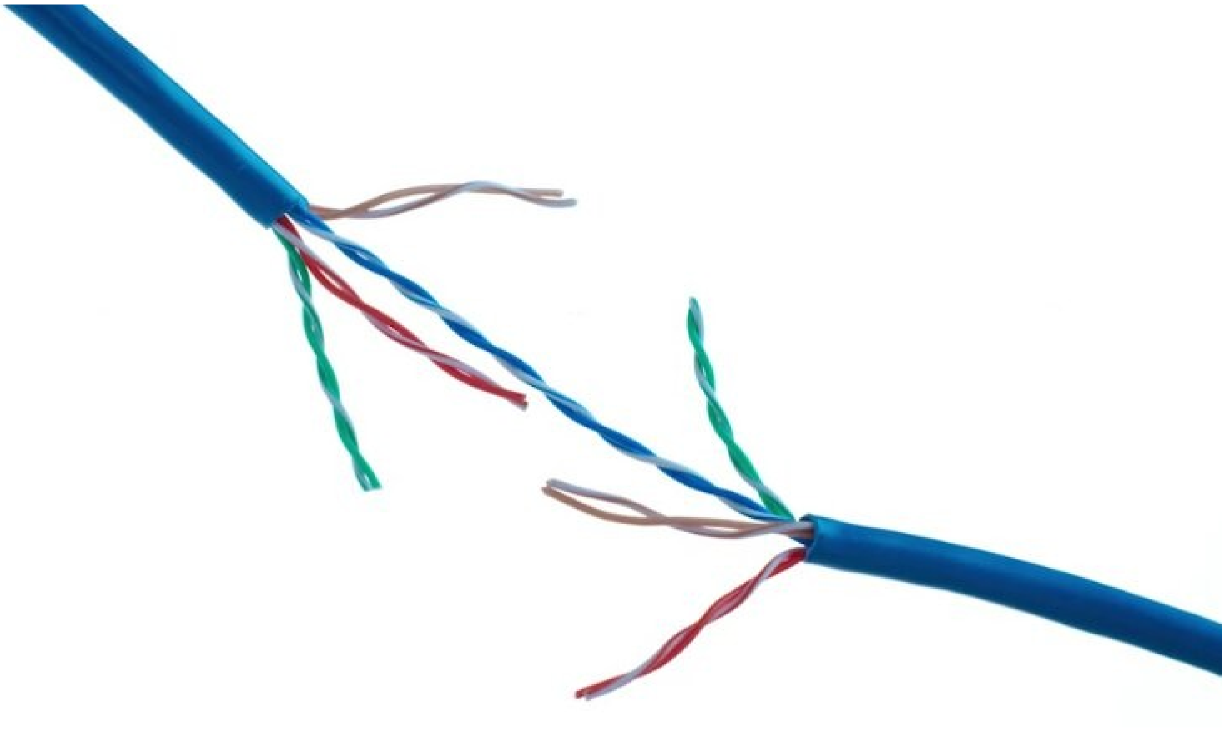
A way of varying the voltage of the charge moving across the cable is called modulation.this is bacically and electrical engineering term when we are talked in the networking area we call that a line coding

LINE CODING

line coding allow devices on either end of the link to understand a specific state as 0 and another state as 1 with this simple technique mordan network can send 10 billion 1 and 0 acceross the tiny copper cable every second

TWISTED PAIR CABLE

The most common tye of cable for communication is called twisted pair cable.it is called twisted pair because it fetures pairs of copper wires that are twisted togather for a special purpose.this twisted nature protect against the electromagnetic interference and crosstalk from neighbourng pairs.these pairs act like a single conduit of information



exactly how many pairs are going to used depends on the transmission technology .But no matter what technology we use we must ensure that we have to ensure the duplex communication.

WHAT IS DUPLEX COMMUNICATION

The concept of the duplex communication is that information can flow in both direction across the cable

on the other hand the SIMPLEX communication is the unidirectional communication

duplex communication example can be the phone call or mobile communication.

And the simplex communication can be like televesion transmission

the way that networking cables ensure that duplex communication is possible is by reserving one ortwo pair of cable communicating in one direction and then use the other one or two pair for communicatng in the other direction.This is known as a full duplex.
If there is some wrong with the full duplex you can see the it is reported as the hals duplex communication.

WHAT IS HALF DUPLEX

in half duplex both side can communicate with each other but one device at a time like a walki talki

NETWORK PORT AND THE PATCH PANEL

the final steps of how the network layers take place take place at the end points of out network links.Twisted pair network cable are terminated with a plug that takes place that takes the individual internal wires and exposes then.The most common plug is the rj45 connector(registered jack 45).it is the most common plug by far.a RJ45 cable can connect toa rj45 network port

WHATS A NETWORK PORT

Generally a network port directly attached to the devices that make up a computer network

switches and hubs have a lot of the network ports because their work is to connect to a lot of devices but the workstation or server may have one or two network port .

Most network port have two small LED one is the link light and the other is the activity light.the link light will glow only if the cable are properly connected to the two nodes and the activity LED will glow if there are transmission going on.the port light can help you to troubleshoot the fault in the network

ETHERNET AND MAC ADDRESS

although the wireless network is the most common in the home and small office but the data center and the server are always work with the network cable.the mainpurpose of the ethernet protocol and the data link layer is to abstract away the the need of care which hardware it is going to used in the physical layer.So when the data link layer takes this responsibility the upper layer no longer have to worry about the physical layer no matter what layer they have the transmission application and the internet layer works the same.

If you browse the internet with browser your browser does not need to know wither you use the wireless connection or the wired connection

HOW THE SWITCHES DETECT THIS COLLISION IN THE NETWORK

The switches use a technique called CSMA/CD

WHAT IS CSMA

CSMA stands for Carrier Sense Multiple Access it checks if the network or the port is clear for the transmission of the data,If there is no data to transmit the computer is clear to send the data .if multiple connection is detected at the same time then it stop sending data it send the computer a signal to wait until the path is clear

but now a question can arise

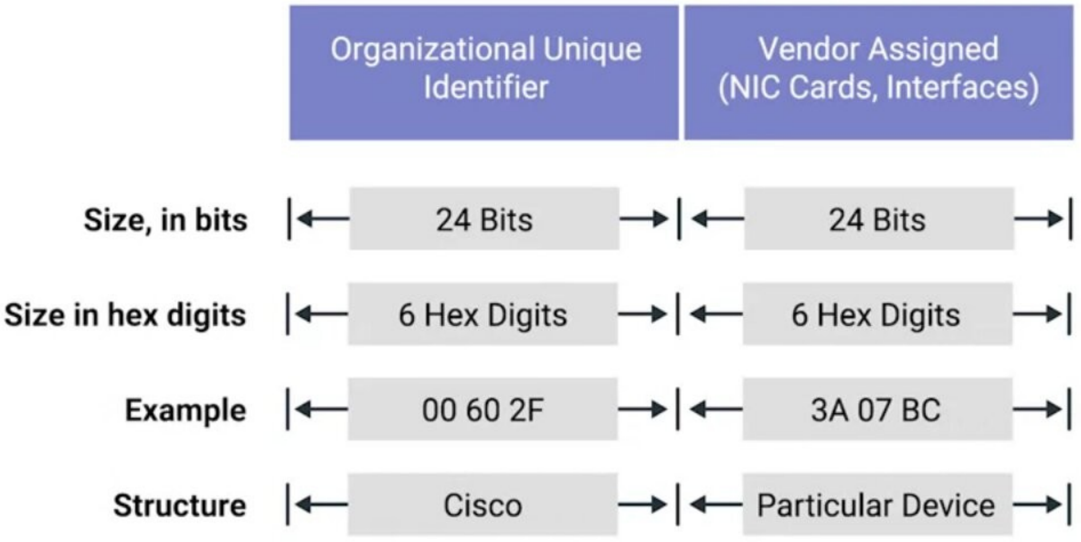
HOW THEY DETECT A NODE?

Uinng MAC address.MAC address is stands for media access control. A mac address is a globally unique identifier attached to a individual network interface .every mac address in every device is unique

its a 48 bit [MAC ADDRESS HAS 6 OCTETS]number normally represented by six grouping of two hexadecimal numbers the mac address are divided into two groups

first three octets of a MAC addres is known as

OUI



	Organizational Unique Identifier	Vendor Assigned (NIC Cards, Interfaces)
Size, in bits	24 Bits	24 Bits
Size in hex digits	6 Hex Digits	6 Hex Digits
Example	00 60 2F	3A 07 BC
Structure	Cisco	Particular Device

IEEE assign them to different organization and the rest of it is vendor assignment

[IMPORTANT:YOU CAN FIND THE VENDOR OF A NETWORK CARD JUST BY USING THE MAC ADDRESS]

Ethernet uses MAC address to ensure that the data it sends has both an address for the machine that sent the transmission sa well as the one the transmission was intended for

UNICAST MULTICAST AND BROADCAST

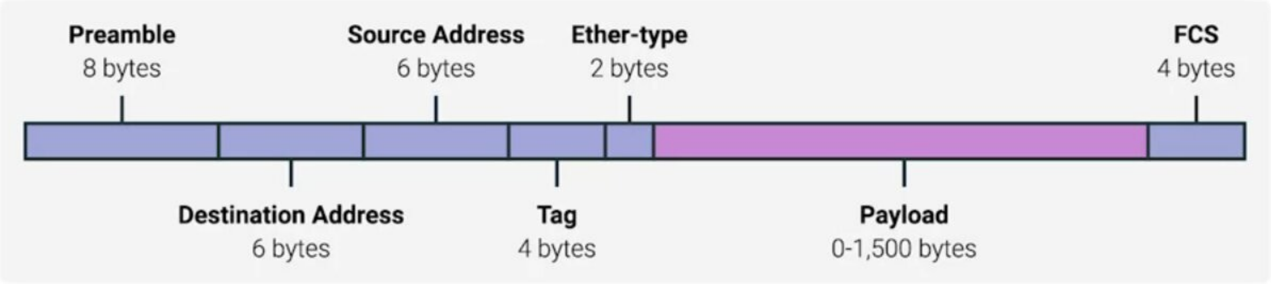
if one devices transmit to only another devices it is called a unicast transmission.
A unicast transmission is always ment for just one receiving address.
At the ethernet level it is done by this way
if the data that are sending to a MAC address and the last bit (least significan bit) is zero then this transmission is intended for this protocol.
How this is send?
Well it send to every body only the selected mac address will discard it

but what happen If it is not zero.well if it is 1 then It called a multi cast address that means it is intended for multiple clients and it is detected by the other portion of the MAC address

The third type is called broadcast.Braodcast means it will be send and accepted by everyone.why it is needed?

It is used to make familiar with every node with every noode.It is used for ARP protocol

ETHERNET FRAME



DATA PACKET

data packet represents a set of binary data that being sent across a network link.its just a set of data sending one part to another

ETHERNET FRAME

A highly structured collection of information presented in a specific order.With this structured information the network interface at the physical layer can convert a stream of bits in to meaningfull data the first part of the Ethernet Frame is called the Preamble

WHAT IS A PREAMBLE?
Its a 8 bytes or 64 bits long and can be splitted into two sections.
The first 7 bytes are the series of ones and zeros it helps the network interface to synchronize the internal clock they use.to regulate the speed

the Second byte in preamble is called SFD (Start frame delimiter

it give signal to the reciving devices that the preamble is over and that the actual frame contents will now follow

AFTER THE PREAMBLE THERE ARE DESTINATION MAC ADDRESS

the hardware address of the intended recipient

THEN COMES THE SOURCE MAC ADDRESS

the address of the sender

[remember the address is 6 bytes long

THEN COMES THE ETHER TYPE FIELD

16 bits long and used to describe the protocol of the contents of the frame

THERE CAN BE SOMETHING CALLED VLAN HEADER TOO

IF A VLAN HEADER IS PRESENT THE ETHER TYPE FOLLOWS IT

WHAT IS VLAN??

vlan is a technique that lets you have multiple logical Lan operating on the same physical equipment
any packet with vlan tag will be relayed by the switched to that specfic VLAN
we talk about VALN in the upcoming slide

AFTER THAT THE PAYLOAD COMES IN

PAYLOAD is the real data that are goinf to transported .all the things that are we taking about before the payload is in the header payload is something that is other than header.it can be 46 to 15000 bytes long.this contain all the data

THEN COMES THE FCS

FCS STANDS FOR THE FRAME CHECK SEQUENCE
A 4 bytes or 32 bit number that represents a checksum value for the entire frame

WHAT IS A checksum value?
The checksum value is calculated by performing whats known as a cyclical redundancy check against the frame

on now whats a Cyclical Redundancy Check??
its an important conecpt of data integrity and is used all over the computing not just network transmission

if you calculate the CRC of a data you will end up the same checksum data if the data is un courrepted data.
[CRC is used to just check the data that the other end receive is the same that is sent by the sender]

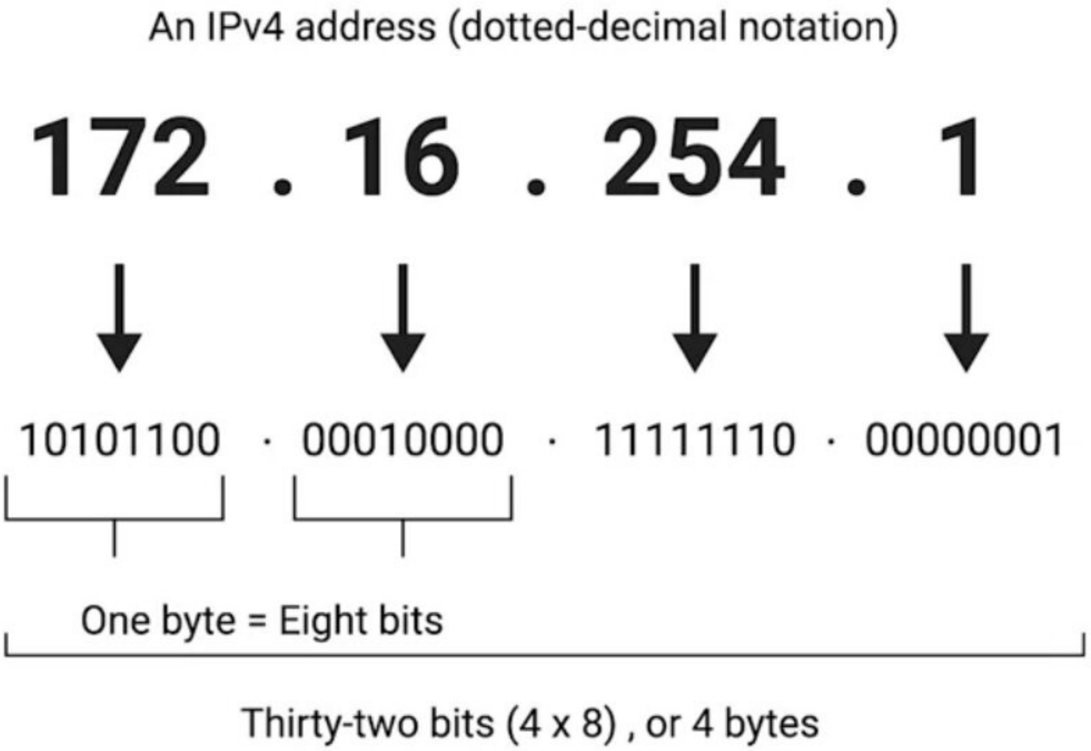
when a netwoek interface is ready to send the data
it collect the destination address and ethernet type and the vlan tag then collect the data then apply CRC on the data and kept the checksum in the FCS part then send the data to the sender.then the sender will apply

another CRC on the data and match the generated checksum to the senders checksum if the checksum does not match the data is thrown out. and a request is send to resend the data

INTRODUCTION TO NETWORK LAYER

we know that the MAC adddress is unique so every network card in the world has a unique number.so in a Local area network the switch can remember the MAC address and then just forwared the data in the preffered destination.but what about the whole wrold ? What happened if you want to send a messgage to a friend whois at the other side of the world.you dont know which network card he is using and even you know the MAC address is not given in any order and there is no way that you can identify the location of any node using the MAC address so you need another approach which is the IP address

IP ADDRESS

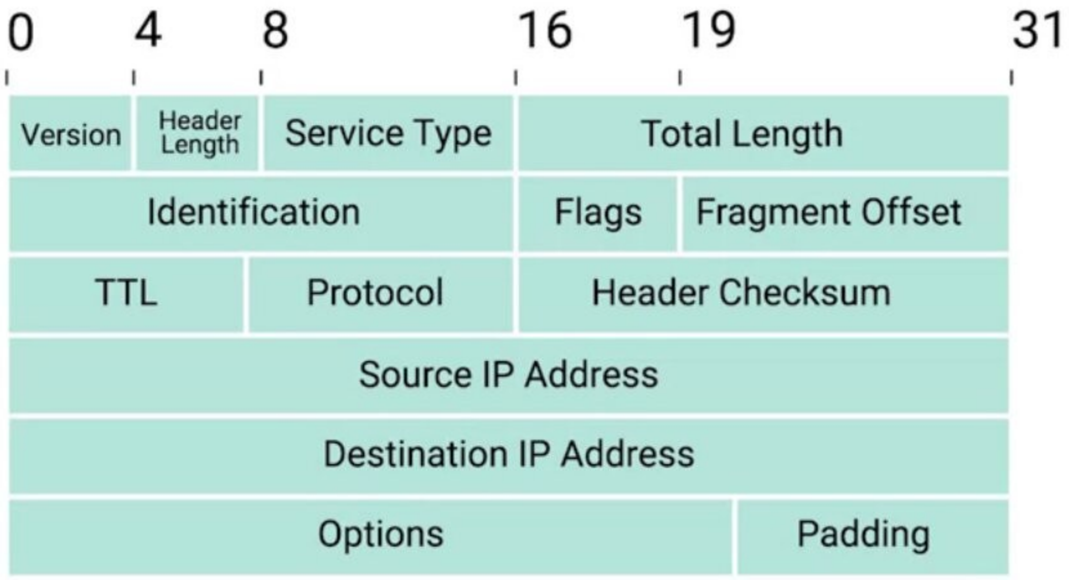


ip addrress are 32 bits octet.means 8 bit of data a single octet can represent decimal data from 0 to 255.ip address is distributed in large section in different organization. IP address is hierarchical . One of the most important thing is IP address belongs to a networks no the devices that means if you change the network your ip address will change.but your mac address will not change.you may never set ip address in your laptop you just connect to your wireless network and start working ever wonder how your laptop got an ip address??.its because mordan networks used DHCP (dynamic host configuration protocol) so your laptop will automatically get an ip address and all other configuration to be a part of the network.but you cant do it on a server becayse server needs a static and permanent address .for server you have to give static address

IP Datagrams and Encapsulation

data packets in the ethernet layer known as the ethernet frames . And data packets in the network layer known as another name called ip datagram.the maximum size of the ip datagram is the largest number that you can represent with 16 bits which is 65535.

ip datagram is a highly structured series of fields that are strictly defined



0 4 8 16 19 31

Version | Header Length | Service Type | Total Length

Identification | Flags | Fragment Offset

TTL | Protocol | Header Checksum

Source IP Address

Destination IP Address

Options | Padding

two primary section in the ip datagram is headers and payload the first field is

1) version : uses 4 bits and it shows what version if internet protocol is used (ipv4 or ipv6)

2) headerlength: this is also a 4 bit field that shows the length of the total header length
[remember the minimum size of the header length is 20 bytes.it is impossible to store all the header information in less than 20 bytes]

3)service type: this is a 8 bits of information and it stores the quality of operation

5) Total length: this is a 16 bit filed called the total length field.it indicate the toal length of the ip datagram

6) identification field: identification field is a 16 bit number thats is used to group messages together.if for some reason the data you sending needs to sen is larger than what can fit in a single datagram.the IP layer needs to split this data up to many individual packets.so then the receiving end it will know with the help of the identification number that these data packets are under the same transmission

7) flag fild: now when we talk about the fragmentation .there is a field that is called flag field that indicate if the data gram is allowed to be fragmented.or it shows if the datagram is already fragmented.

8) Fragmantation offset : supoose your network devices is configured with a specfic fragmentation size and it enter another network devices that has smaller fragmentation size .then the datagram have to be fragmented into smaller datagram.so the fragmantation offset will cobine them with corrcnt order

9) TTL (Time To live) field:

An 8 bit field that indicates how many router I will traverse before its thrown away.it is very necessary to solve the forever loop.every time pachet reach the router it TTL filed decrement by one so when it becomes 0 the data packet is thrown away it no longer routed to another router.

Suppose your router has a misconfiguration .so ti send the data to the router it coming from so it will create a loop data will be go back and forth and create problem in the network.so TTL prevents that.even there is a misconfiguration the data packet will be thrown away after the ttl is going to be 0

10)Protocol: Protocol is another 8 bit field that contains the data about what transport layer protocol is being used.the most common is TCP and UDP

11) Header Checksum : Header checksum field is another field that contains the checksum of the entire datagram header.it works like the ethernet frame checksum

12)Source IP address: its 32 bit long ip address that gives the source ip address

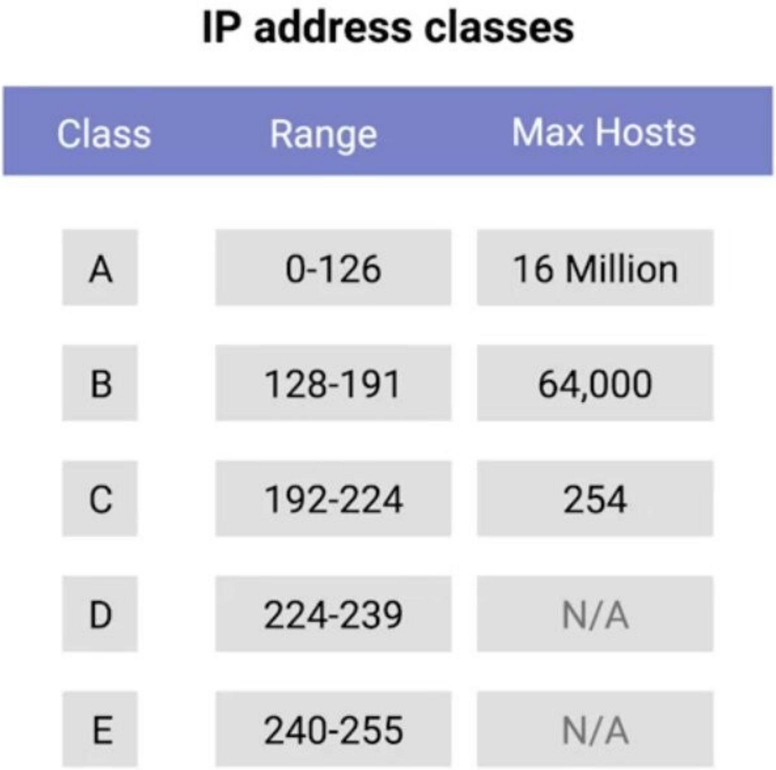
13)Destination Ip address: 32 bit destination ip address

14)IP options field: An optional field that is used to set special characteristics for data grams primarily used for testing purpose

15) padding: padding filed is a series of 0 to make sure that the data is the correct total size

[RELATION WITH THE IP DATAGRAM AND THE ETHERNET FRAME]

REMEMBER the payload section in the ethernet data frame is the ip datagram.This process is called encapsulation. The entire data of the ip datagram is encapsulated as a payload in the ethernet frame. But remember the ip datagram also has a payload section



IP address classes

Class	Range	Max Hosts
A	0-126	16 Million
B	128-191	64,000
C	192-224	254
D	224-239	N/A
E	240-255	N/A

ip address can be split into two sections:

1) Network ID
2) Host ID

ADDRESS CLASS SYSTEM

address class system is a way of defining how the global IP address space is split up threre are three primary class

→ class A
→ class B
→ class C

class A → first octet used for the network last three use for the host address

class B → first two octet used for the network and the last two octet is used for the host

class C → first three octet used for the network and the last one octet used for host

if the very first bit of an ip address is 0 it belongs to a class A ip address

if it is 10 then it belongs to class B network

if the it is 110 then it belongs to clas C network

there are two other class

class D and class E

class D range is 224-239 and it is used for multicasting

and class E are reserved for testing purpose

But in the Paractical life this system is actually replaced by a system classed CIDR

CIDR (Classless interdomain routing)

So now you know the ip address and the network layer and MAC address at the data link layer
now you can combine those with another prtotocol called ARP . Lets see how to find your destination using ARP

ARP

ARP is a protocol used to discover the hardware address of a node with a certain ip address

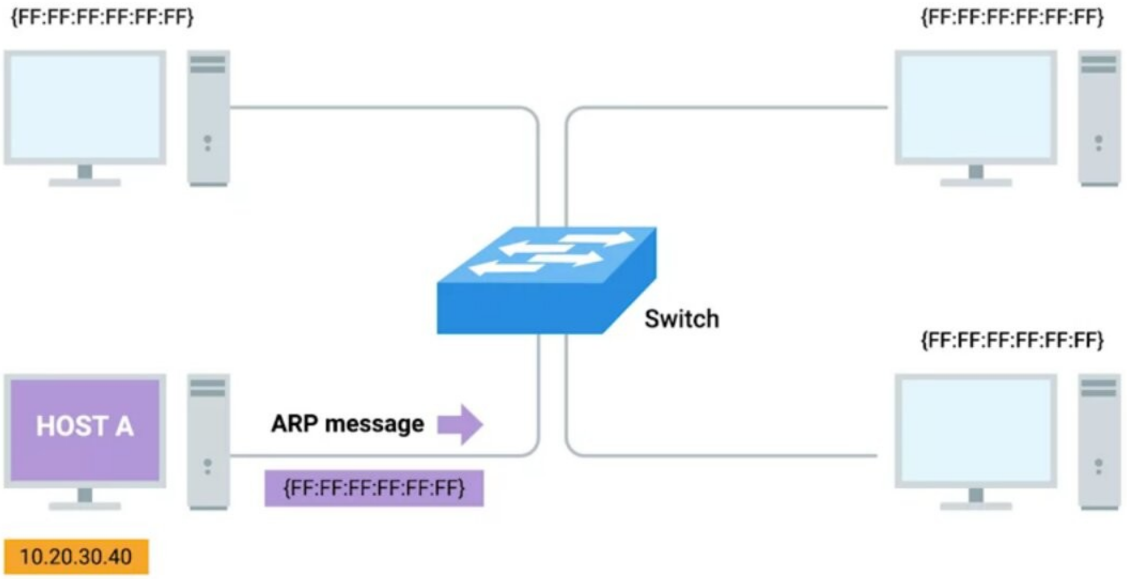
ARP starts for adress resolution protocol.you already know that the IP datagram is encapsulated in the ethernet frame.so the transmitting device needs a

MAC address to complete the trasmission.so how to find the mac address then??

ans :
using ARP table

ARP TABLE

a list of ip address and the MAC address associate with them



suppose the host A try to send an information to

10.20.30.40 thse things will happen

1) it will send a Broadcast message to the network

(its like announcing “is anyone in the network has ip 10.20.30.40”)

2)then the device with ip send a reply message called arp response and in the arp response it will give the MAC address

(like telling yes I am here and here is my MAC address)

3) then transmission device know the MAC of the destination ip

4) they also store the mac address in their local arp table so they dont have to broadcasr a arp request everytime.

[But remember Arp table enrty is not parmanent it expires after a short ammount of time.to ensure the change in the network]

SUBNETTING

The process of taking a large network and splitting it up into many individual and smaller subnetworks is called subnetting as you know them the address class system divide the total ip address in to groups.but you can see that the that a class A ip addres has almost 16 million user you can easily understand that you can never connect this ammount of user in a single router. So now we are goining to devide them further and each of the segment have their own gateway router to communicate with each other .

SUBNET MASK

A ip address is a 32 bit number and some portion is used for the network and the rest is used for the host portion .when you are dividing the network even further some portion that are used for the host id may used for the network.and to to do this a new concept arrived which is subnet ID.subnet id is calculated by SUBNET MASK

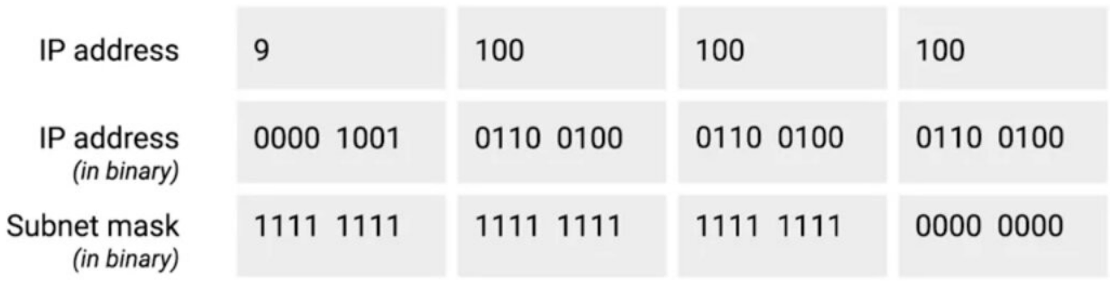
WHAT IS SUBNET MASK?

Subnet mask is a 32 bit number that are normally written out as four octets in decimal
that separate the network id and the host id

lets see an example to see this clearly. Suppors an ip address is 9.100.100.100

you can easily remember that it is a class A ip address.and the first octet is used for the network id and the last three octets is used for the host id.

But what if I want to use the first three octets for network id and the last one for host id like a class C address.is it possible? Yes. you can do it with subnet mask



IP address	9	100	100	100
IP address *(in binary)*	0000 1001	0110 0100	0110 0100	0110 0100
Subnet mask *(in binary)*	1111 1111	1111 1111	1111 1111	0000 0000

now if we use the subnet mask as 255.255.255.0
and we can see in the picture if we convert this on binary.we can see that the first three octet is filled with ones and the last is zero.the octet with one will be considered as a network id and the zeros will be considered as a host id.su by using subnet mask you

can explicitly say which one will be network id and which one will be host id .so using this subnet mask we get the total 256 hosts.because asingle 8 bit number can represent 256 different numbers or numbers between 0-255.

but you can use only 254.because the first host id 0 is not used and the host id 255 is used for broadcasting .so just remember that the usable host is 2 less than the total number

now we see that the subnet mask that cover 8 bit in octets .Lets see another ip address that do not cover totally the 8 nits of actets

what will happen if I use 255.255.255.224 as asubnet mask