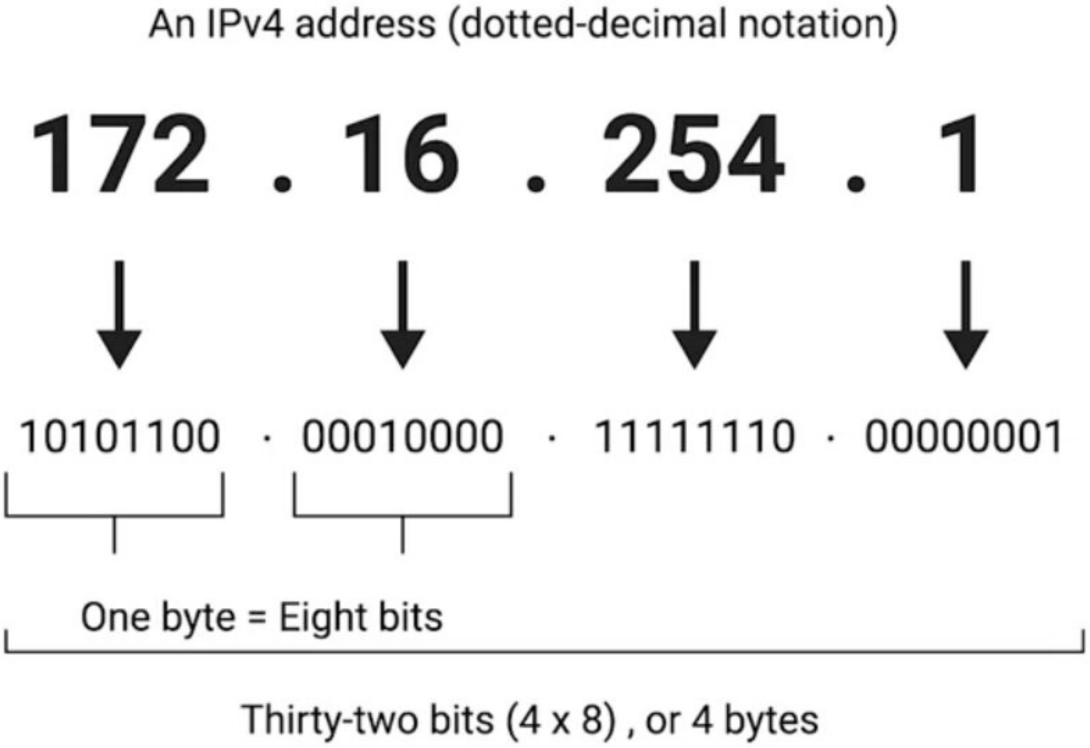
INTRODUCTION TO NETWORK LAYER

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 who is 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

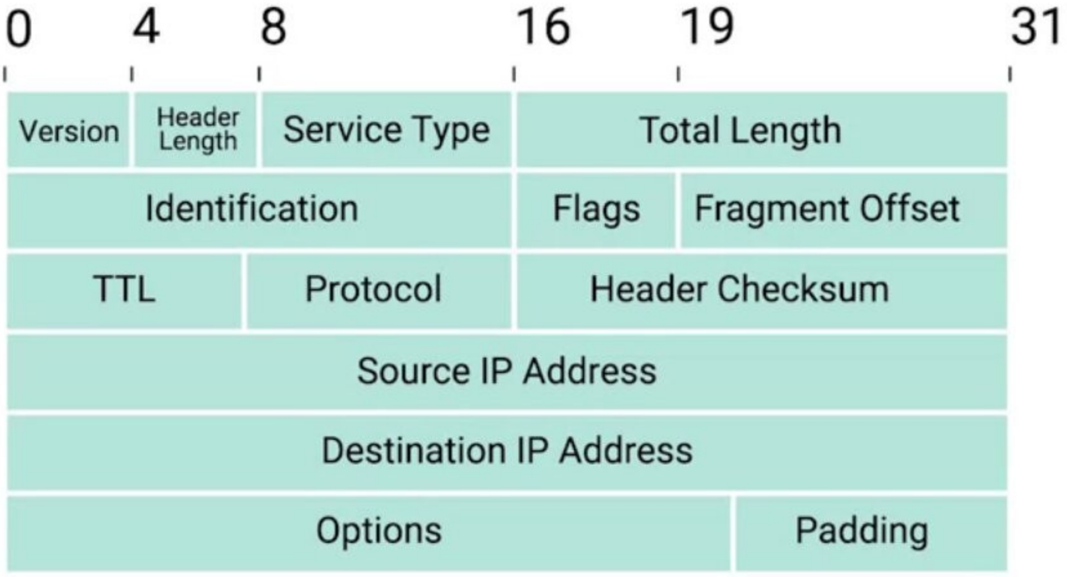


ip addrress are 32 bits octet.means 8 bit of data a single octet can represent decimal data from 0 to 255.ip address is distributed in large section in different organization. IP address is hierarchical . One of the most important thing is IP address belongs to a networks no the devices that means if 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



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) header length: 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 total 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 send 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 specific 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 combine them with correct 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 packet 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 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

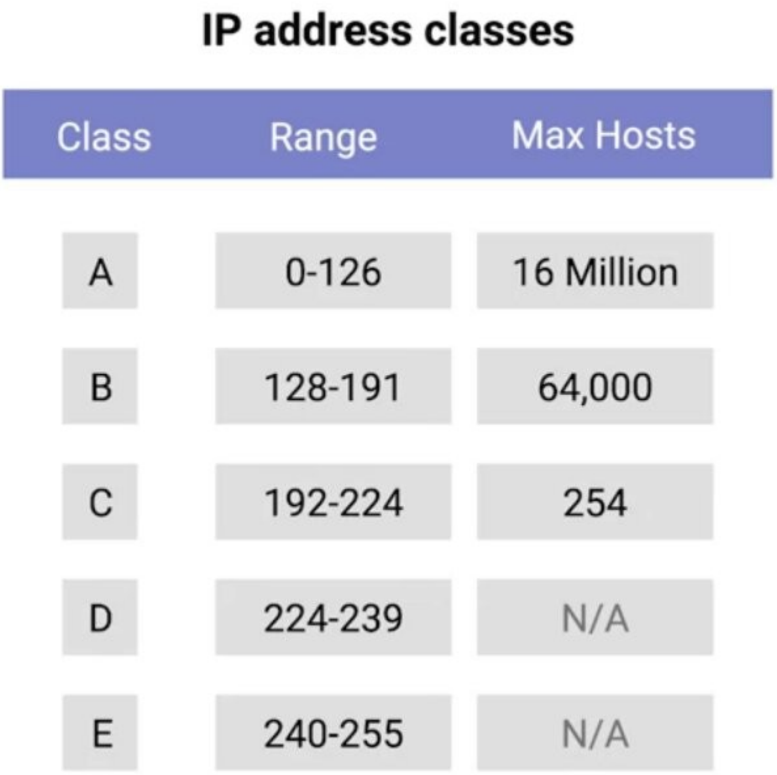
if the it is 110 then it belongs to class C network

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



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

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

CIDR (Classless inter domain 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

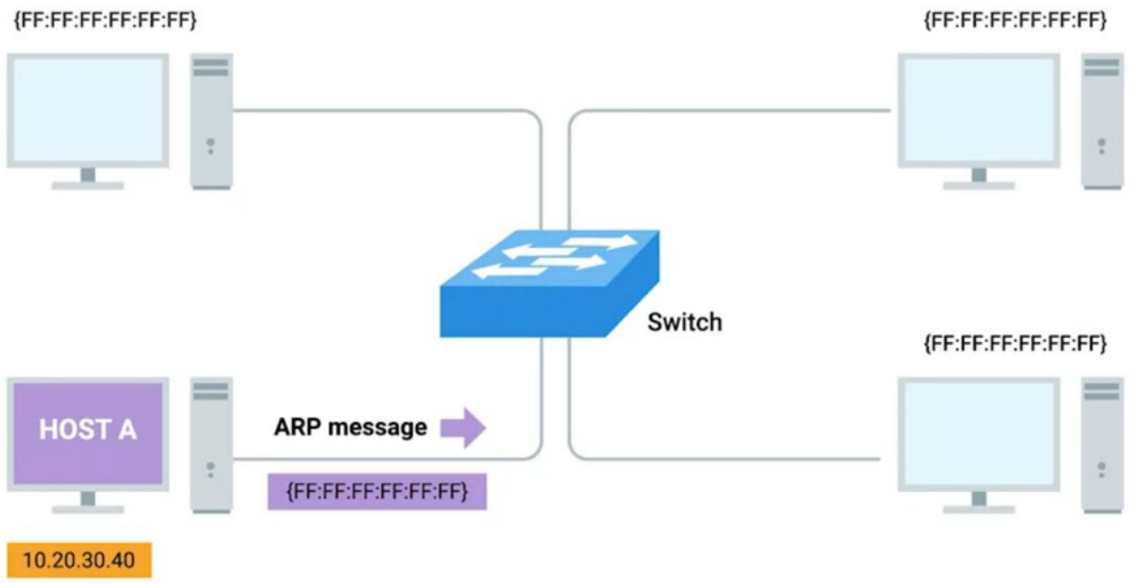
ARP is a protocol used to discover the hardware address of a node with a certain ip address

ARP starts for address resolution protocol 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 subnet works 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 going to divide 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

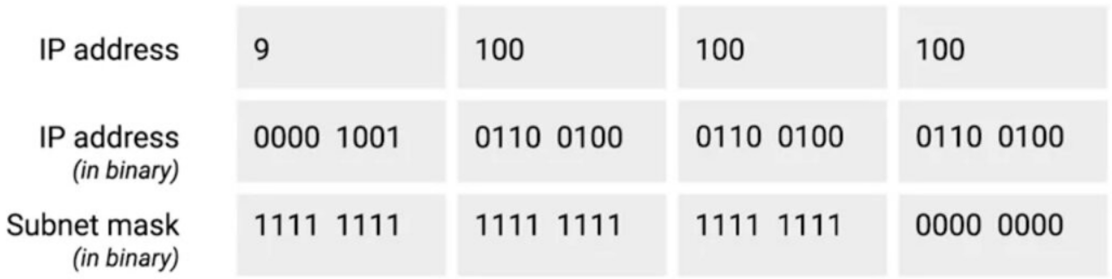
WHAT IS SUBNET MASK?

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



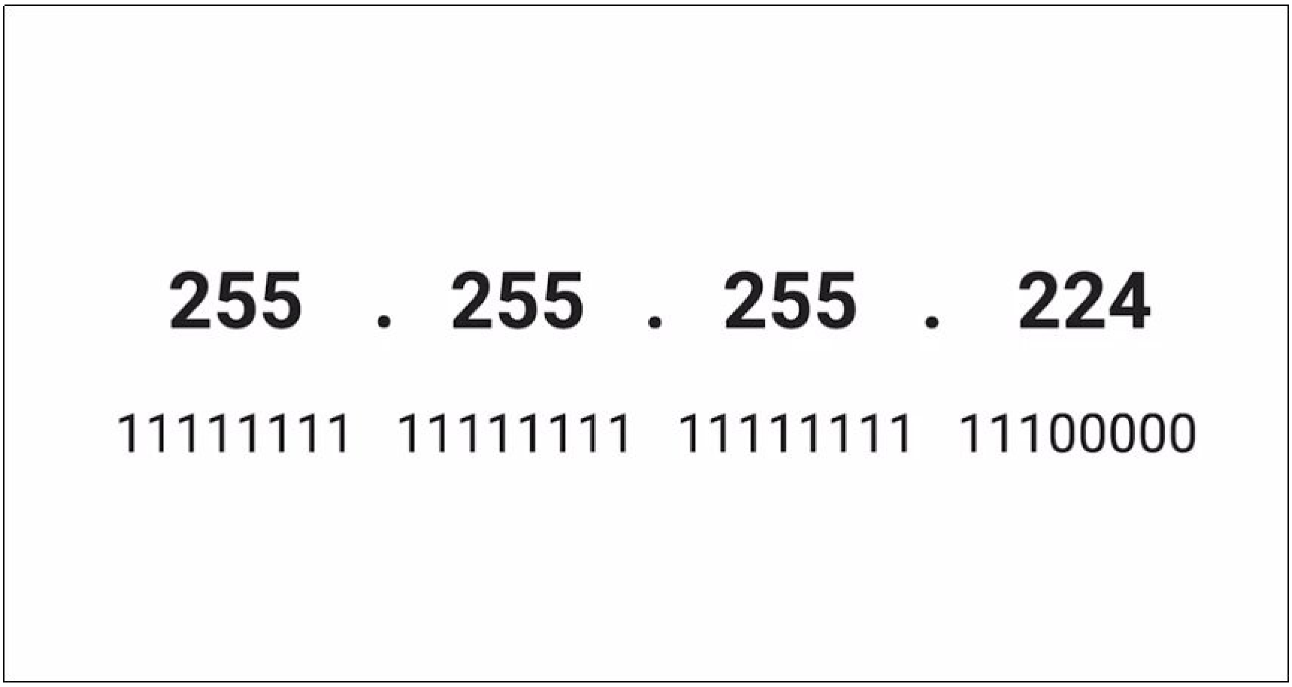
IP address	9	100	100	100
IP address *(in binary)*	0000 1001	0110 0100	0110 0100	0110 0100
Subnet mask *(in binary)*	1111 1111	1111 1111	1111 1111	0000 0000

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.so 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 bits of octets

what will happen if I use 255.255.255.224 as a subnet mask

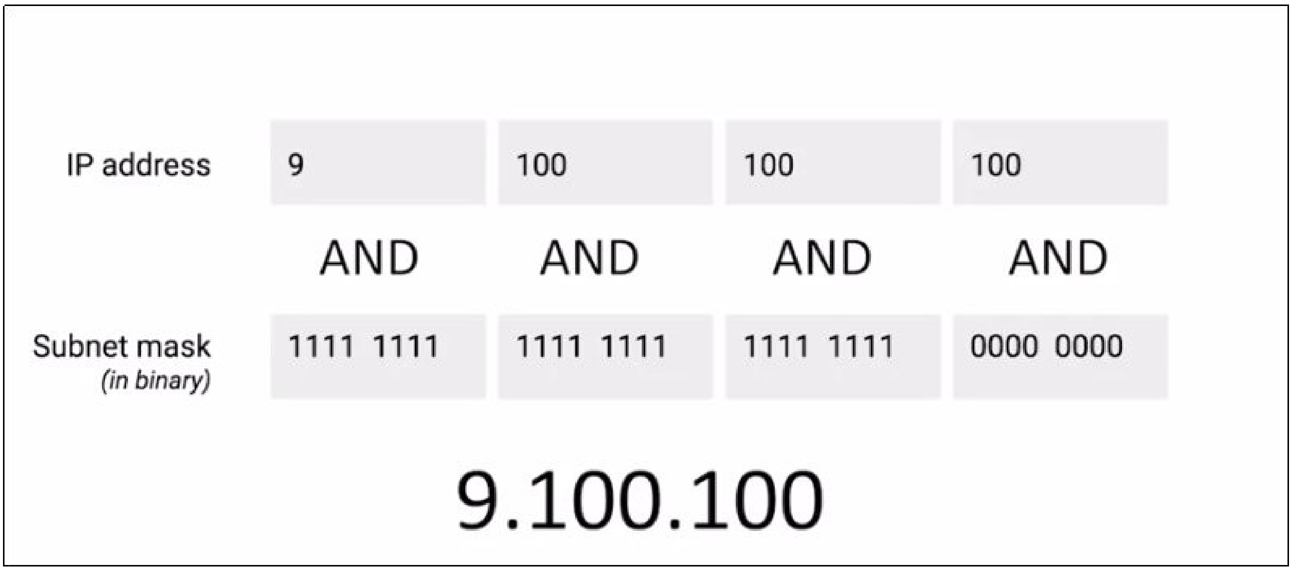


255 . 255 . 255 . 224

11111111 11111111 11111111 11100000

it takes 27 ones and 5 zeros.so if we suppose the ip address is 9.100.100.100 and the number of ones is 27 we call the ip address in a CIDR notations which is 9.100.100.100/27

how to determine the host and the network portion with bits like this you have to do simple binary operation to extract the network and the host id,in fact the computer find the network id and the host id the exact same way

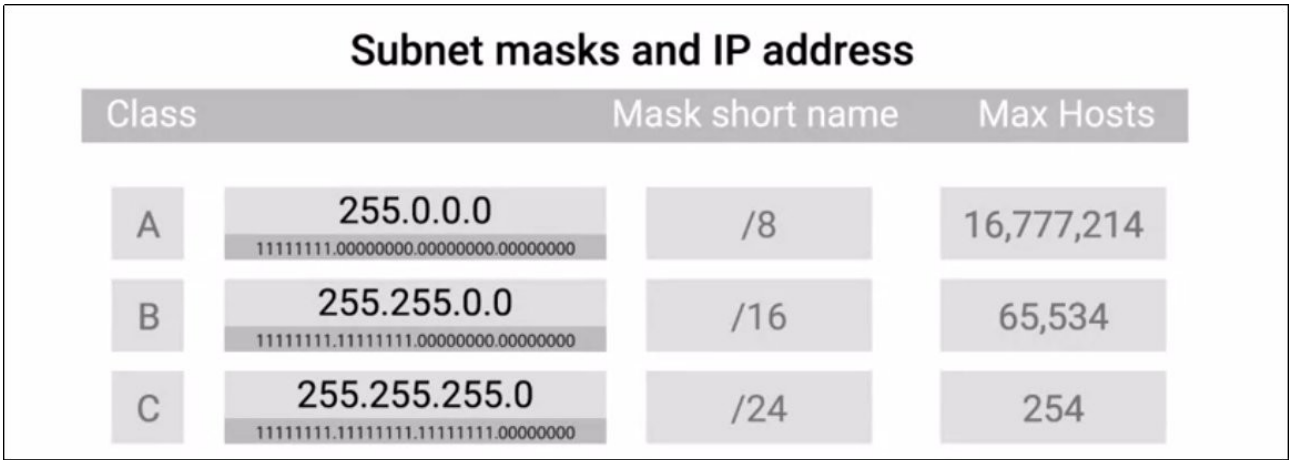


IP address	9	100	100	100
	AND	AND	AND	AND
Subnet mask *(in binary)*	1111 1111	1111 1111	1111 1111	0000 0000

9.100.100

suppose your ip address is 9.100.100.100/27 in the CIDR notation now if you look at the image and perform a binary AND operation you will get the 9.100.100 which is the network id and the rest is the host id

CIDR



Subnet masks and IP address

Class		Mask short name	Max Hosts
A	255.0.0.0 11111111.00000000.00000000.00000000	/8	16,777,214
B	255.255.0.0 11111111.11111111.00000000.00000000	/16	65,534
C	255.255.255.0 11111111.11111111.11111111.00000000	/24	254

254 hosts can be small for use cases but for the class B and the class A there are 65534 and the 16777214 ip address respectively which is a huge number of ip address is very large. And cant be under a single router so most of the time these ip address are broken down into smaller network and multiple class C address is joined togather and routed to the same palce.this is where the CIDR comes .CIDR is used for this doing this . Suppose in a office there are hosts more more than a class C ip address can accommodate so you need two class C ip address could you join this togather and routed to a same palce .yes it is possible you just need to use the the netmask /23.that means the router needs one gateway router to deliver path to all the two different class C network.

Lets do some math to understand whats going on we know for a /24 network with 8 host bit we have the host = 2^8 =256-2 = 254 [2 for the broadcast and the network]

so if we need two class C ip address we get the hosts 254+254 = 508

now if we use the /23 ip address we get the host bit 9 so the hosts is 2^9 = 512-2 = 510

so we can see by using the CIDR we can accommodate any combination of network and the host id.

ROUTING

when you say the word cloud in the IT field.it does not mean anu location in the sky. When you say I am storing the data in the cloud it means you are storing the data in a computer someplace else. You already know the internet is not just a specfic place with a lot of resource .internet is just a interconnection between millions of individual networks.so on one side can access resources shared by other people or organization on the other place of the world.But how this communication done? Because you already know that it is not possible to exactly locate a host using just their MAC address.Then we introduce the ip address.but how one individual network can communicate with other individual network.and how the travel from one side of the world to another side within a fraction of second? The way one network find and communicate with other network is called ROUTING.Routing is not a simple task in low lavel.thats why we will talk about the high level concepts about the Routing.

Now first thing first .where this ‘Routing ’ happens? Well obviously in a router.

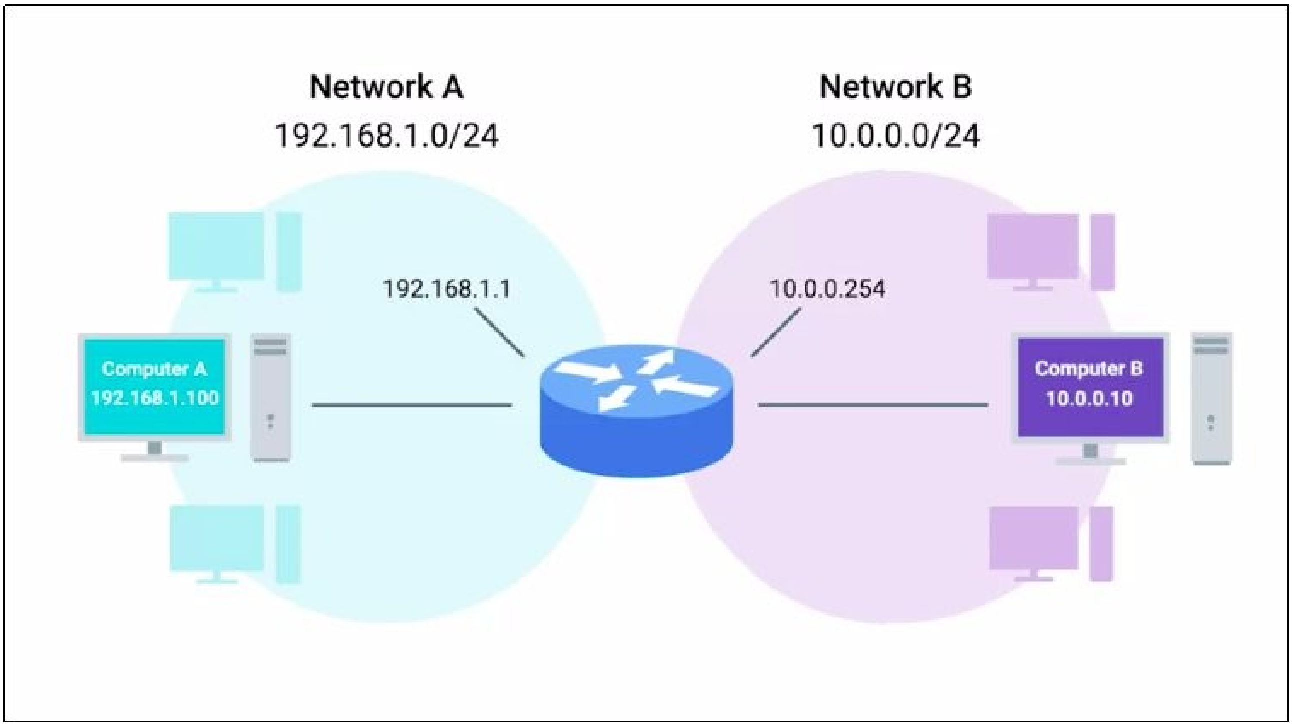
Router is a network devices that forwards traffic depending on the destination address of that traffic .

Since the Router actually forward the traffic to a different network .So in a Router there must be at least two network interface.and it has to connect to two network at the same time

HOW ROUTER WORKS:

there are four steps

1) it receives a data packet from one of its interfaces.
2) it look for the destination address in that packet
3) it search for the destination network in its Routing table
4) Router forwards to the information to the network.



Suppose there are two different network
network A → 192.168.1.0/24

and
network B → 10.0.0.0/24

host ip in network A → 192.168.1.100
connected to the Router interface 192.168.1.1 (gateway)

host ip in network B → 10.0.0.10
connected to the Router interface 10.0.0.254 (gateway)

This is how the packet sends from Host A to Host B

1) host A tries to send the data and he finds out that
   the destination is not in its network
2) so it send the data to its gateway (the router)

3) Router knows where to send it because it knows in which network it has to send

4) Then Router does these following things

→ Router remove the data link layer content
  from the packet

→ Router search the ip datagram filed for the destination address (you already know the destination ip address in the ip datagram)

→ After finding the destination ip address it looks its Routing table.and find which network it belongs.
→ it search for the hop (we will discuss it later) and it finds that it only one hop away

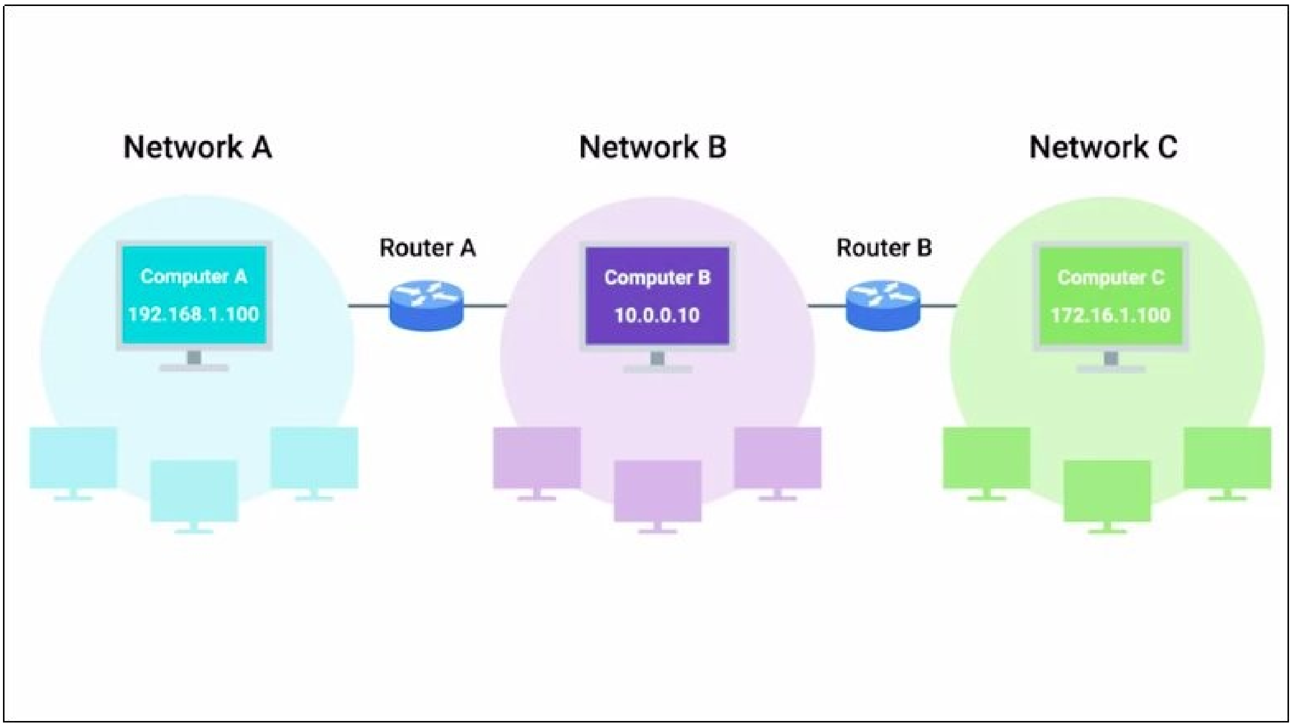
→ router search for its ARP table and find the MAC address

→ It decrement the TTL 1 and add the new ether net header and footer for the new destination

→ send the packet the to that destination interface

Thats easy to understand but what happen if it is on the third network and not directly connected to the router.

Lets find out



you can see there three different networks

network A host ip → 192.168.1.100 (network 192.168.1.0/24)

network B host ip → 10.0.0.10 (network 10.0.0.0/24)

gateway (192.168.1.1,10.0.0.154) (A-B)
network C host ip → 172.16.1.100 (network 172.16.1.0/23)

gateway (10.0.0.1,172.16.1.1) (B-C)

you you know the ip address class you can tell that these are three different network.

Host with a ip address 192.168.1.100 wants to send data to 172.16.1.100

→ Host 192.168.1.100 know that the destination is not in its network so it sends to the gateway 192.168.1.1

→ Router remove the datalink layer and find that the destination address is 172.16.1.0.0 and find that it is not in its network either

→ then router find the quickest way to send it and it finds that the router B is the quickest way

→ so it add the add the data link layer with the datagram with the router B gateway address decrement the TTL 1 and send it to the Router B and then Router B just repeat the process (Removind the data link ,search for the destination , find MAC address,decrement TTL, add the data link layer with the datgram)

→ After that router B send the data to the destination host.

This is a straight forward process for sending data .In real life a router is connected to multiple network .and it is connected with a mesh so that if one connection goes down another will automatically take the duty to send the information

we talk about the Routing table in routing. Router search for Routing table before forwarding the data. Routing table can have a lot of information now a days but it must contain this information bellow

1) destination network: (with CIDR or with ip and netmask)

2)next HOP: (other networj that is directly connected with the router)

3) Total Hops : in real life you can send the data with multiple path. but the router finds the shortest path to do that . The router has to know the number of hops to go through to send the information to another router.with the total hop number router can decide which is the best and shortest path

4) interface: Router also has to know the interface.and which interface it has to forward the data.

Routing table is not parmanent .it will constantly change depending on the network status.

But now the question arrives how this routers learn this information?

The ans is ‘with different protocols’

Routing protocols are some special protocols that the routers use to talk to each other

there are two main protocol

→ IGP (interior gateway protocol)
→ EGP (exterior gateway protocol)

IGP has two categories

1) Link state routing Protocol
2) distance-vector Routing protocol

Before telling about the the protocols there are something you need t know

1) autonomous system: every single network or a group of networks is controlled by a common administration on behalf an entity which can be

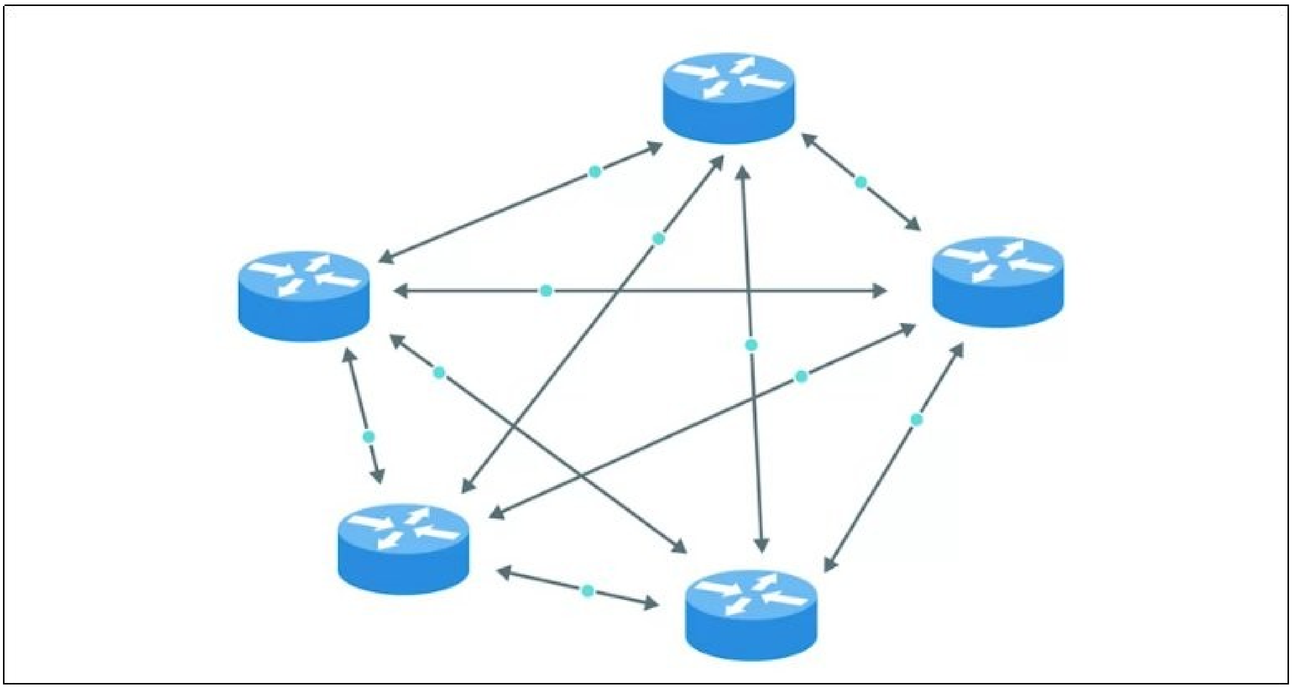
national in scale. An AS (autonomous system) can also reffered as a routing domain .and this is not identified by any ip address .it actually identified by the ASN (Autonomous system number)

Network within the autonomous system communicate routing information with IGP. And the autonomous system itself share routing information with other autonomous system with EGP. But EGP is not used now a days . Basically BGP (Boarder gateway protocol is used) and it will soon be replaced by IDRP (inter domain routing protocol) .

So lets talk about the distance vector protocol

in distance vector protocol a router store every routers network and its hops then router send the list of this information to every directly connected router and thats it. When a data is sent the router calculate which router it should choose for passing minimum hops

but it has a problem .it only know the status if the router thats is near to it. So the change of the router condition far away from it takes time to affect the change thats why the link state protocol comes in . In the link state protocol every router is connected with every router in every possible way



so every router in a AS (autonomous system) knows the status of every other router status. this significantly improve the performance. But it needs the router to store all the information and also apply different algorithm to find the best and the shortest path to the destination. It require more memory and also the processing power to apply this .but now a days we can have high processing power with a very cheap price. So this link state protocol is basically used now a days.

EGP:

exterior gateway protocol for communicating with different Autonomous system. And it is managed my a organization called IANA (internet Assigned Numbers Authority) the IANA provides a 32 bit autonomous system number (ASN). Important thing this ANS is not a volatile number that is going to change.

PRIVATE IP (Non Routable) ADDRESS

if you calculate the total ipv4 address.you can understand that it is not enough for every computer providing a ip address. And consider if a company needs a thousands of computer to go online they will need thousands of different ip address.so it will be impossible for assigning ip address to every single computer.

The solution is the NON ROUTABLE IP ADDRESS in every ip address there is a range of non routable ip address

these range are

1) 10.0.0.0 -10.255.255.255 (10.0.0.0/8)
2) 172.16.0.0-172.32.255.255 (172.16.0.0/12)
3) 192.168.0.0-192.168.255.255 (182.168.0.0/16)

any one can use this ip address. You can use this ip address in your office or home to communicate with each other.and it will not be forwarded by the gateway router .

So you can access to the public world wide web using these ip address.because non routable address is not used for this.thses are called the private address .and with this address you cant go to the public network.

Now lets look at your laptop ip address that you are using. You will be surprised that your ip addrress is a private ip address. But you already know that private ip address can not access the public network. Actually we use a technology called NAT to do that.with NAT all the computer in your company can use the private ip address and still can access to internet