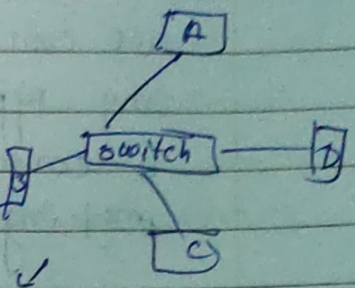
Date:
P. No:

→ What is Network ?

Ans

Two or more computer are connected this is network



This is also network

→ What is Host ?

Ans It can be PC / Laptop / Server which got an IP Address

→ What is Networking ?

Ans Sharing of data & resources in a network.

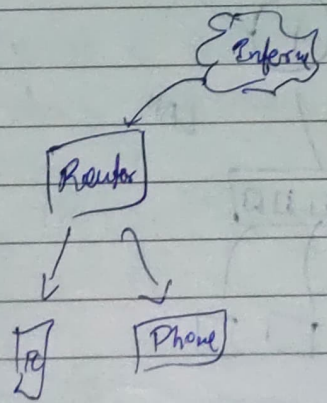
LAN → local Area Network
WAN → Wide Area Network

→ What is Router

Ans when you want to connect two or more different network, then we use this Router.

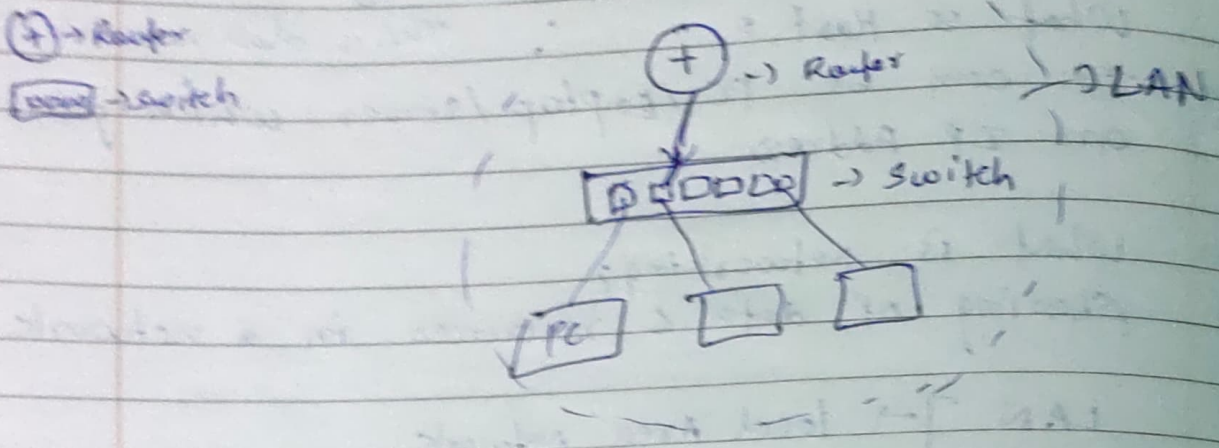
→ What is Internet

Ans It is a Network of network.



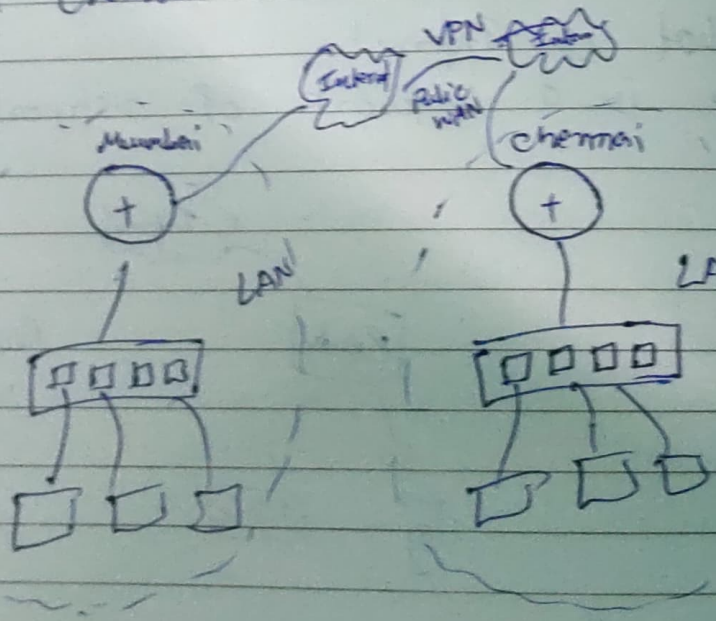
Router help us to connect with other network.

Here we have switch, it has ports where we can connect our computer, servers, printer or any type of network device and this switch is connected to our router. These all thing making an LAN.



WAN are of two type → Public
→ Private

Suppose you have two office one in mumbai and one in Chennai

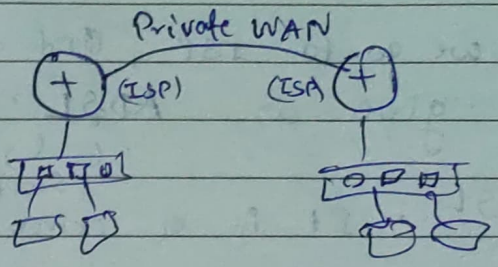


Date:
P. No:

Now, Mumbai device is connected through Internet and Chennai device is also connected to Internet, and you are connecting Mumbai & Chennai through Internet. This is called VPN. or Public WAN, bcos you are using public resources.

When we want to connect branch office at that time we can say we need to create VPN connection b/w Mumbai and Chennai, that is your public WAN

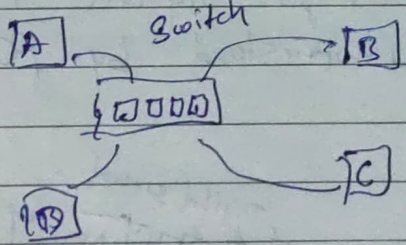
If we want secure connection b/w our branches we can use dedicated line that is known as Private WAN.



It is highly expensive. Bcos we connecting through cable or leased line

To connect in Private WAN we have to use same ISP. Then only ISP will able to create virtual connection.

Switch → It is a device use to connect two or more Host / computer.



Now in Market, there are cheap as well expensive Switch are there. But what are difference b/w them.

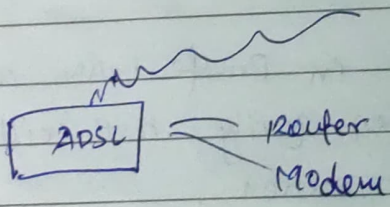
see in cheap one, when we want to pass any information from A to D, it will also go to C and B. They are unmanagable Switches, they don't have features

Where as expensive one are come up with features like it has VLAN. They are managable Switches. for Industry work we use these.

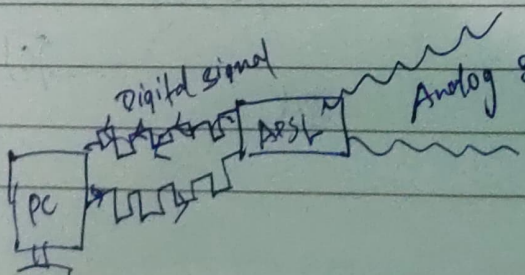
ADSL → Asymetrical Digital Supply line

When we go to ISP, and ask for a wifi connection they give us ADSL → Router
↳ Modem
↳ Switch

ADSL - It is a combination of Router & Modem

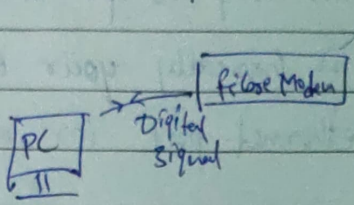


Modem → It Does Modulation & Demodulation, when the connection come, it comes in a Analog signal, it changes signal into Digital signal that can be understand by PC.



Modem also changes the Digital signal to Analog signal that are coming from PC.

In case of fibre Modem, light signal converted into electrical / digital signal.



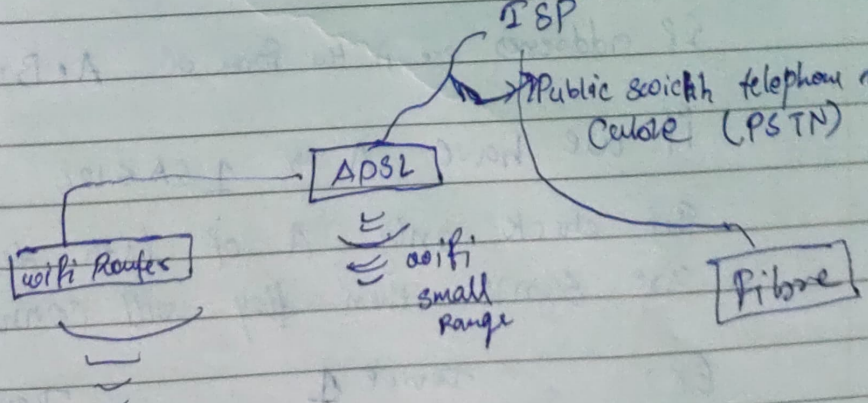
The ISP doesn't provide us wifi router, if provide us ADSL

It has 1) DSL port → Telephone line (it gets Analog signal through)
2) switch (LAN1, LAN2, LAN3
3) Modem

Usually DSL have little range of wifi, Router about 100 sq m.
But in Big house we need a internet in all house, so we use wifi router

It has eternal cable port, no such DSL port

→ wifi router we for extend the range of wifi



Date:
P. No:

→ Router have SFP a small chip which converts optical signal to electrical signal.

What is Nic. (Network Interface Card)?

Ans Nowdays this chip is pre integrated in motherboard.
NIC card is basically your ethernet port. When we we have ethernet port in my PC it means it has nic.
And all nic have different MAC address.
PC doesn't have MAC address, it's a nic which has

→ Wired Nic
→ Wireless Nic
→ Bluthooth Nic

If we have 3 things it will have 3 MAC Address

MAC Address is a address of those hardware that we are giving to these chips.

→ If somebody ask for how many MAC address do your pc have, you just need to count NIC chip.
→ Command to check → ipconfig

When two device are going to connect each other?

Ans IP addresses are in the form of A.B.C.D

if we have A → $1 \leq A \leq 126$ N.H.H.H

Then check only A of both device, if they are same then they will connect

Ex → Device A — they will connect → Device 2
1.1.1.1 — 1.7.3.5
7.5.4.126 — Not connect → 11.5.4.1

Date:
P. No:

If in A.B.C.D N.N.H.H

A is → $128 \leq A \leq 191$

then to connect two device both should have A & B same

150.1.1.7 ⟷ (Not connect) 150.2.1.5

130.5.1.7 ⟷ (connect) 130.5.7.5

If A is $192 \leq A \leq 223$ N.N.N.H

→ we have to match 3 portion to connect

192.168.1.1 ⟷ (connect) 192.168.1.5

→ We have A = 127 is not, so does it mean we dont have ip start with 127?

Answer is no. we have ip that start with 127 but they are for loopback ip, means self owned ip. It for local Host.

For example → when we start a pc, its shows logo or many other services (log, inside service) that mean laptop is itself working as a server for our pc. So it all have self host ip that start with 127. No, outside device can connect with this ip.

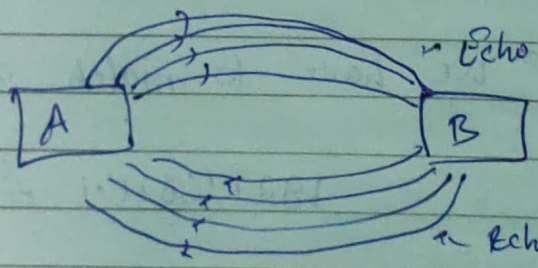
→ How to check if the pc2 is connected to PC1.

Ans Use command { ping <ip Address of PC2> } In PC1.

Use command on PC1 → (ping ip address of PC2)

Your PC1 coill send 4 Request (code), if it got 4 Reply from PC-2, that means it is connected with PC-2.

This Request is Echo Request (these is code in this Request)



The request it send is basically a code - 8 ← Type code

and Echo Reply, is [0] ← code

8 in the form of binary No is 0000|000

and 0 in form of binary No is 00000000.

When 2nd device get a code 0000|000, it has to reply is zero - 00000000.

1 bit → 0 or 1
8 bits → 1 byte

Date:
P. No.

What is TTL (Time to live) ?

TTL refer to the amount of time or "hop" that a packet is set to exist inside a network before being discarded by a router.

When packet of info is created and sent out across the internet, that ~~thread~~ is risk it will continue to pass from router to router indefinitely. To solve this problem, packet are desined with an expiration called time to live or hop limit. Every time a router receives packet, it subtract one from TTL count and then passes it onto next location in network. If at any point TTL count is equal to zero after subtraction the router will discard the packet and send an ICMP message (Error message) back to originating host.

→ To get the mac Address of all device use command → getmac -v or ipconfig /all

IP Address

IPV4
32 bits
Each of 8 bit
so 8bit × 4 = 32 bit
X.X.X.X
200.1.1.1
In decimal form

IPV6
128 bits
Each of 16 bit
16×8 = 128
X:X:X:X:X:X:X:X
2001:1234:0000:00123:CAFE:1237:1111
Hexa Decimal form

Date:
P. No:

Decimal to Binary

8bit 8bit 8bit 8bit

192.168.1.1 X.X.X.X

Decimal system

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

192 → 1 1 0 0 0 0 0 0

168 → 1 0 1 0 1 0 0 0

1 → 0 0 0 0 0 0 0 1

1 → 0 0 0 0 0 0 0 1.

IANA → Internet Assigned Numbered Authority

X.X.X.X

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

0 0 0 0 0 0 0 0 = 0

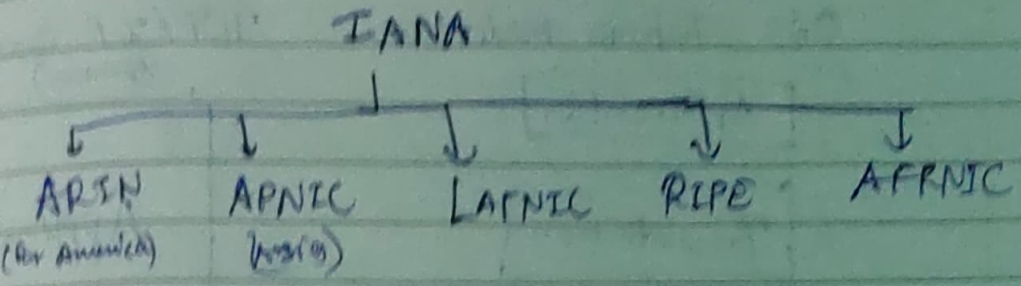
1 0 0 0 0 0 0 0 = 128

1 1 0 0 0 0 0 0 = 192

1 1 1 0 0 0 0 0 = 224

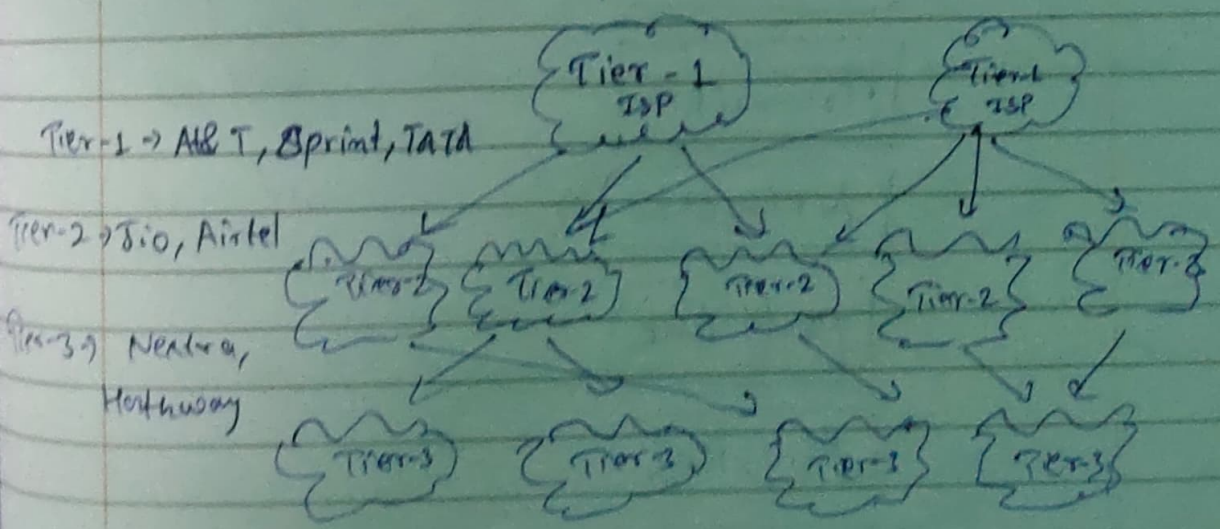
1 1 1 1 0 0 0 0 = 240.

Class	A	B	C	D	E	
	0-127	128-191	192-223	224-239	240-255	0 and 127 are Reserved



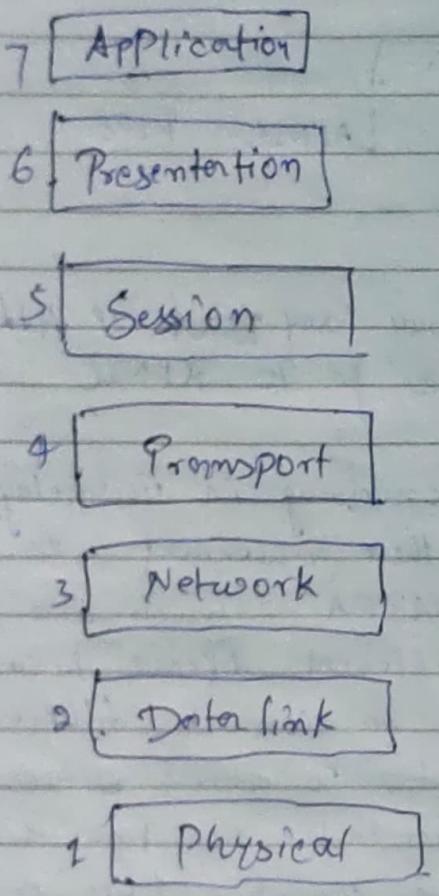
in India
If I want to buy any private IP Address then I will have to go to APNIC

→ As Russia was involving in Technology, America was jealous with their achievment, so they formed an organization DARPA, which was successful in connecting different defence area, After that they form ARPA to connect different cities and provide Internet. To connect cities, they need big investment for cable so from their company which investestment connecting cities were Tier-1 ISP. They are responsible for connecting different countries through submarine cable. Then they give internet to Tier 2 ISP and they give to Tier-3 ISP (local ISP).

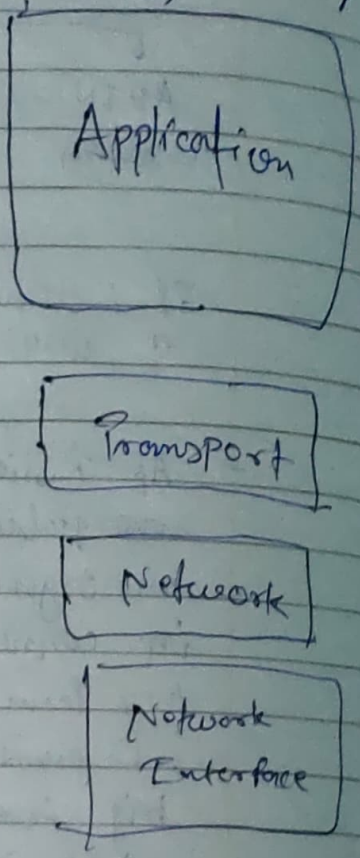


Date:
P. No:

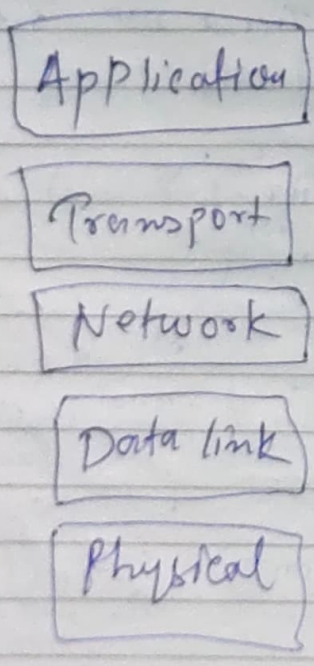
OSI Refrence Model



TCP/IP Conceptual Layers (earlier)



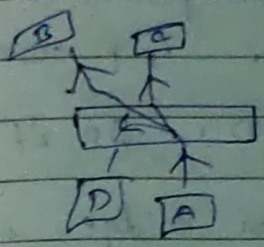
TCP/IP (updated version)



Date:
P. No:

(We Don't Use HUB nowadays)

Hub



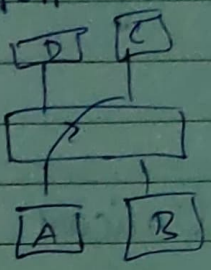
It doesn't store MAC Address so when we want to send info, it will go to every Device.

It Brodcast the Message

It send message through Signal (It come to physical layer)

Less no. of Ports

Switch

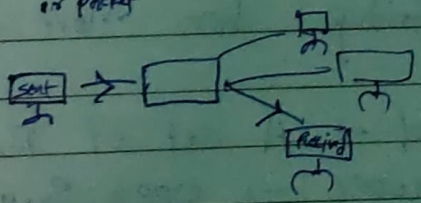


It does store MAC address so we can send data to specific Device

Large no. of Ports

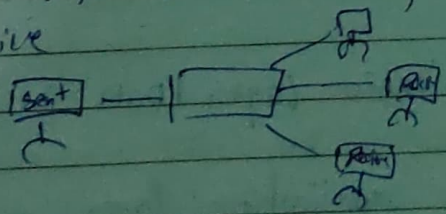
Unicast → When Info is sent to single Device (or Packet)

One to One



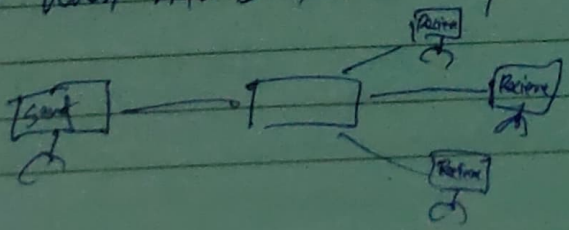
Multicast → When Info is recieved by Multiple Device

One to Many

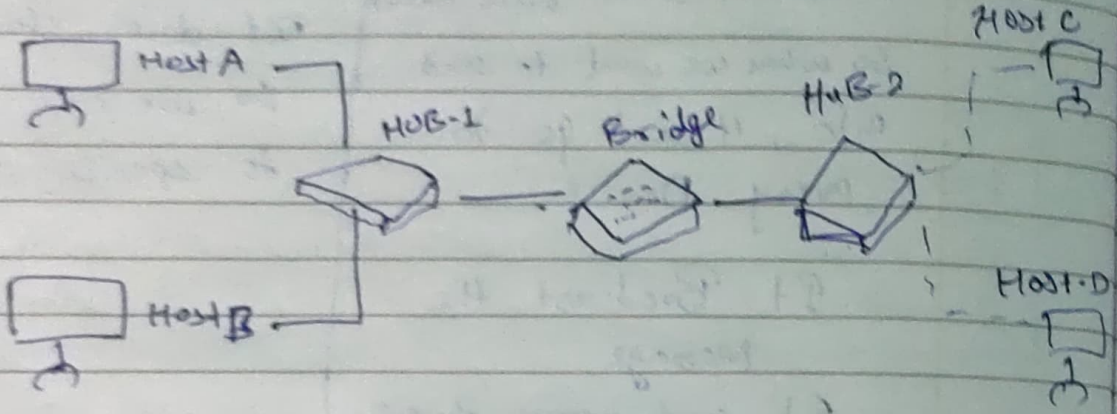


Broadcast → When info is Recieved by every Device

One to All



Bridge → We can say this was older version of switch. It can store MAC address. So if want to Unicast packet we use Bridge with Hub.



Now Bcoz Bridge stores MAC Address, we can send packet from Host A to Host D, without sending to Host B & C.

Bridge has more no. of ports.

Protocol → A set of Rules
OSI Model → Open System Interconnection
TCP/IP → Transmission Control Protocol / Internet Protocol

Application Layer (Data) → The software which interact on human to another works in application layer.

Web browsers → HTTP, HTTPS, SMTP, TELNET, POP

To access website you will use → HTTP / HTTPS

Send email you use protocol → SMTP (simple mail transfer protocol)

To receive email → POP (Post office protocol) / IMAP (Internet message access protocol)

To send file to server → File Transfer protocol

You want to access any device remotely you use → TELNET / SSH (secure version)

2 Presentation layer | Data > Format of data

Image - Png, Jpeg; Audio → MP3, wav;

Video - mp4 or avi.

Encryption / Decryption

Compression / Decompression

3 Session layer | Data > Create and maintain the session.

Timeframe

4 Transport layer | segment > End to End delivery of data.

TCP

UDP

So in above three layer Data will be in form Data form, But it comes to Transport layer it divide Data into segment.

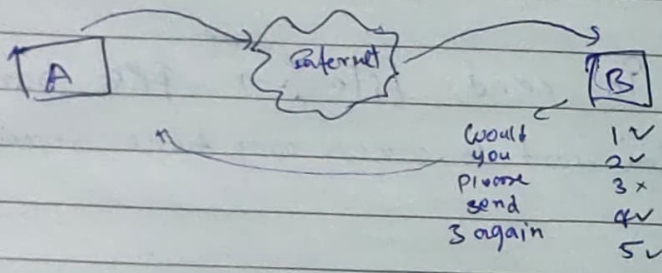
Suppose - we are sending HELLO, so it will divide it into segments called segmentation.

H | E | L | L | O

Date:
P. No:

it will also do Sequencing → 1 H | 2 E | 3 L | 4 L | 5 O

There is a chance when we are sending any data through Internet there is possibility, any packet get lost in way.



So if any packet got lost, it will again ask for that packet to A. So it also perform Retransmission

So Transport layer is devided into TCP & UDP itself.

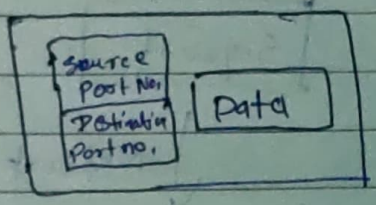
So these things like → Retransmission come under TCP

TCP	UDP
→ When other end get the packet it send Acknowledgment message to sender, to tell that it got the packet. So it Reliable Protocol	→ No Acknowledgement → Not Reliable
→ Retransmission, if segment got lost	→ No Retransmission
→ Connection Oriented	→ Connectionless
→ Size of packet = 20 byte (It takes to add information)	→ less overhead, (It takes) 8 byte to add info

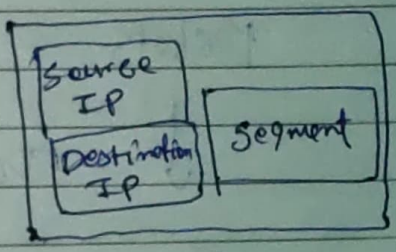
what it adds in this 20 byte?
Ans → Port Numbers

Both comes under IP protocol and TCP protocol no. is 6, where as UDP no. is 17.

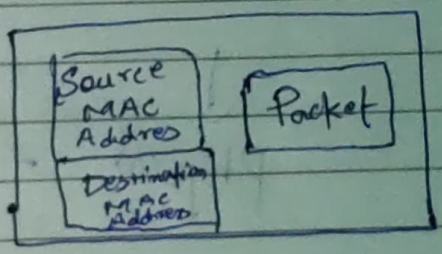
Segment →



Packet →



Frame →

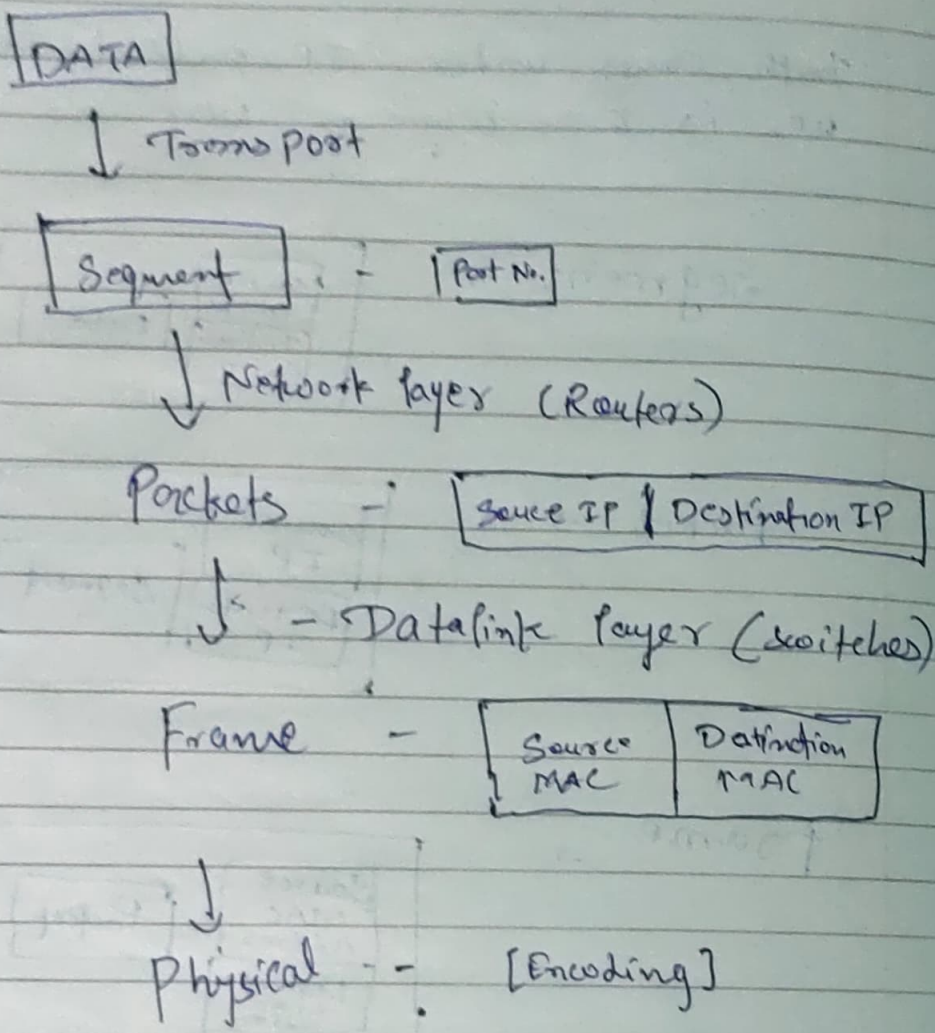


5 Network layer | Packet | - IP address | ICMP | IPv4 | IPv6 - Routers.

6 Data link layer | Frame | Mac address | Switches

7 Physical | Bits | - Cables | Connector

Date:
P. No:



At last physical layer - (NIC card) will change it into 0101 [encoding] form and send it into signal

This whole process is known as Encapsulation.

Now this physical layer send in 0101 form, now another Device physical layer send it into Datalink it will check MAC and it will send to Network layer now it will check IP Address (check if IP address of this Device or not) then it will go in Segment (check Port No.) and then into DATA form

Date:
P. No:

Decimal to binary

bits → 0/1

IPv4 — X.X.X.X
32 bits — 8bits 8bits 8bits 8bits

For Ex → we have IP → 192.168.10.7 then converting it into binary

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

192 → 1 1 0 0 0 0 0 0
168 → 1 0 1 0 1 0 0 0
10 → 0 0 0 0 1 0 1 0
7 → 0 0 0 0 0 1 1 1

IP Adress Range

Class A → 0-127
Class B → 128-191
Class C → 192-223
Class D → 224-239
Class E → 240-255

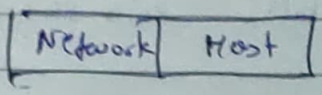
Class D & E are of no use bcos D is used by router, it can't be understand by PC and E is for future use.

D is use for Multicasting.

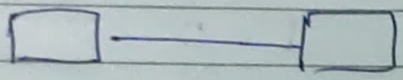
ncpa.cpl

Date:
P. No:

All Ip Address have two parts one is Network and one is Host



If two Device has to communicate each other these network port should be same

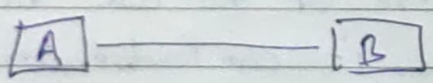


N.H.H.H ⓥ N.H.H.H

			By Default subnet Mask
A	N.H.H.H	(1-126)	255.0.0.0
B	N.N.H.H	(128-191)	255.255.0.0
C	N.N.N.H		255.255.255.0

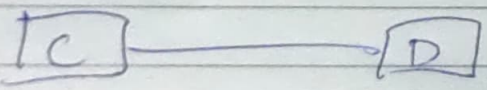
→ We always check the class by first no. of IP not subnet Mask.

Beas we can provide manually 255.255.0.0 or even 255.255.25.0 Subnet Mask to A class.



1.1.1.1 1.100.1.2

255.0.0.0 255.0.0.0



19.1.1.1 150.2.3

255.0.0.0 255.0.0.0

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
128 64 32 16 8 4 2 1 = 255

So we can assign 0 to 255

A —— B

200.1.1.1 200.1.1.3

255.255.255.0 255.255.255.0

You can assign this number of IP to their respective classes.

A - N.H.H.H = 2^{24} = 16,777,216

B - N.N.H.H = 2^{16} = 65,536

C - N.N.N.H = 2^8 = 256

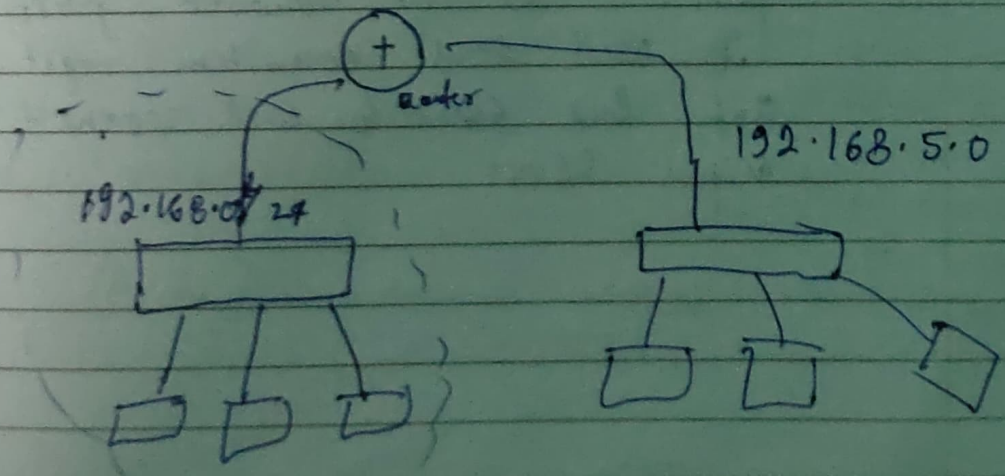
If we are in clg, they are mostly use 172.16.... Bcos we don't need many IP. But in company we use Class A

Fancy way to represent IP

A → N.H.H.H /8 → CIDR

B → N.N.H.H /16

C → N.N.N.H /24



Router is used to connect two or more different Networks

Here on side has 192.168.10.1/24 and one 192.162.5.0 so their N.N.N is different so router help them to connect each other even though their N.N.N is different.

Basically all Router are sharing their Network port. so when we send any connection request for any IP through Router, Router will help this IP to connect to right Router. by showing right path.

you can understand by this terminology, as

network port is like street address
and Host port is like House address

So when we want to connect any Device, we will have IP of that Device, so from our router, it will try to find IP of same Network to which we want to connect. Bcos Router shares only their network port, as the network port matches it will send connection reqst to switch and this switch will connect us to Right Device

SHORTCUT → 1 - 128 5 - 248
2 - 192 6 - 252
3 - 224 7 - 254
4 - 240

Data:
P. No:

Subnet Mask - Represent Network bit

8	/8	→	255.0.0.0
8+1	/9	→	255.128.0.0
8+2	/10	-	255.192.0.0
8+4	/12	-	255.240.0.0
8+8+4	/20	-	255.255.240.0
8+8+8+1	/25	-	255.255.255.128

SHORTCUT

Here /8, /9, /25 is the no. of bits and we can maximum fill any Network up to ~~network~~ octet.

X.X.X.X ⟶ $2^7\ 2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$

$2^7\ 2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$
1 1 1 1 1 1 1 1
= 255

$2^7\ 2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1$
1 1 1 0 0 0 0
= 192

/11 → 255.192.0.0

{ Here we have to fill 11 bit, so after 8 bit we have to shift to second part for more 3 bits to fill

Value are from

/8 to /30

Every IP address must be accopanied by subnet mask. By now you should able to look at an IP address and tell what class it is. Unfornately your computer doesn't think that way. For your computer - to determine the network and subnet portion of an IP address it must AND the IP address with Subnet mask

Default Subnet Mask

Class A · 255.0.0.0
Class B 255.255.0.0
Class C 255.255.255.0

Anding Eqn
1 And 1 = 1
1 And 0 = 0
0 And 1 = 0
0 And 0 = 0

When you see

IP Address: 192.100.10.33

What can you figure out

Class → C
Network Portion - 192.100.10.33
Host portion - 192.100.10.33

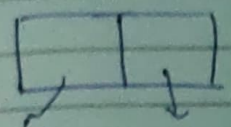
In order for your computer to get the same info it must AND the IP Address with subnet mask in binary

(192.100.10.3) → 11000000.01100100.00001010.00100001
(255.255.255.0) → 11111111.11111111.11111111.00000000

AND 11000000.01100100.00001010.00000000

AND with default subnet mask allows your computer to figure out the network portion of addr

Suppose we have two labs and each 100 computer and we want to provide IP Address



Our IP Address is
192.168.1.0 /24
Default Subnet 255.255.255.0

Now we know
$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$ → It can provide 100 IP (Although 28 IP getting waste for 1 lab)
$2^8 = 256$

Here → N | H
24 | 8

(8 bit so IP Range From 192.168.1.0 → 192.168.1.255)

After Dividing → 7 / 1

But we want to Divide when 1

New NW → N | H
After Dividing /25 | 7

So lab 1 will have IP in Range 192.2.168.1 → 192.2.168.127
lab 2 will have IP in Range 192.2.168.128 → 192.2.168.255

0	128
↓	↓
127	255

So for Any Computer in lab 2
IP → 192.168.1.1
Subnet → 255.255.255.128

for lab - 2
IP → 192.168.1.130
Subnet → 255.255.255.128