NET-WORKING Basics

Kushal Kumar's
21291CM052,
DCME.

Network: Linking of a computer to allowing them to operate interactively

LAN: Local Area Network
WAN: Wide Area Network
WLAN:
SAN:

protocols ← Network router protocol.
Internet protocol
wireless Network protocol

Major protocols: TCP, UDP etc...

protocols
UDP
Topologies
Servers
HOST
DNS.

Topologies.
different types
bus topology
ring topology
Mess Topology

OSI - Open System Interconnection. — Transmission of data according to layers.

1. Application Layers: HTTP, HTTPS, SSH, FTP.
2. presentation Layer: SSL, SSH, JPEG, MPEG. } software
3. Session Layer: Major(API), SOCK, Port
4. Transport Layer: TCP, UDP
5. Network Layers: IP, ICMP, GMR.
6. Data Link Layers: switch, Branches, Ethes } Hard ware
7. physical Layer: fiber, wireless, Hubs.

IP: internet protocol:

protocol - set of instruct

IP:

Version
↓
IPv4 - 4 billion
↓
IPv6 → Trillions

DYNAMIC IP: Public IP.

STATIC IP:

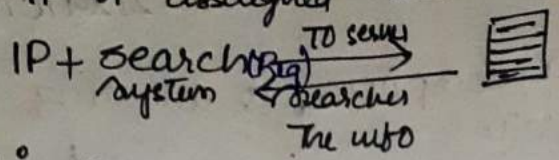
When the system is connected to network the network provider gives or allocates an ip to the system. Its volatile it is DYNAMIC Memory.

STATIC IP: Constant IP which doesn't change

eg: instagram.com
The companies buy set of static IPs.
when when we type instagram.com.

DNS translates domain names to IP addresses so Brg can load internet resources.

→ the computer cant understand domain so
Then IP is assaigned with help of ip-



IPV4: 172.16.254.1

↓ octaves.

10101100 — 8 bits = 1 byte

0001.0000

11111110 — 8bits

IPV4:
could assaign 4 billion ips

00000001

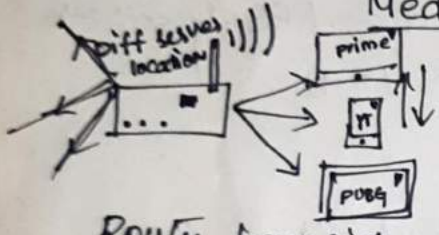
2^{32} + combination.
= 4 billion

IPV6: [2001:0DBB:AC10:FE01:0000:0000:]

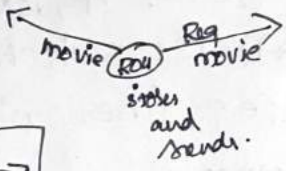
128 bites = Trillions combination.

Servers of majour DNS they belongs to IPV4:

MAC Addres: MAC ANALYSES the Data either it ∈ to it or not
Media access control



why the content in the systems doesent interchange



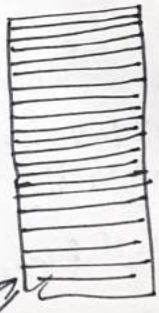
Routes backside:

Mac Address.

Eg: 9C-35-5B-5F-4C-D7

MAC SPOOFING: — we can change the MAC address. by simple commands.

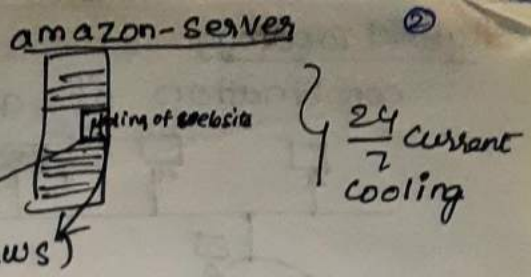
Servers: — A Server is a software or hardware that accepts and responds to the request made over a network the device that makes the request, and receives the response from the server called as client.



Eg:

Req 3types

3 TYPES OF SERVERS:



Webservers
email servers.
Database servers

Bigrock → domain names (buy)

Hosting (aws)

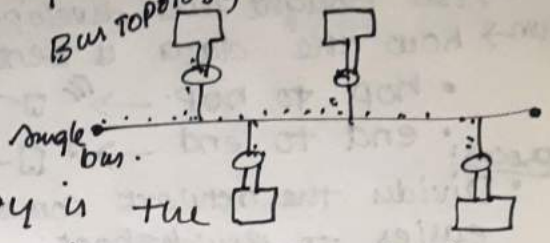
Hosting: a small piece of space in big servers to the website etc..

(In Servers → 2 processers.
→ Data Transmissions fast.

It serves the data as per request

TOPOLOGY:

Types



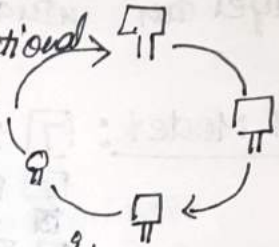
Bus TOPOLOGY:

Single bus topology is the simplest topology. if the data is to transffered from one to another it checks sequentially with help of Mac it reaches the client system.

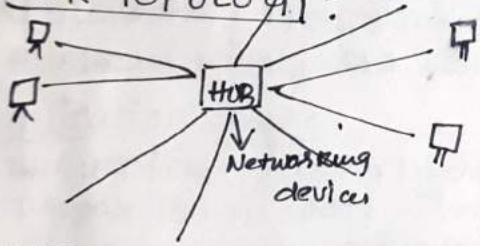
RING TOPOLOGY:

Data transfer → Tokens.

Data Transmusion might be uni directional
Token transmission could processed as.
Similar to Bus.



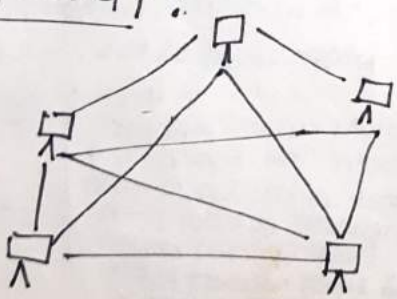
STAR TOPOLOGY:



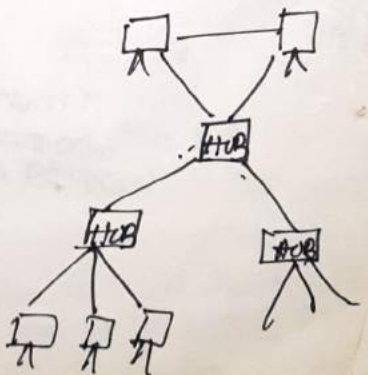
Token.
Data Transfer towards hub.
it can transfer tokens as per req and MAC.

It was connected Series ~~Parallely~~ so if one system went off all assam.

MESH TOPOLOGY:

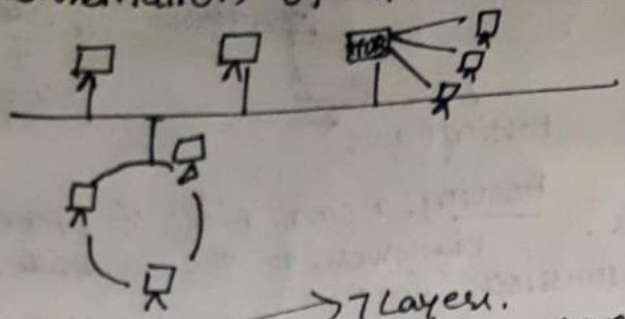


TREE TOPOLOGY:



Limit:
high cost due to cables

Hybrid Topology:
combination of all Topologies.



OSI MODEL: → 7 Layers.
Open System interconnection.
→ ISO bought and developed
Aim → how the data is sent and received.
- hop to hop. →
- end to end → Long distance

Process:
- Divides the network communication process into layers to easies to troubleshoot:
- Allows multiple-Vendor development through standardiza of Network components.
- Various types of Network hardware and software can communicate.
- Layers can interact with each other.

OSI Model: 7 ~~physical~~ Application Layer.
6 Presentation Layer.
5 Session Layer.
4 Transfer Layer.
3 Network Layer.
2 Data Link Layer.
1 physical Layer.

OSI MODEL: (Open System Interconnection)

7. Application ← data ← Sender
6. Presentation ↓
5. Session ↓
4. Transport ↓
3. Network ↓
2. Data Link ↓
1. physical Link ↓

Receiver:
1. physical Link ↓
2. Data Link ↓
3. Network ↓
4. Transport ↓
5. Session ↓
6. presentation ↓
7. Application ↓

Network PROTOCOLS: (Set of Rules)

- Net BEUI → Net BIOS Extended User interface → LAN protocol → Limited performance
- IPX / SPX → Standard, WAN, Vendor oriented, Poor performance for other vendors
- Apple Talk → Standard supports WPN, Vendor oriented

TCP/IP → Very imp

TCP/IP:

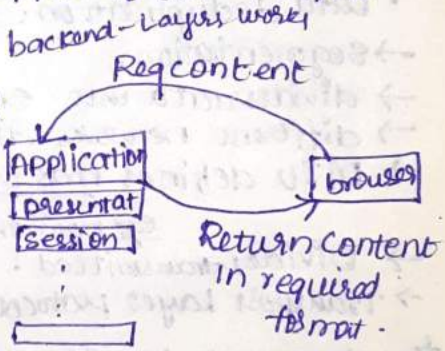
Transmission control protocol:

1) Standard 2) Supports WAN 3) Not Vendor oriented
4) Almost widely used over internet 5) Mapped to OSI 7 Layers.

Application Layer:

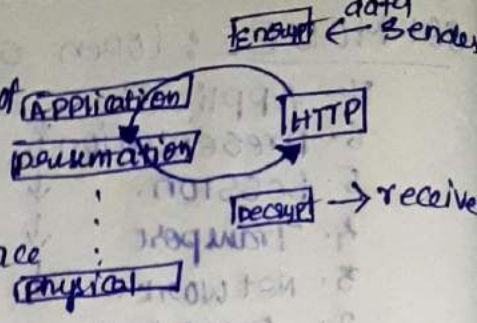
- User interface to lower layers.
- preparation of data for each service.
- End to end communication
- Software applications reside in it.
- Sends request and receives reply

eg:



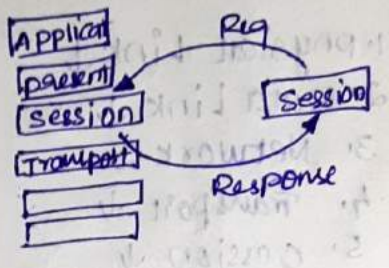
Application Layer { protocols present in
- HTTP
- FTP (File Transfer protocol)
- SMTP (Simple Mail Transfer protocol)
- POP3 (post office transfer protocols.
- IMAP (Internet Message Access protocol)
- Telnet (Secure shell)
- DNS (Domain Name Issues)
- RTP (Real-time protocol.

6. PRESENTATION LAYER:



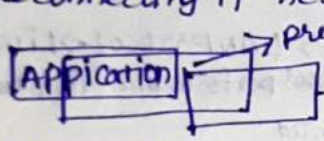
- Responsible for common representation of data b/w source and destination.
- Provides transformation of data.
- Supports standardized application interface
- Coding of data syntax.
- Data Encrypt/decryption.
- Data Compression.

5. SESSION LAYER:



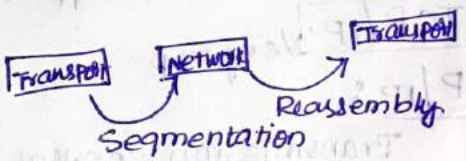
- Establishing session.
- MANAGING SESSION.
- Controlling session.
- Termination session.

→ Making sure connection is active.
→ Secure connection.
→ Dialogue connection.
→ Reconnecting if network errors.



& content formatting.

4. Transport Layer:



- Organize data into segments
- Reliable end to end transport
- Loss recovery
- Flow control
- Data ordering
- Data deduplication

• Adds port Layer.

→ if the sender sends 2 times the data then duplicate will be deleted.

→ segmentation.
→ divides data into small fragments
→ different networks different max Transmission unit (MTU)
→ DTU defines max size of one data piece carried through network
eg: how the header is carried in a website
→ Divided, transmitted.
→ Transport Layer protocols reconstruct data to its intial form.

3 Network LAYER:-

→ organise data into packets
→ Responsible if end to end addressing and routing.
→ identifies unique logical address for machines.
→ selects best path for destination.
→ Routers work in network layer.
→ fragmentation if segmentation is not enough

Routing :- The shortest path in which the data should be transferred

- Receives the segments of data from Transport layer.
- Converts them to packets by adding addressing and routing
  - Source address.
  - Destination address.
- Finds a route for data to be delivered to receiver.
- Routes may differ because it is being determined based on
  - Network overload.
  - Quality of service.
  - cost of alternative routes
  - Delivery priorities.

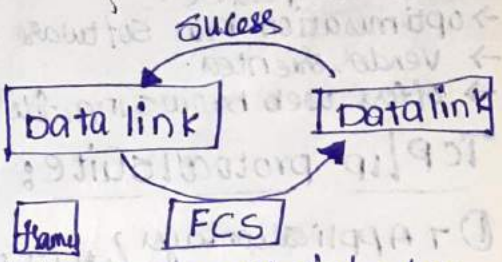
What is Logical Address :?

→ unique identifier.
→ Bound to Geographical location.
→ used for end to end routing.
→ can be changed.
→ Not vendor oriented.
eg: IP and TCP/IP.

3. Network and Transport Layer.

2. Datalink Layer :-

- Reliable data Transfer.
- Responsible of physical Addressing
- Organize data into frames.
- puts frames on physical Address.
- check frames from errors.
- Hop to Hop addressing.



→ it assigns physical address to sender and receiver.
→ Error checking.

Physical Address:

→ unique identifier.
→ Not bound to Geographical location.
→ used for hop-to hop addressing.
→ Burned on the NIC → Network interface card.
→ cant be changed.
→ ex: MAC Address, hardware address.

Frame check Sequences:

→ if the frames are somewhere lost it sequentially checks for frames.
→ if the data is lost it req the sender to resend data in form of data.

Data Link Layer:

- it could function even with heavy data flow.
- DLL → LLC (Logical link layer) → it communicates only with network layer
  - hop to hop
  - MAC: Responsible for adding physical address.

physical Layer: ← Sends (Frames)

- Transfers bit stream over physical layeyes through cables.
- Sends data signals to media and recieves it.
- Adapts transmission media.
  - cables.
  - Fibre optics.
- NIC, HUb,

INTRODUCTION TO PROTOCOLS:-

1. set of rules governing communication process.
2. intries addressing, routing, ceasion management
3. SMTP as an ex: PSTN, Mobile networks
4. Net bui, TCP/IP

TCP/IP:

- standard protocol over internet
- OSI Compatible.
- optimisation b/w software & hardware
- Vendor oriented.
- offers web browsing, file transfer, V_4, V_6 are at current.

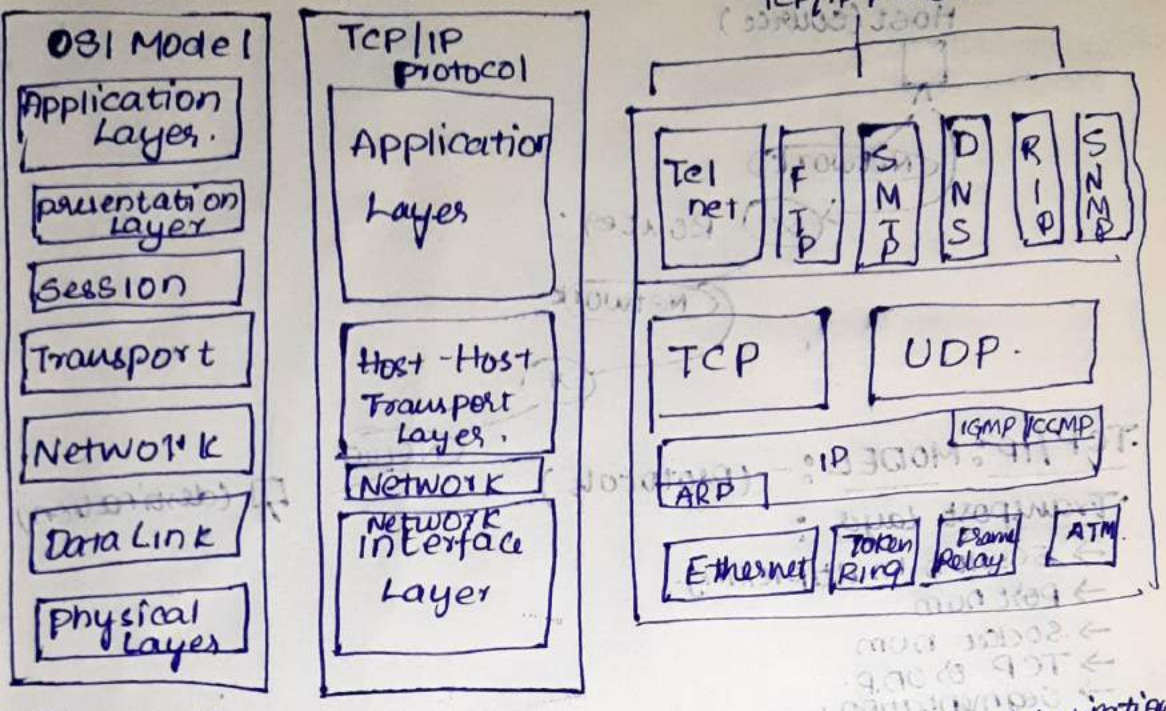
TCP/IP protocol suite:

1. Application layer / process/APP layer → HTTP, FTP, Telnet, SMTP, Utils, DNS, RPC
2. Transport Layer: TCP | UDP
3. Network Layer: Routing protocols, IP/ICMP, ARP, RARP
4. Data Link Layer: Ether type, Token ring.
5. Physical: Ethernet V.24, ISDN, ATM.

Distinguish b/w TCP/IP & OSI

- Merging of 7 layers to 4 in TCP.
- Physical and data link as Network access
- up 3 lay to Application.

TCP/IP VS ISO/OSI



PROTOCOL:

- Defines addressing to label the data with source and destination IP.
- Relaying packets across Network boundaries.
- Routing function enables networking and essentially makes internet.
- Delivers packets solely based on IP address in packet headers.
- Unique, Logical Address, 32 bit, idifinessing be machine on internet
- Routing b/w source → Destination → IP helps to make trai process.

Classes of IPs: A, B, C.

→ Class C - LAN → 192.168.0.0 to 192.168.255. ↳Range.

Reserved IP Address ← 32 bits →

Network Address [Net] [000000000000]

Broadcast Address [Network] [111111111111] ↳32 bits.

- Layer Devices:-

Router — IP → sub net mask.

Layer 3 switch ↳superfast routers.

t forward packets based upon the destination IP.

Network ID = IP Address x Subnet mask.

uting Table:

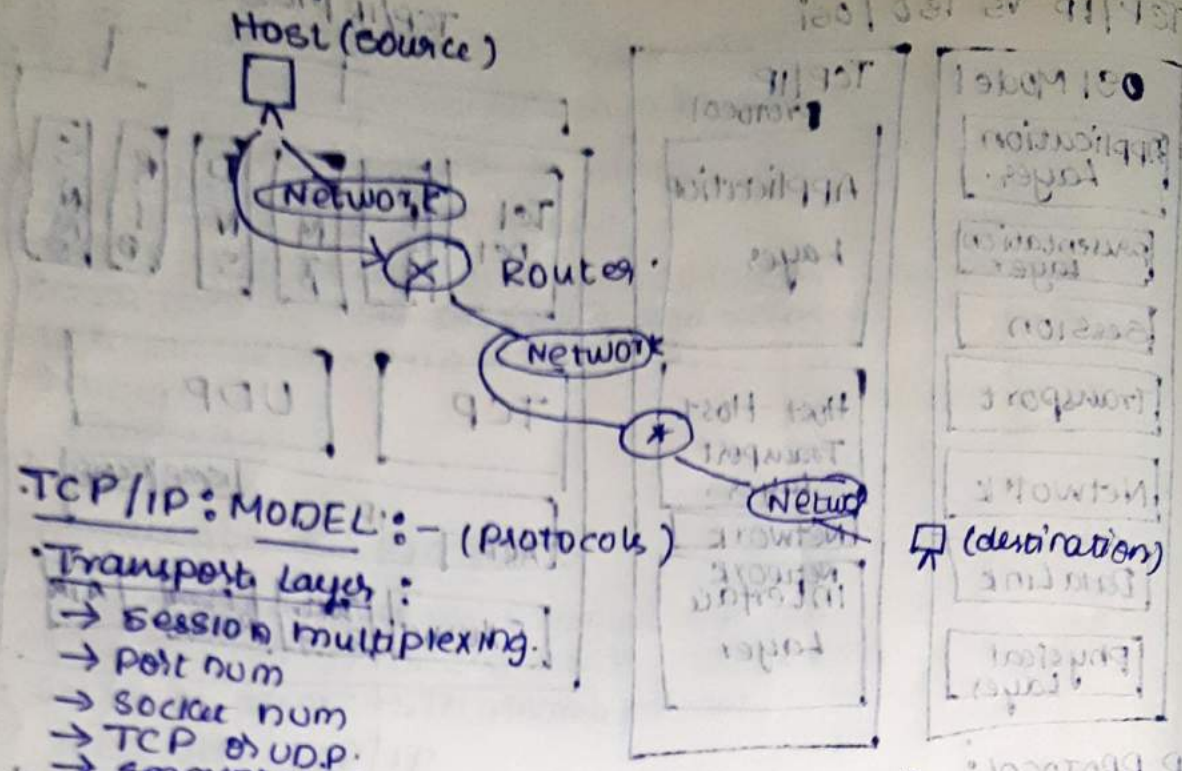
Composed of rows that are read sequentially.

Destination network.

subnet mask

Gate way

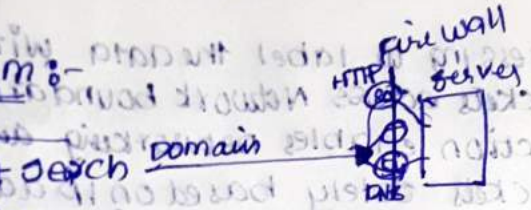
cost / metric.



TCP/IP MODEL :- (Protocols)

Transport layer :
- → Session multiplexing.
- → Port num
- → Socket num
- → TCP & UDP.
- → Segmentation.

What is port num :-



- Service identifier
- Length : 16 bits
- Range from 0 to 65,535.

Well known Port.

HTTP : 80
FTP : 21
DNS : 54
SMTP : 25

IP : 200.23.56.8 → v4
- port num = 80

Socket address = IP + PN

Ephemal ports

we can enter into the servers with port Support only limited ports are maintained to prvent hacking. port is entrence for req to enter into it These port numbers are constant doesnt change

eg: If we are opening any web page of http means the request is entering through the port num 80.

Firewalls acts as variable aperture of restrictive

protocol → TCP (up) → Reliable → connection oriented
UDP → Best effort → connectless

→ TCP examines the packet data is either transferred or not, it sends sequential packets of data
→ UDP is quite opposite.

UDP Protocol:

continuous packet sending without analysing.
→ Best effort delivery (unreliable)
→ provides application with access to network layer.
→ saves the overhead of reliabity.
→ connectionless, Limited errorchecking.
→ Data loss like duplication etc…, we cant recover data.

UDP Header: → present in TCP & UDP.

Packets → → → → → → → →

16 bit source port	16-bit destination port
16 bit UDP length	16 bit UDP check sum
Data	

It checks for satisfying the conditions then it sends data

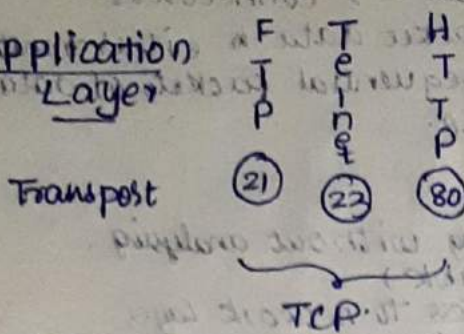
TCP PROTOCOL:

→ Reliable.
→ provides access to network layer for application
→ connection oriented protocol.
→ Error checking (Data recovery) ← (3 way hand shaking process)
→ Sequencing.

TCP header:

16 bit source port								16 bit desti port	
32-Bit sequence number									
32 bit Acknowledgement num									
4 bit header length	resv	ns	cwr	ece	urg	ack	psh	rst	syn	fin	16 bit window size
16 bit TCP check sum								16 bit urgent pointer	
options									
Data									

MAPPING LAYER 4 TO Applications:

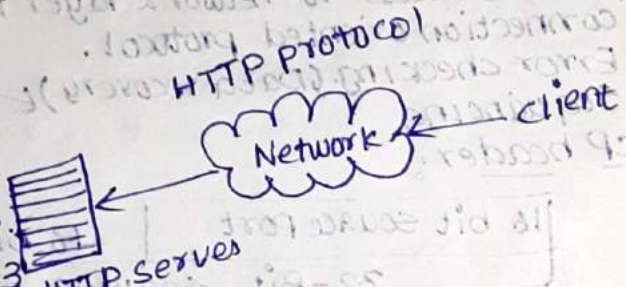


Application protocols:

- Web services
  - HTTP
  - HTTPS
- File sharing services
  - FTP
  - TFTP
- Mail services
  - SMTP
  - POP3/imap
- DNS services
  - DHCP

HTTP:

- Supports web services
- uses portnum 80.
- Secure version #HTTPS
- HTTPS-Portnum-443
- Transfers Text/Images, Hyper Links



FTP:-

- File Transfer protocol
- Portnum-21
- 3rd party programs
- MS windows OS
- web browsers works as FTP client

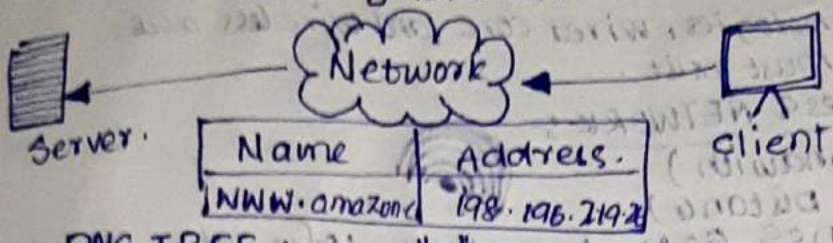
Email protocols:

- SMTP
- POP3
- IMAP-internet message ACESS protocol

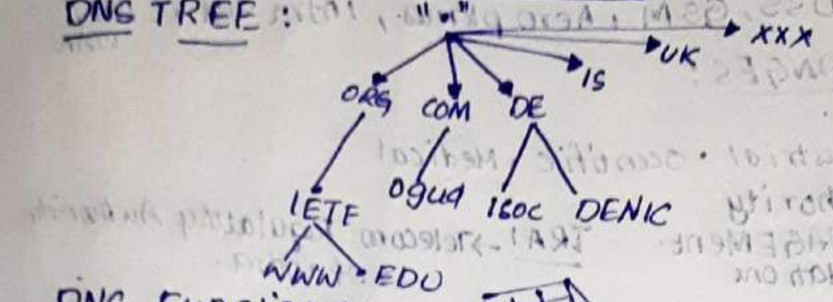
DNS server:

→ Translates Domain names to IP Address

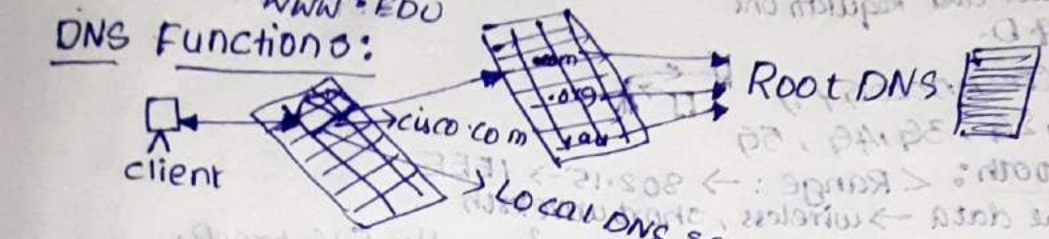
Resolving DNS Addresses.



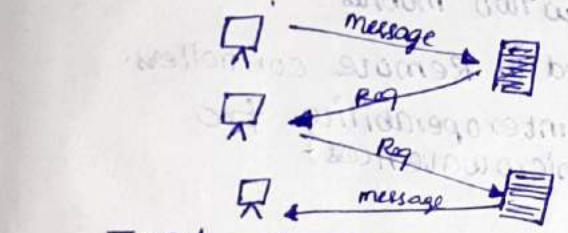
DNS TREE:



DNS Functions:



DYNAMIC HOST CONFIGURATION PROTOCOL:



TCP/IP TOOLS:

IPCONFIG: in cmd:

command: ping www.google.com

sent 4 packets and received 4 packets

cmd → ftp

cmd → arp -a.

PING TOOL

PING:

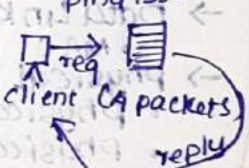
ping -l

ping -n

ping -r

ping -w

PUBG → PING ISSUE



Time gap b/w the req and reply b/w system and server.

BENIFITS OF WIRELESS NETWORK.

- Mobility, flexibility, scalability etc.

Wired vs Wireless:

- Mixing both Technologies, wired core and wireless access.
- wired network must exist.

Types of Wireless NETWORK:-

- Frequency (Bandwith)
- Covered Area (Distance)
- Satellites, GMDSS, GSM, Aero planes, Infrared, LAN, WAN

FREQUENCY RANGES:

- Licensed band.
- ISM Band - industrial - scientific - Medical
- Regulatory Authority
  - Spectrum MANAGEMent.
  - Rules and Regulations
  - R&D.

IRAI → Telecom Regulatory Authority of India.

GSM (Technology:)
1G, 2G, 3G, 4G, 5G

Bluetooth: < Range :→ 802.15 → IEEE
→ share data → wireless, shortwavelength.
Personal Area Network. } handles SIG group.
↓
creating a network medium b/w two mobiles.

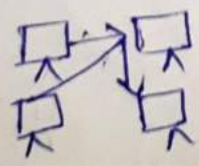
Infrared:
⇒ EMR → Longer wavelengths. → used in Remote controllers.

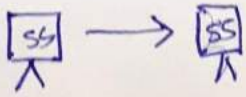
Wimax: 802.16. (world wide interoperability for microwave Access)
→ WAN Technology
→ compact LTE.
→ provides triple play data sharing.

→ WiFi:
→ wireless Fedility → 802.11 → LAN Technology.
→ ISM band → uses 2.4GHz and 5GHz.
→ Governed by wifi Alliance.
→ Data Link Layer.
  - MAC, LLC.
→ physical Layer.
  - Physical Layer convergence procedure PLCP
  - Physical Medium dependent (PMD)

→ infrastructure
  - USES Access point
  - Star topology.
  - More comonly used

AD HOC MODES
→ Direct communication
→ more flexible





Vulnerability and Exploit:

- Vulnerability.
  - weakness or absence of safeguards.
  - Holes or gaps software (bugs.)
  - Can be exploited by threats
  - it is a backdoor in our protection efforts.

Exploit:-

- An exploit is a program, script, or code.
- Aim to perform unauthorized operation.
- An example is a backdoor Trojan used to grant unauthorized access to machine.

RISK: → The potential of loss.

- Measure of cost of vulnerability.
- Result of a Threat exploiting a Vulnerability.

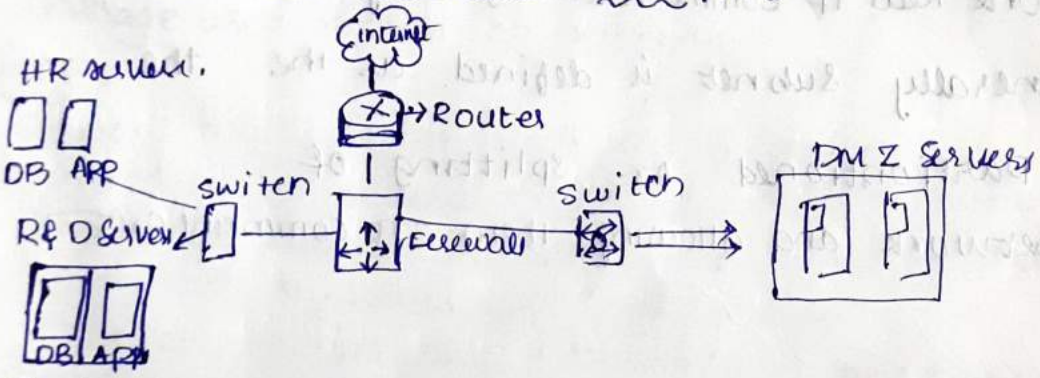
IMPACT:-

The result of an exploited vulnerability.

- Deleted files. • Loss of data • Privacy.

RISK = Threat × Vulnerability × Impact.

SECURING The NETWORK DESIGN:-



Goals OF Network Design:

→ Publish separate mail, web, DNS servers to Internet.
→ required appropriate access, protection.

Network SECTIONS:-

- Public.
  - internet.
- Semi public.
  - web server. Mail, DNS servers.

•Private
internal systems.

FIREWALL PLACEMENT :-

→ B/w internet and other networks.
B/w the semipublic and private network path.

DEFENSE IN DEPTH :

- Protect the fire wall.
- Limit the visibility of traffic

VIRTUAL LANS VLANS

- Segment physical switches into two or more virtual swi
- VLAN can span multiple switches.
- Intercommunication computers belonging to same networ

IP Header :

protocol, TTL, source, destination ip.

SUBNETTING :

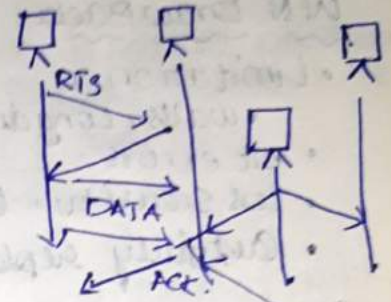
Subnet is broadcast domain same as VLAN
NAT and private addressing

- NAT is Network Address Translation.
- One Real IP communicating a group of IPs.

- Generally subnet is defined as the the partitioned or splitting of network and allowing them to communicate

SSID:
- Service set identifier
- used to identify wireless LAN.
- can be broadcasted or hidden
- length: 32 alphanumeric character.
- Can be composed of several access points.
- Single access point can connect to several SSIDs.

CSMA/CA:-
→ Carrier sense Multiple Access collision avoidance.
→ uses Request to send RTS and clear to send CTS.
to avoid collisions.
→ Possibility of collisions still exists.
- Led to slower performance.
- Recovered by retrieding



Wireless Network Devices:
- WAN (or) WAP.
Wireless access point → uses in physical and data link collision
- Networking hardware device.
- has ethernet interfaces RJ45 and antennae.
- Coverage area depends on antenna.

WAP:
- Supports multiple standards a, b, g, and n.
- Divided into several radio channels to avoid interface
- Configured through firmware direcly or web based.
- Obstructed by walls and Long distances.
- Connects Multiple SSIDs broadcasted and hidden.

WAP (> Vulnerability)
- Hidden SSIDs.
- Filtering based on:
Mac address, IP, port numbers, DN.
- Encryption
  - WEP.
  - WPA
  - AES.

USB Modem :-

- Connects pcs/laptops to GSM Network via mobile operator.
- Depends on network Gen 3G or 4G
- Needs wired infrastructure.
- charging fees according to subscription.
- less network speed than wifi.

SMART PHONES :

- WiFi . GSM . Bluetooth . Can acts as hotspot.

WN Draw Backs :

- Limitations :
  - walls, Long distance, weather conditions
- bit errors.
- Less security. (Sniffing)
- Can't fully replace the Wired infrastructure.

COMPUTER SECURITY :—

→ Network administrator seek to find a balance b/w →

Sec Goals 1 confidentiality → The data should only accessable to the required users
2 Availability → consistency of data, detect any modifications of data.
3 Intigrity → Legitimate users are not denied.

ASSETS :

- DATA, SOFTWARE, physical devices and documents.
- An asset is what we try to save or protect.

Threat :

- A person, thing, event or idea which poses danges to asset.
- A breach to following.
- A possible means of breaching a security poli
- Exploiting a vulnerability, intentionally or accidentally.

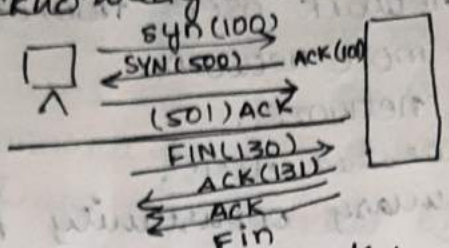
Information

~~SCID~~:

Tcp Flags :-

Control data flow and signal info to receiving host.

Flags are used to examines the data transfers based on Acknowledgement.



Port scanning and Tools :

checking which ports are active is called portscanning.

- Passive way of hacking.
- active attacks.
- Scan - 65,535 twice.
- once UDP and TCP.

Tools used → Nmap, Zenmap.

Types of port scanning Types.

- Ping Scan.
- TCP Full open Scan (SYN, SYNACK, ACK)
- TCP half open Scan( )

Port scanning can be done by taking permission from owner.

OS- Identification :-

→ Looks for subtle differences in target response.
→ Develops a fingerprint.
→ Compares fingerprint against a pre build dB OS Fingerprints.

⇒ NMAP :

- Port scanning software.
- used on Ms windows and linux.
- Zenmap with GUI.

Sniffing and Tools :

- Allows to capture data as it is transmitted over a network.
- To diagnose network issues.
- Malicious users to capture unencrypted data.
- Way of passive attacking.
- Breaching confidentiality.

Tool for Sniffing. - TCP Dump.
Wireshark :- used for Sniffing.

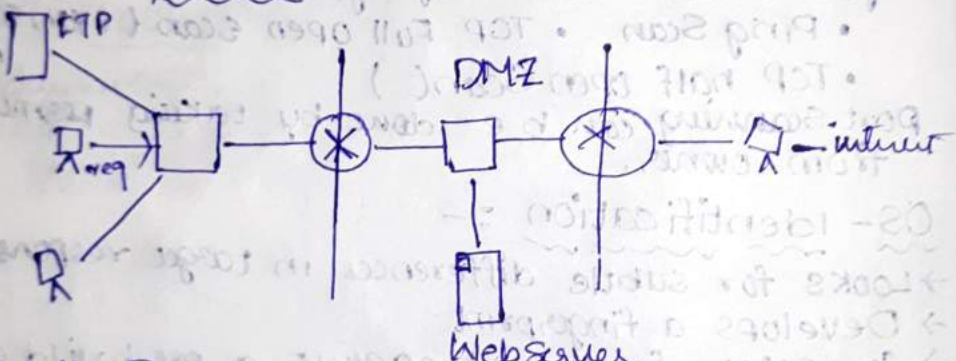
Firewall :-

- Firewall is one of the most effecitive security tool
- protects internal network users from external threat
- Resides b/w two or more networks.
- Controlls traffic b/w networks.
- To prevent unauthorized Acess.
- A Firewall is the primary opportunity for attack negation

Benifits :-

- Filters communication based on Content.
- protect internal / external systems from attack.
- perform NAT (Networks Address Translation)

Firewalls placement :-



Firewall Rule :-

- Firewaal rule controls the decision of the Firewall on inspected traffic.
- Controls what happens what a packet doesnt match an existing rule:
  - Default deny - more restrictive.
  - Default allow - more permessive.

Ingress : incoming traffic.
Egress : Out Going data.

Transfer of data Transfer over a wireless Network:

Most wireless networks work of radio waves
Each component of a wireless network nan adapter or network has an network card it was designed to intercept and broadcast specifically tuned radio waves.

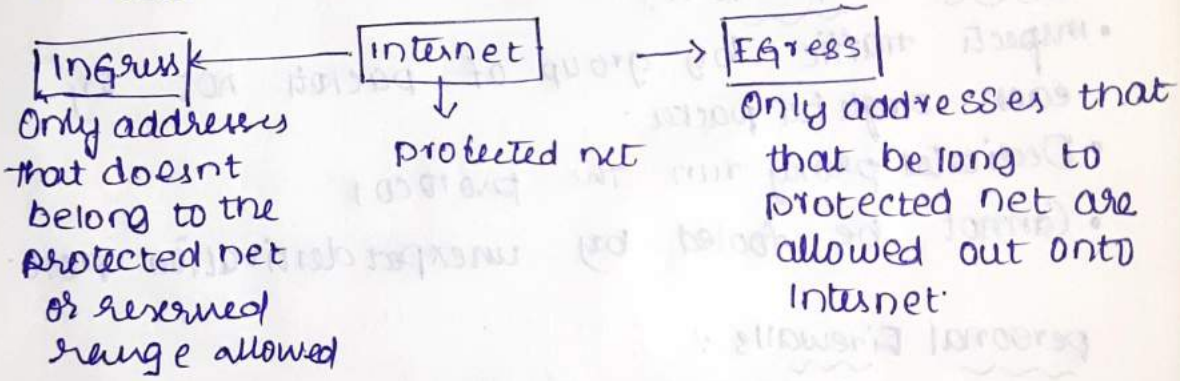
Usually the wireless router takes the physically transmitted data and converts into radio waves. which it transmits through antenna.

Data is tranemitted by being converted from its binary form of zeros and ones into radio waves. media. The newly converted data is then broadcasted and intercepted by wireless adapters

Wireless network radio frequencies 2.4GHz or 5GHz. user higher frequency allows more data Transmesion.

Firewall is primary oppurtunity for attack negotiation.

Firewall

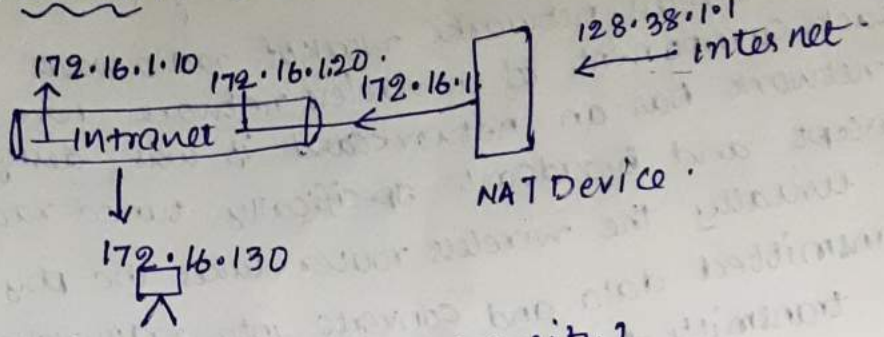


Firewall filtering:

→ packet filter fire walls:

- Low end firewalls.
- Can enhance security.
  - Very fast
  - Reliant on DESTPORT
- Data content passes unchecked.

NAT Firewall: (Network Address Translation



Proxy Firewalls: (high security)

→ Maintains complete TCP connection state and sequencing through 2 connection.

- user to proxy session.
- proxy to destination server session.

- Process table manger to keep connection straight
- Slow performance.
- The most secure form of firewall.

STATEful inspection:

- inspects traffic by group of packets not by each single ful packet.
- Dedicated proxy run the protocol
- Cannot be fooled by unexpect destination port.

personal Firewalls:

- windows firewall
- packet filters.
- Stateful firewalls of unix.

Firewall:

Firewall can be a primary intrusion detection.

Honey pots:- (Trap to find intruders (or) host trap)

A kind of network of host trap.

- Network trap.
- A decoy - if a machine becomes hot for attackers.
  - change the ip address and name.
  - put in a honey pot.
- DNS, Mail, Web servers make great honey pots on their unusual port.

When to use Honey pot:-

The firewall, properly configured, stop this attack. That good. But you can't learn anything about attack. that bad.

Honey pot products:

DTK, Symantic Decoy server, Honeynet etc...

By pass Firewalls and Tools:

1) Peer to peer file sharing: (one to one)
   - introduces security weakness.
   - loop hole in a firewall.
   - users give away network information.
2) Modems:

The more restrictive a site's firewall policy, the more likely the employees will modems.

IDS: (intrusion detection System)

- Host - based.
  - HIDS.
- Network based
  - NIDS.

• Reports against attack of

IDS Alerts:

- Alerts auto generated from Event of intrest.
- Alert can be line on screen, msg.
- Rules to specify which events genarated.

- HR IDS
  - content monitoring system.
  - Ethical spy on employee.
  - inside intruder can be detected.
  - company ensuring their policies.

NIDS:

- Deployed as a passive sensor at network aggregation points.
- Captures traffic like a sniffer.
- Detects EOI on network.
- uses the analysis of
  - signature.
  - Anomoly.
  - Application/protocol.

Signature Analysis:

- Rules indicate criteria in packet that represent EOI
- Rules are applied to packets as they are received by the IDs.

Anamoly Analysis:

- Flags anomolies conditions
- Unexpected conditions are identified
- Requires understanding of what normal.

Network IDs:

Application / Protocol Analysis:

- IDS has understanding of logic for a specific application or protocol.
- Any protocols activity that is not known as normal is flagged.
- Difficult to implement

NID challanges:

- Deployment & acess limitations.
- Analyzing encrypted traffic.
- Quantity vs quality of signatures.
- Performance limitations.

SNORT AS IDS:

↳ Type of tool for ids (less cost)

- Suitable for monitoring multiple.
- low false alarm rate.
- low effort for reporting.

SNORT Capture:

Detail analysis of the Root logging. (evidences).

NIDs pros and cons:

- PROS:
  - Fairly easy to setup.
  - Does not affect the speed of network.
- CONS.
- Low sensor speed.
- Almost impossible to detect

IPS: intrusion prevention system.

- IPs stops attack on any systems and networks from being effective.
- NIPs and HIPs.
- Technology more recent than IDs.

1. Introduction to computer Networks.

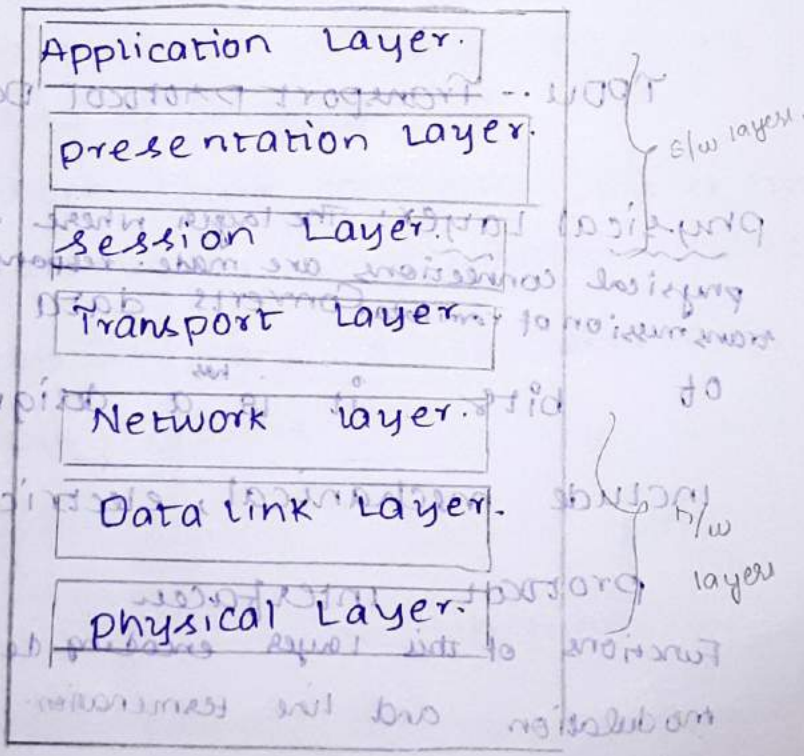
. Explain OSI refrenced model with its archetecture and layer structure?

- Open System interconnection Model was developed by ISO (International standard organization) in the year 1983.

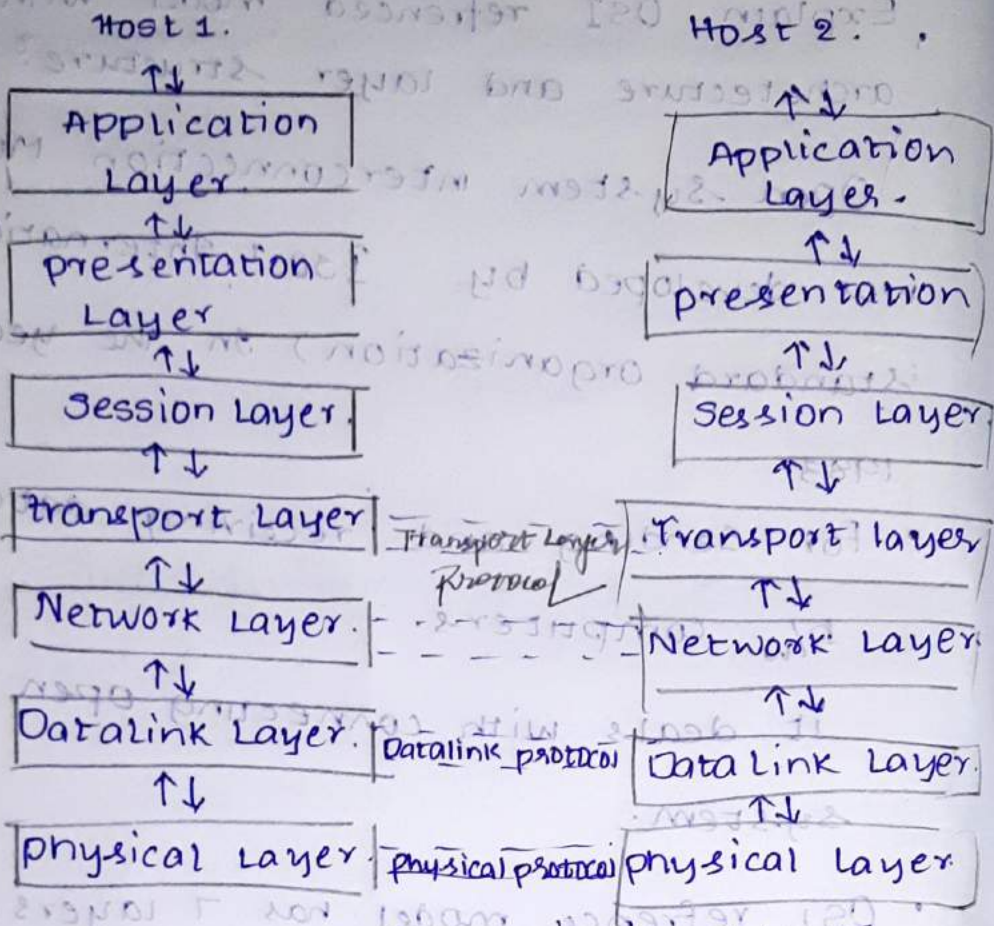
- For sending and receiving data b/w computers.

- it deals with connecting open system.

- OSI refrence model has 7 layers.



Architecture:



TPDU -- Transport protocol Data unit.

physical Layer: The layer where all the physical connections are made. responsible for transmission of raw data. Converts data in form of bits it is has a design issues include mechanical, electrical, protocol interfaces.

Functions of this layer encoding decoding modulation and line termination.

Data Link Layer: divided into two layers
Logic link layer, MAC sublayer
Above the physical Layer the function of datalink Layer is to break data into frames, manages access to physical medium
• it regulates the flow of traffic in case of fast senders transmitting the data (Transmitting data) to slow receiver
• it provides error free transmission
• reliable

Network Layer:

The function of network layer is to convert input data into packets
• it is also route the packet from source machine to destination by appling algorithms.
• Network Layer controls the entire operations of communication subnet.
• Establish and delete connection across network.

Transport Layer
• reliable.

The function of transport layer is to convert

i/p data into segments.

- it accepts data from session layer and divides into small pieces. and each piece is called TPDU.
- it regulates flow of information, controls the dataflow from fast sender to slow receiver.
- it establish multiple connections

Session Layer:

responsible for conducting sessions among differenet machines.

- it receives the data from session Layer. from presention Layer and divided data into small piece. each piece is called SPDU.
- it prevents both sides from attempting the same operation at same time by using token Management system.

it mainly concentrated on syntax and symantics of the data.

- it receives data from Application layer and divides data into small pieces each piece is PPDU. presentation protocol data unit

Application Layer

→ Implementation of various protocols used for uses interactions.

- All high level protocols are implemented in this Application Layer.

http, Ftp, DNS, RTP, POP3, IMAP, Telnet, DNS.

TCP / IP:

Transmission control protol / internet protocol:

- TCP / IP refrence model was developed to acheive the following goals.

1) connecting multiple networks to make look as single network.

2) Enabling network to service from partial failures

3) TCP/IP model consists of 4 layers which is shown in below figure.

Application Layer.

transport Layer.

internet Layer.

Host to network Layer.

- Host to network Layer:

This Layer is similar to physical and datalink Layer in OSI refrence model

- Internet Layer:
  This Layer is very similar to network Layer in OSI.
- The responsibility of internet layer is to send packet from a source machine in one network to destination machine in different network.
- These packets are routed independently by taking a different path from source to destination.
- internet protocol is a connection less protocol (IP)
- Transport Layer:
  very similar to transport Layer in OSI model
  This Layer is end to end protocol or Defined in this Layer enables the source and destination machine to exchange data with each other.
- TCP, UDP - 2 types of protocol.
- TCP: - Transmission Control protocol
  - Reliable connection Oriented protocol
  - Error free transmission is allowed.

- Tcp segments input data stream into discrete messages at the source and receiver end.
- Tcp groups the received messages and produce output data stream.
- It handles flow control.
- To control the data flow b/w fast sender, slow receiver.

UDP protocol: (user datagram protocol)
- unreliable connection less protocol.
- it doesnt handle flow control.
- Generally used in application like speed and video, audio.

Application Layer: All high level protocols are implemented in this Layer they are http, FTP, RTP, POP3, Telnet

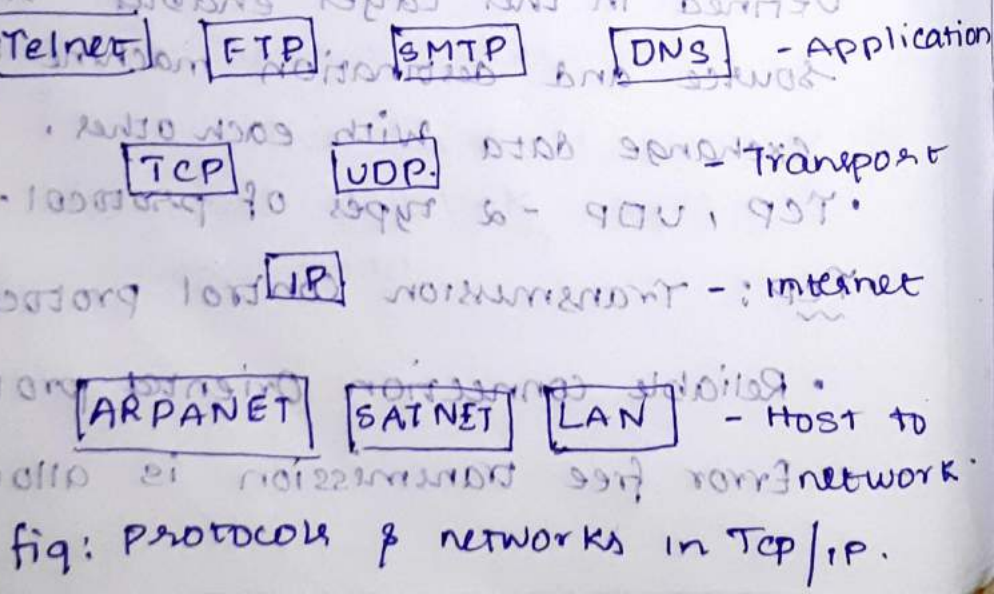


fig: protocols & networks in Tcp/IP.

Classification and features of networks:
(LAN, WAN, MAN)

1. LAN: Local area network.

In Lan usually all the systems are connected to a single cable.

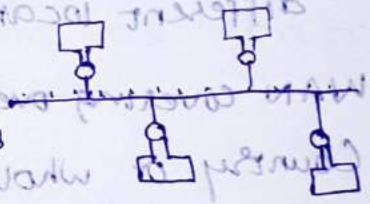
For eg: in single office all computers are connected to a single cable and they exchange information with each other by using the cable.

LANs are limited size upto few Km(100)

The transmission technology used in LANs is a single cable to which all the machines are connected.

The most common network topologies used by LAN are: Bus, Ring topology.

Bus topology: single bus



Ring topology:

MAN: Metropolitan area Network.

similar to MAN but Larger than LAN and smaller than WAN.

The area covered by a man is upto a city (50 Kms)

The transmission technology implemented in MAN is distributed queue through dual Bus (DQDB) consists of two unidirectional buses to which all the computers are connected.

WAN:

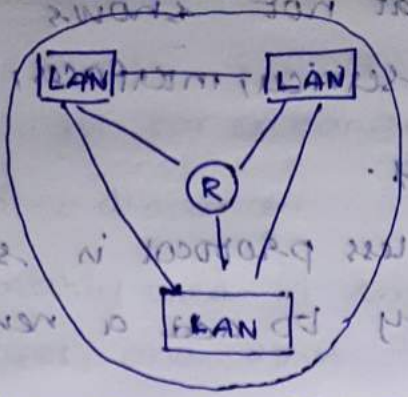
It used to connect two or more LANs that are present in different locations.

It is used for different communications from two or more LANs with different locations.

WAN covering over very Large region such as Country or whole world.

In WAN all the computers are connected to a communication subnet, subnet consists of transmission lines and routers.

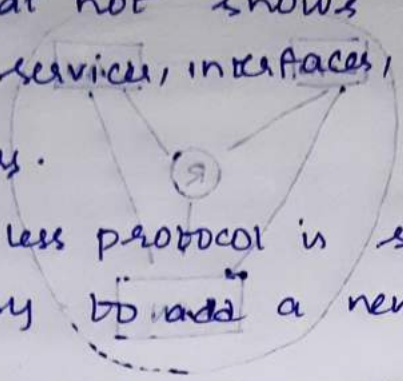
Subnet:



Difference b/w OSI and TCP/IP model:

- OSI model clearly shows the difference b/w services, interfaces and protocols.
- It has 7 layers.
- Supports connection oriented and connectionless.
- New technology can be added easily.
- It was designed before the protocols came into existance.

- Tcp/ip model that not shows the differences b/w services, interfaces, protocols
- it has 4 Layers.
- only connection less protocol is supported.
- it is not easy to add a new technology.
- First protocol came into existance then model was designed.



Importance of WiFi, Bluetooth:

WiFi:

it is a technology that enables your WiFi Devices using radio waves.

it is most commonly used homes schools and offices etc....

wifi works sending packets from one device such as laptops, mobiles, through access points.

- 18M Band - high bandwith.

uses faster internet connection.

Connect device

To Transfer files.

WIFI calling.

Bluetooth : SIG groups

It is a low power wireless technology for exchange of data over a short distance.

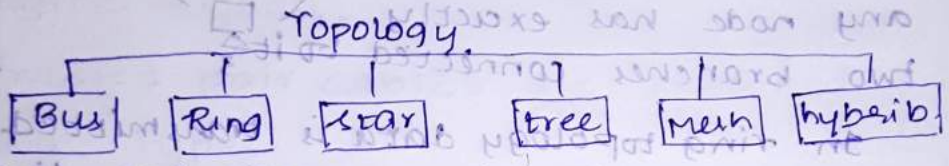
- Primarily used in smartphones, Laptops, tablets, and other devices.
- Low power and Low bandwith to connect other devices. (headsets, cars) playing games, transfer files to connect audio devices.

• Explain about topologies.

physical and logical arrangement of nodes is called topology. (network topology)

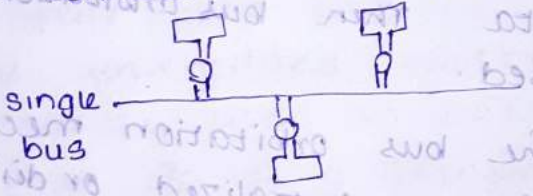
There are six network topologies

1) Bus topology.
2) Ring topology.
3) Star topology.
4) Tree topology.
5) Mesh topology.
6) hybrid topology.



Bus Topology:

In Bus topology all the machines or nodes are connected to a common bus.



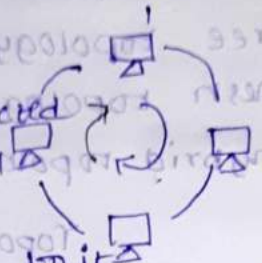
at any time any computer can send the data to the bus to another computer.

* When more than one computer wants to send data at a time in such situation buses orbitation mechanism is used.

The bus orbitation mechanism may be either centralized bus orbitation mechanism, distributed orbitation mechanism this mechanism will decide which computer has to send the data first.

Ring topology:

As the name indicates the computers are connected in the form of ring



any node has exactly two branches connected to it

In ring topology data is transmitted among the ring in a particular direction.

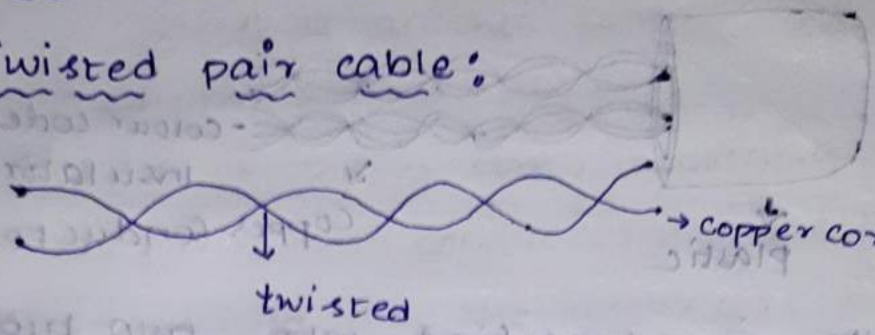
In ring topology also if more than one computer wants to store or send the data then bus orbitation mechanism is used.

The bus orbitation mechanism may be either centralized or distributed. which decides which computer should transfer data first.

if link fails entire network is collapsed.

Explain about LAN CABLES:

1) Twisted pair cable:



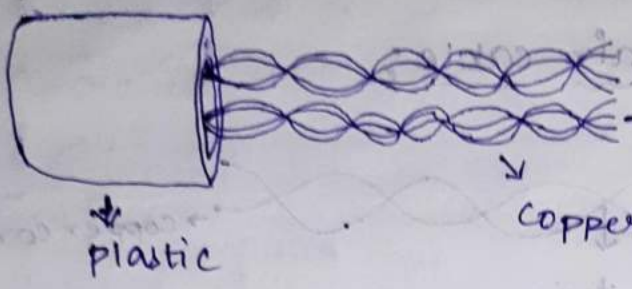
It consist of two insulator copper wires which are twisted together it is used to transmit analog and digital signals.

Twisted pair cables are classified into two types.

1) unshielded twisted pair cable.
2) sheilded twisted pair cable.

1) unsheilded Twisted pair cable:

- A twisted pair cable without sheilded is called as unsheilded twisted pair cable mostly used in LANs.
- i.e; LAN users UTP as a transmission media and the data rate of UTP is 10 mps to 1 Gbps.
- The data rate depends on the thickness of wire and distance travelled by signal between transmitter and receiver.



UTP is classified into two types

1) category 3 twisted pair cable.
mainly used in telephone systems.
a) it supports the data rate upto 10mbps.

category 5:

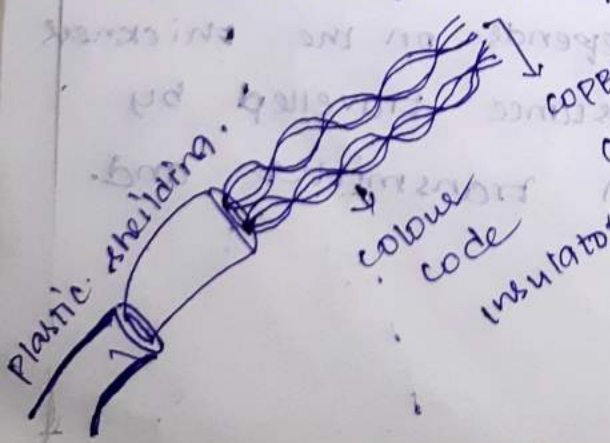
Mainly used in LANs.
the data rate supports upto 100 mbps.

Sheilded Twisted paircable:

A twisted pair cable covered with sheild is called stp.

Not commonly used in network

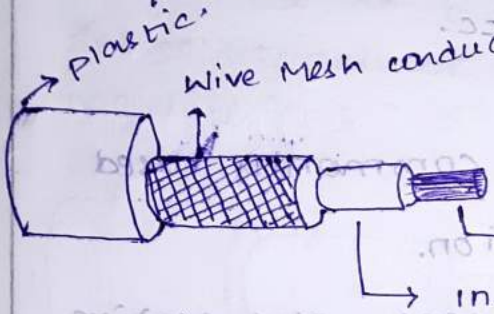
stp data rate is upto 1000 mbps.



Co axial cable:

It is another common transmission medium

- It consists of copper core, insulating material, Wive mesh conductor, protective plastic covering. Here the copper core is enclosed with insulating material, it is surrounded by Wive Mesh conductor, the Wive Mesh conductor is covered by a plastic.



it is used to transmit both analog and digital signals.

- Data rate / Transmission Rate of coaxial cable is 10 mbps.
- Divided into two types.
  1. Base Band coaxial cable. (Thick cc)
  2. Broad band coaxial cable (Thin cable)

Base Band cc:

- also known as 50 Ω cable. It is very thick cable.
- Base Band cc is commonly used for digital transmission
- Here Base Band means entire cable Bandwidth is used to transmit a single stream of digital data.

Broad Band cc:

- also known 75 Ω cc.
- very thin cable.
- Broad Band cc is commonly used for analog transmission.
- Here Broad Band means the entire cable bandwidth is used to transmit multiple analoge over same cable.

Fibre optical cable or optical Fibre:

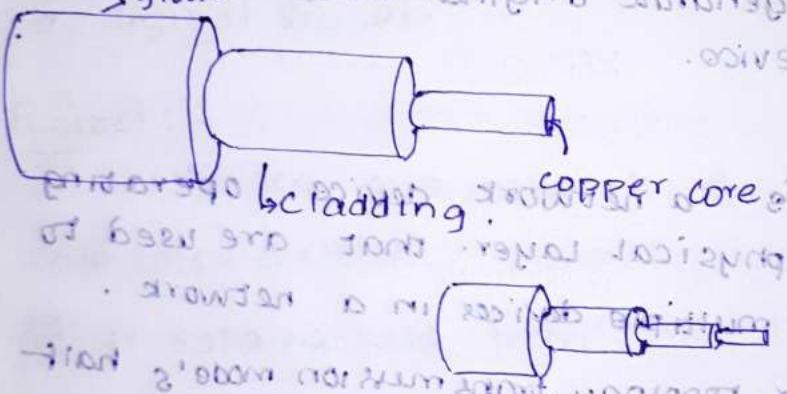
guided media.

it uses light instide of electrical signals to transmit signals.

Fibre optical cable made up of glass or plastic with a diameter 8 to 100 micro metres.

In Fibre optical cable the core is surrounded by cladding. the purpose of cladding to keep all the light in the core.

Optical fibres are bounded together and covered by the protective jacket. The jacket can be made up of plastic material.



high inflamation capacity, more secure less repeaters are required, less expensive. digital transmission high speed, light weight, more flexible and strong.

Applications:

- Cable Tv systems.
- Tele communication.
- Communication network LAN & MAN
- Secured communication system of military
- CCTV.

Explain about LAN Devices:

i) repeaters:

repeaters is a network device, it operates at physical layer in OSI model it regenerate signals over the same network before the signal become too weak corruted. when the signal become weak than copy of the signal bit by bit regenarate original data it is two ports device.

(ii) HUB:

HUB is a network device operating at the physical layer. that are used to connect multiple devices in a network.

ex: star topology, transmission mode's half-duplex.

(iii) Switches:

Switches are network device. operating at Data link layer. switching network is a multiport device in users mac address. To send data packet to selected destination ports transmission mode is

is full duplex. That is communication in both direction at same time switching com perform some error checking before forwar ding data to destination port ports are high.

(iv) NIC:

NIC is a hardware components without computer cant be connected over a network it is also called as network interface controller, Network adaptor, LAN Adaptor. NIC both wired and wireless communi cation. NIC operator at the physical layer and Data Link Layer. NIC is used to convert the data into a digital signal.

Router:-

Router is a network device. It connects different networks together and send data packets from one to one another network. a Router can be used both LAN TO LAN and LAN TO WAN. it transfer data in the form of IP packets.

(vi) modem: (56 kbps) internal (or) external, ADSL Modem.

Modem is a network device, modem stands for modulation and demodulation modem converts digital data signal to analog data signal. some modem corportive bubble sumeoutly voice and data. They on detive calls and telephone numbers.

(vii) gateways:

gateways is a network device that forms a two network operating with different transmission protocols. gateways operator a network layer: gateway generally implements as a node with multiple NIC connected difference network it uses packet switching techniques to transfer the data access the network.

Explain about LAN connectors:

1. Registered jack (RJ-45):

- It is a standard interface which often connects a computer to a local area network (LAN).
- It is an 8 pin connector.
- 45 is the number of interface standard.
- RJ 45 connector are also called as RJ-45 cable.
- RJ 45 interface is considered the most common twisted pair connector for ethernet and network cables.

2. Straight tip (ST):

It uses fibre optical cable.

- These straight tip connector is often seen on the end of a Multimode cable.
- It has been commonly seen with SC connector older version. i.e; slowly replaced by Multifibre connectors.
- ST is bidirectional transmission.

3. Subscriber connector:

It uses fibre optical cable i.e; uses a pushpull latching mechanism

similar to common audio video cables.

- It is a bidirectional transmission.
- It can be seen commonly on (MMF) Multi Mode Fibre (SMF) single mode fibre.

Lucent connector:

It also uses fibre optical cable or optical fibre cable.

It uses single mode

LC was developed for high density develop ments. (deployments)

where multiple cables would be terminated with in a confied modes.

Network Addressing & Subnetting.

Version:

which is four for IPv_4. It has four bits.

HCEN header Length:

The minimum value of this field is 5 and the maximum is 15. IP header length 4 bits which is the number of 32 words in header.

Type of service:

Type of service is also called differencial service core point (DSCP). It is a 8 bit field and low daily high throughput Realiits.

Total Length:

Length of header data. It is 16 bits which as minimum value of 20 bytes maximum 65,535 bytes.

Identification:

unique packet ID for identifying. group of fragment of a single IP datagram. It has 16 bits.

flags:

Three flags of 1 bit each. reserved bit must be 0, Do not fragment flag. more fragment flag same order.

fragment offset:

It represents the no. of data bits ahead of the particular fragment in particular datagram. specified in terms of no of 8 bytes which has maximum value of 65,520 bytes.

Time to leave:

It is an 8 bit feed that indicates the maximum time datagram will be live in the internet system.

The time duration is measured in seconds it prevents the datagram to loop through the network by restricting the no of hops taken by a packet before delivering to the destination.

protocol:		

Name of the protocol to which the data is to be passed.

It has 8 bits.

Header checksum:

for checking errors in data gram header it has 16 fields.

Source ip address:

32 bit ip address of sender.

32 bit ip addresses of the reciever.

option:

information such as source root, reciever root, used by the network administrator to check where path is working or not.

IPv4 is a connection less protocol used for packets switched network.

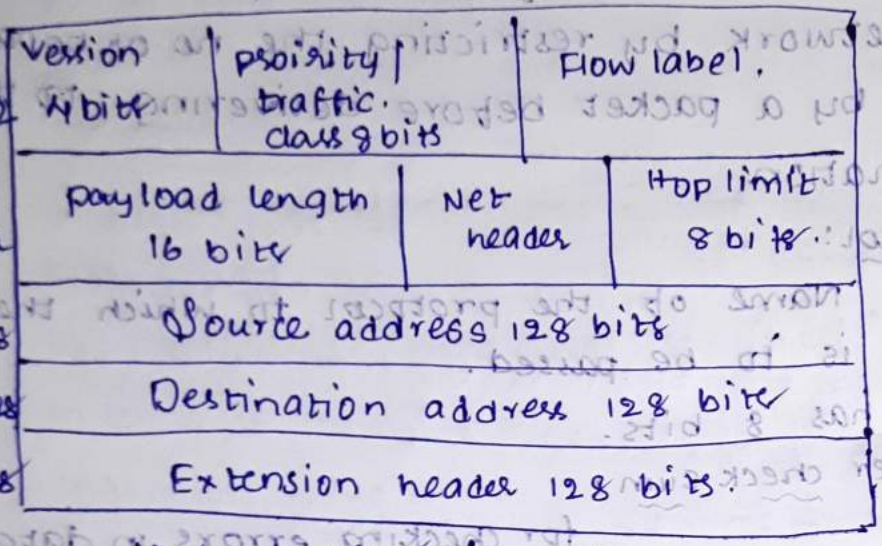
IP v4 is a 4th version of the internet protocol and widely used protocol

In data communication over different kinds of network.

It uses 32 bit address for ether net communication in 5 classes A, B, C, D, E.

→ IPV_4 address are written in dot decimal notation compreses of 4 octs.

eg: 198.168.1.2.



IPV_6 header format.

version:

It indicates the version of internet protocol which contains 4 bits. Traffic class. This field is similar to the service field of IPV_4 it signifies priority of IPV_6 packet

It is responsible for having the traffic based on the priority of packets

In case of congestion on router it dispose packet with low priority.

It is a 8 bit traffic class filed the source node can send priorities to the destination.

Node cant expect the same set of properties can change priorities on the way.

Flow label:

It is a 20 bit field this label ensures that the packet maintain the sequential flow belonging to same communi-cation. This source label sequence to help the router identifies that a particular packet belonging to a specified flow of information. This field helps avoiding of reording of data packets

while setting up the flow label the source is also supported specify the life time of flow.

payload length:

It is a 16 bit field that payload length indicates the routes about the size of information contained by a packet. This field is used to tell the routers how much information a particular packet payload contains in it packet

payload is composed of extension header and upper layer data.

It 16 bits = 65,530 bytes.

If the extension header contains nope by nopit extension header.

Net Header:
It indicates the type of extension header.
Where as in some cases it indicates protocols contains with in upper layer packets with in UDP, TCP.
It is a 8 bit field

Hop limit:
It is same as TTL (Time to leave) in IPv_4.
- It indicates maximum number of intermediate nodes IPv6 packets allowed travel.
- The value of hope limit field is decremented by 1 as it passes a link (router / hop)

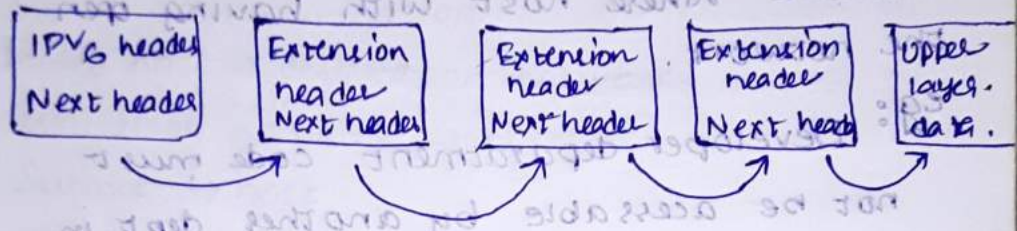
When the field reaches '0' this packets is discarded.

Source address:
It is 128 bit, IPv6 address of the original source of the packet.

Destination address:
It is 128 bit field
this field indicates address of destination, all the intermediate nodes can use this info, in order to crctly root the packet.

Extension header:

Introduced in IPV6 extension header mechanism is a very important of the IPV6 architecture. the next header part of IPV6 fixed header points to the first extension header. The first extension header points to the second extension header until it reach upper layes.



Subnetting:

Dividing the network into small networks

Small network maintainance is easy, it provides security from one to another network it provides higher network priorities.

Broad cast address:

A Broadcast address is an IP address that is used to target all systems on a specific subnet network instead of single host.

It allows information to be sent to all machines on a subnet.

Advantages of Subnetting:

Advantage is it reduces network traffic by loading the no. of broad cast sent out.

- It helps in overcoming limitations in LAN such as the maximum no. of allowed in host
- It allows people to connect to a work network where host with having open the network.

eg: Developer department, code must not be accessable by another dept in an organization.

Some Subnets may require higher network priority then others

eg:

A Sales department may need to host web cast or video conferences, maintainance is simple.

Maintainance is simple.

It we increases the no. of allowed hosts in LAN.

Subnetting decreases volume broadcast hence, minimizing the network traffic.

Subnetting is used to manage for maintainance and more flexibility.

Network security can be readily employed Subnetwork rather than employing with in the whole network.

To reach the process in a single network there are only 3 steps:

Source host network to destination host network.

destination network to destinatio host :

destination host - process.

Subnetting on other hand it uses 4 phases for internet communication.

Source host → destination network.

destination network → host

Subnet → host.

host → process.

Different Subnets need an intermediate device known as routers to communicate with each other.

It uses its own IP address. Network, Broadcast address.

More Subnets uses wastages of IP addresses.

Explain about class full b addressing in IPV4

- communication between network layer is host to host a computer some where in the world needs to communicate with another some where in world.
- usually computers communicate through internet

The packets transmitted by the sending computer passes through several LANS

or WANS before reaching destination computer.

We need a global addressing scheme we call this logical address as IP address on the network of TCP/IP protocol IP suite.

The Internet addresses are 32 bit length and the maximum of 2^{32} address (4.3 billions)

IP addresses:

It is a 32 bit address that defines a connection of a devices to Internet

2 devices on the Internet can never have the same address at same time.

A device operating at the network layer

Max addresses 2^{32} (4.3 billions)

Notations:

There are 2 Notations in IP address

1.) Binary Notation.

2.) Decimal Notation.

1) Binary notation:

In Binary notation IP is displayed as 32 bits, each oct is often refered as byte

• 4 byte address

ex: 198 . 12 . 0 . 1 . (identical to all ip's address.)

↓

10000 1001 1000 1000 0010 0000 0001

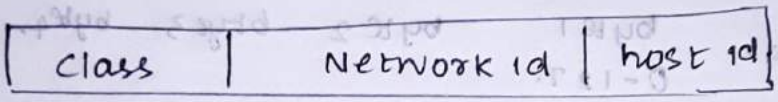
Dotted Decimal Notation:

ip addresses is easy to read, internet addresses are usually written in decimal form with a decimal point.

Separating with dot (.)

Parts of IP address:

Class Network bits, Host bits:



Classes of IPs: IP address space is derivided into 5 classes they are

class A:

For large organizations with a a large no of attached host or routers

class B:

Designed for Mid size organizations with 10's of 1000's attached host or routers.

class C:

These are designed for small organizations with a small or attached hosts or routers.

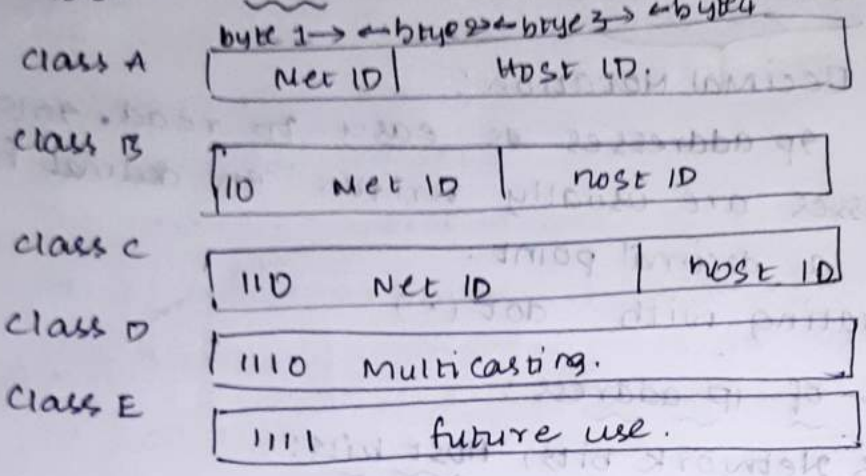
class D:

It is designed for multitasking each address in this class is used to define one group of hosts on the internet

Class E:

Reserved for future use

Internet classes:



	byte 1	byte 2	byte 3	byte 4.
Class A	0-127.			
Class B.	128-191			
class C	192-223			
Class D	224-239.			
Class E	240-255.			

Class LESS Addressing:

To overcome addresses and few more organization acess to Internet classless Addressing mode designed and implemented in this scheme there are no classes but the addresses are still guranteed in blocks.

address prevention on deplementation of addresses.

STATE NEED FOR IPV6:

- More allowance of unique TCP/IP addresses.
- NAT functionality vanished.
- Identifieres to be created, 4.3 billion created with IPV4

Types: security, scalability, connectivity.

- IPV6 allow better control of heavy media and critical acts perform on a network & allow faster.
- New field is included in IPV6

Networking protocols

Network protocol:

It is an established set of rules determined how data is transmitted bw different devices in same network.

HTTP:

- HTTP is a protocol that can transfer information over the network.
- It is the internet protocol suite method and defines commands and functions used for sharing web page data.
- HTTP uses the server client model

A client for ex: Laptop / telephone devices

characteristics:

It is ip based communication protocol which is used to deliver data from server to client.

- A server process a request by client and also server and client knows each other only during current request and response period.

Any type of content can be exchanged as long as server and client are compatable with it.

One data is exchanged then server and client are no more connected with each other.

it is a request and response protocol based on client and server based protocol.

It is connection less protocol bcz after connection is closed, server doesnt rembes anything about client.

It is stateless protocol because both client and server doesnt expect anything from each other but they are still able to communicate.

Advantages:

- Memory usage and CPU usage are low bcz less simultaneous connections.
- Since there are few TCP connections hence network congestion is less.
- The error can be reports without closing connections.
- HTTP allows HTTP pipelining of request or response.

Disadvantages:

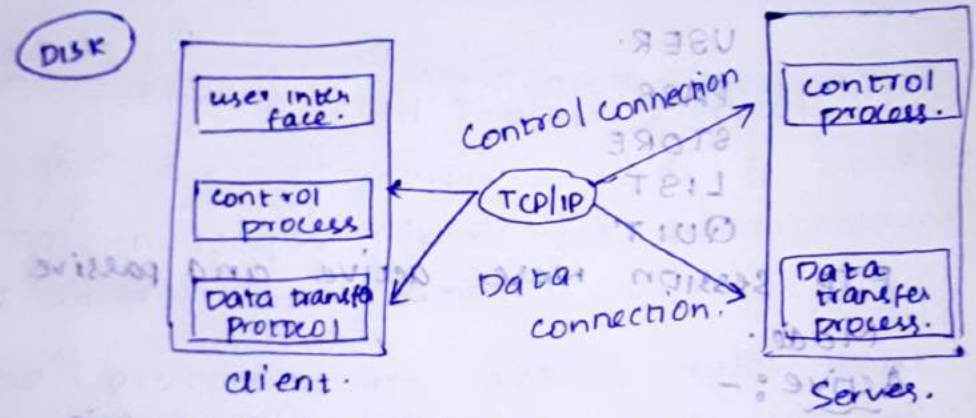
- HTTP requires high power to establish communication and trans fer data.
- Less secured because it doesnt uses any encryption method.
- HTTP is not often genimue exchange of data bcz less secure.

FTP:

- File transfer protocol
- client server protocol it is an application layer protocol that moves files b/w local and Remote file system.
- It runs on the TCP, HTTP
- To transfer files TCP is used by FTP in parallel.

1.) Control ~~protection~~ connection.

2.) Data Connection.



1.) Control connection:

for sending control info like user identification, pswds, cmds to change the remote directly cmds, retrieve and store files, port num: 21

2.) Data connection:

for sending the actual file FTP makes use of a data connection.

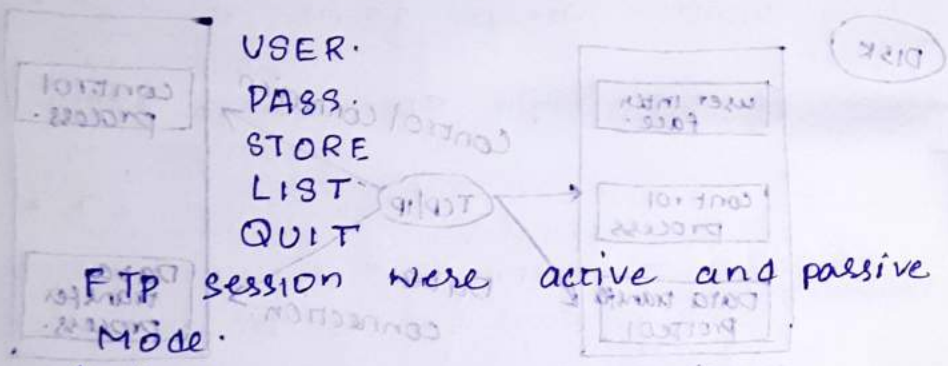
A data connection is initiated on port no. 20.
FTP uses separate control connection.
FTP needs to maintain a state about its user through out the session.
• It uses ds.

3 FTP ds :-

1.) File structure.
2.) Record structure.
3.) page structure.

Commands and Replies:

FTP commands are:



USER.
PASS.
STORE
LIST
QUIT

FTP session were active and passive Mode.

Active :-

After a client gntiates a session via command channel request, the server creates a connecton back to client and begin data transfer.

passive:

This server uses cmd channel to send the client gnformation gt needs to open a data channel. because passive mode has the client gntiating all connections it works fireworks and network address translation gateways.

FTP Types:

- Anonymous FTP

it provides supports for data Transfers Without encrypting data.

or

Using a username, password.

it is most commonly used for download of material i.e., allowed for unrestricted distribution it works on port.

password protected FTP:-

FTP secure:- ETC

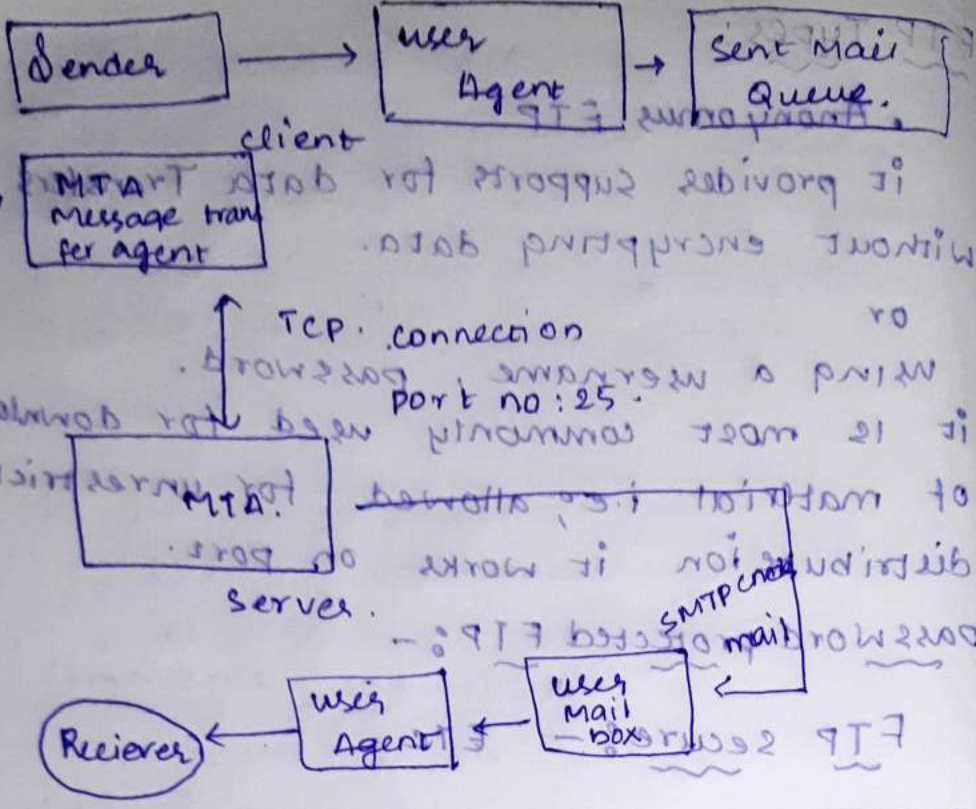
SMTP:

Simple Mail Transfer protocol.

It is an email protocol used for sending email messages from one email account to another via internet.

Email protocols are set of rules that are different email clients and accounts. easily exchange information and SMTP is one of the most common one analog style for POP and IMAP.

Push protocol and is used to send the Mail where as POP3(post office protocol) IMAP(internet Message Access protocol) used to retrieve those emails at reciever side.



SMTP Model Two types:

- End to End Method.
- Stored Forward Method.

- End to End Model used to communicate bw different organizations.
- Store and Forward Method is used within organization.

Both the SMTP client & server should have 2 components 1) user agent (UA)

a) Local MTA.

Communication b/w Sender & Reciever:

(The senders user agent prepares) message. and sends to MTA

MTA responsibility is to transfer the Mail across network to the recievers MTA. To send Mail system must have a server MTA.

SMTP commands:

DATA - Send data line by line
MAIL - Message transfer
HELO - identifies client to server only sent to one person.

ARP: (Address Resolution protocol)

1. Stands for ARP.
2. important protocol in OSI model. which helps to find MAC using systems IP.
3. The ARP main Task is to convert 32. bit (IPV_4) into a 48 bit MAC address.
4. It is a communication protocol. is mostly used to determine the hardware MAC Address from an IP.
5. It is also used when one device want to communicate with some other on a local network.

- physical Address.

- logical address.

Working of ARP:

RARP (Reverse address resolution Protocol)

- it is a protocol it is a type of client server model
- A client computer requests its IP address from gateway servers address resolution table.
- A network administrator creates a table in gateway which is used to map the Mac address to an IP address.

Mac address Requires: individual configuration on Server.

- RARP server will return the IP addresses to the computers or Machines.

Working of RARP:

- It is on the network access layer and it sends data between 2 points.
- Each network participants a pair of unique address (IP + MAC).
- IP addresses gets assigned by software and after Mac addresses is constructed into process of hardware.
- RARP servers that Responds to the Request
- RARP Data transfered in form of packets
- It must hold the data of all of the Mac address with their assigned IP addresses.
- If a RARP Request and Response from RARP servers.

Uses of RARP:

- Used to convert ethernet addresses to an ip address.
- It is available for LAN technologies like token ring FBDDIC.(Fiber Distributed Data Interface).

Telnet :-

It is a type of protocol that is used to connect computer to local computers
used as standard TCP/IP protocol for virtual terminal server given by ISO.
Telnet operation being performed on Remote Computer displayed by local computer.
client Server Model.
it allows user to connect and logon to another host on network from their computer from using login credentials.
It uses TCP protocol for connections.
Telnet uses port number 23.

Advantages:

used to send and receive information
it supports authentication.
Telnet client and server implements NVT Network virtual Terminal.

Disadvantages:

Not possible to run GUI Based tools.
it is not possible to transmit GUI

expensive.

- It uses more switches.
- user id and password transmitted without encryption.
- Security issues.

SNMP:

Simple Network Management protocol

- Application layer protocol for Managing and Monitoring networking devices of LAN or WAN.
- The purpose of SNMP is to provide Network devices.

Routers, hubs, switches, servers

- SNMP has 3 different versions:

  $SNMPV_1$ - RFC 1157 (cmds)
  $SNMPV_2$ - RFC 1901 to RFC 1441
  $SNMPV_3$ - RFC 3410.

  - $SNMPV_1$ implemented using structure
  - $SNMPV_2$ Error handling is used to Error detection. more efficient
  - $SNMPV_3$ security and privacy
  - It consists of SNMP Manager

A Manager system is a separate entity to responsible to communicate with SNMP agent implemented Network devices.

SNMP Key functions:

- Query agent; gets response from agent
- set variable in agent
- Acknowledge from agent

SNMP agent:

allows agent to collect Management DB to SMNP Manager.

In agent program packaged within network element.

Management information DataBase (MIB):

Commonly shared DataBase between Agent and Manger is called MIB.

MIB contains standard set of statistical and control values.

Network Management:

Process of configuring and monitoring and managing the performance of network.

Features:

Network automation.

administration.

Network operation.

Network assurance

Network provisioning.

Network Maintainance

Network Analytics

Network automation:

procedure of automating the configuring, handling, testing, deploying and operating of physical and virtual devices inside a Network.

Network service availability increases.
Network administration uses the tracking of network resources, including switches, hubs and servers
it also include performance monitoring and software.

Network operation:
It is easy to identify the problems because network functioning as created an including monitoring of activities.

Network assurance:
Features helps improves network performance
- Customer experience
- Security
- Assurance System includes
- Improves network Analytics, application analytics, policy analytics.
- Network provisioning:
  involves network resource conjugation for purpose of given service support, like voice functions etc.,
- Network Maintenance:
  Covers upgrades to network resources

Network analytics :

S/w tool that compares incoming information against preprogramed operational Model.

DHCP :-

DHCP server maintains pool of IPs and leases and address to DHCP enabled client when it starts up on network. Because the IP addresses are dynamic rather than static, addresses no longer in use are automatically returned to the pool for reallocation.

The network administrator establishes DHCP servers that maintain TCP/IP configuration information & provide address configuration

- valid TCP/IP configuration params.
- valid IP address.
- Reserved IP address associated with DHCP

RMON

Remote Network Monitoring:

Process of monitoring network traffic on a remote ethernet segment to detect network issues such as dropped packets, network collisions and traffic congestion.

The Working:

RMON implemented as a standard MIB (Management Information Base) or RMON is enabled in devices.

Including the

Standard Alone devices called dedicated RMON

- probes permanently installed / Temporarily where designed on the network.
- Existing Network devices such as switches, Routers, hubs etc.. or ethernet switches RMON probes embed into their circutary.
- Normally implemented on only device or entire phase for subnet.

Advantages:

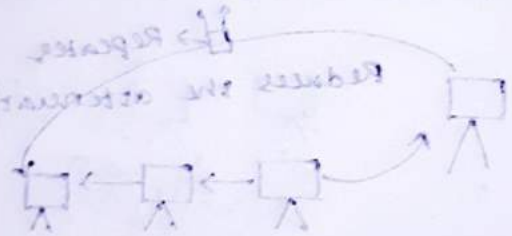
RMON identifies the trouble shooting requirements

easily collects the information

- Easily manages the network.
- Reduces the work load of your network management system.
- Productivity significantly increases.

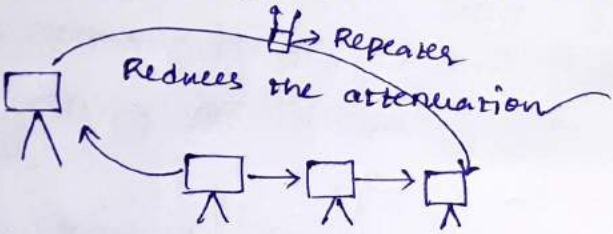
Dis Advantages :-

- The system used to retrive the data extremely slow.
- The system not be used in allocated Bandwidth.
- RMON system store using the 32 bit register.



Repeaters :-

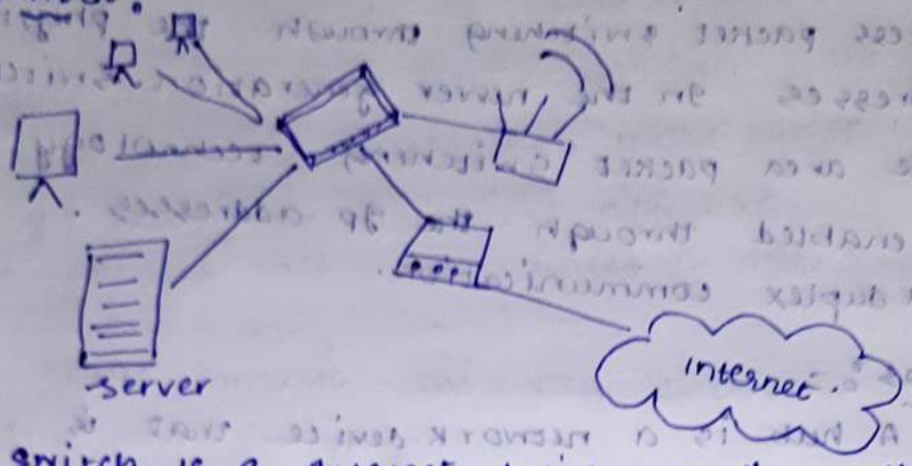
In an local area network the signal along the network attenuates due to the free space electromagnetic divergence caused this weak signal or data loss from the cable so to regenerate the signal over a local area network we use the Repeaters, Repeaters are the Lan devices that could Regenate the signal bit by bit through the Reference the Repeaters Remove the unwanted noise and filters and Regenerates the signal Repeaters are generally placed across the local area Networks.



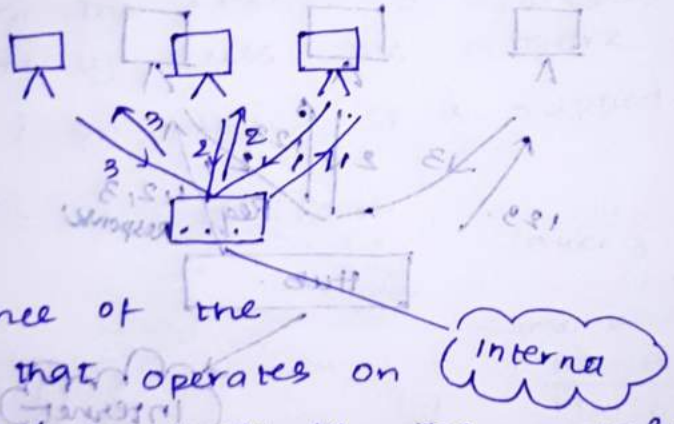
Repeters generally dont amplify the signal amplifiers in analog communications amplify the signals amplify in the sense x3, x4 times this causes the noise also to be amplified so this Repeaters are extensible in signal recovery.

- Kushal

Switch:



Switch is a internet device, much intelligent than hub. Switch is the device that integrates different nodes in a network. It has more no. of ports compared to hub. it performs full duplex data transmission. it combines the nodes in star topology, simultaneous functioning.

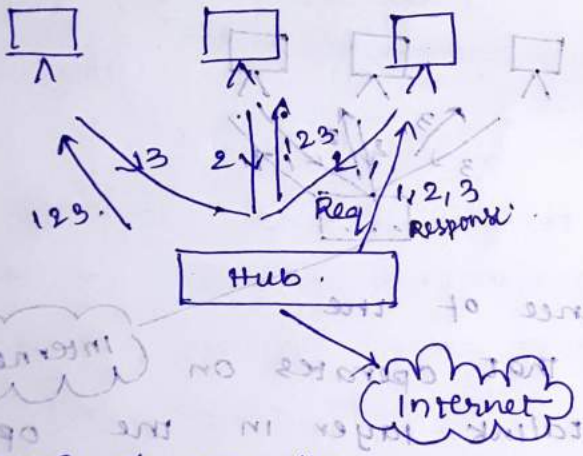


intelligence of the switch that operates on the datalink layer in the open system interconnection works with the collection of macaddresses updated list in the hub responsible for the intelligent data transfer. No packet loss, error free transmission, reliable data transfer no data mismatch from the hub to the node.

In the traditional network switches the Mac address packet switching through the physical addresses in the newer generation switches wide area packet switching technology is enabled through the ip addresses. Full duplex communication.

Hubs :-

A hub is a network device that is deployed in the physical layer and mainly used to connect the nodes in a local area network. Hub provides half duplex way of data transmission. hub is less intelligent compared to switch.



functioning of the Hub:

The hub the network device that collects all the request fromes the clients and sends the requests to the internet to access the information. The response is been sent to the every system

that is been connected to the network. The more chances of data collusion and data leaks, packet loss occurs in the hubs. hubs are less intelligent, more power consuming, hubs are less cost effective.

It connects all the nodes in the star topology

Router :-

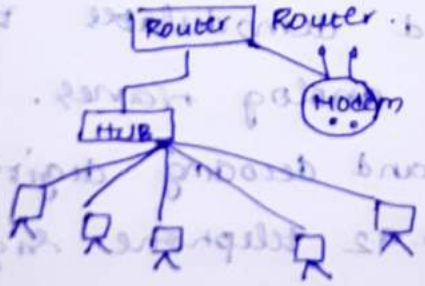
Router connects the two networks with same network type.

Router consists a table that assigns the ip (public) address.

Router maps public ip address to the requested static ip node.

These static ips are assigned by the user or network Administrator.

So with the static ip addresses we cant directly access the network (internet) so public ip is mapped.



layer 3

same networks

192.168.10.1

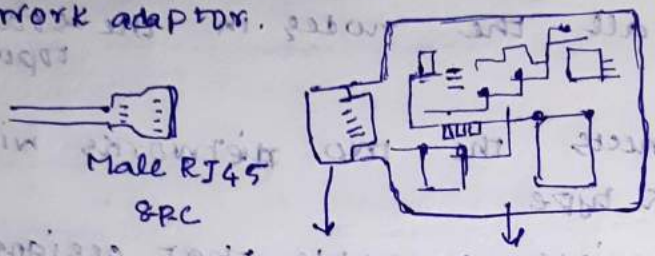
192.168.11.1

The Router also finds the shortest path to route the packet to host and destination, Routing Algos are embedded in them.

Supports to connect through Internet.

NIC:

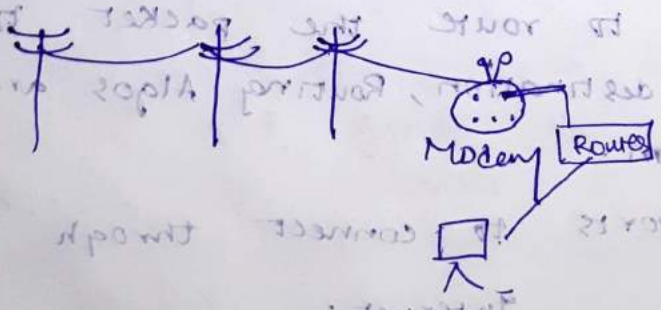
Network interface card is a piece of hardware that allows to connect to the internet also known as network adaptor.



The circuit that is been connected for Lan communications and supports for internet connectivity Maenly operates on the physical and Network layer (3)

Modem:

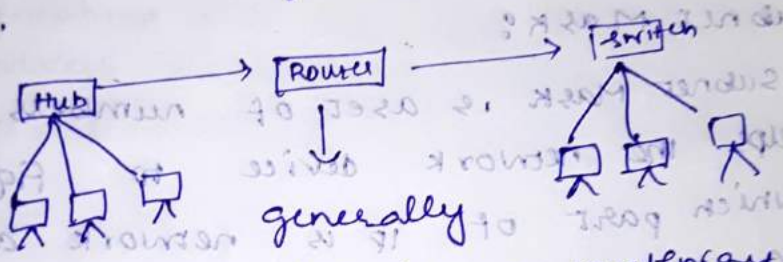
It is a network device that modulates and demodulates the sine patterned analog waves. for encoding and decoding digital informations. V.92 telephone signal analog data transmission



Gateway:-

The gateway acts as an entry point for two different networks, communication bw the two networks operating with the different transmission protocols.

. Layer 3. in OSI acts as the entry exit point for slice.



generally A router can also be a gateway,

Subnet and necessity of subnetting:

- Dividing the network into smaller portions is called subnetting.
- The subnets are made by borrowing the bits from the host portion of IP address

IP components = network comp + host bits + subnet bits.

Subnet Mask:

- Subnet Mask is a set of numbers that helps the network device to figure out which part of IP is network and host component.

It is like a filter that separates the network addresses with host addresses.

Subnet Mask and IP relation.

eg: 192.168.1.10. the subnetMask 255.255.255.0(A)

3
↳ Network identification bits

The three 255 represents that the first three octects are network identification bits in an IP address.

There are 2 methods in creating the subnet.

1. By grabbing the host component of the ip address also called as variable length subnet mask. In this method you borrow the bits from the host component of the ip address and use them to create subnets. This means you can have subnets of different sizes depending on the borrowed bits

2) By grabbing bits from the network component of ip address. Fixed length subnet mask. Simplier to use, less flexible more ip wastage.

Requirements to create a subnet:—

1. no. of hosts in the network.
2. No. of subnets required.

Fixed Length Subnet Mask:—

if we have ip range 192.168.1.0 to 192.168.1.255, we need to create smaller subnetworks within this.

We should borrow bits from network portion equal no. of host capacity on one such subnet.

→ Here we need to create 4 subnets within 192.168.1.0 network we need to borrow 2 bits here. 2 bits can create combination of (00, 01, 10, 11) which is used to represent 4 subnets.

Borrow from host add to network

let subnet mask of 255.255.255.192 first 2 octets network component while the last two octets are divided into subnets.

Subnet 1: 192.168.1.0 - 192.168.1.63

Subnet 2: 192.168.1.64 - 192.168.1.127

Subnet 3: 192.168.1.128 - 192.168.1.191

Subnet 4: 192.168.1.192 - 192.168.1.255

: 64 each subnet.

IP Range:

Range of IP addresses only defines the possible IP addresses that can be assigned.

To determine the no. of systems present we need to know the subnet mask

255.255.255.0

class c — 8 bits

2^8 = 128 hosts can be situated.

255.255.254.0 the range of IPs expanded 192.168.0.0 TO 192.168.1.255

512 hosts (2^9)