* Computer network is a communicational network established between many electronic devices not necessarily computers only for sharing resources and data. Such network is established using physical links or can be wireless

Types of systems

1) Open system:- A system that is connected to the network and is ready for communication
2) Closed system:- A system that is not connected to the network and cant be communicated

Network devices

There are also multiple devices or mediums which help in intercommunication between two different devices which are known as network devices
e.g router, wireless router, bridge, wireless bridge switch, ~~hub~~ hub.

OSI

OSI stands for open system interconnection it is a reference model that specifies standard communication protocol and also the functionalities of each layer.

Protocol:-

A protocol is the set of rules or algorithms which defines the way how two entities can communicate across the network and there exists different protocol define at each layer
e.g FTP, SMTP, TCP, UDP.

*Computer network is a communicational network established between many electronic devices not necessarily completely only for sharing resources and data. Such a network is established using physical links or can be wireless

Types of systems

1) Open systems - A system that is connected to the network and is ready for communication
2) Closed systems - A system that is not connected to the network and cant be communicated

Network devices

There are also multiple devices or mediums which help in interconnecting [illegible]

Networking elements.

1. atleast two electronic devices
2. transmission media
3. protocols
4. system software

Network criteria

The criteria that have to be met by a computer Network are

1. performance → transit time → time between two hop
   response time → send receive time.
2. reliability → frequency of errors / fault / failure
   recovery from errors / faults / failure
   robustness during catastrophe
3. Security :- protecting data from unauthorized access

goals of CoN

1. Resource sharing
2. High reliability
3. inter process communication
4. flexible access.

Transmission modes

Transmission modes determines how data is transfered between two devices in a CoN

1. Simplex
   operation only one way only one sender and only one reciver
   e.g radio station

② Half duplex
both can send and recive in a con but not at same time or simultaneously
e.g Walkie Talkie.

③ full duplex
both can send and recive and can be done simultaneously
e.g a phone call.

Network topologie

The arrangements of nodes in a network follows some pattern or organisation each of these patterns have their set of advantages / disadvtanges.
such arrangements are collectively refferred to as network topologie.

① mesh
* robush & easy fault-detection
* installation is difficult & expensive
* fully connected ~ lots of cables ${}^nC_2$

② Star
* easy and cheap (n cables)
* single point of failure (center node)

③ Bus.
* easy and chip installation (n+1) cables
* single line on failure (back bone coaxial cable)
* Heavy traffic collisions.

#Ring
#easy & cheap
difficult in troubleshooting
addition/removal of nodes disturbs the topology.

#hybrid
* combination of all
* scalable and flexible
* difficult to develop

TCP VS OSI

OSI → open systems interconnection

① Physical layer:- it is responsible for actual physical transmission of data. it receives / transmits signals and then converts it to physical bits
It handles bit synchronisation, bit rate control, physical topology and transmission mode.

② datalink layer:- it is responsible for node to node delivery of packets, framing, error control, flow control, physical addressing (MAC)
upon receiving packets from network layer it encapsulates it within a frame with hardware (MAC) address of receiver (obtained via ARP)

③ Network layer:- it is responsible for IP and routing. various routing algorithms are implemented at this layer.

* less reliable * ~~it~~ model then protocol
* strict boundries, * vertical approach

~~# Ports~~

⑤ Transport layer
* it is responsible for end to end delivery of packets
it also does segmentation & reassembly of packets
, multiplexing and demultiplexing
, TCP and UDP are present here

⑥ Session layer:- it is responsible for session management, Authentication, security, synchronization & restoration, Dialog control

⑦ Presentation layer it is responsible for translation, encryption, decription, and compression

⑧ Application layer :- It implements application specific protocols (HTTP, HTTPS, FTP, SMTP)

TCP/IP

① Network access layer :-
Datalink + physical layer

② Internet layer / Network layer :-
Network layer

③ transport layer
transport layer

④ Application layer :-
Application layer + presentation layer + session layer

* more reliable
* horizontal approach
* protocal then model
* not having strict boundries

Data link layer

the main function of this is to ensure data transfer from one node to another is error free.

* it is divide into two parts
  1. logical link control (LLC)
  2. media access control

the packet received from the N.L is further divided into frames depending on frame size of (NIC) network interface card. DLL also encapsulates sender and receiver MAC address in header

The receiver MAC address is obtained by placing an ARP

helps in LAN and WAN

functions
1. framing → based on NIC
2. error detection
3. error / flow control
4. Physical addressing
5. access control,

* packet in DLL is called frame
* handeled by NIC
* Switch and bridge are DLL devices

Network layer (N.L)

* Network layer works for the transmission of data from one host to the other host located in different networks.

* Selection of shortest route is done here
* Placing of sender and receiver IP is done here
* Segment in N.L is refereed as Packet
* Router is a N.L device

Technical devices

1) Switch
* DLL device
* used for packet filtering and forwarding good selected packet are sent rest are filter. the good are sent to respective port.

2) routers -
* N.L device
* routing, routing tables, ~~port~~ packet forwarding based on IP
* connects LAN and WAN together and update Routing table dynamically

3) Brooters - ~~bridging~~ routes
* data link layer or N.L
* working as a bridge it is capable of filtering LAN traffic.

4) ~~repeater~~ repeater
* Physical layer device
* makes weak signal strong by copy paste or duplication not ~~regeneration~~ amplify

Hub)
* a multiport repeater
# does not filter data
- active Hub
- passive Hub

⑥ Bridges
same as repeater
it can filter the content over a network by reading MAC address.
- transperent Bridge
- sourcerouting bridge

⑦ Gateway
- a passage to connect two network together that may work upon the different networking model. - works as an messenger / mediator between two network

function of N.L
* helps in deliver of data in form of packets
* from source to destination delivery
* NL is used when we need to send data over different Networks

circuit switching Vs packet switching

* are two ways of transmitting packets between to end to end devices over a network

(1) circuit switching

* network resources are dedicated to establish a connection between the end devices where a dedicated fixed path is established where data is transmitted without delays and there is no concept of network congestion a telephone system works under this scheme
* suitable for continious transmission
* garanted datarate
* inefficient
* under utilization

(2) packet switching

* packet switching is a methode of transfering the data in a network in the form of packets.
* for efficiency, and less latency data is broken down in to small ~~per~~ peice of variable length called packet
* No prisetup or reservation of resources is needed
* reassamble of packet take place at destination
* USES store and forward . each hop first store the packet and then forward
* multiple paths betwee S and D is possible
* each patern contain S and D address
* No dedicated line is established.
* can cause delay and out of order reception.

- efficient utilisation of Network resource
- out of order reception
- Transmission delay.

#advantages
* efficient in terms of bandwidth.
* minimal transmission latency
* more reliable
* fault tolerant
* cost effective and cheaper

disadvantages
* out of order requires reassembly
* complex
* Transmission delay
* only for small messages

for busty (large) data circuit ~~to~~ switching is better.

Modes
(1) connection-oriented packet switching (virtual circuit)
* along to predefined logical path
only packets are noted.
* setup ⟹ data transfer ⟹ teardown

(2) connection less packet switching (dynamic circuit)
→ never one
no predefined virtual paths present.

IP and classful addressing

to uniquely identify an device on an etwork we use logical address called IP
internet protocol

The whole 32-bit address space is devided into classes obviking capcuty depending on the size and need of an organisation

* This form of division is called classfull addressing

* each of the class has a valid range of IP address

* E for experimental & military
D for multicasting

* address bits are divided into
* Network ID - same for a network an address in same class
* HOST ID - ID of HOST on net

① Class A
Network ID - 8bit HOST ID - 24bits
1st bit always 0
subnet mask - 255.0.0.0.

② Class B
Network ID - 16bits HOST ID - 18 bits
Subnet mask - 255.255.0.0.

Class C

N.ID :- 24 bits and HOSTID - 12 bits

subnetmask - 255.255.255.0.

Class D :-

222.0.0.0 - ~~00~~ 239 - 255.255.255

does not have subnet mask

Class E :-

240.0.0.0 - 255.255.255.254.

flow control protocols

flow control is required ~~at the~~ to in the CN because most of the time the sender has no idea about the capacity of buffer at the receiving ~~end~~.

end. and thus may ~~reject~~ transmit packets exceeding the ~~current~~ capacity causing them to get dropped at the receiving end.

thus the flow control mechanism is required for the retransmission in case the packet gets lost

① Stop and wait (ARQ)

* in this scheme the sender ~~sends an (ACK)~~ waits for an (ACK) from the recver, before transmitting the next packet. If it does not recive ACK for a certain packet within a predefined timeout (ARQ - automatic repeat request) it retransmits same packet

#in this Schemepackets are descent one by one inefficient

(2) Go back N

data is send in the form of an packet or small chunckes ~~in~~ and wait for ACK from reciver is done for that chunk. eachchuck has seavenced pcckets. and reciver checks this seavence. if it does not recive whole chunck the whole packet is then re transmited from sender.

reciver end drop all the ~~the~~ packet ahed of the lost ~~or~~ numbe and sends ~~a~~ a negative ACK to recive the lost and ahed chunck one lost and ahead. of it. is re transmited

(3) Selective repeat

only lost one re transmited.

only a particular lost packet is re transmimed after reciving -ive ACK. and rest are accepted at the reciver end.

Error detection

due to noise in network and signal interference bit values may get changed during transmission leading to so called errors. They need to be detected at the DLL and upon detection retransmissions reverted or correction is done.

Some common error detection scheme are

① Parity check

Parity check works by counting the no of 1s in the bit representation and then appending 1 incase of even no of 1s or 0 incase of even no of 1s. Thus the total no of 1's become even. Hence the scheme is also called even parity check. Thus if due to error any bit is changed the total no of 1's will become odd and packet will be rejected.

② 2D parity check

Parity check bits are calculated for each row which is equivalent to a simple parity check. Parity check bits are also calculated for all columns then both are sent along with data.

Original Data

10011001	11100010	00100100	10000100

1 0 0 1 1 0 0 1	0
1 1 1 0 0 0 1 0	0
0 0 1 0 0 1 0 0	0
1 0 0 0 0 1 0 0	0
0 1 0 1 1 0 1 1	0

10011001	11100010	00100100	10000100	01011011

Data to be sent.

Checksum

* Data is divided into k segments each of m bits
* at the sender segments are ~~divided~~ added using 1's complement arithmetic to get the sum
The sum is complemented to get checksum
* the checksum segment is sent along with data segment
* at the receiver all received segments are added using 1's complement arithmetic. the sum is complemented
* if the result is zero the received data is accepted
Otherwise discarded

Original Data

10011001	11100010	00100100	10000100

k=4 m=8

Sender

```
1  10011001
   11100010
  ----------
1 01111011
  ↳        1
  ----------
   01111100
3  00100100
  ----------
   00100100
         ↳ 1
  ----------
Sum → 00100101
C.sum → 11011010
```

receiver

```
1  10011001
2  11100010
  ----------
1 01111011
  ↳        1
  ----------
   01111100
   00100100
  ----------
   10100000
4  10000100
  ----------
1  00100100
         ↳ 1
  ----------
   00100101
   11011010
  ----------
Sum 11111111
Complement. 00000000
```

Accepted

(a) cyclic redudancy check
CRC is based on binary division

#subnetting
When a bigger network is devided into smaller network inorder to maintain security then that is known as subnetting. So maintenence is better and easier for smaller networks.

Network address :- It identifies a network of Internet using this we can find range of address in the network and total possible number of hosts in the netwok

Mask :- It is a 32 bit binary number that gives the network address of the address block when AND operation is bitwise applied on the mask and any IP address of the block. Then you get Network ID of the subnet mask to which IP belongs.

*advantage
* Security to one network against another.
* setting priority to one network over other
* makes easier maintenance

* disadvantage
* complex

#ARP (Address resolution protocol) & Reverse ARP

* to finally transmit data from one device to another however physical (MAC address is required (at DLL) but all the network layer knows is logical address / IP of the next hop-device.
ARP is the defacto methode of acquiring MAC address from its logical address. similarly revers ~~RAP~~ ARP is process of getting IP from MAC.

#ARP

To get the MAC address of target machine the sender sends broadcast special ARP message over its immidiate neighbours requesting a MAC addre. The contents of this message

- sender IP
- receiver IP
- sender MAC
- receiver MAC initially filled with zero

When this is broadcasted to neighbours the neighbour having matched IP address (destination) fills ~~it~~ its mac address and rest none matching neighbours reject it.

Reverse

when a machine needs to know its IP it sends a special RARP message to its router in which routing table with IP MAC mapping is present for nodes in the network. on receiving the RARP request router key to match the MAC address and responds with respective IP

IPV4 VS IPV6

- # 32 bit length
- # manual and DHCP address config support
- # End to end connection integrity is unachievable
- # security feature are dependent on application
- # representation is Decimal
- # fragmentation performed by sender and forwarding routes
- # packet flow identification not available
- # checksum brand is available
- # broadcast scheme is available
- # Encryption and authentication facility is not provide

- # 128 bit length
- # auto and renumbering address config
- # end to end connection integrity is achievable
- # IPSEC is inbuilt security feature
- # representation in Hexadecimal.
- # fragmentation performed by only sender.
- # packet flow are available uses flow label in header
- # Checksum field is not available.
- # multicast, and any cast message transmission is available.
- # Encryption and authentication are provided.

Important Portnumbers in use

80	HTTP
443	HTTP
53	DNS
22	SSH
110	POP3
25	SMTP

TCP vs UDP (both are Transport layer protocol)

TCP is a connection oriented protocol. connection orientation means that the communicating devices should establish a connection before transmitting data and should close after transmitting data

UDP is a User Datagram protocol this is a Datagram oriented protocol this is because there is no overhead of opening a connection, maintaining a connection and termination it UDP is best suited for broadcast and multicast type of network transmission

TCP is reliable as it guarentees delivery of data to the destination

the delivery of data to the destination cannot be guaranteed

TCP provides extensive error checking mechanisms. It is because it provides flow control and ack of data

UDP has only basic error checking using the checksum

sequencing is a feature of TCP data is in order always

there is no sequencing in UDP if required it is done by Application layer.

#comparatively slower
#retransmission of lost packet is possible
20 bytes header size
heavy weight
HTTP, HTTPS, FTP SMTP, Telnet

faster, more efficient
not reliable as retransmission
8 bytes header size
light weight.
DNS, DHCP, TFTP, SNMP, RIP, VOIP

Application layer
topmost layer of OSI
Application runs in this layer

protocol of AL
HTTP:- Hyper text transfer protocol:- request-response protocol use to recive web pages on client server architecture.
uses TCP in underhood.

HTTPS:- more secured version of HTTP uses SSL certificates and encrypted data using transport layer security

TELNET:- Telecommunications network
it is used in terminal emulation but now a days SSH secured SHell is used as it uses encryption
→ bi-directional text communication protocol
FTP:- between client and sever or remote system

FTP:- file transfer protocol
it provides reliable and efficient file transfer between two remote machines

SMTP:- Simple mail transfer protocol

TCP underhood
uses store and forward
moves email on and across network
works with MTP (mail transfer agent)

DNS:- Domain name service
DNS maps human-addressable english domain names to IP address

DHCP:- Dynamic host configuration protocol
Used for the dynamic addressing of devices
In a network DHCP server keep a pool of available IP addresses. whenever a new device join the network it provide it with an IP from the available pool with an expiration time