Network Fundamentals

Network

* Network is the Interconnection of devices in order to exchange the data in any one of the medium. data may be in the form of Text, Video, audio, number etc ....

olden days

* very limited & used for military purpose only.

ARPANET (the Advanced Research projects Agency Network)

* It is a computer network considered the foundation of Internet.
* In 1969 ARPANET was connected to 3 university networks in the USA, creating a network.

Network Transmission Types

* Unicast
  -> one to one (or) one node to another node
* Multicast
  -> one to Many, but Specific Group
* Broadcast
  -> one to all eg (An ARP request to all devices in a network) (who has the IP)

Data flow

i) Simplex -> data can flow in only one direction (one way communication) eg: TV Broadcasting, Radio Broadcast.

ii) Half duplex -> data flow in both directions, but only one side can communicate at a time. eg: walkie-Talkie

iii) Full duplex -> data flow in both direction at the same time
eg: Mobile Phones.

Types of Network

i) LAN ii) WAN iii) MAN iv) PAN v) CAN

	LAN	WAN	MAN
i)	covers small area eg: within the building, Room. 10m, 100m, 1km	covers very large geographical area 100km, 1000km (country, continent)	covers larger than LAN but smaller than WAN (10km city)
ii)	Error rate: low	high	Moderate
iii)	Speed: high	low	moderate
iv)	BW: low	high	moderate

personal area Network (PAN)

* ultra small networks used for personal use to share data from one device to another. eg: USB, BT...

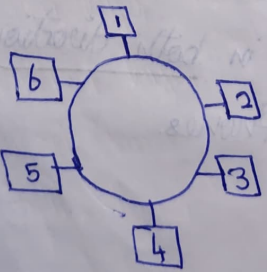
campus area network (CAN)

* geographically smaller than MAN & larger than LAN
* contains several LANs i.e university, institution, companies

Network Topologies

i) Ring Topologies

* It works in closed loop logic, Ring is active network, Termination not required.
* The sent data travels around the ring in one direction until it reaches the destination.



Advantages

i) It performs better than bus topologies in heavy data traffic

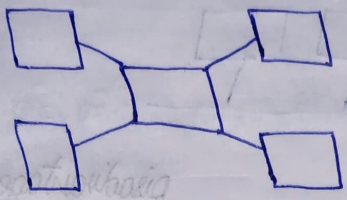
ii) It does not need a central node

Disadvantages

i) The whole network can be adversely affected if nodes are added or migrated.

ii) The transmission delay in the n/w increases in direction propotion to the no. of nodes.

ii) Star Topology



* each node in the star Topology is connected to ~~be~~ a central node.

Advantages

i) when a node is disconnected, other node are note adversely affected.

ii) it provides good network performance under heavy traffic

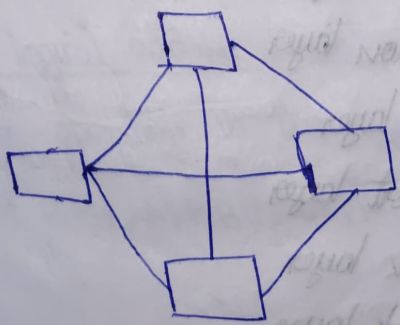
Disadvantages

i) The cost is high due to the cabling required for each node.

ii) central node failed → all node affected.

iii) Mesh Topology

* The mesh Topology has a link b/w each devices in the n/w. it is more diffult to install as the number of devices increases.

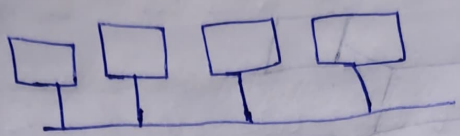


Disadvantages

* Difficult of Installation
* costly because of maintaining redundent links
* difficult of reconfiguration.

iv) Bus topology

* also called horizontal topology
* nodes are located on a common path and data transmission is made with a bidirectional connection on this path.



Advantage

* Adding nodes is pretty easy
* Good for small network
* Extending the bus is easy

Disadvantages

* high probability of packet loss
* performance may suffer as bw is shared among all nodes in the n/w.

OSI model

* open system Interconnection - 7 standard layers
* conceptual framework that make easier to understand n/w structure.
* developed in 1978 by ISO - published in 1984

i) Application layer
ii) presentation layer
iii) session layer
iv) Transport layer
v) Network layer
vi) Data link layer
vii) physical layer

Application layer

* provides network services directly to user applications
* It provides user Interface

Examples: HTTP, FTP, DNS, SMTP, HTTPS

presentation layer

* It deals with Syntax & Semantics of the Information being exchanged
* The function is formats & encrypts/decrypts data for the application layer.

Examples: SSL/TLS (for encryption), JPEG, MP3

Session layer

* the function is to establishes, maintains and terminates sessions b/w application.
* Authentication → Authorization → Session Management

Example: NETBIOS, RPC

Transport layer

* the function is to Ensure reliable data transmission, error detection, flow control and segmentation.

Example: TCP, UDP

Network layer

* The network layer is responsible for delivering the data to the destination logical address (IP address)
* The basic operation in this layer is logical addressing.

Example: IP, ICMP, ARP, RIP, OSPF

Data link layer

* Ensures reliable data transfer between adjacent nodes.
* It deals with MAC & LLC
* MAC - physical addressing using MAC address
* LLC - Error checking, flow control
* protocols : Ethernet, Wi-Fi, ARP

Physical layer

* handles the transmission of raw data bits over a physical medium.

Example: Ethernet cables, fiber optics, radio signals

Network devices

1) Switch

* operates in layer 2 (data link layer)
* used to connect multiple devices within a network, enabling efficient data transfer.
* some switches with more manageable features operates in layer 3 (Network layer)

Functions of Switches

i) MAC Address learning -> Switch maintains a mac address table to map devices

ii) Frame forwarding (unicast, Broadcast, Multicast)

iii) Full duplex communication

Switching -> deciding the best route for data transmission if there are multiple paths in a larger n/w.

Switching Techniques

i) circuit Switching
ii) Message Switching
iii) packet Switching — datagram approach, virtual circuit approach

2) Router

* can be wired or wireless and can connect multiple switches.
* operates in layer 3 (Network layer) is responsible for forwarding data between different networks using IP addresses.
* Smarter than Switches & hubs

Function of a Router

i) IP Routing
ii) NAT
iii) DHCP
iv) Firewall & security Features → can filter traffic using (ACLs) Access control list

3) Hub

* operates in layer 1 (Physical layer)
* Similar to Switch but send all incoming data to all ports.

Function of Hub

i) Broadcasting Data
ii) No MAC Address learning
iii) Shared BW

4) Repeater

* operates in layer 1 (Physical layer)
* Boosts or amplifies a weak signal to extend the distance it can travel.

5) Bridge

* operates in layer 2 (data link layer)

* connects two LANs together or divides a network into segments to reduce traffic.

6) Modem

* Modulator - Demodulator → operates in physical layer

* converts digital data from a computer to analog for transmission over phone/cable lines & vice versa.

7) Firewall

* serves as a protective mechanism, either in the form of a device or software, tasked with monitoring network traffic to identify and thwart potential threats
  ↳ means to prevent or stop a possible danger or risk

* operates in layer 3 & 4

8) Gateway

* operates in all layers

* It acts as a translator between different n/w that use different communication protocols, ensuring seamless data exchange

TCP/IP Model

* designed & developed by the Department of Defense (DOD) in 1960s
* 4 layers
* conceptual framework & more practical & straight forward than OSI model & widely used

TCP/IP	OSI
4. Application	7. Application
	6. Presentation
	5. Session
3. Transport	4. Transport
2. Internet	3. Network
1. Network Access	2. Data link
	1. Physical

IP address mechanism

IP address -> Internet protocol (logical address)

* Every node in the computer network is identified with the help of IP address.
* IP addresses are divided into IPV4 & IPV6
* Assigned by manually or dynamically
* can be change based on the location of the devices.
* Represented in decimal & it has 4 octets (X.X.X.X)

Binary to Decimal

1 0 0 1

$2^3\ 2^2\ 2^1\ 2^0 \rightarrow 9$

1 byte = 8 bits

1 octet

* dotted - decimal Notion

IPv4 Address

10 . 5 . 37 . 156

00001010 . 00000101 . 00100101 . 10011100

4 octets
or
32 bits

Network ID Host ID

IP address

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

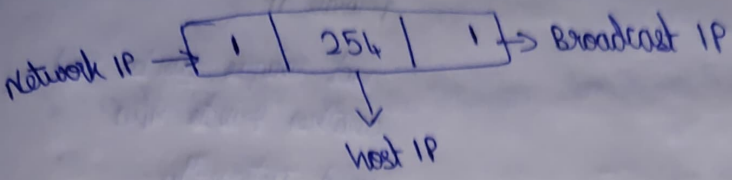
255

Minimum to Maximum

0.0.0.0 - 255.255.255.255

IP address classes

classes	Range	length of N/H	no. of networks	no of hosts
A	0-126	N H H H	126 (of 127 are reserved) (2^7)	16,777,214 16 million
1 bit - 0				
B	128-191	N N H H	16,384 (2^{14})	65,534
2 bit - 10				
C	192-223	N N N H	2,097,152 (2^{21})	254 $2^8=256-2$
3 bit - 110				
D	Multicast	224-239		
E	Experimental	240-254		
4 bit - 1111				



127.0.0.1 (loopback Address)

* Special IP address used for self testing or loopback
* Send traffic to itself without needing a physical n/w.
* 127.0.0.0/8 → fully reserved

APIPA (Automatic private IP addressing)

* IP Range - 169.254.0.1 to 169.254.255.254
* if can't find a DHCP server to get an IP automatically, it assigns itself an APIPA Address.
* allow local communication b/w devices without DHCP
* No Internet access if APIPA is assigned.

IPV4

i) In 1981
ii) 32-bit
iii) 4 billion addresses
iv) Dotted-decimal notion
192.149.0.0

IPV6

1999
128 bit
2^{128} Addresses
hexadecimal notion
3FFE:F200:0234::/48

Advantages of IPV6

* dual stacking → Both IPV4 & IPV6 at the same time
* Tunneling → IPV6 (source) → IPV4 → IPV6 (designation)
* Supports unicast, multicast, Anycast but no Broadcast ⇒ reduci n/w traffics

Public IP	Private IP
i) unique	not unique, can be used on another private n/w
ii) used externally	used Internally
iii) Assigned by ISP	assigned by DHCP in router
iv) Not Secure	Secure

Network Address Translation (NAT)

* converts private IP addresses to Public IP addresses
* it is a usually a router or firewall that modifies IP address when traffics goes in or out

Advantages	Disadvantages
i) it slows down the exhaustion of IPv4 addresses	End-End traceability is reduced
ii) IP address conflict is significantly reduced	Some application do not have NAT compatibility
	it may cause delay