Computer Network

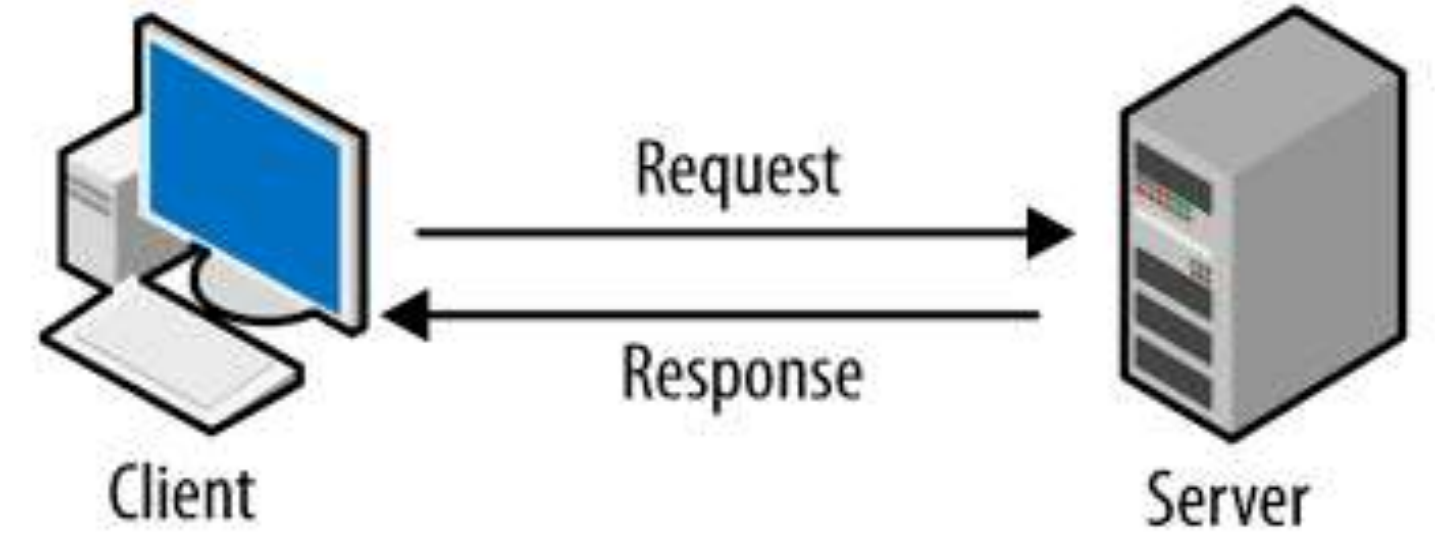
By Anju

Computer network

- A **computer network** is a collection of interconnected computers and devices that communicate with each other to share:
- Data
- Resources (printers, storage)
- Applications
- Services

Networking

- Computer networks have opened up an entire frontier in the world of computing called the **Client/Server Model.**



Networking

- **File server** A computer that stores and manages files for multiple users on a network.
- **Web server** A computer dedicated to responding to requests (from the browser client) for web pages.

Need for Computer Networks

- Resource sharing
- Fast communication
- Centralized data management
- Cost reduction
- Reliability and scalability

Components of a Network

- **Nodes**: Computers, servers, mobiles
- **Transmission Media**: Cables, fiber, wireless
- **Networking Devices**: Router, switch, hub, modem
- **Protocols**: Rules for communication (TCP/IP, HTTP)

Types of Networks

- **LAN (Local Area Network)**
- **MAN (Metropolitan Area Network)**
- **WAN (Wide Area Network)**
- **PAN (Personal Area Network)**

What is Network Computing?

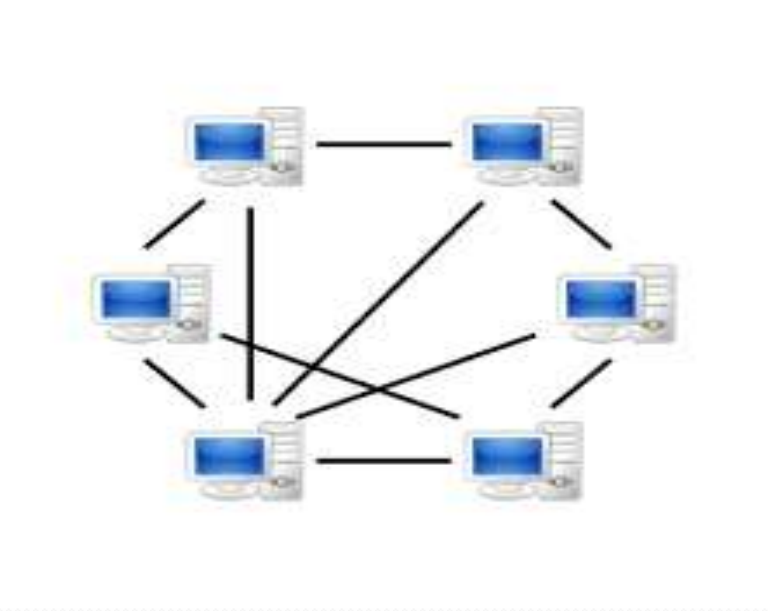
- **Network computing** refers to using networked systems to perform computing tasks by sharing processing power, data, and applications across multiple computers.
- **Models of Network Computing**
- Client–Server Model
- Peer-to-Peer (P2P) Model

Peer-to-Peer (P2P) Model

- **Peer-to-peer, or P2P,** computing is a distributed application architecture in which peers—equally privileged and equipotent network participants—share tasks or workloads. In this way, a peer-to-peer network of nodes is created in which other network users can directly access resources such as computing power, disk storage, or network bandwidth without the need for central coordination. Unlike the conventional client-server approach, peers are both resource providers and consumers.

Cont.

- All nodes act as both client and server
- No centralized server
- **Examples**
- File sharing networks
- Small office networks

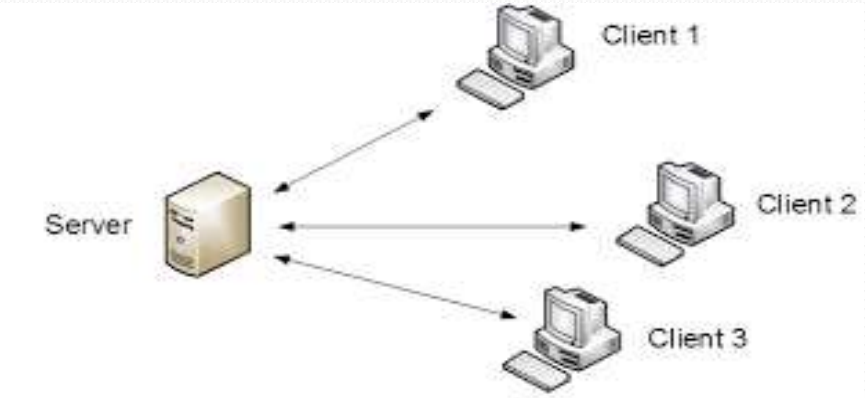


Cont.

- **Advantages**
- Low cost
- Easy setup
- **Disadvantages**
- Low security
- Poor scalability

Client-Server Model

- Client server network consists of a common server that shares data with multiple connected computers. These networks are quite scalable in nature and come with high storage capacity which is also expandable. This article will explain you about the client server network, its working, applications, and benefits.



Cont.

- **Advantages**
- Centralized control
- High security
- **Disadvantages**
- Server failure affects all clients
- Expensive

Peer to Peer Vs Client Server network

Client/Server	Peer-To-Peer
Server has the control ability while clients don't	All computers have equal ability
Higher cabling cost	Cheaper cabling cost
It is used in small and large networks	Normally used in small networks with less than 10 computers
Easy to manage	Hard to manage
Install software only in the server while the clients share the software	Install software to every computer
One powerful computer acting as server	No server is needed

Network Types

- The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN, and WAN are the three major types of networks designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.
- **Network types**

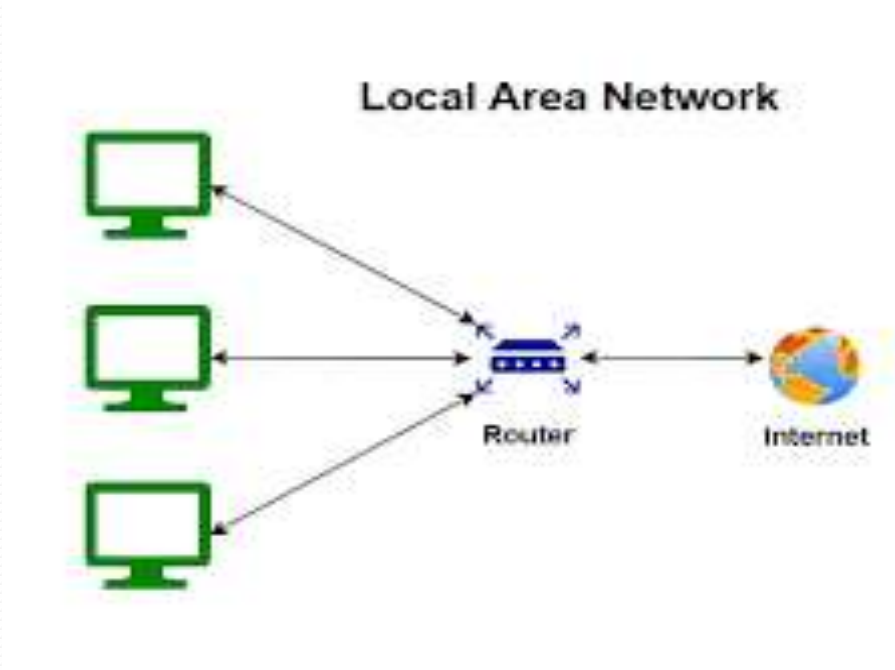
  LAN

  MAN

  WAN

LAN (Local Area Network)

- A **Local Area Network (LAN)** is a network that connects computers and devices within a **small geographical area** such as:
- Home
- School
- Office
- Laboratory
- **Features of LAN**
- Covers small area
- High data transfer speed
- Low cost
- Privately owned
- High security



Advantages of LAN

- Resource sharing (printers, files)
- Fast communication
- Easy maintenance
- Data security

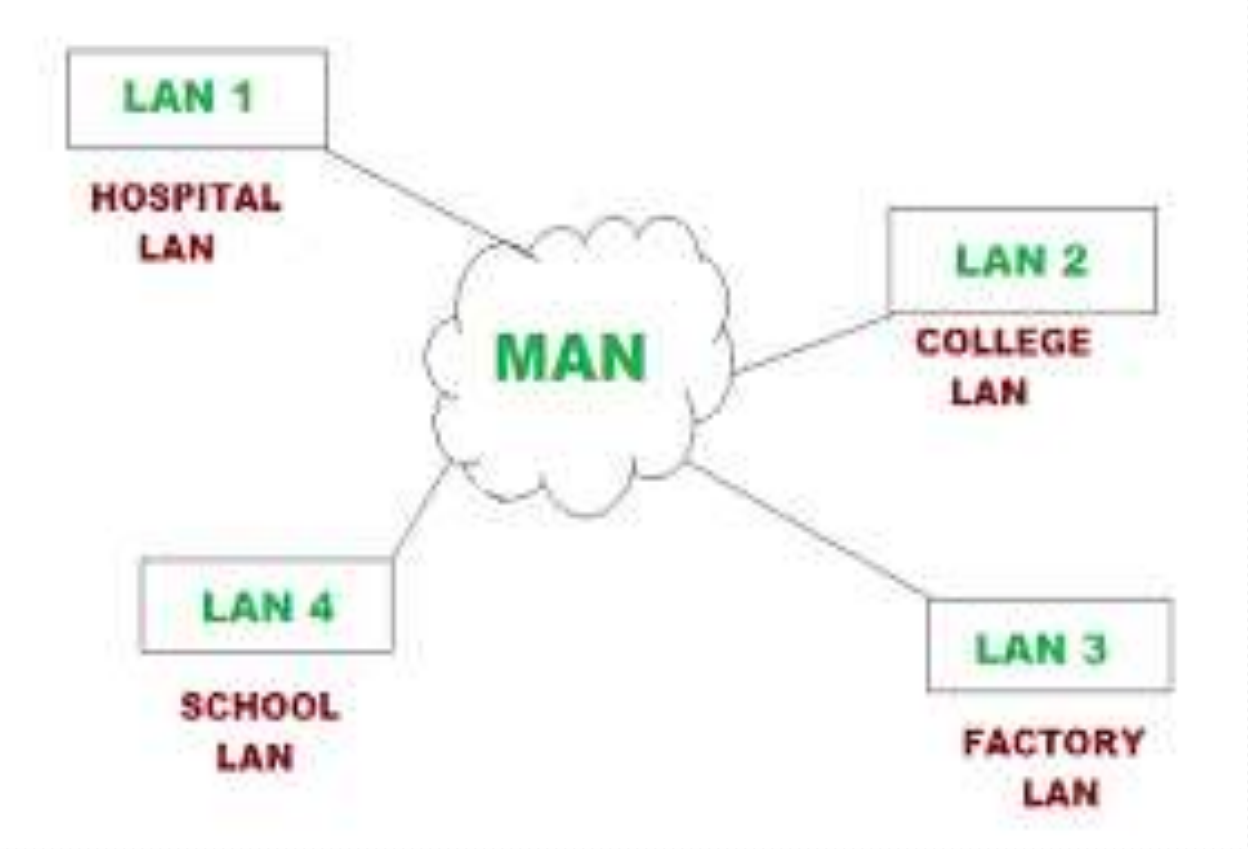
Disadvantages of LAN

- Limited area coverage
- Setup cost (cables, devices)
- Requires technical maintenance

MAN (Metropolitan Area Network)

- A **Metropolitan Area Network (MAN)** connects multiple LANs within a **city or metropolitan area**.
- **Features of MAN**
- Covers city-wide area
- Medium data speed
- Moderate cost
- Usually owned by government or large organizations

MAN


LAN 1
HOSPITAL LAN
MAN
LAN 2
COLLEGE LAN
LAN 4
SCHOOL LAN
LAN 3
FACTORY LAN

Advantages of MAN

- Larger coverage than LAN
- Efficient data sharing across city
- High-speed connectivity

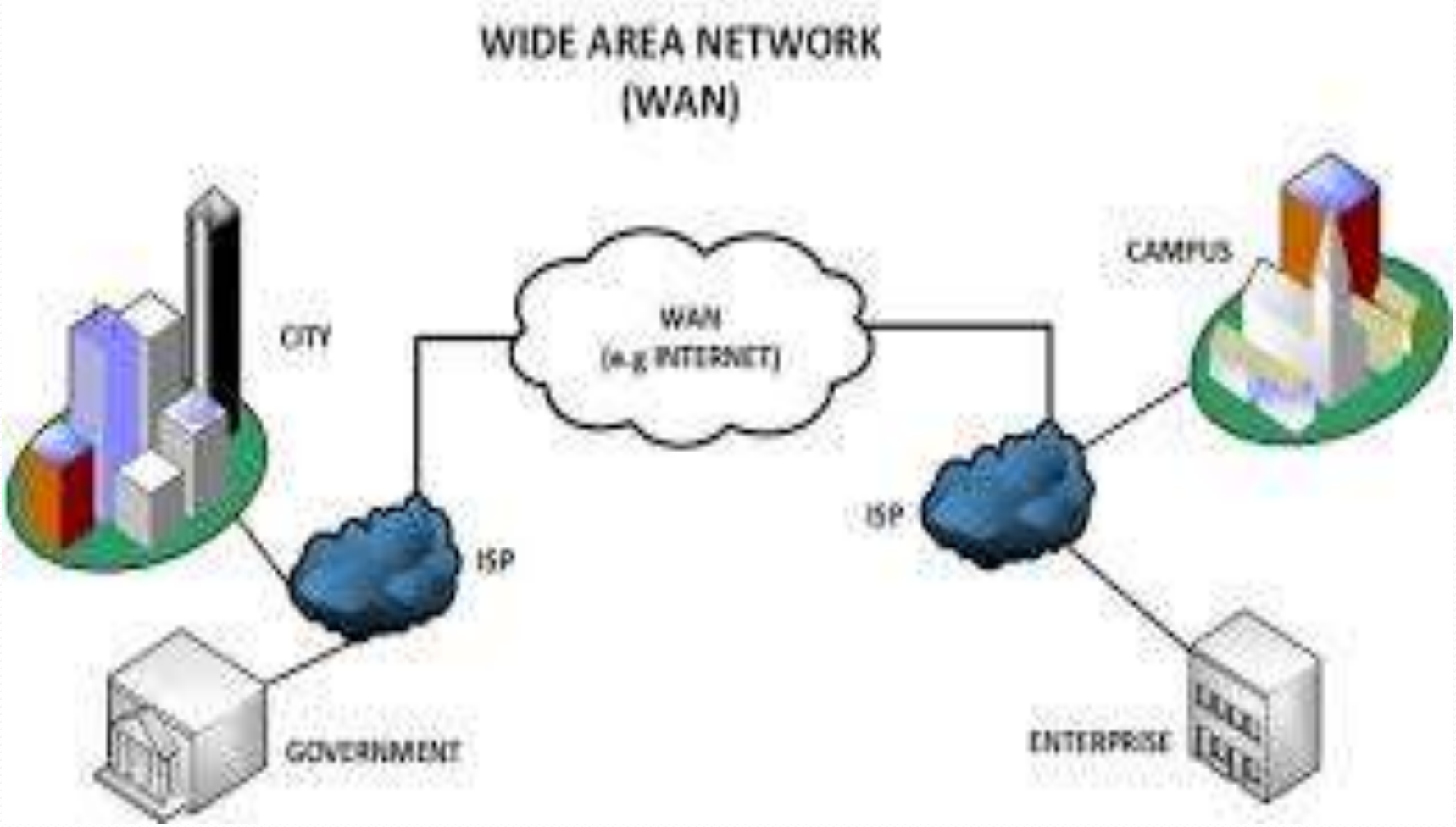
Disadvantages of MAN

- More expensive than LAN
- Security issues
- Complex management

WAN (Wide Area Network)

- A **Wide Area Network (WAN)** covers a **large geographical area** such as:
- Country
- Continent
- World
- **Features of WAN**
- Very large coverage area
- Lower speed compared to LAN
- High cost
- Uses public or private communication lines

WAN


WIDE AREA NETWORK
(WAN)
CITY
WAN
(e.g. INTERNET)
CAMPUS
ISP
ISP
GOVERNMENT
ENTERPRISE

Advantages of WAN

- Global communication
- Access to remote information
- Supports e-commerce and online services

Disadvantages of WAN

- High setup and maintenance cost
- Slower speed
- Security risks

Comparison between LAN,MAN & WAN

Network Topology

Computer network topology is the way various components of a network (like nodes, links, peripherals, etc) are arranged. Network topologies define the layout, virtual shape or structure of network, not only physically but also logically. The way in which different systems and nodes are connected and communicate with each other is determined by topology of the network.

Topology can be physical or logical

- Physical Topology is the physical layout of nodes, workstations and cables in the network.
- Logical topology is the way information flows between different components.

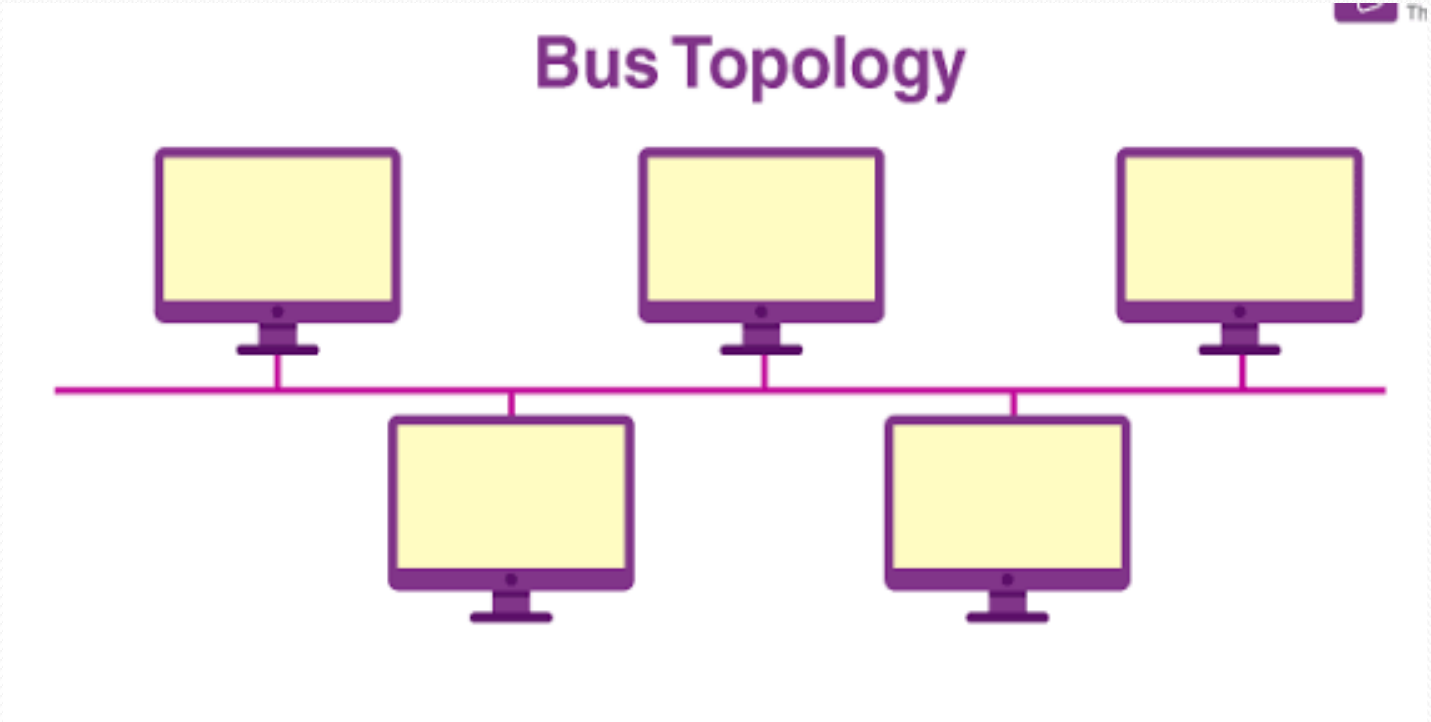
Types of Physical Network Topologies

- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Tree Topology
- Hybrid Topology

Bus Topology

- In the bus topology, the computers are connected through a common communication media. A special type of central wire is used as communication media. This central wire is called Bus. The computer are attached through the bus the ends of the bus are closed with the terminator .The terminators are used to absorb signals.

Bus Topology Diagram



Advantages of Bus Topology

- Easy to install and configure
- Inexpensive
- Easily extended

Disadvantages of Bus Topology

- Performance decreases
- Weak signals
- Difficult troubleshooting

Star Topology

- The star topology uses a separate cable for each work station as shown in fig. The cable connects the work station to a central device typically a HUB. The configuration provides a more reliable network that is easily expended. With star there is no central point of failure in the cable .if there is a problem with the cable only the station connected to that cable is a effected .to add more work stations simply connect another HUB

Star Topology Diagram

Advantages of Star Topology

- Easily expended and modified
- Easy to troubleshoot
- Multiple cable types supported by hub

Disadvantages of Star Topology

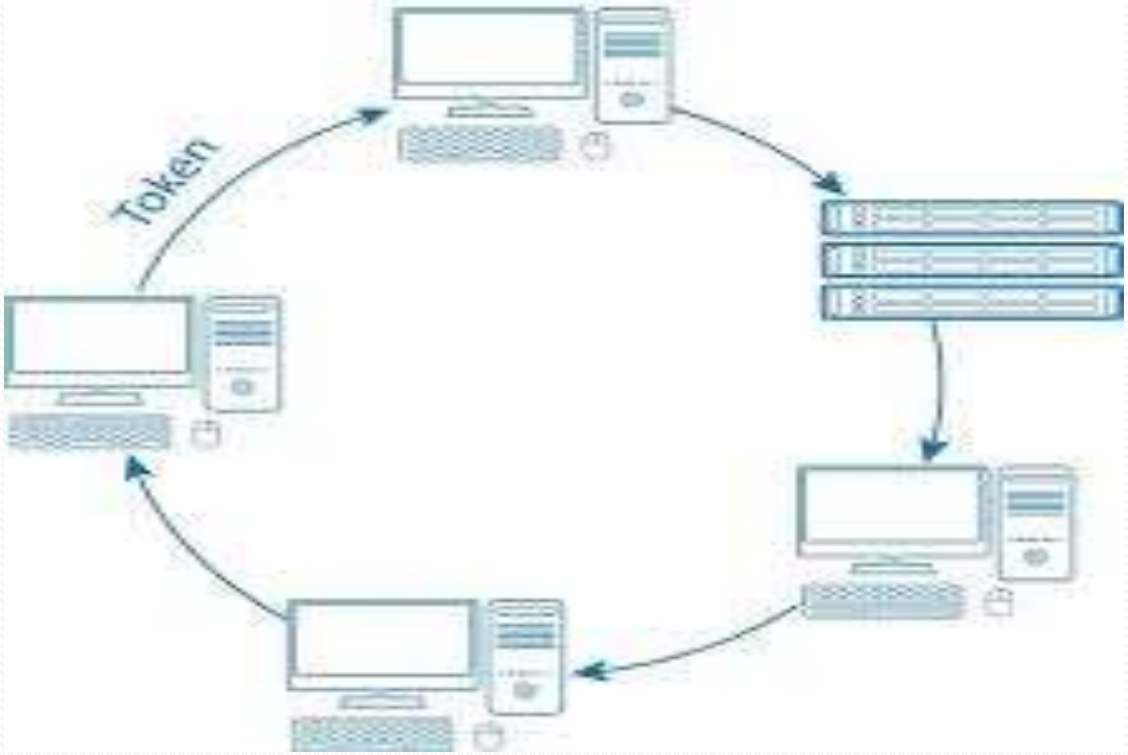
- If hub fails then entire network will fail
- Require more cables
- May require a device to rebroadcast signals across the network

Ring Topology

- Every computer is connected to the next computer in the ring and each transmits what it receives from the previous computer. The messages flow around the ring in one direction.

  Some ring network do ring token passing. A short message called token (memory area)is passed around a ring until a computer wishes to send information to other computers. That computer modifies token, adds an electronic address and data and send it around the ring. Each computer in sequence receives the token and next computer until either the electronic address matches the address of a computer or the token return to its origin .The receiving computer returns a message to the sender indicating that message has been received.

Ring Topology Diagram



Advantages

- It provides an orderly network in which every device has access to the token and can transmit.
- It performs well under a heavy load.

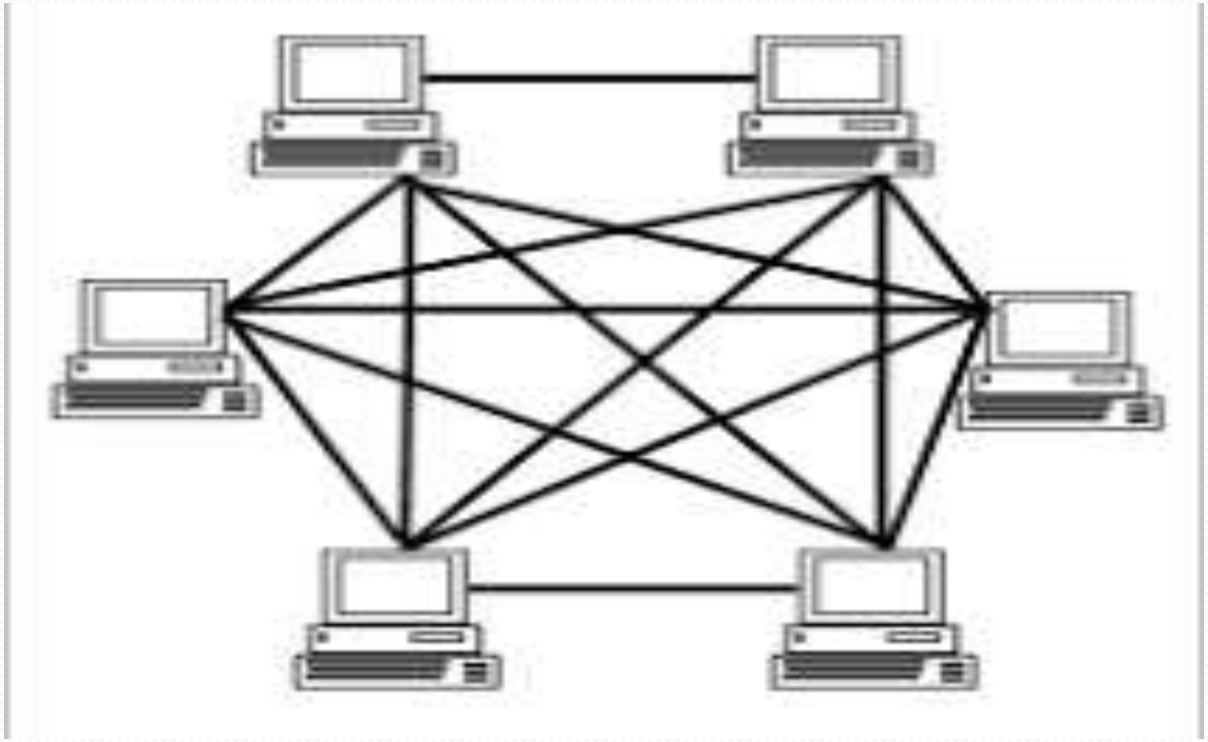
Disadvantages

- Failure of one computer can effect the whole network .
- Difficult to troubleshoot.
- Change mode with adding or removing a device effect the entire network.

Mesh Topology

- A mesh network or mesh topology uses separate cable to connect each device to every other device on the network, providing a straight communication path. For sending messages, check the cable connected into two devices. A message is send directly from sender to receiver because each one has individual and separate connection.

Mesh Topology Diagram



Advantages

- Enhance for error tolerance provided by redundant links.
- Easy to troubleshoot.

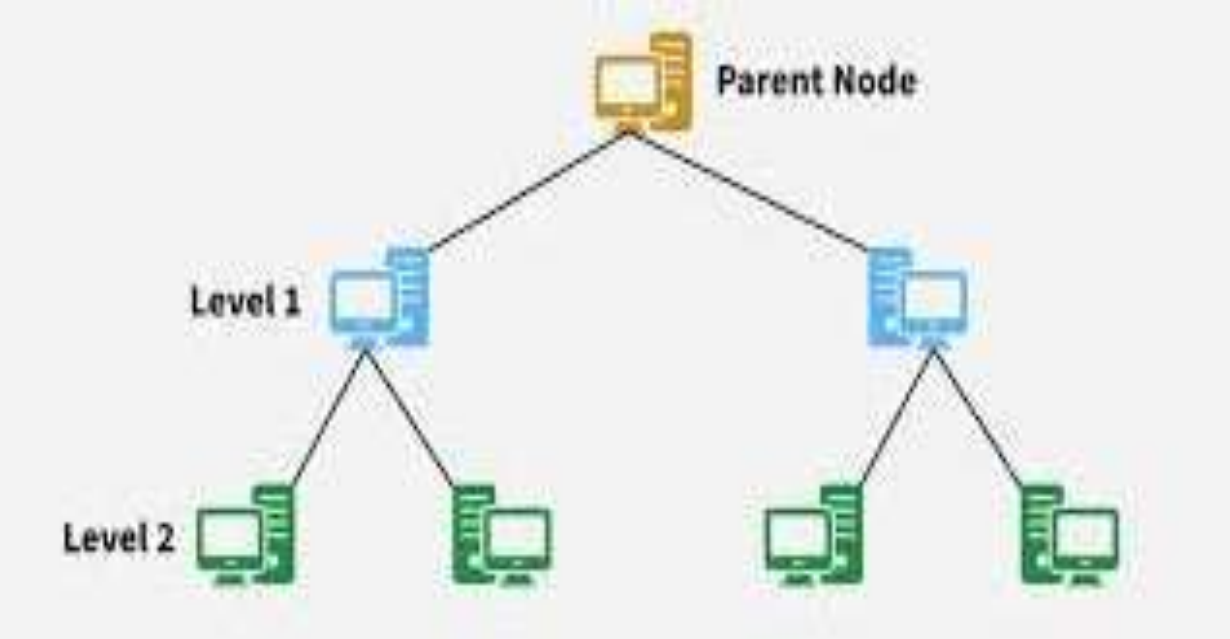
Disadvantages

- Difficult to install and maintain.
- Expensive.

Tree Topology

- The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy (The hierarchy of the tree is symmetrical.) Each node in the network having a specific fixed number, of nodes connected to it at the next lower level in the hierarchy, the number, being referred to as the 'branching factor' of the hierarchical tree.

Tree Topology Diagram



Advantages

- **It is scalable.**Secondary nodes allow more devices to be connected to a central node.
- Point to point connection of devices.
- Having different levels of the network makes it more manageable hence easier fault identification and isolation.

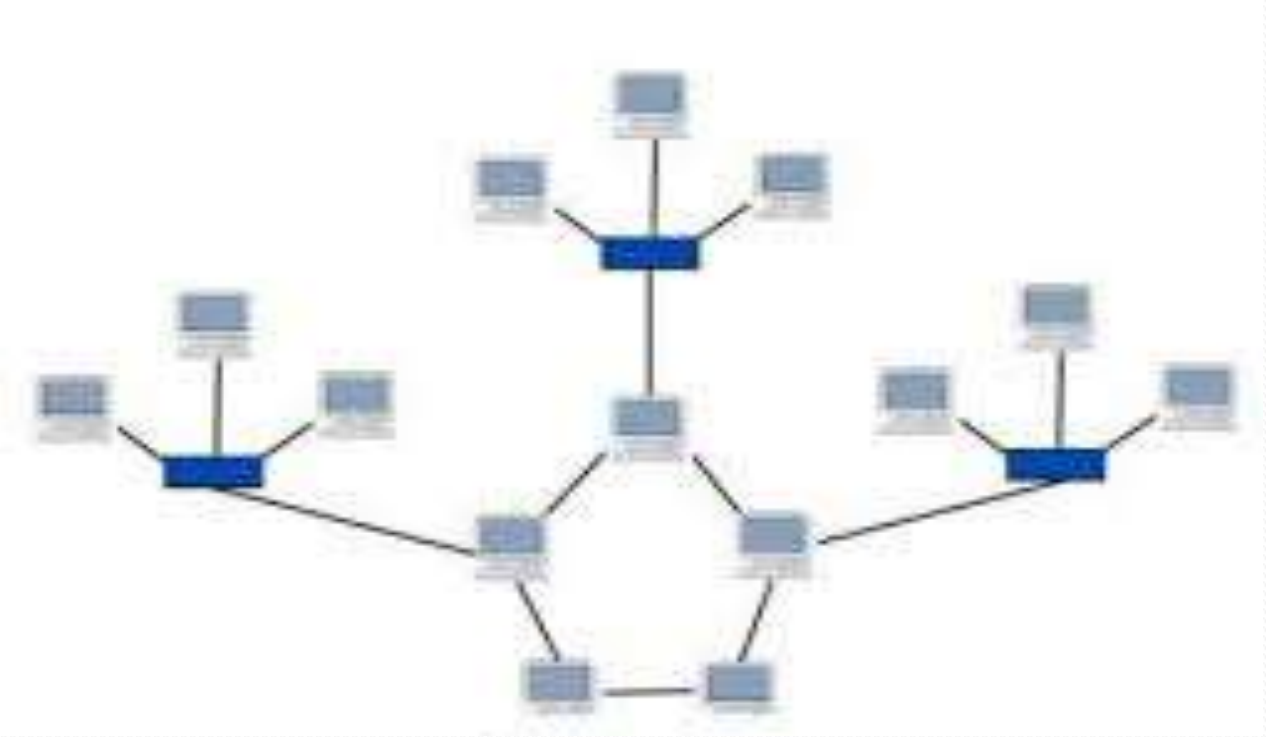
Disadvantages

- Maintenance of the network may be an issue when the network spans a great area.
- Since it is a variation of bus topology, if the backbone fails, the entire network is crippled.

Hybrid Topology

- Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network topology. A hybrid topology is always produced when two different basic network topologies are connected. Two common examples for Hybrid network are: *star ring network* and *star bus network*.

Hybrid Topology Diagram



Switching Techniques

In large networks there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels. There are three typical switching techniques available for digital traffic.

- Circuit Switching
- Message Switching
- Packet Switching

Circuit Switching

- Circuit switching is a technique that directly connects the sender and the receiver in an unbroken path.
- Telephone switching equipment, for example, establishes a path that connects the caller's telephone to the receiver's telephone by making a physical connection.
- With this type of switching technique, once a connection is established, a dedicated path exists between both ends until the connection is terminated.
- Routing decisions must be made when the circuit is first established, but there are no decisions made after that time.

Circuit switching

Advantages:

- The communication channel (once established) is dedicated.

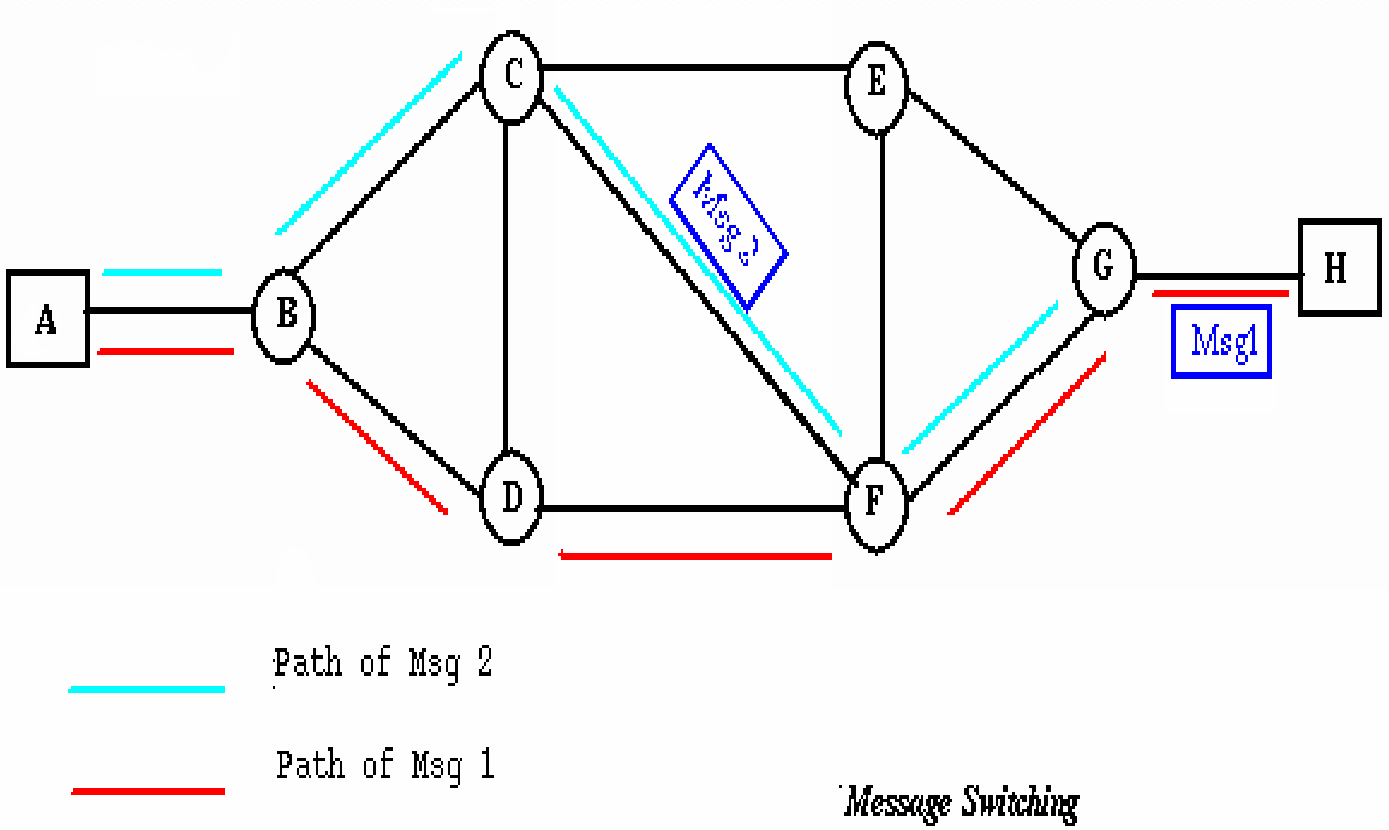
Disadvantages:

- Possible long wait to establish a connection, (10 seconds, more on long- distance or international calls.) during which no data can be transmitted.
- More expensive than any other switching techniques, because a dedicated path is required for each connection.
- Inefficient use of the communication channel, because the channel is not used when the connected systems are not using it.

Message Switching

- With message switching there is no need to establish a dedicated path between two stations.
- When a station sends a message, the destination address is appended to the message.
- The message is then transmitted through the network, in its entirety, from node to node.
- Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.
- This type of network is called a store-and-forward network.

Cont.


A
B
C
D
E
F
G
H
Msg2
Msg1
Path of Msg 2
Path of Msg 1
Message Switching

Cont.

- A message-switching node is typically a general-purpose computer. The device needs sufficient secondary-storage capacity to store the incoming messages, which could be long. A time delay is introduced using this type of scheme due to store- and-forward time, plus the time required to find the next node in the transmission path.

Advantage

Channel efficiency can be greater compared to circuit-switched systems, because more devices are sharing the channel.

- Traffic congestion can be reduced, because messages may be temporarily stored in route.
- Message priorities can be established due to store-and-forward technique.
- Message broadcasting can be achieved with the use of broadcast address appended in the message.

Disadvantages

Message switching is not compatible with interactive applications.

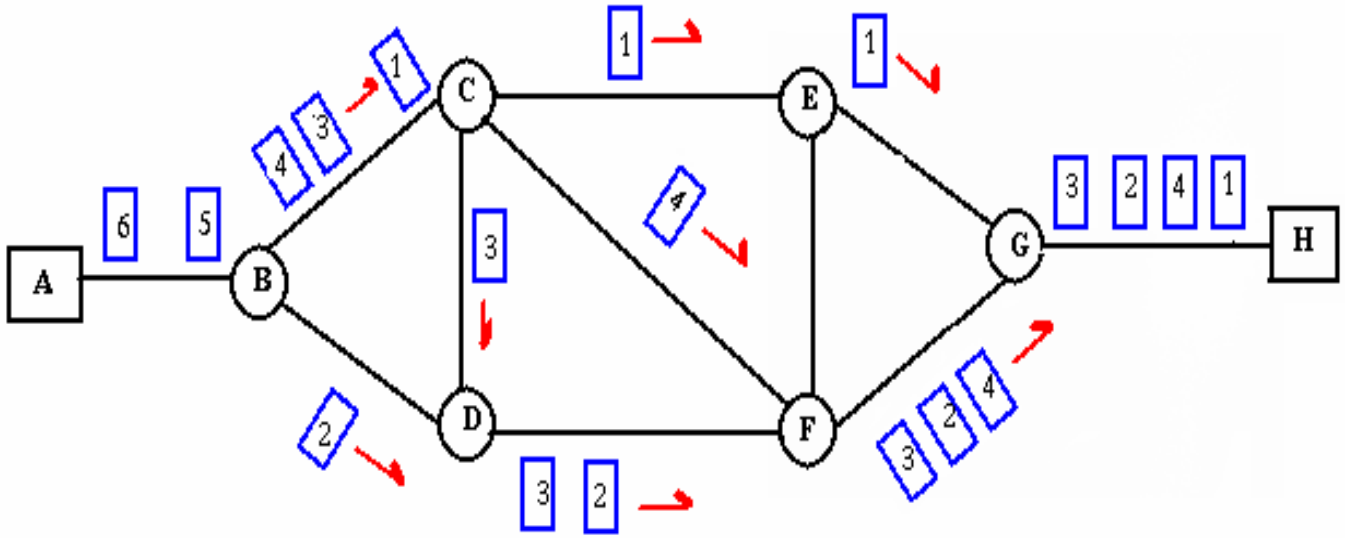
- Store-and-forward devices are expensive, because they must have large disks to hold potentially long messages.

Packet Switching

• *Packet switching* can be seen as a solution that tries to combine the advantages of message and circuit switching and to minimize the disadvantages of both.

• There are two methods of packet switching: Datagram and virtual circuit.

Cont.



Packet Switching

Cont.

- In both packet switching methods, a message is broken into small parts, called packets.
- Each packet is tagged with appropriate source and destination addresses.
- Since packets have a strictly defined maximum length, they can be stored in main memory instead of disk, therefore access delay and cost are minimized.
- Also the transmission speeds, between nodes, are optimized.
- With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded (``dropped'').

Packet size

- The size of the packet can vary from 180 bits, the size for the Datakit® virtual circuit switch designed by Bell Labs for communications and business applications; to 1,024 or 2,048 bits for the 1PSS® switch, also designed by Bell Labs for public data networking; to 53 bytes for ATM switching, such as Lucent Technologies' packet switches.

Packet switching

- In packet switching, the analog signal from your phone is converted into a digital data stream. That series of digital bits is then divided into relatively tiny clusters of bits, called packets. Each packet has at its beginning the digital address -- a long number -- to which it is being sent. The system blasts out all those tiny packets, as fast as it can, and they travel across the nation's digital backbone systems to their destination: the telephone, or rather the telephone system, of the person you're calling.

Cont.

- They do not necessarily travel together; they do not travel sequentially. They don't even all travel via the same route. But eventually they arrive at the right point -- that digital address added to the front of each string of digital data -- and at their destination are reassembled into the correct order, then converted to analog form, so your friend can understand what you're saying.

Packet Switching: Datagram

- Datagram packet switching is similar to message switching in that each packet is a self-contained unit with complete addressing information attached.
- This fact allows packets to take a variety of possible paths through the network.
- So the packets, each with the same destination address, do not follow the same route, and they may arrive out of sequence at the exit point node (or the destination).
- Reordering is done at the destination point based on the sequence number of the packets.
- It is possible for a packet to be destroyed if one of the nodes on its way is crashed momentarily. Thus all its queued packets may be lost.

Packet Switching:Virtual Circuit

- In the virtual circuit approach, a preplanned route is established before any data packets are sent.
- A logical connection is established when
  - a sender send a "call request packet" to the receiver and
  - the receiver send back an acknowledge packet "call accepted packet" to the sender if the receiver agrees on conversational parameters.
- The conversational parameters can be maximum packet sizes, path to be taken, and other variables necessary to establish and maintain the conversation.
- Virtual circuits imply acknowledgements, flow control, and error control, so virtual circuits are reliable.
- That is, they have the capability to inform upper-protocol layers if a transmission problem occurs.

Cont.

- In virtual circuit, the route between stations does not mean that this is a dedicated path, as in circuit switching.
- A packet is still buffered at each node and queued for output over a line.
- The difference between virtual circuit and datagram approaches:

➢ With virtual circuit, the node does not need to make a routing decision for each packet.
➢ It is made only once for all packets using that virtual circuit.

Cont.

VC's offer guarantees that

- the packets sent arrive in the order sent
- with no duplicates or omissions
- with no errors (with high probability)

regardless of how they are implemented internally.

Advantages of packet switching

Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.

- Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).
- Packet can be rerouted if there is any problem, such as, busy or disabled links.
- The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.

Disadvantages of packet switching

Protocols for packet switching are typically more complex.

- It can add some initial costs in implementation.
- If packet is lost, sender needs to retransmit the data.
- Another disadvantage is that packet-switched systems still can't deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.

Introduction OSI

- The **Open System Interconnection Reference Model** (OSI Reference Model or **OSI Model**) is an abstract description for layered communications and computer network protocol design.
- It divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers. It is therefore often referred to as the **OSI Seven Layer Model**.

OSI Layers

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections and reliability, Flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Layer1: Physical Layer

- The Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium.
- This includes the layout of pin, voltages, cable specification, hubs, repeaters, network adapters, host bus adapters, and more.

Cont.

- The major functions and services performed by the Physical Layer are:
  - Establishment and termination of a connection to a communication medium.
  - Participation in the process whereby the communication resources are effectively shared among multiple users. For example, flow control.
  - Modulation, or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

Cont.

- The same applies to local-area networks, such as Ethernet, token ring ,

  FDDI(Fiber Distributed Data Interface),

  ITU-T(International Telecommunication Union Telecommunication Standardization Sector) G.hn and IEEE802.1I.
- Personal area networks such as Bluetooth and IEEE 802.15.4.

Layer 2: Data Link Layer

- The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.
- Originally, this layer was intended for point-to-point and point-to-multipoint media, characteristic of wide area media in the telephone system.
- The data link layer is divided into two sub-layers by IEEE.

Cont.

- One is Media Access Control (MAC) and another is Logical Link Control (LLC).
- Mac is lower sub-layer, and it defines the way about the media access transfer, such as CSMA/CD/CA(Carrier Sense Multiple Access/Collision Detection/Collision Avoidance)
- LLC provides data transmission method in different network. It will re-package date and add a new header.

Layer 3: Network Layer

- The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer.

Cont.

- The Network Layer performs
  - network routing functions,
  - perform fragmentation and reassembly,
  - report delivery errors.
- Routers operate at this layer—sending data throughout the extended network and making the Internet possible.

Layer 4: Transport Layer

- The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers.
- The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.

Cont.

Feature Name	TP0	TP1	TP2	TP3	TP4
Connection oriented network	Yes	Yes	Yes	Yes	Yes
Connectionless network	No	No	No	No	Yes
Concatenation and separation	No	Yes	Yes	Yes	Yes
Segmentation and reassembly	Yes	Yes	Yes	Yes	Yes
Error Recovery	No	Yes	No	Yes	Yes
Reinitiate connection (if an excessive number of PDUs are unacknowledged)	No	Yes	No	Yes	No
multiplexing and demultiplexing over a single virtual circuit	No	No	Yes	Yes	Yes
Explicit flow control	No	No	Yes	Yes	Yes
Retransmission on timeout	No	No	No	No	Yes
Reliable Transport Service	No	Yes	No	Yes	Yes

Layer 5: Session Layer

- The Session Layer controls the dialogues (connections) between computers.
- It establishes, manages and terminates the connections between the local and remote application.
- It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures.

Layer 5: Session Layer

- The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check pointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.

Layer 6: Presentation Layer

- The Presentation Layer establishes a context between Application Layer entities, in which the higher-layer entities can use different syntax and semantics, as long as the presentation service understands both and the mapping between them.
- This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa.
- This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems.
- It is sometimes called the syntax layer.

Layer 7: Application Layer

- The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.
- Application layer functions typically include:
  - identifying communication partners,
  - determining resource availability,
  - synchronizing communication.

Layer 7: Application Layer

- Identifying communication partners
  - Determines the identity and availability of communication partners for an application with data to transmit.
- Determining resource availability
  - Decide whether sufficient network or the requested communication exist.
- Synchronizing communication
  - All communication between applications requires cooperation that is managed by the application layer.

Cont.

- Some examples of application layer implementations include
  - Hypertext Transfer Protocol (HTTP)
  - File Transfer Protocol (FTP)
  - Simple Mail Transfer Protocol (SMTP)

OSI Feature

- Open system standards over the world
- Rigorously defined structured, hierarchical network model
- Complete description of the function
- Provide standard test procedures

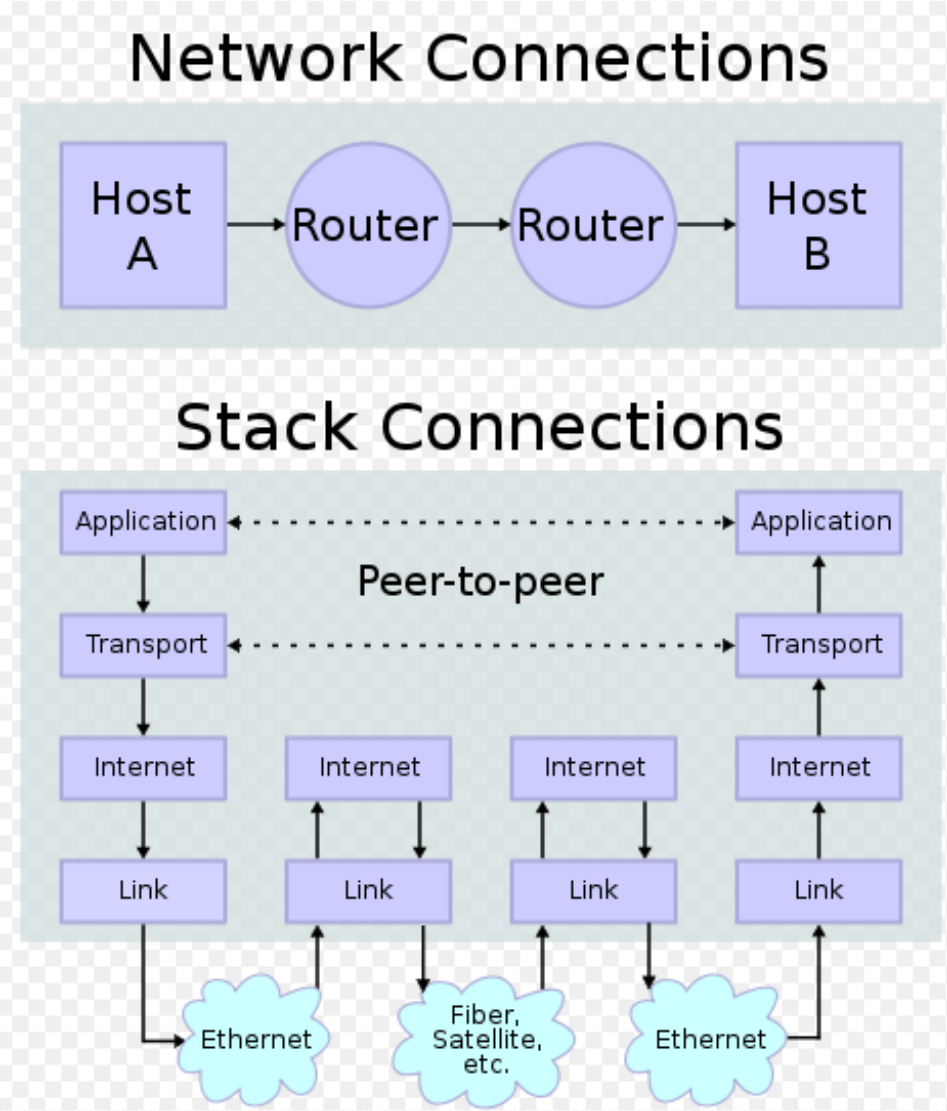
Introduction TCP/IP

- The **Internet Protocol Suite** (commonly known as **TCP/IP**) is the set of communications protocols used for the Internet and other similar networks.
- It is named from two of the most important protocols in it:
  - the Transmission Control Protocol (TCP) and
  - the Internet Protocol (IP), which were the first two networking protocols defined in this standard.

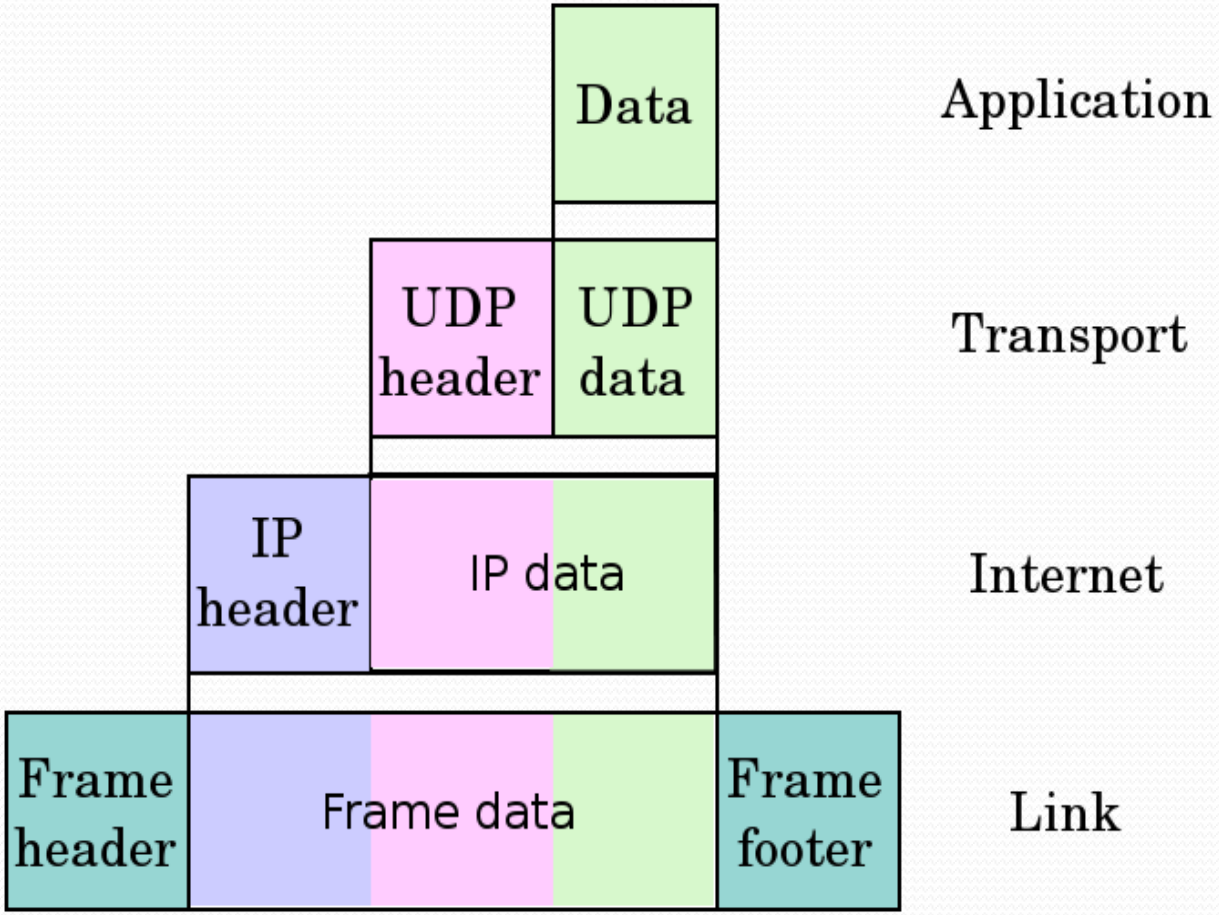
TCP/IP Layers

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>Application Layer</td><td rowspan="3">Application Layer
TELNET, FTP, SMTP, POP3, SNMP, NNTP, DNS,NIS, NFS, HTTP, ...</td></tr>
<tr><td>Presentation Layer</td></tr>
<tr><td>Session Layer</td></tr>
<tr><td>Transport Layer</td><td>Transport Layer
TCP , UDP , ...</td></tr>
<tr><td>Network Layer</td><td>Internet Layer
IP , ICMP, ARP, RARP, ...</td></tr>
<tr><td>Data Link Layer</td><td rowspan="2">Link Layer
FDDI, Ethernet, ISDN, X.25,...</td></tr>
<tr><td>Physical Layer</td></tr>
</table>

TCP/IP Stack


Network Connections
Host A
Router
Router
Host B
Stack Connections
Application
Application
Peer-to-peer
Transport
Transport
Internet
Internet
Internet
Internet
Link
Link
Link
Link
Ethernet
Fiber, Satellite, etc.
Ethernet

TCP/IP Encapsulation



TCP/IP Some Protocol

Layer	Protocol
Application	DNS, TFTP, TLS/SSL, FTP, Gopher, HTTP, IMAP, IRC, NNTP, POP 3, SIP, SMTP, SMPP, SNMP, SSH, Telnet, Echo, RTP, PNRP, rlogin, ENRP
	Routing protocols like BGP and RIP which run over TCP/UDP, may also be considered part of the Internet Layer.
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, RSVP
Internet	IP (IPv4, IPv6), ICMP, IGMP, and ICMPv6
	OSPF for IPv4 was initially considered IP layer protocol since it runs per IP-subnet, but has been placed on the Link since RFC 2740.
Link	ARP, RARP, OSPF (IPv4/IPv6), IS-IS, NDP

Why Layering Considered Harmful?

- In the data networking context structured layering implies that the functions of each layer are carried out completely before the protocol data unit is passed to the next layer.
- This means that the optimization of each layer has to be done separately.
- Such ordering constraints are in conflict with efficient implementation of data manipulation functions.

Why Layering Considered Harmful?

- As a result of inter-layer dependencies, increased layering can quickly lead to violation of the Simplicity Principle.
- Industry experience has taught us that increased layering frequently increases complexity and hence leads to increases in OPEX(Operating Expense), as is predicted by the Simplicity Principle.
- It is always possible to agglutinate multiple separate problems into a single complex interdependent solution. In most cases this is a bad idea.

Comparison Between OSI and TCP/IP Model

TCP/IP Model	OSI Model
TCP refers Transmission Control Protocol & IP means Internet Protocol.	OSI refers Open System Interconnection.
Implementation of OSI Model	Reference Model.
It has only four layers.	It has seven layers.
It is model around which internet is developed.	It is a theoretical model.
It is more reliable.	It is less reliable.
TCP/IP follows horizontal approach.	OSI follows a vertical approach.
Protocol dependant standard.	Protocol independent standard.

IP addressing

- IP addressing is used to **identify devices uniquely** on a network
- Two main versions:
- **IPv4**
- **IPv6**
- Addressing is essential for **routing and communication**

PHYSICAL ADDRESSING

- **Physical Address (MAC Address):**
- Assigned to **network interface card (NIC)**
- 48-bit address
- Written in hexadecimal
- Example: 00-1A-2B-3C-4D-5E
- Used at **Data Link Layer**

Cont.

- The physical address refers to a location in the memory. It allows access to data in the main memory. A physical address is not directly accessible to the user program hence, a logical address needs to be mapped to it to make the address accessible. This mapping is done by the **MMU** . Memory Management Unit(MMU) is a hardware component responsible for translating a logical address to a physical address.

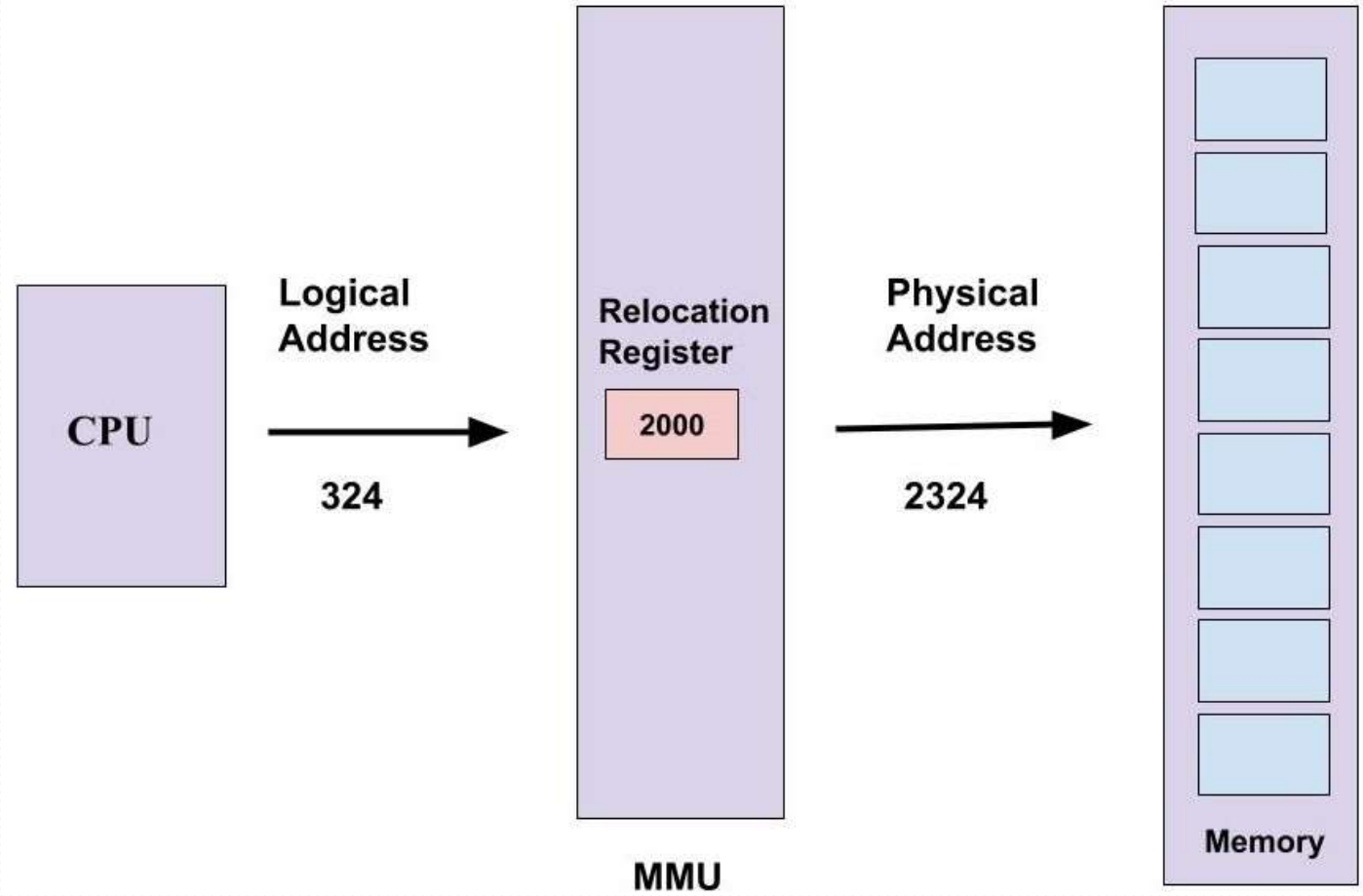
LOGICAL ADDRESSING

- **Logical Address (IP Address):**
- Assigned by **network administrator or ISP**
- Can be changed
- Used at **Network Layer**
- Enables routing across networks

Cont.

- A logical address or virtual address is an address that is generated by the CPU during program execution. A logical address doesn't exist physically. The logical address is used as a reference to access the physical address. A logical address usually ranges from zero to maximum (max). The user program that generates the logical address assumes that the process runs on locations between 0 to the max. This **logical address** (generated by CPU) combines with the **base address** generated by the MMU to form the **physical address** .

The diagram below explains how the mapping between logical and physical addresses is done.



Cont.

- The CPU generates the logical address(here, 324).
- The MMU will generate the base address (here, 2000) which is stored in the Relocation Register.
- The value of Relocation Register(here, 2000) is added to the logical address to get the physical address. i.e. 2000+324= 2324(Physical Address).

Difference between the physical and logical address

- The fundamental difference between a physical address and the logical address is that logical address is generated by the CPU while the program is running whereas the physical address is a location in memory.
- The logical address is generated by the CPU whereas physical address is computed by the MMU.
- The logical address does not exist physically in the memory hence it is sometimes known as virtual address whereas the physical address is a location in the memory unit.
- The logical address is used as a reference to access the physical address. The physical address cannot be accessed directly.

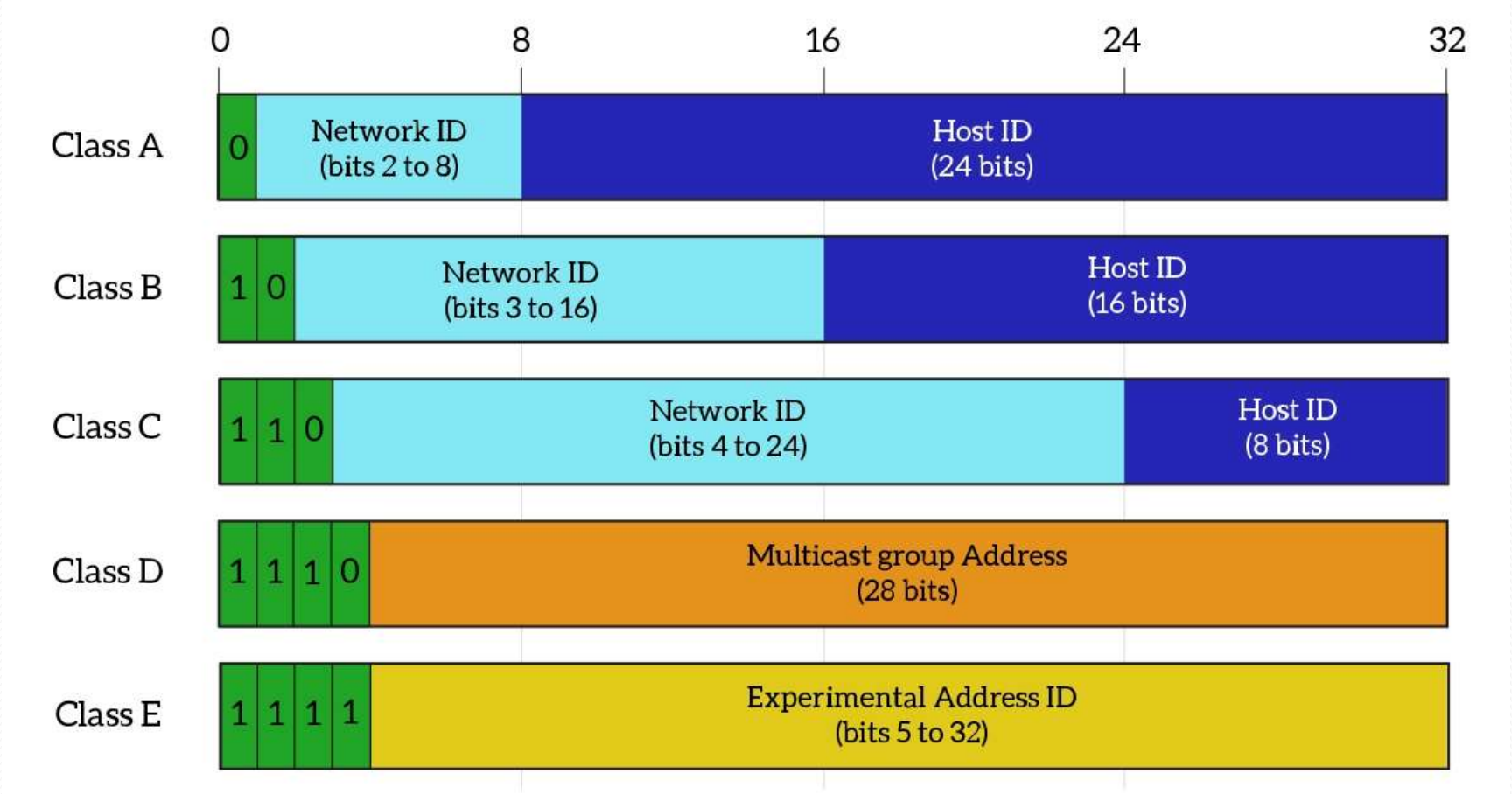
Cont.

- Users can view the logical address of a program. But, they cannot view the physical address of a program.
- The set of all the logical addresses generated in reference to a program by the CPU is called **Logical Address Space** whereas the set of all the physical addresses mapped to the logical address is called **Physical Address Space** .

IPv4 ADDRESSING

- IPv4 is a **32-bit address**
- Divided into **4 octets**
- Each octet = 8 bits
- Total addresses = **$2^{32} \approx 4.3$ billion**
- **IPv4 ADDRESS NOTATION**
- **Dotted Decimal Notation**
- Example: 192.168.1.1
- Each octet ranges from **0 to 255**

IP ADDRESS CLASSES



NET-ID

- **Net-ID**: Identifies network
- A network ID also known as NetID is a fixed bit in the IP address that represents the entire network of any host It is connected to the network. i.e., it tells the network of the host by which the host is connected.
- The total size of the IP address is 32 bits and the IP address is divided into four octets each of size is 8 bits.

Host-ID

- **Host-ID**: Identifies device within network
- It is the fragment of an IP address that uniquely identifies a host within a network. The network ID can be found by ANDing the IP (in binary) and subnet mask (in binary). The host ID is found in the same way, except one must first invert the subnet mask (not an official term, but could that binary value the 'host mask').

ADDRESS DEPLETION

- Classful addressing wastes IPs
- Limited IPv4 address space
- Growth of Internet caused exhaustion
- Solution:
- CIDR
- NAT
- IPv6

Special IP addresses

- There are several IP addresses that are special in one way or another. These addresses are for special purposes or are to be put to special use.
- Addresses significant to every IP subnet
  - Network Address
  - Broadcast Address
- Addresses significant to individual hosts
  - Loopback Address
- Special Addresses of Global Significance
  - Private Addresses
  - Reserved Addresses

Subnetting

- Subnetting is the process of stealing bits from the HOST part of an IP address in order to divide the larger network into smaller sub-networks called subnets. After subnetting, we end up with NETWORK SUBNET HOST fields. We always reserve an IP address to identify the subnet and another one to identify the broadcast subnet address. Here are three reasons why you may want to use subnetting:
- Conservation of IP addresses: Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses (254-20=234). Breaking up large networks into smaller parts would be more efficient and would conserve a great amount of addresses.
- Reduced network traffic: The smaller networks that created the smaller broadcast domains are formed, hence less broadcast traffic on network boundaries.
- Simplification: Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

Supernetting

Supernetting is the procedure of combine the small networks into larger space. In subnetting, Network addresses’s bits are increased. on the other hand, in subnetting, Host addresses’s bits are increased. Subnetting is implemented via Variable-length subnet masking, While supernetting is implemented via Classless interdomain routing.

Cont.

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically,

.

Cont.

When multiple networks are combined to form a bigger network, it is termed as super-netting

Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

- There are some points which should be kept in mind while supernetting:
- All the Networks should be contiguous.
- The block size of every networks should be equal and must be in form of 2^n.
- First Network id should be exactly divisible by whole size of supernet

Difference between Subnetting and Supernetting

S.NO	SUBNETTING	SUPERNETTING
1.	Subnetting is the procedure to divide the network into sub-networks.	While supernetting is the procedure of combine the small networks.
2.	In subnetting, Network addresses's bits are increased.	While in subnetting, Host addresses's bits are increased.
3.	In subnetting, The mask bits are moved towards right.	While In supernetting, The mask bits are moved towards left.
4.	Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
5.	In subnetting, Address depletion is reduced or removed.	While It is used for simplify routing process.

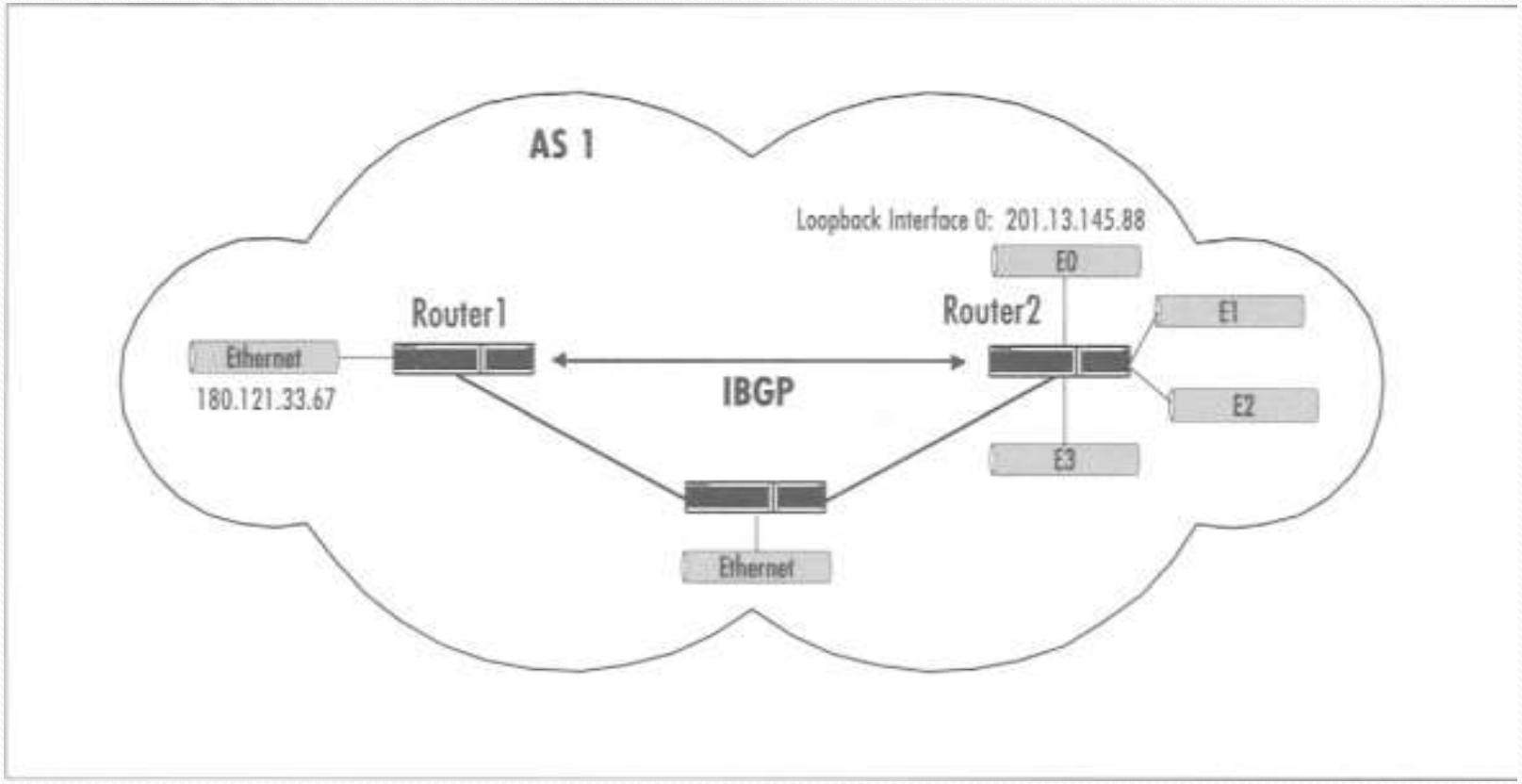
Loop back concept

Loop back concept is the routing of electronic signals, digital data streams, or flows of items back to their source without intentional processing or modification. It is primarily a means of testing the communications infrastructure.

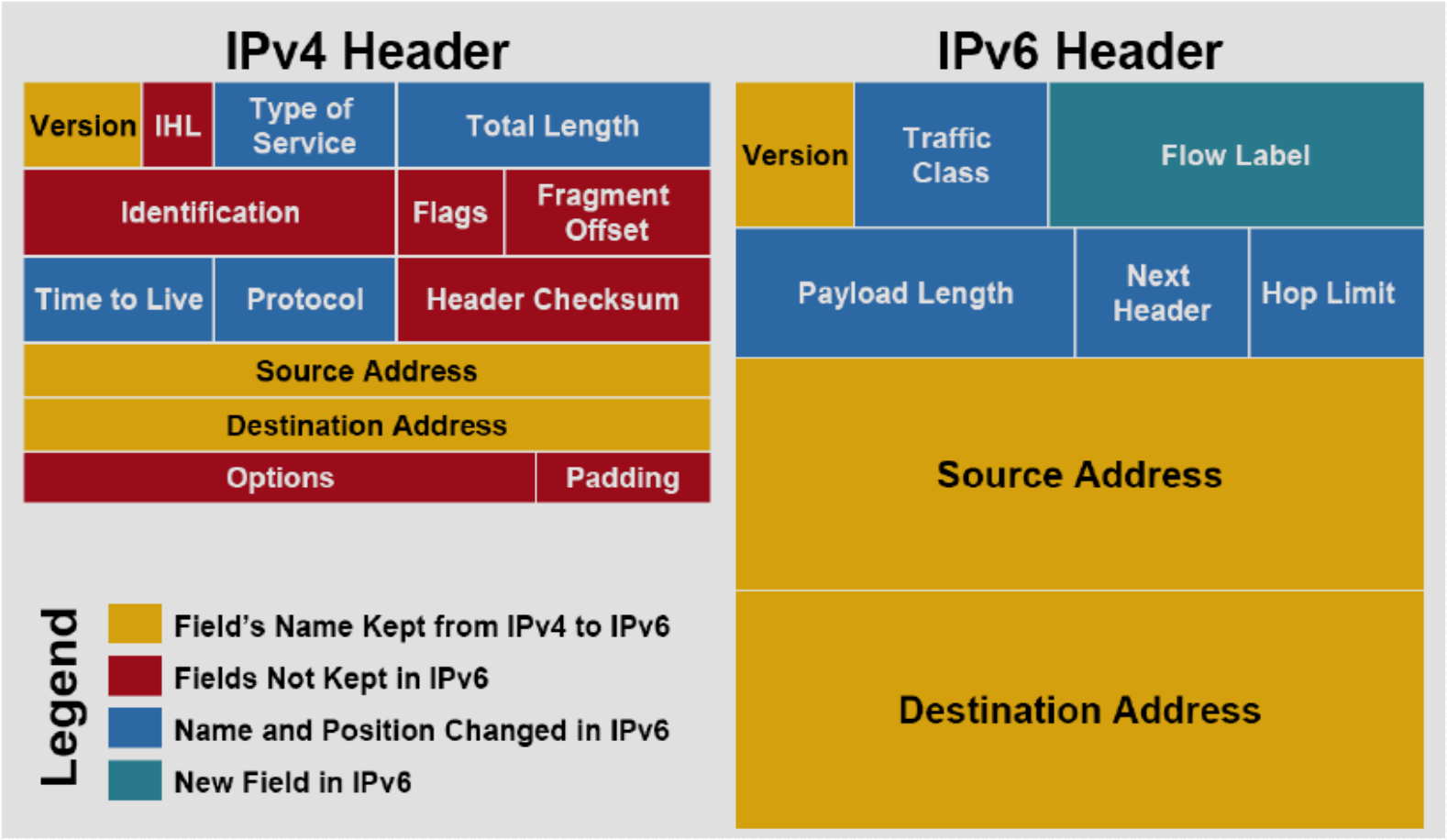
Cont.

There are many example applications. It may be a communication channel with only one communication endpoint. Any message transmitted by such a channel is immediately and only received by that same channel. In telecommunications, loopback devices perform transmission tests of access lines from the serving switching center, which usually does not require the assistance of personnel at the served terminal. Loop around is a method of testing between stations that are not necessarily adjacent, wherein two lines are used, with the test being done at one station and the two lines are interconnected at the distant station. A patch cable may also function as loopback, when applied manually or automatically, remotely or locally, facilitating a loop-back test.

Loop back concept



IPV4 and IPV6 packet Format



Configuring IPv4 or IPv6 Routing

- Click Network and Sharing Center on your computer. Click Local Area Connections and then click Properties to **configure** network addresses and other information. Click the Networking tab and then, click either Internet Protocol Version 4 (TCP/**IPv4**) or Internet Protocol Version 6 (TCP/**IPv6**) and then click Properties.

IPv4 HEADER

- **IPv4 Header Fields:**
- Version
- Header Length
- TTL
- Protocol
- Source IP
- Destination IP
- Header size: **20–60 bytes**

IPv6 INTRODUCTION

- IPv6 uses **128-bit address**
- Total addresses = $\mathbf{2^{128}}$
- Designed to replace IPv4

IPv6 HEADER

- **Simplified Header Fields:**
- Version
- Traffic Class
- Flow Label
- Payload Length
- Next Header
- Source Address
- Destination Address
- Header size: **40 bytes fixed**

IPv4 vs IPv6

Feature	IPv4	IPv6
Address Size	32 bits	128 bits
Address Format	Dotted decimal (e.g., 192.168.1.1)	Hexadecimal (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
Address Space	About 4.3 billion addresses	About 340 undecillion addresses
NAT	Required due to address shortage	Not needed because of vast address space
IPSec Support	Optional	Built-in
Autoconfiguration	Manual setup or DHCP	Automatic address configuration
Header Complexity	Complex	Simple
Fragmentation	Handled by routers and sending hosts	Handled by sending hosts only

ETHERNET

- Ethernet is the **most widely used LAN technology**
- Developed by **IEEE**
- Uses **CSMA/CD** access method (traditional Ethernet)
- Defined under **IEEE 802.3 standard**

10 Mbps – TRADITIONAL ETHERNET

- **Speed:** 10 Mbps
- **Standards:**
- 10BASE5 – Thick coaxial cable
- 10BASE2 – Thin coaxial cable
- 10BASE-T – Twisted pair cable
- **Features:**
- Uses hubs
- High collision rate
- Half-duplex communication

LIMITATIONS OF TRADITIONAL ETHERNET

- Low speed
- High collision
- Limited scalability
- Not suitable for modern networks

100 Mbps – FAST ETHERNET

- **Speed:** 100 Mbps
- **Standards:**
- 100BASE-TX
- 100BASE-FX
- **Features:**
- Uses switches
- Reduced collisions
- Supports full-duplex

ADVANTAGES OF FAST ETHERNET

- Faster data transfer
- Improved performance
- Backward compatible with 10 Mbps

1000 Mbps – GIGABIT ETHERNET

- **Speed:** 1000 Mbps (1 Gbps)
- **Standards:**
- 1000BASE-T
- 1000BASE-SX
- 1000BASE-LX
- **Features:**
- High speed
- Uses fiber or twisted pair
- Full-duplex communication

IEEE 802.3 standards

- IEEE 802.3 standards defines a range of networking systems that are bases on the original Ethernet standard.

Standard	Cable type	Segment Length	Connector	Topology
10Base2	Thin Coaxial	185 meters	BNC	Physical bus
10Base5	Thick Coaxial	500 meters	Vampire Taps	Physical bus
10BaseT	Category 3,4,5 twisted pair	100 meters	RJ-45	Physical star

Fast Ethernet IEEE 802.3u

Standard	Cable Type	Segment Length	Connector	Topology
100BaseTx	Category 5 UTP	100 meters	RJ-45	Physical star
100BaseT4	Category 3,4,5 UTP	100 meters	RJ-45	Physical star
100BaseFX	Multimode/Single-mode fiber-optic cable	412/Multimode fiber-optic 10,000/single-mode fiber-optic	SC,ST,MIC	Physical star

Gigabit Ethernet802.3z and 802.3ab

Standard	Cable Type	Segment length	Connector
1000BaseLX	Multimode/ single-mode fiber	550/multimode 5000/single-mode	Fiber connectors
1000BaseSX	Multimode fiber	550 meters using 50 Micron multimode fiber	Fiber connectors
1000BaseCX	STP twisted pair	25 meters	9-pin shielded connector, 8-pin fiber channel type 2 connector
1000BaseT	Category 5 UTP	100 meters	RJ-45

Ethernet Media Standards

Media Standard	Cable Type	Bandwidth Capacity	Maximum Length
10Base2	Coaxial	10 Mbps	185m
10Base5	Coaxial	10 Mbps	500m
10BaseT	UTP (CAT 3 or higher)	10 Mbps	100m
100BaseTX	UTP (CAT 5 or higher)	100 Mbps	100m
10BaseFL	Fibre Optic	10 Mbps	2Km
100BaseFX	Fibre Optic	100 Mbps	HD 400m/FD 2km
1000BaseT	UTP (CAT 6 or higher)	1 Gbps (1000 Mbps)	100m
10GBase-T	UTP (Cat 6a or higher)	10 Gbps (10000 Mbps)	100m
1000BaseSX	Fibre Optic	1 Gbps (1000 Mbps)	MMF 550m
1000BaseLX	Fibre Optic	1 Gbps (1000 Mbps)	MMF 500m/SMF 10km
1000BaseCX	Fibre Optic	1 Gbps (1000 Mbps)	100m
10GbaseSR	Fibre Optic	10 Gbps	300m
10GbaseLR	Fibre Optic	10 Gbps	SMF 10km

NETWORK CONNECTIVITY

- **Network Connectivity** refers to:
- Connecting devices to enable communication
- Uses hardware devices called **networking devices**
- **NETWORK CONNECTIVITY DEVICES**
- Network Interface Card (NIC)
- Hub
- Switch
- Router
- Repeater
- Modem
- Gateway

NETWORK INTERFACE CARD (NIC)

- Hardware that connects a computer to network
- Has a unique MAC address
- Operates at Physical & Data Link layer
- Wired or Wireless NIC
- In the smooth functioning of a computer , other than computers and wiring , many devices (or) specialized hardware play important roles .

Cont.

Cont.

A standalone computer (a computer that does not attached to a network) lives in its own world and carries out its tasks with its own inbuilt resources.

The (NIC) is a device that is attached to each of the workstations and the server & helps the workstation to establish all the important connections with network.

Each NIC that is attached to a workstation has a unique number identification which is known as note address

Cont.

The NIC is also called as Terminal Access Point (TAP) different manufacturers have different name for the interface .

The NIC is also called as *NIU* – (Network Interface Unit)

The (NIC) manufacturers assigns a unique physical address to each NIC-card , this physical address is know as MAC-address ------ (Media Access Control)

HUBS

A network host is a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network.

There are two types of hub:

(I) ACTIVE HUB

(II) PASSIVE HUB

(I) ACTIVE HUB

(i) **it's electrically amplify the signal as it moves from one connected device to another.**

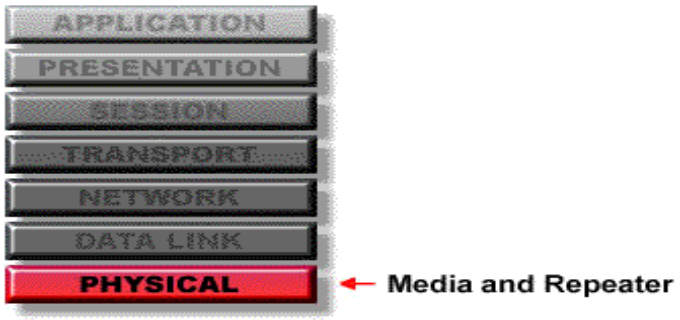
(ii)active concentrators are used like repeaters to extend the length of the network.

(ii) PASSIVE HUB

It allows the signal to pass from one computer to another without any change.

Repeater :

- A repeater operates at the physical layer. Its task is to regenerate the signal over the same network before the signal becomes too weak or corrupted.
- A repeater is a regenerator, not an amplifier.
- When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original
-



The OSI Model

SWITCH


D-Link
D-Link
DGS-108
1000M
10/100M
10/100M Link Act
1000M Link Act
1
2
3
4
5
6
7
8

SWITCH

- A switch is a device that is used to segment networks into different subnetworks called *subnet* or LAN Segment.
- Segmenting the network into smaller subnet, prevents traffic overload in a network.
- A switch is responsible for filtering (or) transforming data in a specific way and forwarding packets between LAN segment.

SWITCH

- A switch can support any packet of protocol.
- LAN’s that are segmented through switches are called as switched LANs.

ROUTER

ROUTER

- A device that works like a bridge but can handle different protocol is know as Router.
- A Router is a network device that forwards data from one network to another network.
- A router works like a bridge but can handle different protocols.

ROUTER

- If the destination is unknow to a router it sends the traffic to another router (using logical address) which knows the destination, Based on a network road map called as (*Routing Table).*

- Routers can help to ensure that packets are travelling the most efficient paths to their destination.

GATEWAY

GATEWAY

- A gateway is a network device that connects dissimilar networks.
- It establishes an intelligent connection between a local network and external network with completely different structures
- Gateway is actually a node on a network that server as an entrance to another network.
- In enterprises the gateway is the computer that routes the traffic from workstation to a out side network that serving the web pages.

NETWORK SECURITY

- **Network Security** is the practice of protecting:
- Data
- Devices
- Services
- Network infrastructure
- From unauthorized access, attacks, and damage.

NETWORK SECURITY PRINCIPLES

- **Confidentiality**
- Prevent unauthorized access
- Encryption, authentication
- **Integrity**
- Data should not be altered
- Hashing, checksums
- **Availability**
- Services available when needed
- Redundancy, backups

CRYPTOGRAPHY

- Cryptography is the technique of **securing data** by converting it into unreadable form.
- **TYPES OF CRYPTOGRAPHY**
- **1. Symmetric Key Cryptography**
- Same key for encryption & decryption
- Fast
- Example: AES, DES
- **2. Asymmetric Key Cryptography**
- Public & Private keys
- More secure
- Example: RSA

SECURE NETWORK PROTOCOLS

- Secure protocols ensure:
- Data confidentiality
- Data integrity
- Secure communication
- **COMMON SECURE PROTOCOLS**
- **HTTPS** – Secure web browsing
- **SSH** – Secure remote login
- **SSL/TLS** – Encryption layer
- **SFTP** – Secure file transfer
- **IPSec** – Network-level security

PING (Packet Internet Groper)

- **PING** is a network troubleshooting command used to:
- Test **connectivity** between two devices
- Check whether a host is **reachable**
- Measure **network delay (latency)**
- It is one of the **most basic and widely used network diagnostic tools**.
- **Protocol Used by PING**
- PING uses the **ICMP (Internet Control Message Protocol)**
- ICMP works at the **Network Layer (Layer 3)** of the OSI model
- PING sends **ICMP Echo Request** messages and waits for **ICMP Echo Reply**

How PING Works

- Source device sends an **ICMP Echo Request** to the destination
- Destination receives the request
- Destination replies with an **ICMP Echo Reply**
- Source measures:
  - Time taken
  - Packet loss
- 📌 If replies are received → host is reachable
  📌 If no replies → network problem or host is down

IPCONFIG

- **IPCONFIG (Internet Protocol Configuration)** is a **command-line network utility** used in **Windows operating systems** to:
- Display current **TCP/IP network configuration**
- Manage IP settings assigned to network interfaces
- **Purpose of IPCONFIG**
- View IP address information
- Check subnet mask and default gateway
- Verify DHCP configuration
- Troubleshoot network connectivity issues

Advantages &Limitations of IPCONFIG

- **Advantages of IPCONFIG**
- Easy to use
- Built-in Windows tool
- Essential for network troubleshooting
- **Limitations of IPCONFIG**
- Works only on **Windows**
- Cannot capture packets
- Provides limited diagnostic details

IFCONFIG

- **IFCONFIG (Interface Configuration)** is a **command-line network utility** used in **Linux and UNIX-based systems** to:
- Display and configure network interface parameters
- **Purpose of IFCONFIG**
- View network interface details
- Enable or disable interfaces
- Assign IP addresses manually
- Diagnose network issues

Advantages &Limitations of IFCONFIG

- **Advantages of IFCONFIG**
- Powerful configuration tool
- Useful for advanced network administration
- Supports manual IP assignment
- **Limitations of IFCONFIG**
- Deprecated in modern Linux systems
- Replaced by **ip** command
- Requires root privileges

Wireless LAN

- Wireless LAN uses wireless transmission medium.
- Problems like high prices, low data rates, occupational safety concerns, and licensing requirements have been addressed.
- Popularity of wireless LANs has grown rapidly.

Features of WLAN

- Wireless communication using **radio frequencies**
- Mobility of devices within network coverage
- Easy installation and flexibility
- Security challenges due to open medium

Advantages & Disadvantages

- **Advantages**
- No physical cables → easy deployment
- Supports mobile devices
- Flexible network expansion
- Cost-effective for large areas
- **Disadvantages**
- Signal interference from other devices
- Security issues (eavesdropping, hacking)
- Limited coverage area
- Dependent on power/battery for devices

IEEE 802.11 and 17.3 (S)

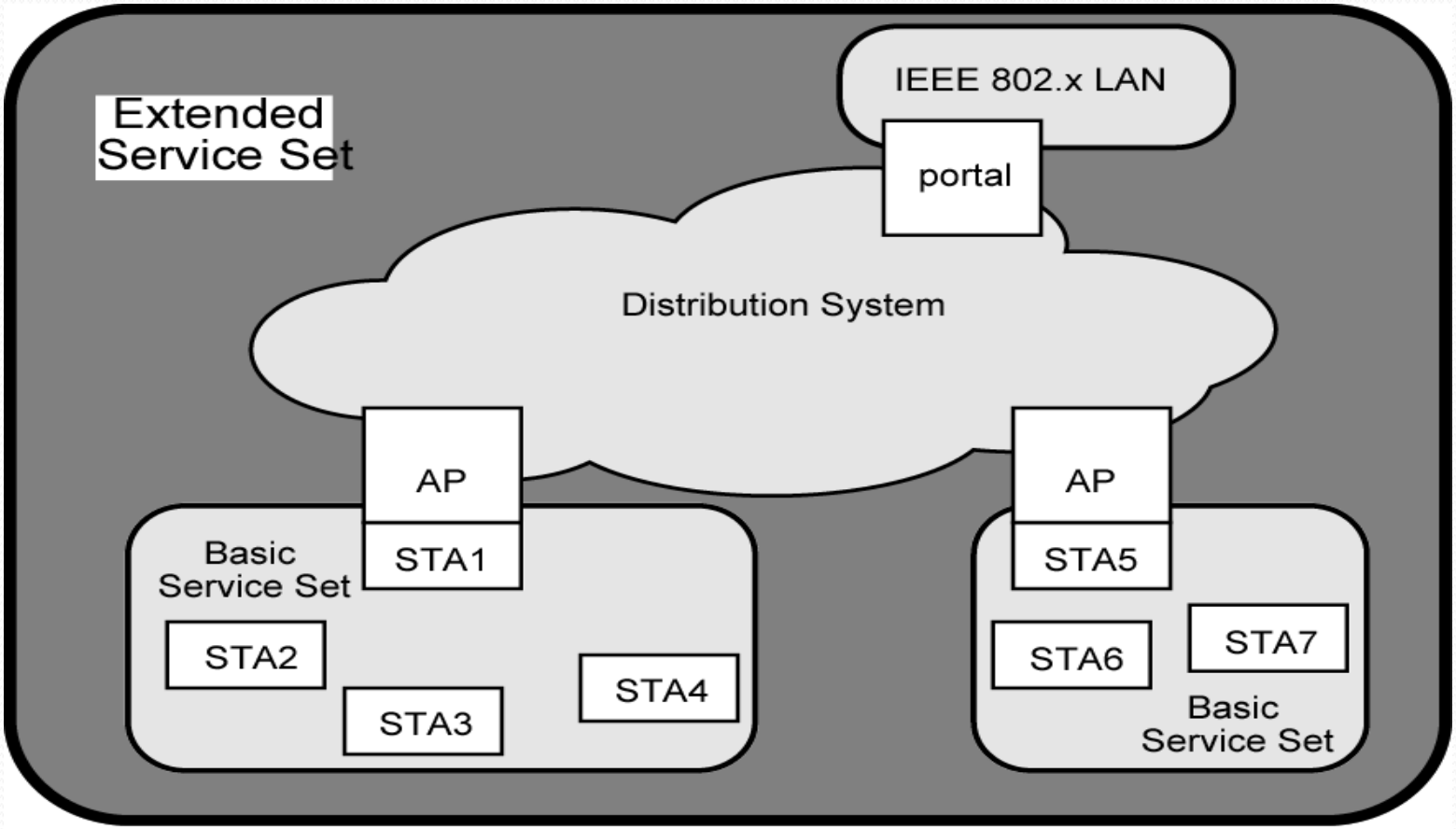
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

IEEE 802.11 – Architecture and Services

1. Architecture

- 802.11 architecture includes
  - ✓ Basic service set (BSS)
  - ✓ Extended service set (ESS)

IEEE 802.11 Architecture

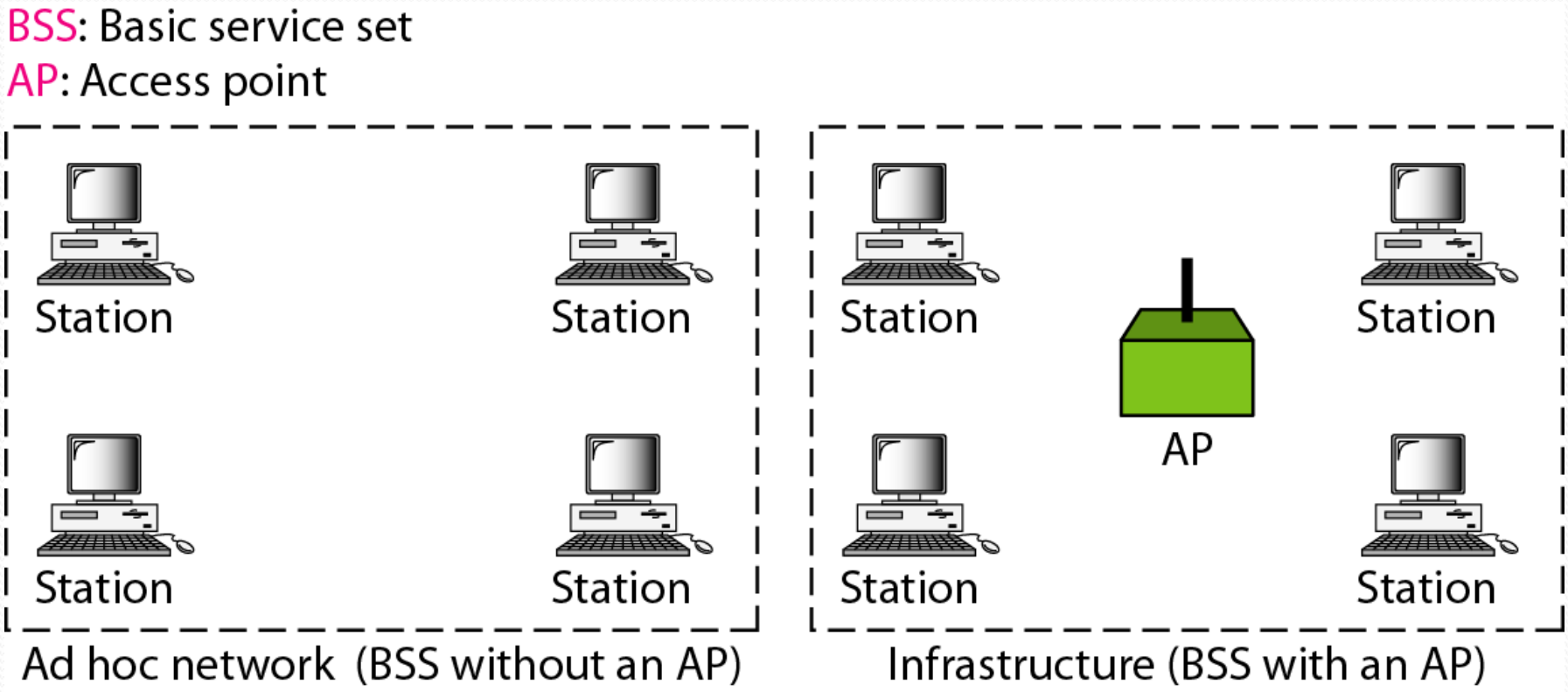


STA = station
AP = access point

IEEE 802.11 – Architecture and Services BSS

- ✓ covers the physical and data link layers.
- Smallest building block for wireless LAN is basic service set (BSS)
  - Contains Number of stations
  - With Same MAC protocol
  - Competing for access to same shared wireless medium
- BSS is made of stationary or mobile wireless stations and an optional central base station, known as the access point **(AP).**
- BSS with an AP - connect to backbone distribution system (DS) through access point (AP)
  - AP functions as bridge
- MAC protocol may be distributed or controlled by central coordination function in AP
- BSS generally corresponds to cell
- DS can be switch, wired network, or wireless network

Figure 14.1 *Basic service sets (BSSs)*



(Cannot send data to other BSSs)

BSS Configuration

- **Simplest**: each station belongs to single BSS
  - Within range only of other stations within BSS
- Can have **two BSSs overlap**
  - Station could participate in more than one BSS
- **Association** between station and BSS **dynamic**
  - Stations may turn off, come within range, and go out of range

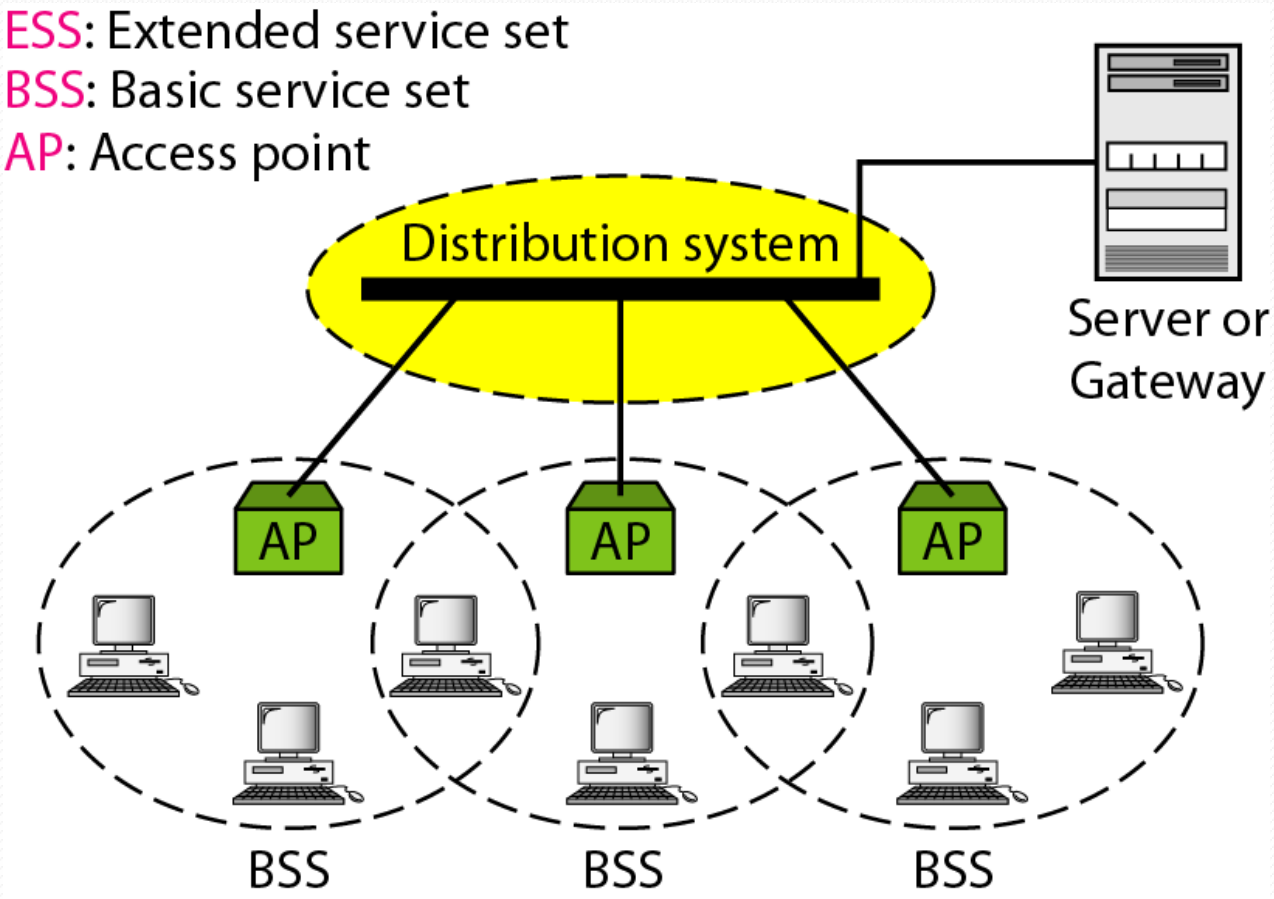
Extended Service Set (ESS)

- Two or more BSS interconnected by DS (backbone distribution system)
  - Typically, DS is wired backbone but can be any network
- Appears as single logical LAN to LLC

Access Point (AP)

- Logic within station that provides access to DS
  - Provides DS services in addition to acting as station
- To integrate IEEE 802.11 architecture with wired LAN portal
- Portal logic implemented in device that is part of wired LAN and attached to DS
  - E.g. Bridge or router

Figure 14.2 *Extended service sets (ESSs)*



WiMAX

- WiMAX (Worldwide Interoperability for Microwave Access) Wireless broadband technology for **long-range communication**
- Based on **IEEE 802.16 standard**
- Provides **high-speed internet** over several kilometers
- **Features of WiMAX**
- Coverage: up to 50 km for fixed, 5–15 km for mobile
- Data rate: up to 70 Mbps (fixed), lower for mobile
- Operates in **licensed and unlicensed bands**
- Supports **point-to-multipoint communication**

Advantages & Disadvantages

- **Advantages of WiMAX**
- Wide coverage → good for rural areas
- High data transfer speed
- Supports mobility
- Cost-effective compared to wired broadband
- **Disadvantages**
- Requires line-of-sight for long distance
- Interference from buildings or weather
- Limited device compatibility

Li-Fi (Light Fidelity)

- Wireless communication technology using **visible light** instead of radio waves
- Uses **LED light bulbs** to transmit data
- High-speed, secure, and energy-efficient
- **Features of Li-Fi**
- Data transmission speed: up to **10 Gbps or more**
- Works using **light intensity modulation**
- Short-range communication (line-of-sight)
- Cannot penetrate walls → more secure

Advantages & Disadvantages

- **Advantages of Li-Fi**
- Extremely high speed
- Immune to radio interference
- Secure communication
- Can operate in areas where Wi-Fi is restricted (airplanes, hospitals)
- **Disadvantages**
- Requires direct line-of-sight
- Limited mobility and coverage
- Cannot penetrate opaque objects

What is Bluetooth?

- Bluetooth is a **short-range wireless communication technology**.
- Operates in the **2.4 GHz ISM band**.
- Designed for **low-power, low-cost data transfer** between devices.
- Typical range: **10 meters (Class 2)**, up to **100 meters (Class 1)**.
- **Key Features**
- Wireless replacement for **cables**.
- Supports **voice, video, and data transfer**.
- Secure communication using **encryption and authentication**.
- Low energy consumption (**Bluetooth Low Energy – BLE**).

ADVANTAGES & LIMITATIONS OF BLUETOOTH

- **ADVANTAGES OF BLUETOOTH**
- Wireless convenience, cable-free
- Low power consumption (BLE for IoT)
- Secure due to short-range & encryption
- Easy to pair and use
- **LIMITATIONS OF BLUETOOTH**
- Limited range and speed compared to Wi-Fi
- Interference with other 2.4 GHz devices
- Not suitable for large data transfer
- Limited number of devices per piconet

What is Wi-Fi?

- Wi-Fi is a **wireless networking technology** that allows devices to connect to the Internet or communicate **without physical cables**.
- Based on the **IEEE 802.11 standard**.
- Operates in **2.4 GHz, 5 GHz, and 6 GHz bands**.
- Commonly used in **homes, offices, public hotspots, and mobile devices**.
- **Key Features**
- Wireless connectivity within a **local area network (LAN)**
- Supports multiple devices simultaneously
- Provides high-speed internet access
- Secure communication using **WPA2/WPA3 encryption**

ADVANTAGES & LIMITATIONS WI-FI

- **ADVANTAGES**
- Cable-free network → easy installation
- Supports multiple devices and mobility
- High-speed internet access
- Scalable for homes and enterprises
- **LIMITATIONS**
- Limited coverage range compared to wired LAN
- Interference from other devices (microwaves, Bluetooth)
- Security risks if not properly encrypted
- Performance drops with too many devices connected

Comparison between bluetooth and Wifi

Characteristic	Bluetooth	Wi-Fi
Frequency	2.4 GHz	2.4 GHz
Range	10 meters	100 meters
Data transfer rate	800 Kbps	11 Mbps
Power consumption	Low	Medium
Primary devices	Mobile phones, PDAs, consumer electronics, office and industrial automation devices	Notebook computers, desktop computers, servers
Primary users	Travelers, office and industrial workers, electronics consumers	Corporate offices, campuses, business or conference venues

THE CLOUDS

- A cloud is a generic term used for “INTERNET”.
- Cloud computing is internet-based computing whereby shared resources, software , and information are provided to computer and other devices are in demand, like electricity grid.
- Cloud computing is a new name for an old concept :*the delivery of computing services from a remote location* .

CLOUD COMPUTING

SERVER

VISUAL DESKTOP

SOFT WARE PLATFORM

APPLACATION

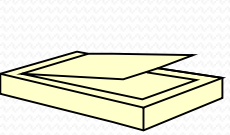
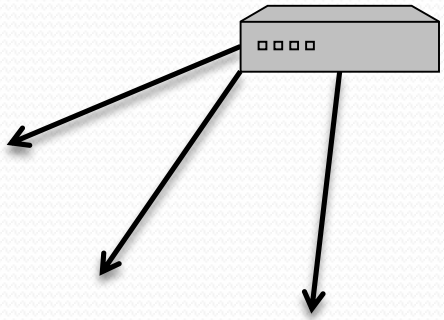
STORAGE/DATA

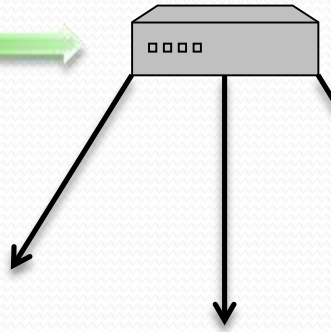
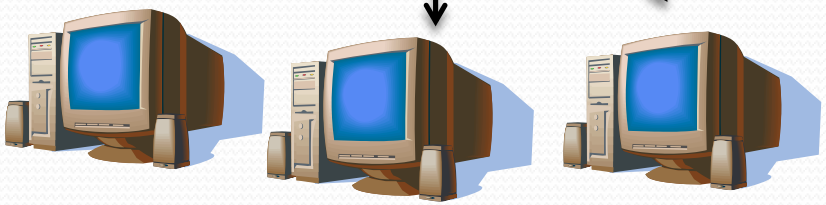
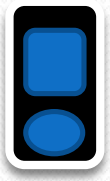
OS

NETWORK DIVECES

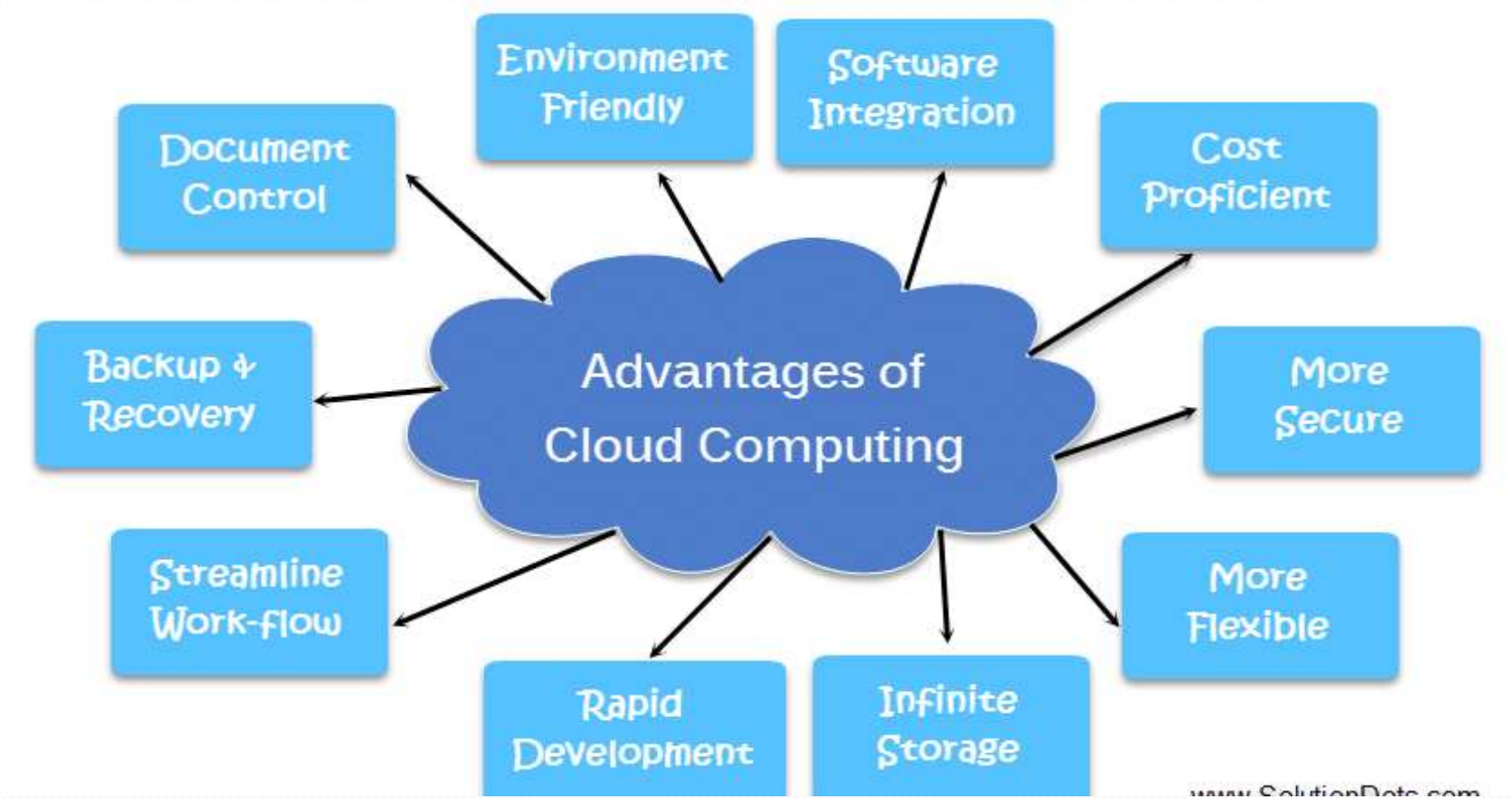
NETWORK DIVECESC

END USERS


Advantages of Cloud Computing



Types of Cloud Computing Services

- Cloud computing has three main types of services:
- IaaS
- PaaS
- SaaS

Infrastructure as a Service (IaaS)

- IaaS offers virtual access to computing resources like servers, storage, and networks. Users manage the software, operating systems, and applications, while the provider handles the hardware. It gives high flexibility and is useful for teams that need more control over their environment without the cost of owning physical infrastructure.

Platform as a Service (PaaS)

- PaaS provides a platform to build and deploy applications without managing the underlying hardware or system software. It allows developers to focus on writing code while the provider manages everything else. This type speeds up development and reduces time spent on maintenance, making it ideal for building apps quickly and efficiently.

Software as a Service (SaaS)

- Software as a Service delivers fully functional software over the internet. Users don’t need to install, update, or maintain anything. They simply access the software through a browser. It’s designed for ease of use and is perfect for individuals or teams who want quick access to tools without dealing with technical setup or management.

TYPES OF CLOUDS

1. PRIVATE CLOUDS
2. PUBLIC CLOUDS
3. COMMUNITY CLOUDS
4. HYBIRED CLOUDS

1.PRIVATE CLOUDS

- These are the clouds for exclusive use by single organization and typically controlled, managed and hosted in private data centers.
- The hosting and operation of private clouds may also be outsourced to third party services provider, but a private clouds remains for the exclusive use of one organization.

1.PRIVATE CLOUDS

Best Private Cloud Providers

- ✓ HPE. By most estimates, Hewlett Packard Enterprise (HPE) is a key leader in the private cloud market.

Vmware Dell Oracle

IBM Microsoft. Cisco.

NetApp.

2.PUBLIC CLOUDS

These are the clouds for use by multiple organization on shared basis and hosted and by the third party services provider.

- ✓ Examples of public clouds include Amazon Elastic ComputeCloud (EC2), IBM's Blue Cloud, Sun Cloud,Google AppEngine and Windows Azure Services Platform

3.COMMUNITY CLOUDS

- These are the clouds for use by a group of related organization who wish to make use of a common cloud computing environment .
- FOR EXP:
  - All suppliers to a larger manufacture.
  - All universities in a given region.

4.HYBRID CLOUDS

When a single organization adopts both private and public clouds for a single application in order to take advantage of the benefits of both.