NET-CENTRIC COMPUTING

INTRODUCTION

- Earlier computer systems functioned in isolation from one another.
- Today it is almost impossible to conceive of a computer system that it not networked in some way to other systems.
- Discuss the Network vs Internet.
- There are a wide variety of devices connected to the Internet.
- Net-Centric Computing is computing where network plays a the central or larger role.

INTRODUCTION:

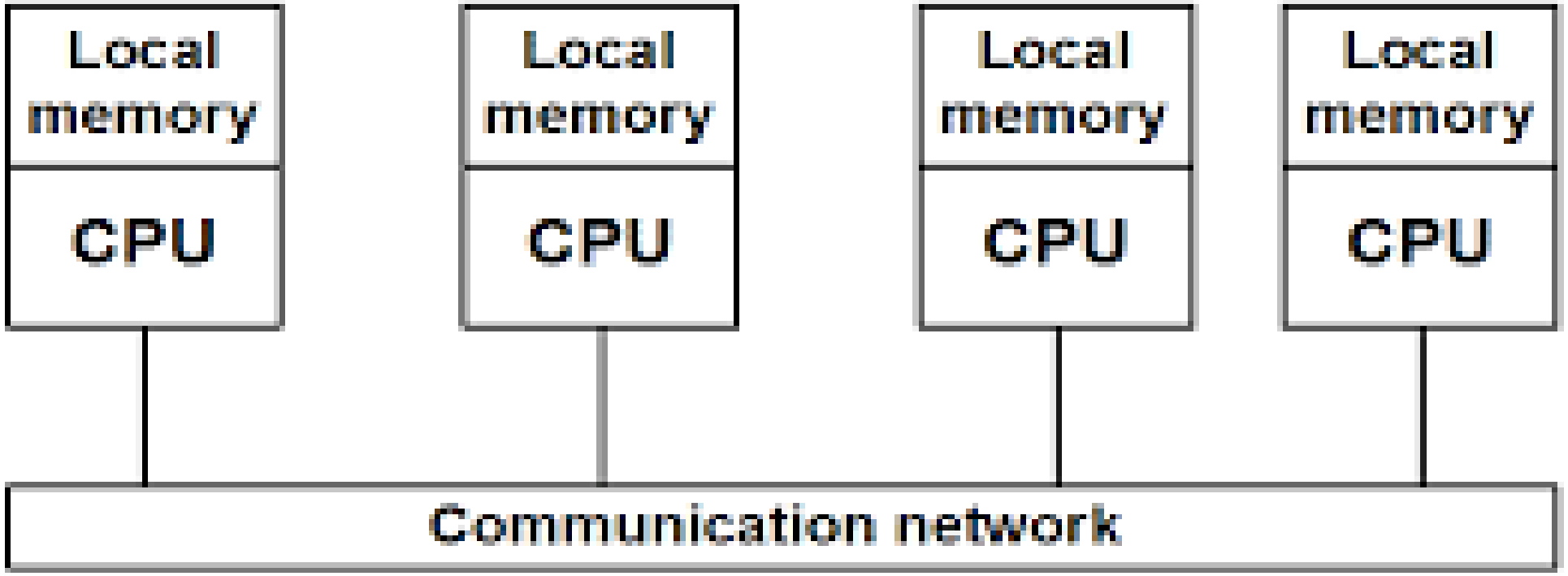
- Computing is the process of using computer technology to complete a given – oriented task.
- Computing may encompass the design and development of software and hardware systems for a broad range of purpose.
- Computing is fundamentally about information process.
- Central Processing Unit (CPU) is a piece of hardware that carries out the instructions of a computer program. It is considered as a brain of computer system.
- It performs the basic arithmetic, logical and input/output operations of a computer system.
- Note that Central Processing Unit is also the processor.

MULITIPROCESSOR SYSTEM

- Multiprocessor is a system which has more than two processors in the system.
- There are two types multiprocessing systems: loosely coupled and tightly coupled.
- Tightly coupled systems are referred to as parallel computing systems and loosely coupled systems are referred to as distributed computing system.
- The degree of coupling between the processors are low in loosely coupled system whereas, the degree of coupling between processors are high in the tightly coupled system.

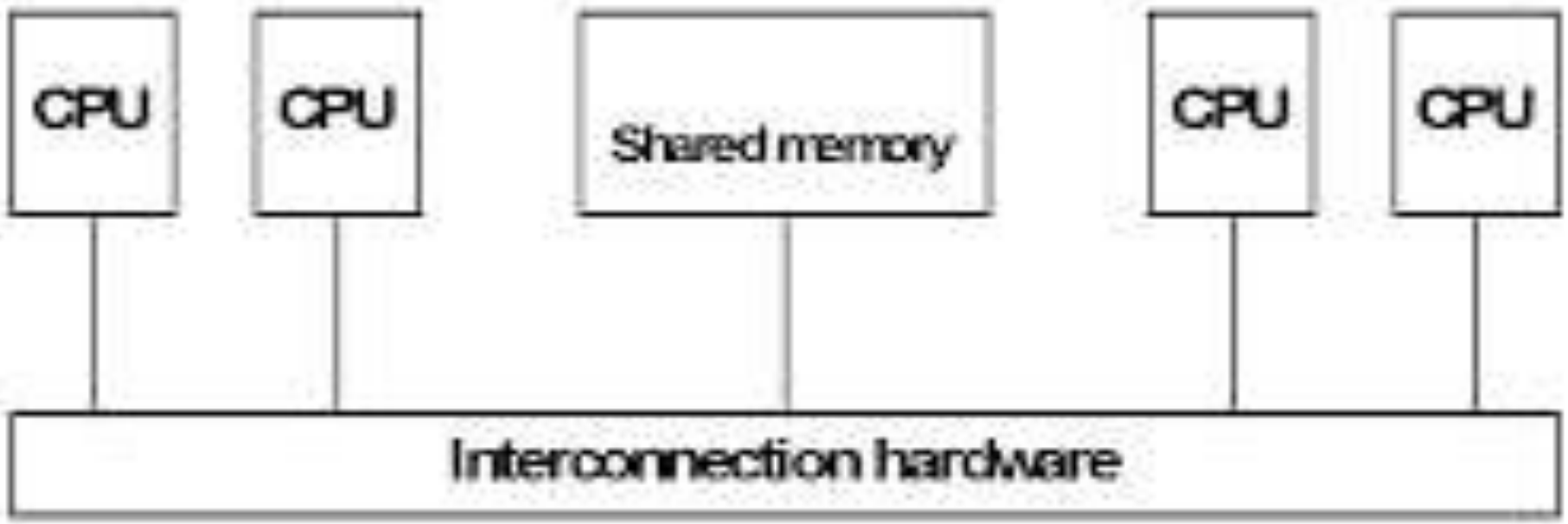
Loosely Coupled System

- Distributed Memory Systems (DMS)
- Communication via Message Passing



Tightly Coupled Systems

- Systems with a single system wide memory
- Parallel Processing System , SMMP (shared memory multiprocessor systems)



KEY DIFFERENCES BETWEEN LOOSELY COUPLED AND TIGHTLY COUPLED MULTIPROCESSOR SYSTEMS ARE:

- Loosely coupled system has distributed memory where as tightly coupled system has shared memory.
- Loosely coupled is efficient when the tasks running on different processor has minimal interaction between then. While, the tightly coupled system can take a higher degree of interaction between processors and is efficient for high-speed and real-time processing.
- The loosely coupled system generally do not encounter memory conflict which is mostly experienced by tightly coupled system.
- The data rate of the loosely coupled system is low whereas the data rate of tightly coupled system is high.
- The loosely coupled system is less expensive but larger in size whereas tightly coupled system is more expensive but compact in size.
- The Interconnection network in a loosely coupled system is message transfer system (MTS) whereas, in a tightly coupled system the Interconnection networks are Processor-Memory Interconnection network. (PMIN) and the Interrupt-signal Interconnection Network (ISIN).

CENTRALISED COMPUTING

- Centralised Computing – is computing done at a central location, that is all or most of the processing is performed on a central server.
- Centralised computing uses client/server architecture where one or more client nodes are directly connected to a central server.
- In this computing, the client sends a request to a server and receivers from server.
- For example, A network of Computer Science Department, where a lecturer, admin, and student requests for a department server.

CHARACTERISTICS OF CENTRALISED COMPUTING

- Presence of Global Clock: All clients modes sync up with the clock of the central node (global clock)
- One Single Central Unit: One single central unit which serves/coordinates all the other nodes
- Department Failure of Components. Central node failure causes system to fail.

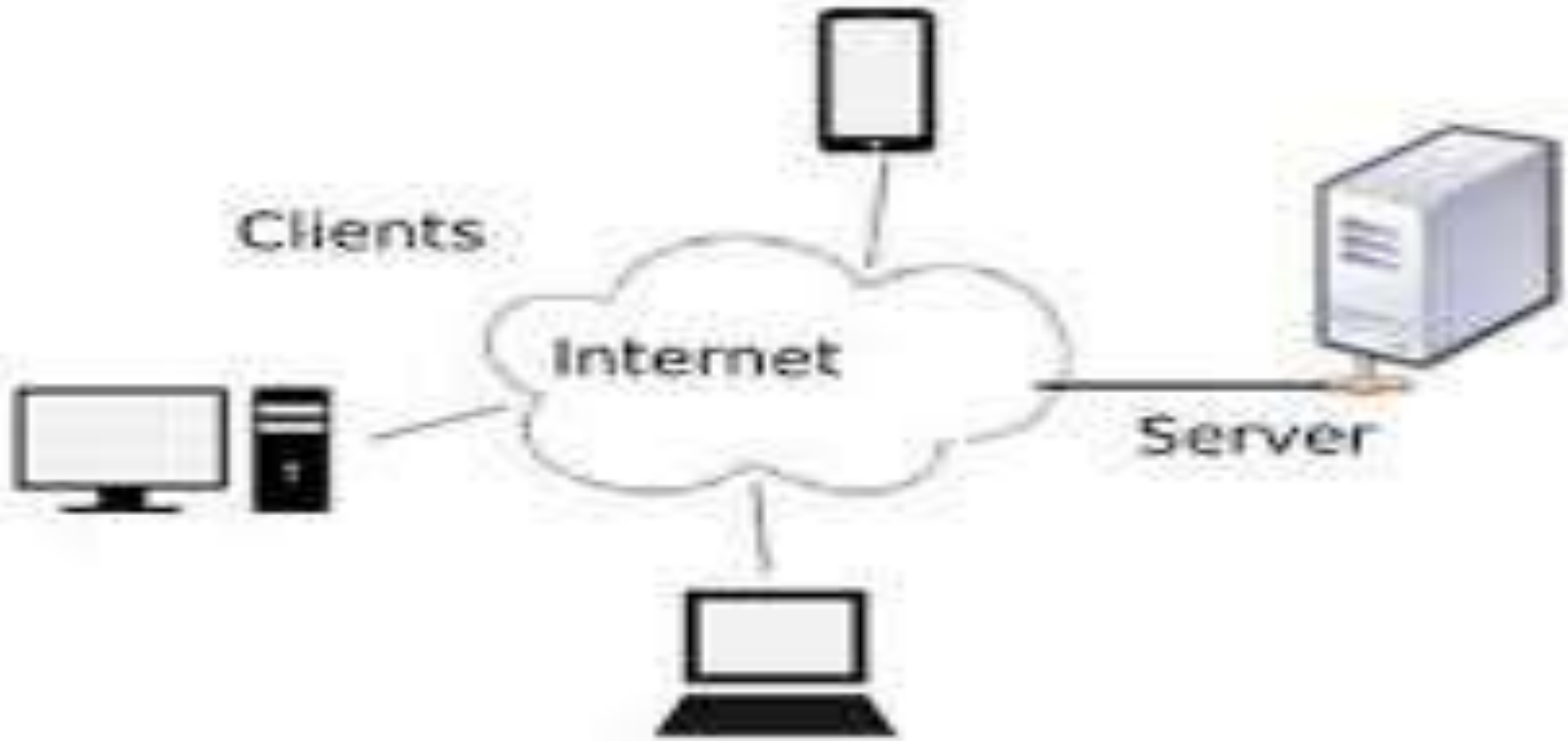


Fig Centralized Computing

ADVANTAGE OF CENTRALISED COMPUTING

- Easy to physically secure.
- Smooth and elegant person experience.
- Dedicated resources.
- More cost effective.
- Quick updates are possible.
- Easy detachment of a node from the network.

DISADVANTAGE OF CENTRALISED COMPUTER

- Highly dependent on system. If the system fails, all nodes fail.
- No graceful degradation of system.
- Less possibility of data backup.
- Difficult to maintain server.

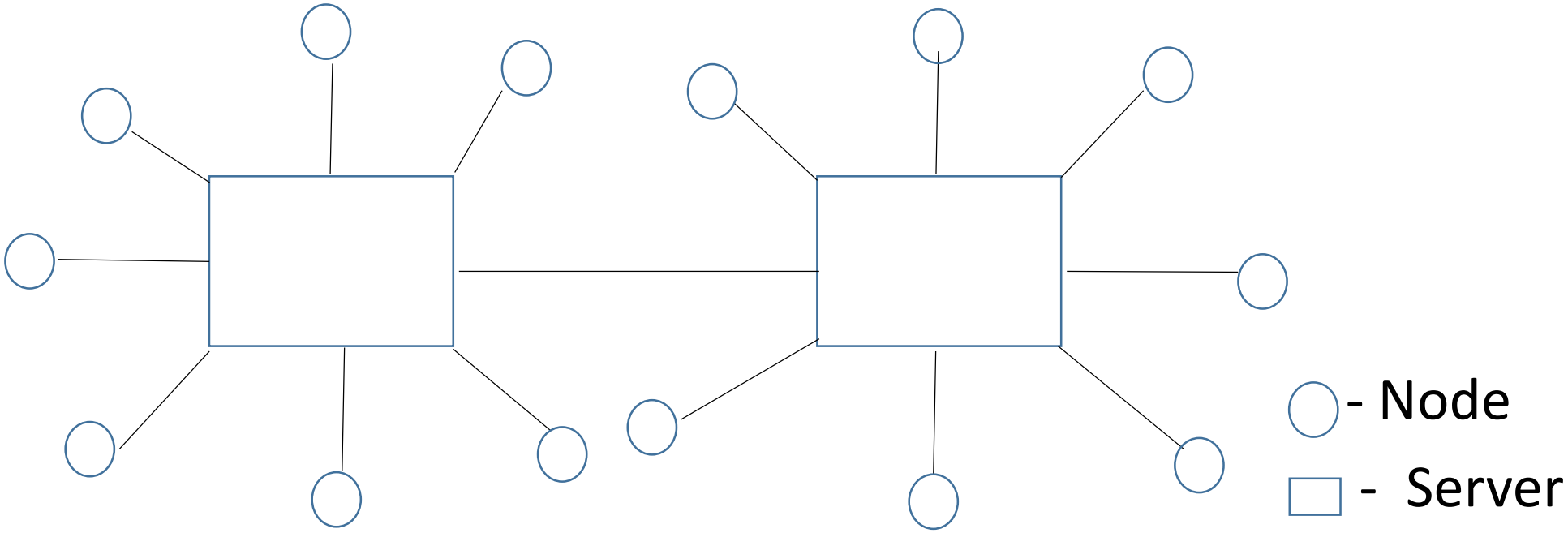
DECENTRALISED COMPUTING

- A decentralised computing architecture distributes workloads among several machines instead of relying on a single central server.
- A decentralised computing is an interconnected information system in which no single entity is the sole authority.
- A decentralised computing generally has multiple authoritative nodes, each of which serves a subset of the total end users.
- a decentralised computing is collection of autonomous computers which communicate with one another to perform a common service.
- In decentralised computing, these are different CPU connected on the network and each processor can do its job independent of each other.

CHARACTERISTICS OF DECENTRALISED COMPUTING

- multiple Central Units – there is more than one central unit which can listen for connections from other nodes,.
- Department failure of components – one central node failure causes only partial system failure and not complete system.
- Lack of a global clock – each node is independent, hence different clocks that they run and follow.

ARCHITECTURE OF DECENTRALISED SYSTEM



Decentralised System.

ADVANTAGE OF DECENTRALISED SYSTEM

- Minimal problem of performance bottlenecks occurring – it allows balancing the network
- High availability
- More autonomy and control over resources

DISAVANTAGE OF DECENTRALISED SYSTEM

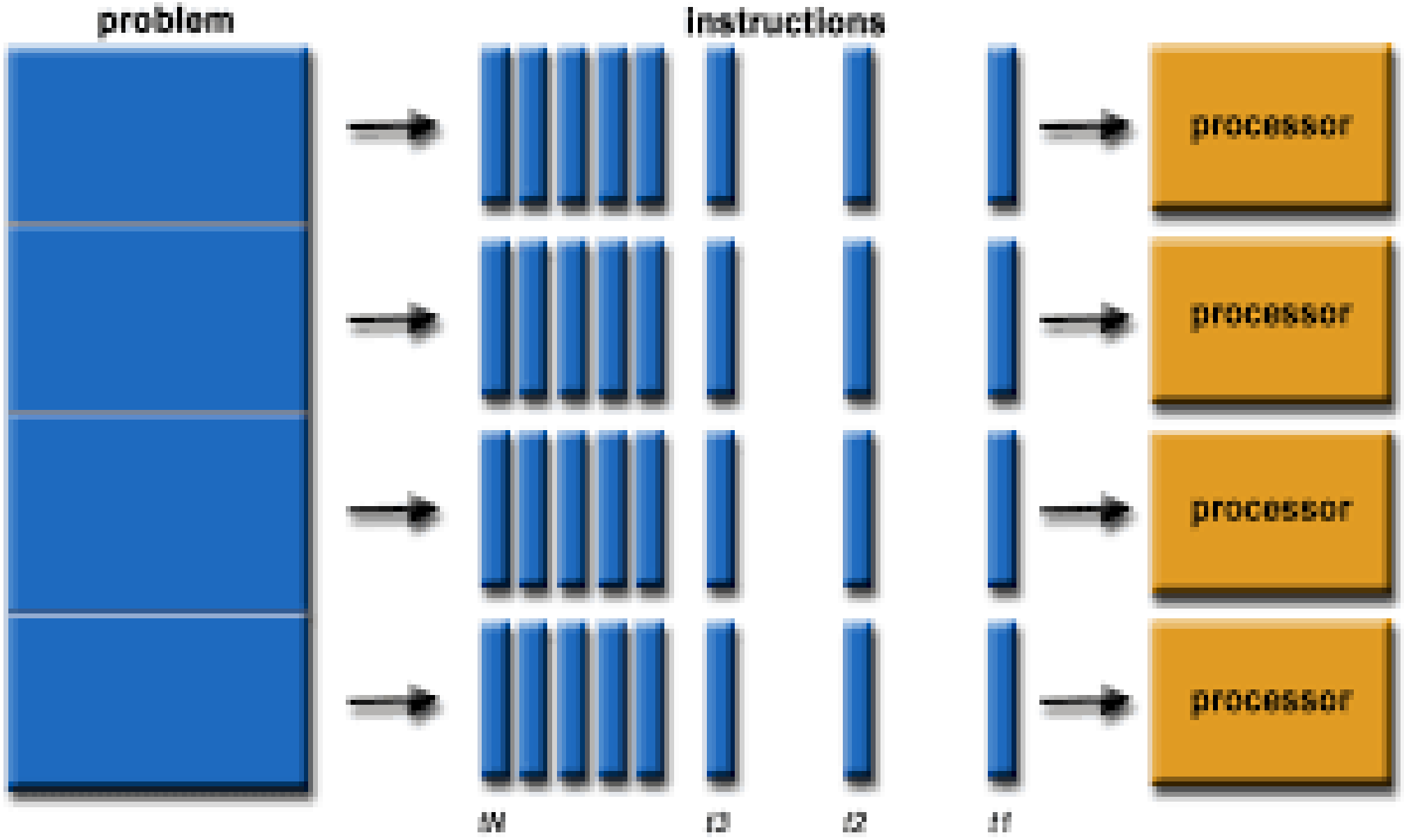
- May lead to problem of coordination of the enterprise level.
- Not suitable for small system.
- Difficult to know which node failed.
- Difficult to know which node responded.
- No regulatory oversight.

WHAT IS PARALLEL COMPUTING

- Parallel computing is a technique of computing where multiple tasks are process simultaneously on multiple processors.
- In parallel computing, a given tasks uses divide – and – conquer technique and each one of them are processed on different CPUs.
- Parallel computing are used for complex calculation.

WHY PARALLEL COMPUTING

- Many applications today require more computing power than a traditional sequential computer can offer.
- Parallel computing provides a cost – effective solution to solve complex problem.
- Parallel computing allow an increase in the number of CPUs in a computer and also adding an efficient communication between the CPUs.
- It allows work load to be shared between processors and hence a higher computing power.

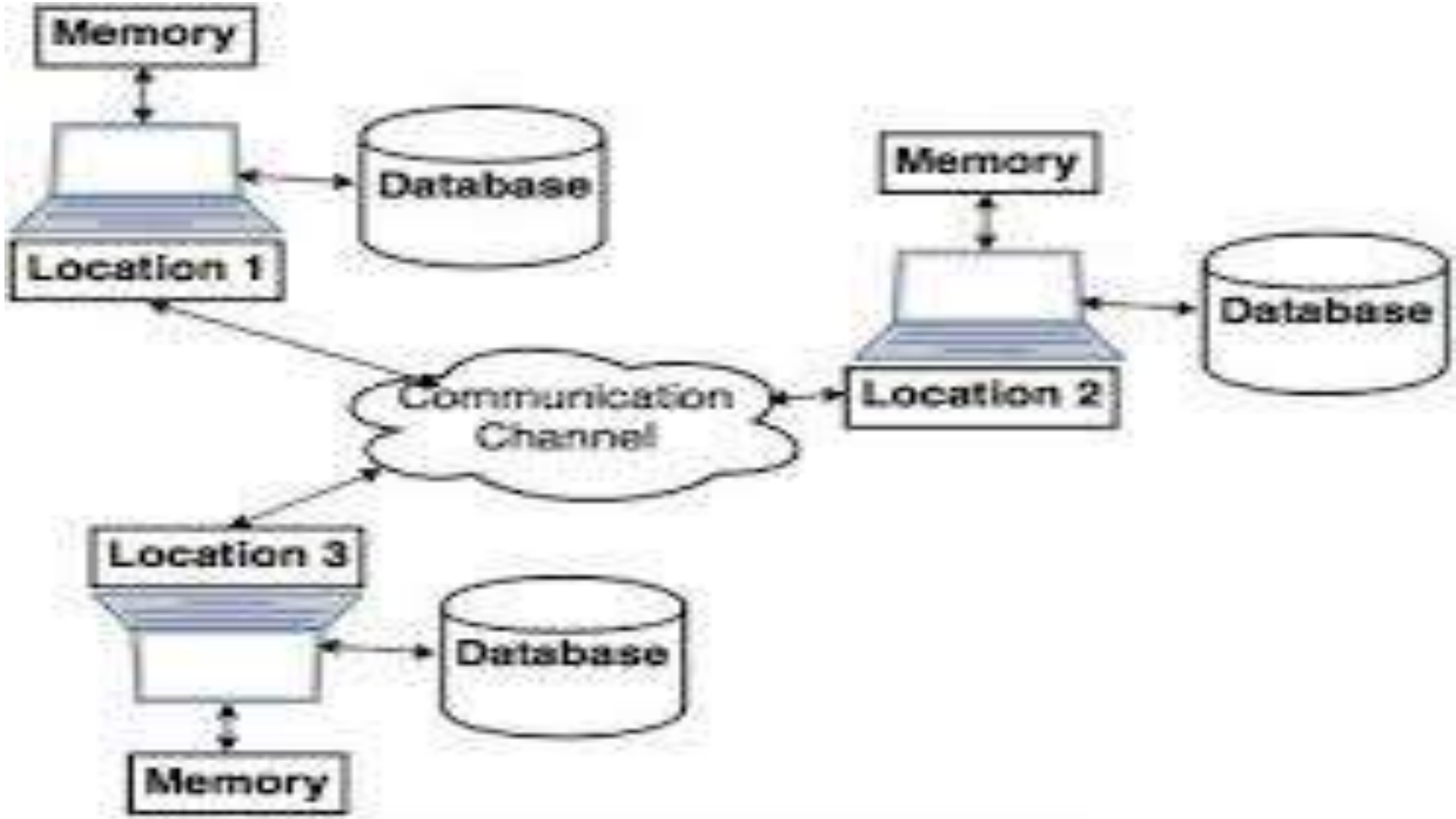

problem
Instructions
processor
processor
processor
processor

DISTRIBUTED COMPUTING

- In a distributed computing, every node on the network communicates with every other nodes and are working together as a single system.
- In distributed system every node make its own decision.
- Distributing computing refers to multiple computer systems working on a single problem.
- In distributing computing, a single problem is divided into many parts, and each part is solved by different computers.
- The aim of distributing computing is maximize performance by connecting users and IT resources in a cost effective, transparent and reliable manner by utilizing computer resources as if it is a single system.

DISTRIBUTED COMPUTING Cont……

- Distributing computing is a computing techniques where a single task can be divided into multiple tasks and distributed to many computer.
- These computers can communicate with other computers through the network.
- Each computer in a distributed system is known as a node. A set of nodes in a cluster.
- Facebook and google uses distributed computing



Distributted Dtatabase system

CHARACTERISTICES OF DISTRIBUTING COMPUTIN G

- Concurrency of components – node apply consensus protocols to agree on same values/transactions/command/logs.
- Lack of a global clock: all nodes maintain their own clock Independently without having a significant effect on the entire system.

Parallel vs Distributed Computing

Parallel Computing

- Parallel Computing is a computation type in which multiple processors execute multiple tasks simultaneously
- Parallel Computing occurs on one computer.
- In Parallel Computing, multiple processors perform processing.
- All processors share a single master clock for synchronization.
- In Parallel Computing , computers can have shared memory or distributed memory,
- Parallel Computing is used to increase performance and for scientific computation

Distributing Computing

- Distributing Computing is a computation type in which networked computers communicate and coordinate the work through message passing to achieve a common goal.
- Distributing Computing occurs between multiple computers
- In Distributing Computing , computer rely on message passing.
- There is no global clock in distributing computing , it uses synchronization algorithms.
- In distributing computing , each computer has their own memory.
- Distributing Computing is used to share resources and to increase scalability

ADVANTAGE OF DISTRIBUTED COMPUTING

- Low latency than centralised or decentralised system.
- It has redundancy and resiliency.
- It has high spread and content distribution.
- A distributed computing is scalable and can be designed parallelism.

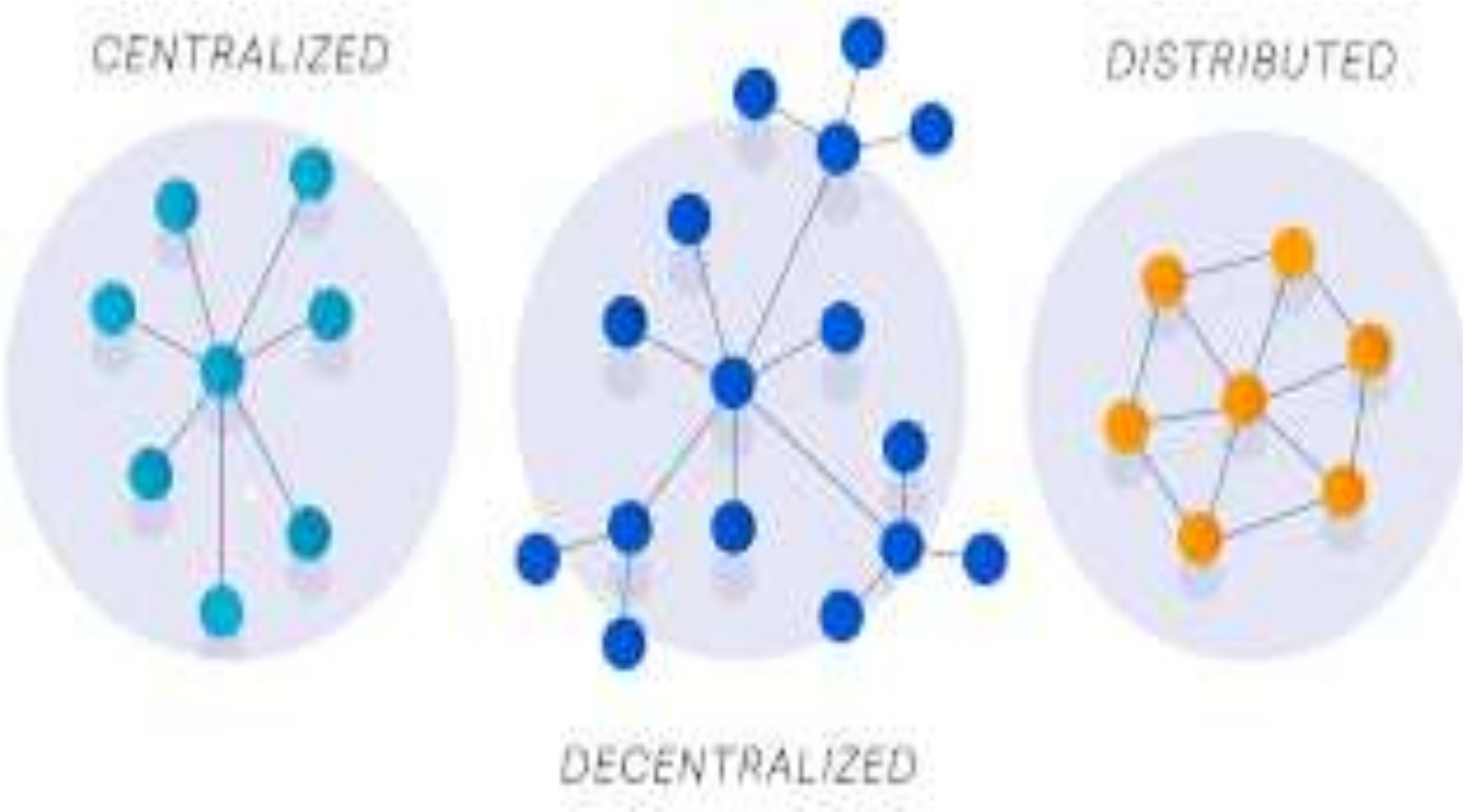
DISADVANTAGE OF DISTRIBUTED COMPUTING

It is difficult to design.

It can be difficult to spot bugs that causes errors

Security and privacy can become an issue with distributed systems.

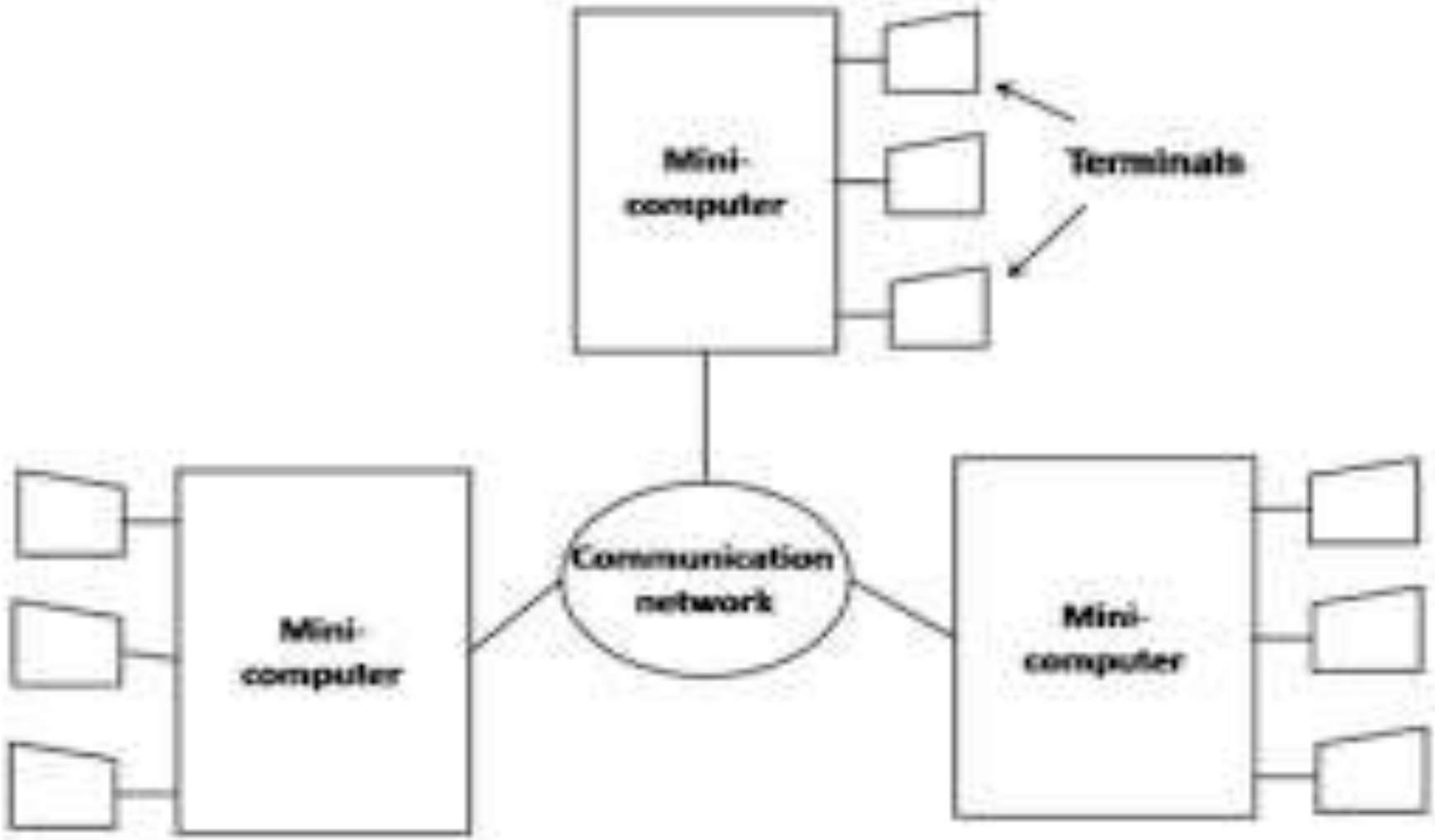
It can be overkill for some tasks, using more physical resources and engineering time than is necessary.


CENTRALIZED
DECENTRALIZED
DISTRIBUTED

Distributed Computing Models

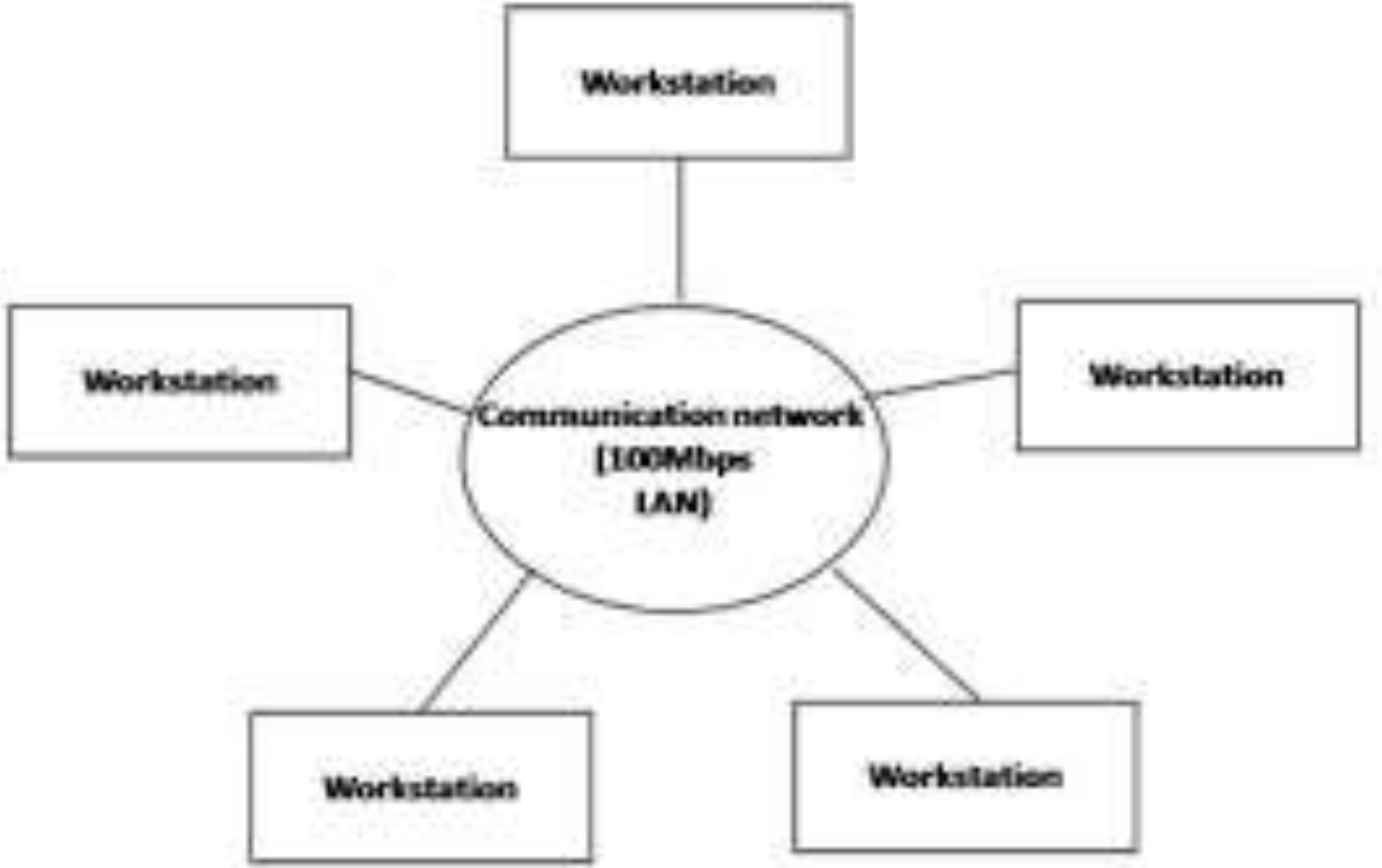
1. **Minicomputer Model**

- The Minicomputer model is a simple extension of the centralized time – sharing system.
- A distributed computing system based on this model consist of few minicomputers interconnected by a communication network where each minicomputer usually has multiple users simultaneously logged onto it.
- Several interactive terminals are connected to each minicomputer. Each user logged onto a specific minicomputer, has remote access to other minicomputers.
- The network allow the user to access remote resources that are available on some machines other than the one on to which the user is currently logged. The minicomputer model may be used when resource sharing with remote users is desired.
- The early ARPA net is an example of a distributed computing system based on the minicomputer model.


Mini-
computer
Terminals
Mini-
computer
Communication
network
Mini-
computer

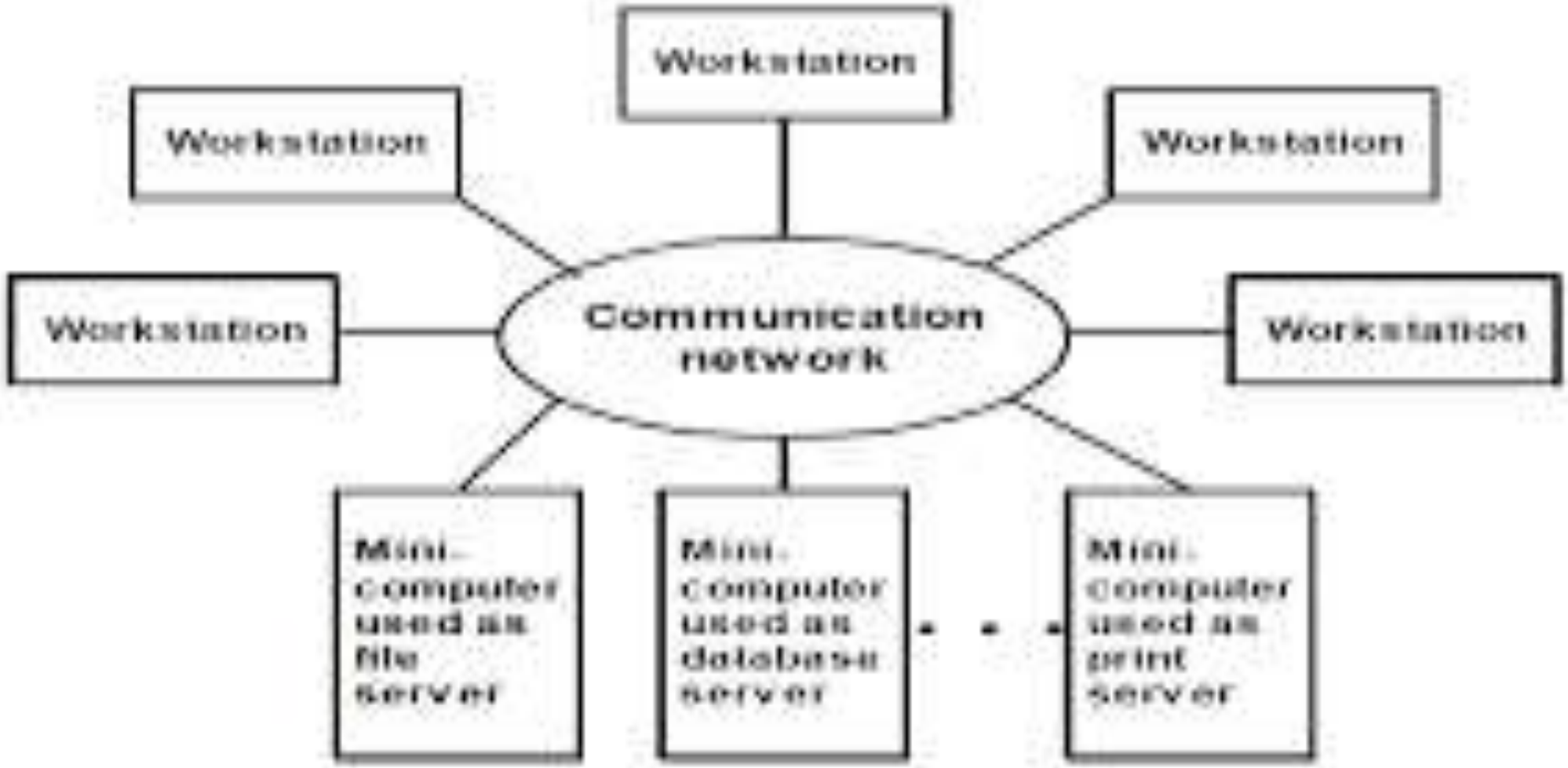
2. Workstation Model

- A distributed computing system based on the workstation model consists of several workstation interconnected by a communication network.
- An organization may have several workstations located throughout an organisation with infrastructure were each workstation is equipped with its own disk and serves as a single-user computer.
- In such an environment, at any one time a significant proportion of the workstation are idle which result in the waste of large amount of CPU time.
- Therefore the idea of the workstation model is to interconnect all these workstations by a high-speed LAN so that idle workstation may be used to process jobs of users who are logged onto other workstations and do not have sufficient processing power at their own work stations to get their jobs processed efficiently.


Workstation
Workstation
Communication network
(100Mbps
LAN)
Workstation
Workstation
Workstation

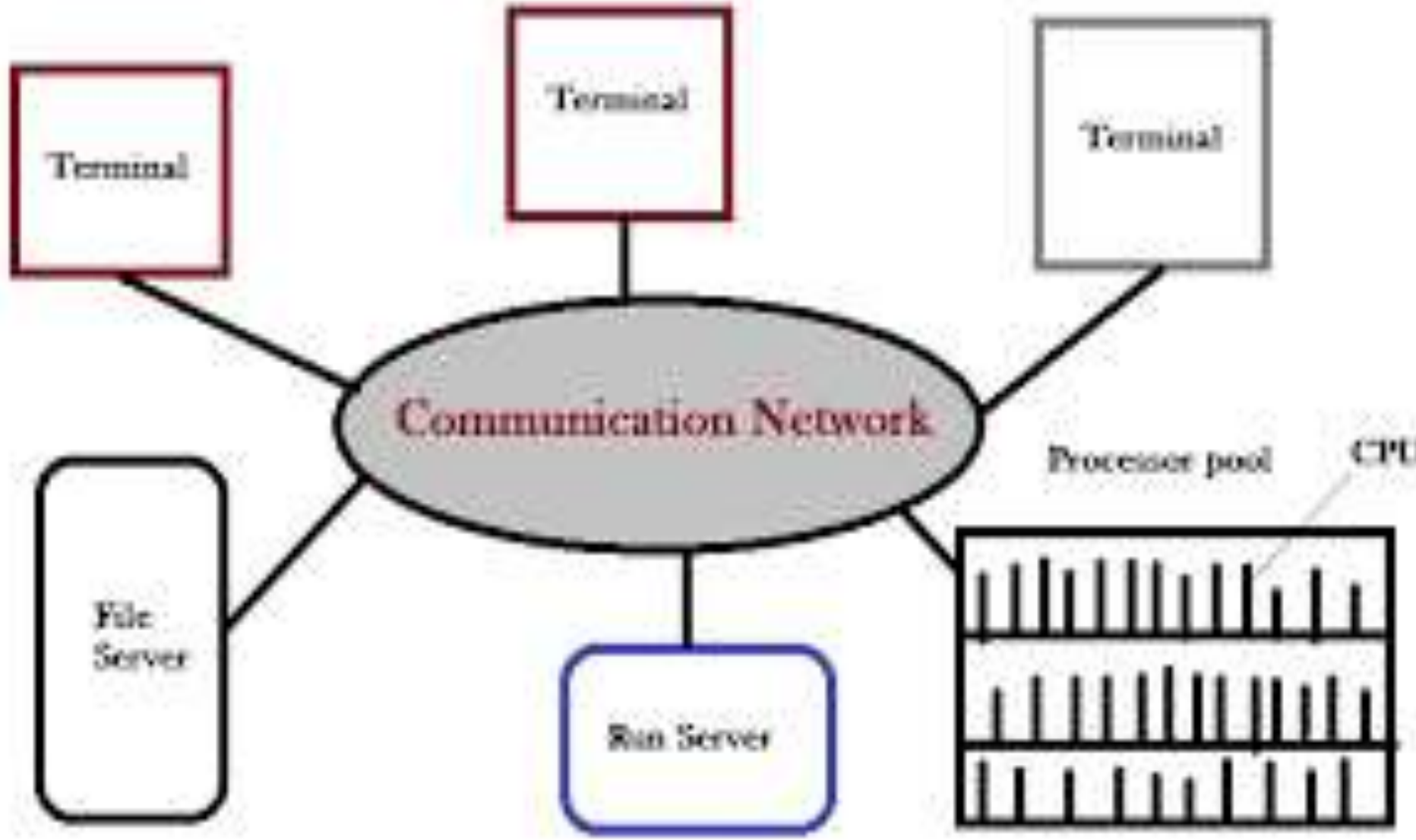
3. Workstation-Server Model

- The workstation model is a network of personal workstations having its own disk & local file system.
- A workstation with its own local disk is usually called a diskful workstation and workstation without a local disk is called a diskless workstation. diskless workstation has become more popular in network environments than diskful workstation, making the workstation-server model more popular than the workstation model for building distributed computing systems.
- A distributed computing system based on the Workstation-server model consist of a few minicomputers and several workstations interconnected by a communication network.
- In this model, a user logs onto a workstation called his or her home workstation. Normal computation activities required by the user's processes are performed at the user's home workstation but request for services provided by special servers are sent to a server providing that type of service that performs the user's requested activity and returns the result of request processing to the user's workstation.
- Therefore, in this model, the user's process need not migrated to the sever machines for getting the work done
- Example: The V-System.


Workstation
Workstation
Workstation
Workstation
Communication network
Workstation
Mini-computer used as file server
Mini-computer used as database server
Mini-computer used as print server

4. Processor-Pool Model:

- The processor-pool model is based on the observation that must of the time a user does not need any computing Power but once in a while the users may need a very large amount of computing power for a short time.
- Therefore, unlike the workstation-server model, in which a processor is allocated to each user, in processor-pool model the processor are pooled together to be shared by the users as needed.
- The pool of a processor consist of a large number of microcomputers attached to the network.
- Each processor in the pool has its own memory to load and run a system program or an application program of the distributed computing system.
- In this model no home machine is present and the user does not log onto any machine.
- This model has better utilization of processing power and greater flexibility.
- Example: Amoeba and the Cambridge Distributed Computing System.


Terminal
Terminal
Terminal
Communication Network
File Server
Run Server
Processor pool
CPU

5. Hybrid Model

- The workstation-server model has a large number of computer users only performing simple interactive task and executing small programs.
- In a working environment that has group of users who often perform jobs needing massive computation, the processor pool model is more attractive and suitable.
- To combine advantages of workstation-server and processor-pool model, a hybrid model can be used to build a distributed system.
- The processor in the pool can be allocated dynamically for computations that are too large or require several computers for execution.
- The hybrid model gives guaranteed response to interactive jobs allowing them to be more processed in local workstations of the users

WHAT IS OPERATING SYSTEM

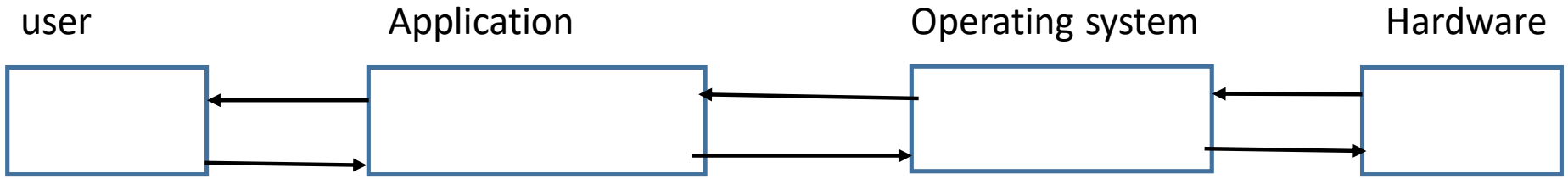
- Operating system is a system software that manages computer hardware, software resources, and provides common services for computer programs.

  examples are windows, MacOS and Linux etc.

  - An operating system is a program that acts as an interface between the software and the computer hardware.

- It is an integrated set of specialised programs used to manage overall resources and operation of the computer.

- It is a specialised software that control and monitors the execution of all other programs that reside in the computer, including application programs and other systems software.



OBJECTIVES OF OPERATING SYSTEM

- To hide the detail of the hardware resources from the users
- To provide users a convenient interface to use the computer system
- To manage the resources of a computer system.
- To keep track of who is using which resource, granting resource requests and mediating conflict request from different programs and users,
- To provide efficient and fair sharing of resources among users and programs.

FUNCTIONS OF OPERATING SYSTEM

- **Memory Management –** keep track of the primary memory, i.e Registering used and empty memory location and allocate the memory when a process or program request it.
- **Processor Management -** Allocates the processor to a process and deallocates the processor when it is no longer required.
- **Device Management -** Keep track of all the devices. This is also called I/O controller. It decides which process gets the device, when, and for how much time.
- **File Management -** Allocates and de-allocates the resources and decides who gets the resources.
- **Security –** Prevent unauthorised access to programs and data by means of passwords and other similar techniques.
- **Job Accounting –** Keeps truck of time and resources used by various jobs and/or users.
- **Interaction with the Operators –** interaction may take place via the console of the computer in the form of instructions.
- **Error – Detecting Aids –** Production of traces, error massages and other debugging and error detecting methods.

DISTRIBUTED OPERATING SYSTEMS

- A distributed operating system is an operating system that runs on several machines whose purpose is to provide a useful set of services, generally to make the collection of machines behave more like a single machine.
- The machine controlled by a distributed operating system are connected by a relatively high quality network, such as a high speed local area network.
- Distributed operating system typically run cooperatively on all machines whose resources they control. It is an extension of network operating system that support higher level of communication and integration of the machines on the network.
- A networking operating system is an operating system designed for the sole purpose of supporting workstations, database, sharing, application sharing and file and printer access sharing among multiple computers in a network.

CHALLENGES IN BUILDING DISTRIBUTED OPERATING SYSTEMS

- Designing a distributed operating system is more difficult than designed a centralised operating system.
- It is assumed that the operating system has access to complete and accurate information about the environment in which it is functioning. However, a distributed operating system must be designed with the assumption that complete information about the system environment will never be available.
- In a distributed system, the resources are physically separated, there is no common clock among the multiple processors, delivery of messages is delayed, messages could even be lost.
- Due to the above reasons, a distributed operating system does not have up-to-date consistent knowledge about the state of the various components of the underlying distributed system.
- Despite these complexities and difficulties, a distributed operating system must be designed to provide all the advantages of distributed system to its user. That is the users should be able to virtue centralised system that is flexible, efficient, secure and easy to use.

TRANSPARENCY

- Transparency is an important characteristic of distributed systems, as it makes their operation in the eyes of the user to be more friendly, easy or simple transparent. Users should be unaware of the complexities and the location of the services, and the transfer from a local to a remote machine should remain transparent to them.
- Transparency can be defined as the concealment from the user and the application programmer of the separation of components such that it is perceived as a single programmers rather than a collection of autonomous systems which are cooperating.
- There are eight types of transparencies in a distributed system, Access, Location migration, Relocation, Replication, Concurrency, Failure and persistence Transparency.

ISSUES OF TRANPARENCY IN DESIGNING OF A DISTRIBUTED SYSTEM

- Access transparency enables users to be unaware of the distribution of files. The files could be present on a totally different set of servers which are physically distant apart and a single set of operations should be provided to access these remote files.
- Location transparency enables sources to be accessed without knowledge their physical or remote location.
- Failure transparency enables the concealment of faults, allowing users and application programs to complete their task despite the failure of hardware or software components.
- Concurrency transparency enables several processes to operate concurrently using shared resources without interference between them.

ISSUES OF TRANPARENCY IN DESIGNING OF A DISTRIBUTED SYSTEM

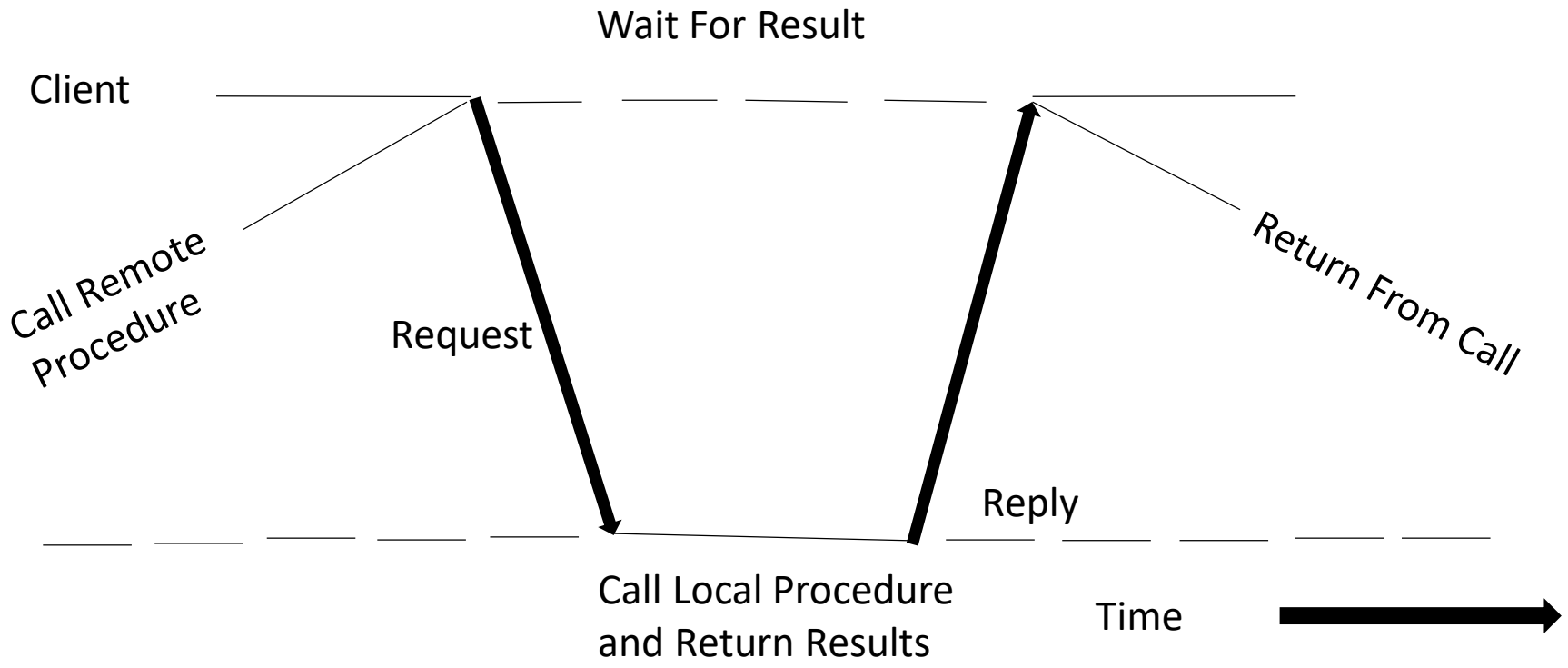
- Scaling transparency enables a system to grow without affecting application algorithm. Note graceful growth and evolution is an important requirement for most enterprises.
- Performance transparency enables systems to be reconfigured to improve the performance if the need arises.
- Migration transparency enables the users to be unaware of the movement of information of processes within a system without affecting the operations of the users and the applications hat are running.

REMOTE PROCEDURE CALL (RPC)

- A remote procedure call is an inter process communication technique that is used for client-server based application. It is also known as a subroutine call or function call.
- A client has a request message that the RPC translates and sends to the server. This request may be a procedure or a function call to a remote server.
- A server receives the request, process the request, and sends the required response back to the client.
- The client is blocked while the server is processing the call and only resumes execution after the server is finished.

REMOTE PROCEDURE CALL (RPC)

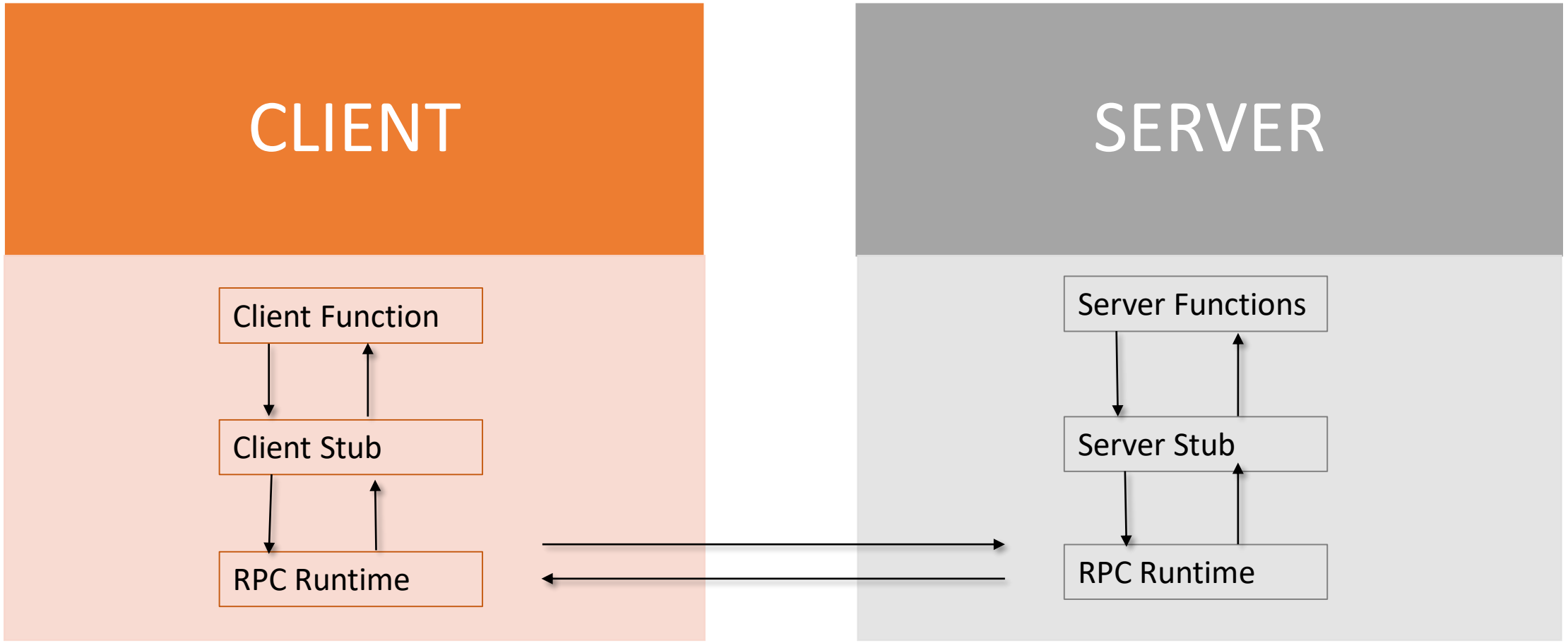
RPC between a client and server program.



Sequence of Events In A RPC

- The client stub is called by the client
- The client stub makes a system call to send the message to the server and puts the parameters in the message.
- The message is sent from the client to the server by the clients operating system.
- The message is passed to the server stub by the servers operating system.
- The parameters are removed from the message by the server stub.
- The server procedure is called by the server stub.

EVENTS OF RPC



ADVANTAGES OF RPC

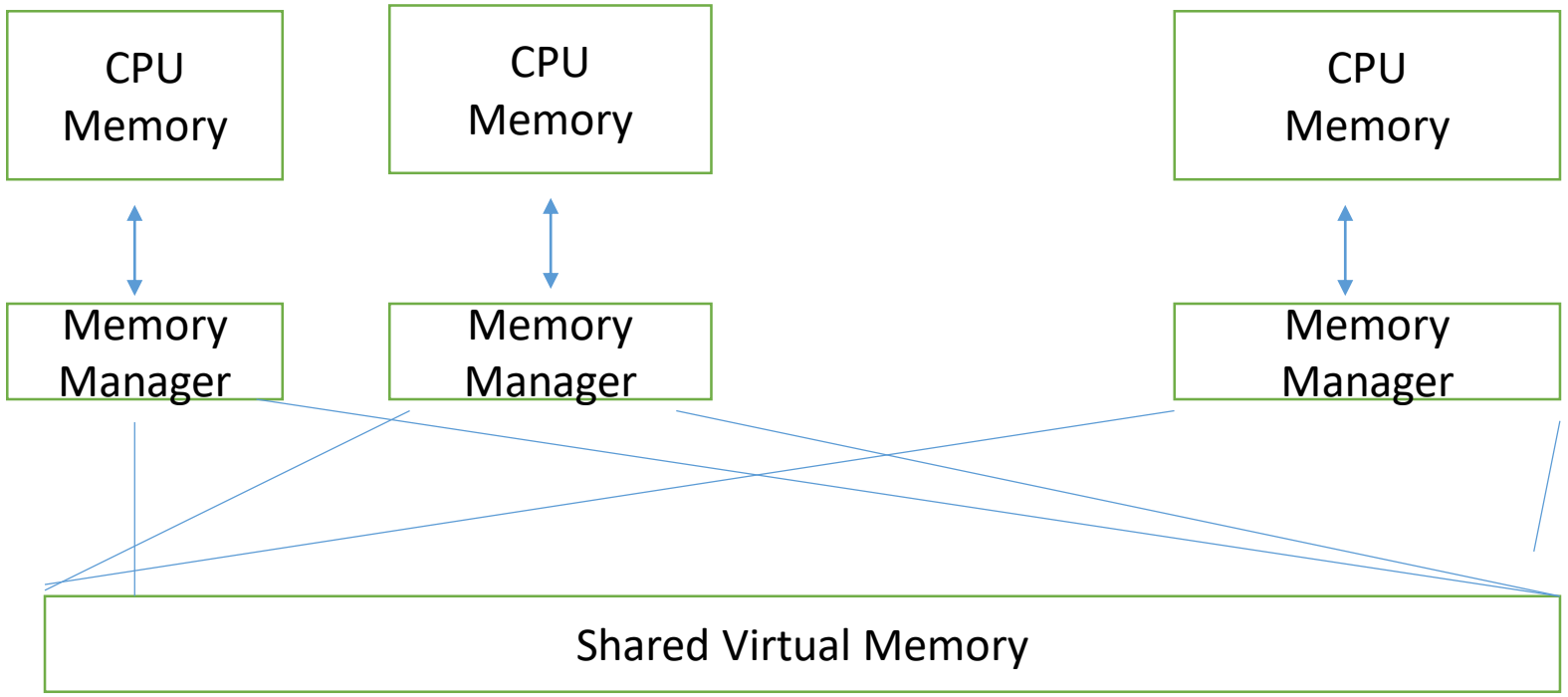
- RPC supports process oriented and thread oriented models.
- The internal message passing mechanism of RPC is hidden from the user.
- The effort to rewrite and redevelop the code is minimum in RPC.
- Many of the protocol layers are omitted by RPC to improve performance.

DISADVANTAGES OF RPC

- It is not standardised, it can be interpreted in many ways.
- There is no flexibility in RPC for hardware architecture.
- There is an increase in costs because of RPC.

Distributed shared memory

- DSM is a form of memory architecture where physically separated memories can be addressed as one logically shared address space.



Advantages/Disadvantages of DSM

- Advantages
  - Single address space; simplifies passing-by-reference
  - No memory access bottleneck as no single bus
  - Large virtual memory space
  - Hide data movement and provide a simpler abstraction for sharing data
  - Cheaper to build than multiprocessor systems
- Disadvantages
  - Programmers need to understand consistency models
  - By yielding control to DSM manager software, programmers cannot use their own msg-passing solutions.

Synchronization

- Generally, synchronization is the coordination of hardware devices, such that the data they contain or provide is made to be identical.

MOBILE COMPUTING

- Is a term used to describe technologies that enable people to access network services anyplace, anytime, and anywhere.
- It can be defined as a computing environment over physical mobility. The user of mobile computing environment will be able to access data, information or other logical objects from any device in any network while on the move.
- The computing environment is mobile and moves along with the user, eg Global system for mobile communication (GSM).
- The communication devices can be on either of the characteristics

- Fixed and wired
- Mobile and wired
- Fixed and wireless
- Mobile and wirelesss

Mobile computing

- Mobile computing refers to the use of small and portable computing devices in wireless enabled networks that perform computation tasks.
- Mobile computing describes technologies that :
  - enable people to access network services anyplace, and anytime, with portable and wireless computing and communication enabled devices
- Mobile Computing allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. It consists of the hardware devices, the software and communication parts

Design issues in mobile computing

Assignment

- Operating system
- File systems
- Database systems
- Programming Languages
- Communication architecture and protocols
- Hardware and architecture
- Real-Time, multimedia, QoS
- Security
- Application requirements and design

APPLICATION OF MOBILE COMPUTING

- Transportation: - Buses, trucks, trains, aircrafts, and ships transmit information (logistic, maintenance , weather reports, news, road conditions, current position of the vehicles through global positioning system (GPS) to their home station. This help in effective management of transportation system which saves time and money.
- Emergencies:- An ambulance with a high quality wireless connection to a hospital can transmit vital information about injured person to the hospital from the scene of the accident. All the needed treatment for the accident person can be prepared and specialist can be consulted for a early diagnosis.

  Also, wireless networks are the only means of communication in the case

  of natural disasters such as hurricanes or earthquakes.
- Business:- Field officers can communicate within their head offices, send and receive information for decision making. Also mobile computing help offices to monitor their field officers etc.
- Financial Services: At point of Sales(POS) terminals in shop and supermarkets, when customer use credit cards for transactions, the mobile network facilitate communication between the POS terminal and the bank central computer system for verification and effective transaction.
- Data Capturing:- Mostly mobile devices are used for data collections in fields, such as weather, despatch delivery information, geo-mining etc.

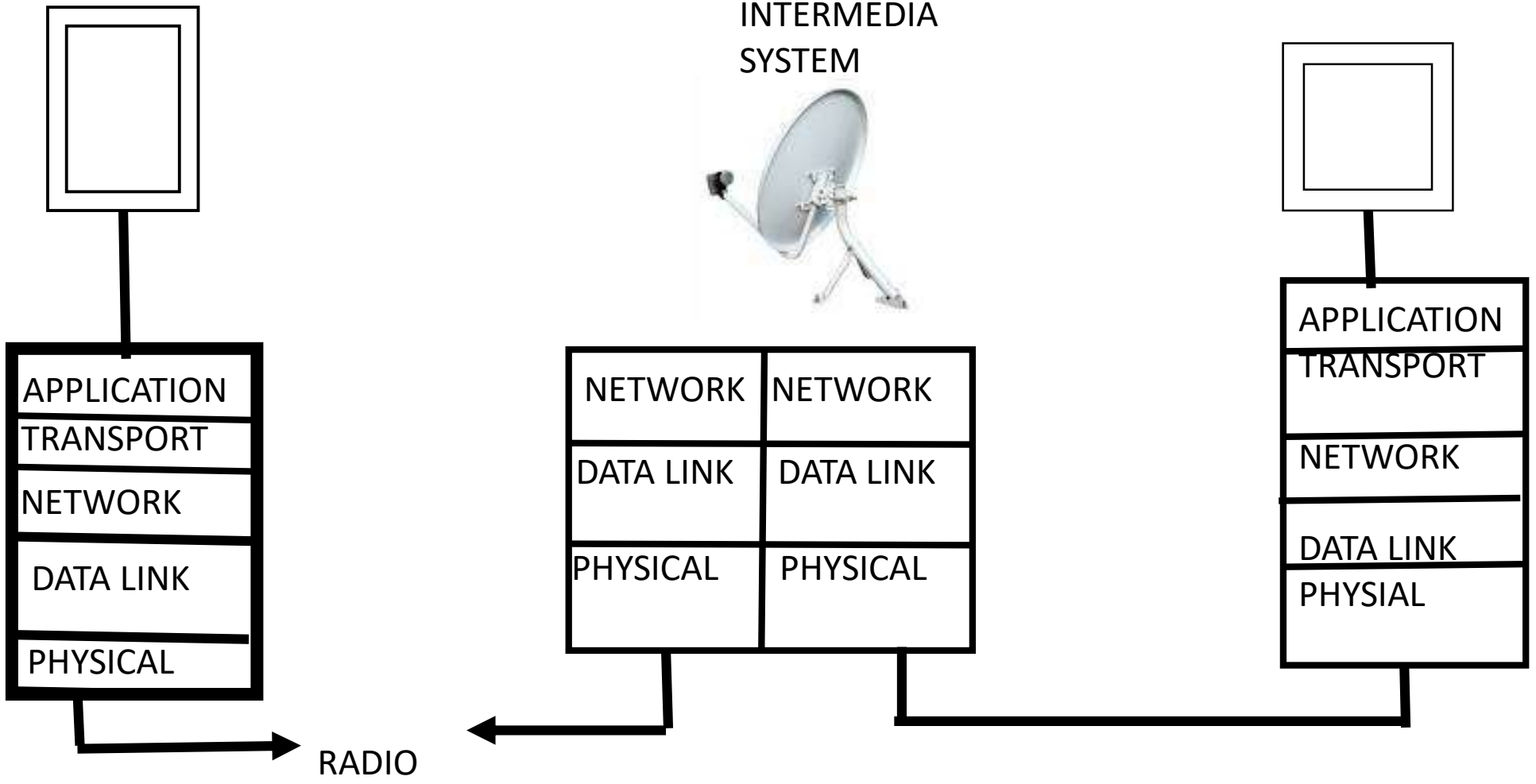
LIMITATION OF MOBILE COMPUTING

- Resource constraints: Battery
- Interferences and loss rates for transmitted data
- Bandwidth: need for more bandwidth as a result of high overhead compare to shield wire.
- Dynamic changes in communication environment.
- Interoperability issues with regard to protocol standard.
- Security constraint: not only portable devices can easily be stolen, but radio interface is also prove to be damage of eaves dropping. Wireless access must always include encryption, authentication, etc.

MOBILE COMPUTING SIMPLIFIED REFERENCE MODEL

- In a mobile computing system, the end-system need a protocol stack as in the OSI reference model, comprising the application layer, transport layer, transport layer, network layer data layer and physical layer.
- The intermediate systems, such as the interworking unit do not necessarily need all of the layers.
- Physical layer: for wireless communication, the physical layer is responsible for frequency selection, generation of the carrier frequency, signal detection (although heavy interference may disturb the signal) modulation of data into a carrier frequency and encryption.
- Datalink layer: The main task of this layer include accessing the medium multiplexing of different data streams, correction of transmission errors and synchronization. It is also responsible for point-point connection between two devices or a point-to-multipoint connection between one sender and several receivers.
- Network Layer: This layer is responsible for routing packets through a network or establishing a connection between two entities (devices) over many other intermediate system. In wireless network, this layer is specifically responding for addressing, routing, devices location, and handover between different networks.
- Transport Layer:. This layer is responsible for end-to-end connection.
- Application layer: This layer is responsible for service location, support for multimedia applications, adaptive application that can handle the large variation in transmission and wireless access to the world-wide web.

- WIRELESS DEVICE



A SIMPLIFIED REFERENCE MODEL

Wireless Transmission

- Communication is a two-way transmission and reception of data streams i.e. two or more Communicating devices where the transmitter sends the signals and received by receivers.
- Mobile communication entails transmission of data to and from communicating devices, whereby at least one of the device is mobile which is remotely located.
- Wireless Communication uses Unguided media for transmission i.e. it does not require a physical conduit for data to be transmitted. In this form of transmission electrical signals are transmitted by converting them into electromagnetic radiation. The radiation transmitted via antennae that radiates electromagnetic signals.
- Wireless systems operate via transmission through space, other than through physical connections

Frequencies for wireless transmission

- Frequency is the rate at which current changes direction per second.
- Spectrum refers to the invisible radio frequencies that wireless signals travel over.
- We have various signal frequency bands within the electromagnetic spectrum, whereby a frequency of a signal is measured by;
  - $f=c/\lambda$
  - Frequency, f is measured in Hz
  - wavelength, λ in meter
  - the velocity of signal propagation,

  Assisgment
- Read about ranges of Frequencies and Wavelengths allocations and spectrum management in Nigeria.

Computation of frequency from wavelength

- Example: A certain sound wave traveling in the air has a wavelength of 322 nm when the velocity of sound is 320 m/s. What is the frequency of this sound wave?
- Answer
- $f=c/\lambda$
- λ= 322**nm** convert to **m** > 322nm X 1m/10^9nm > 0.000000322m
- C= 320m/s
- F= 320m/s / 0.000000322 = 993788819.88 Hz
- F= 9.94 *10^8Hz.

Computation of frequency in a vacuum

- $f=c/\lambda$
- Note the speed of electromagnetic wave in a vacuum is constant given as 3.00 * 10^8 m/s.
- Therefore, if λ = 5.73 * 10^-7 m
- F = 3.00*10^8 m/s / 5.73 *10^-7m
- F = 5.24 * 10^14 Hz

Factors that determine the quality of communication

- Line-of-sight propagation. This is the ideal transmission of signals, without refraction, diffraction, or scattering in between the transmitter and the receiver, but losses do occur.
- Attenuation. When obstacles are greater in size than signal wavelength, the strength of the signal decreases e.g. A GSM 900 MHz ($\lambda >= 33$ cm) signal, will face attenuation in objects of size > 1 m (>> λ~33cm)
- Scattering. When obstacle size is equal to or less than wavelength. This decreases signal strength greatly e.g. A GSM signal, about 33 cm in wavelength, scattered by an object of 30 cm or less makes only a small part of the scattered signal to reach the receive
- Diffraction. A signal bends from the edges of an obstacle of size equal to or less than the wavelength e.g. A GSM signal of wavelength 33 cm will diffract from an object of 33 cm or less causing it to or not to reach its destination

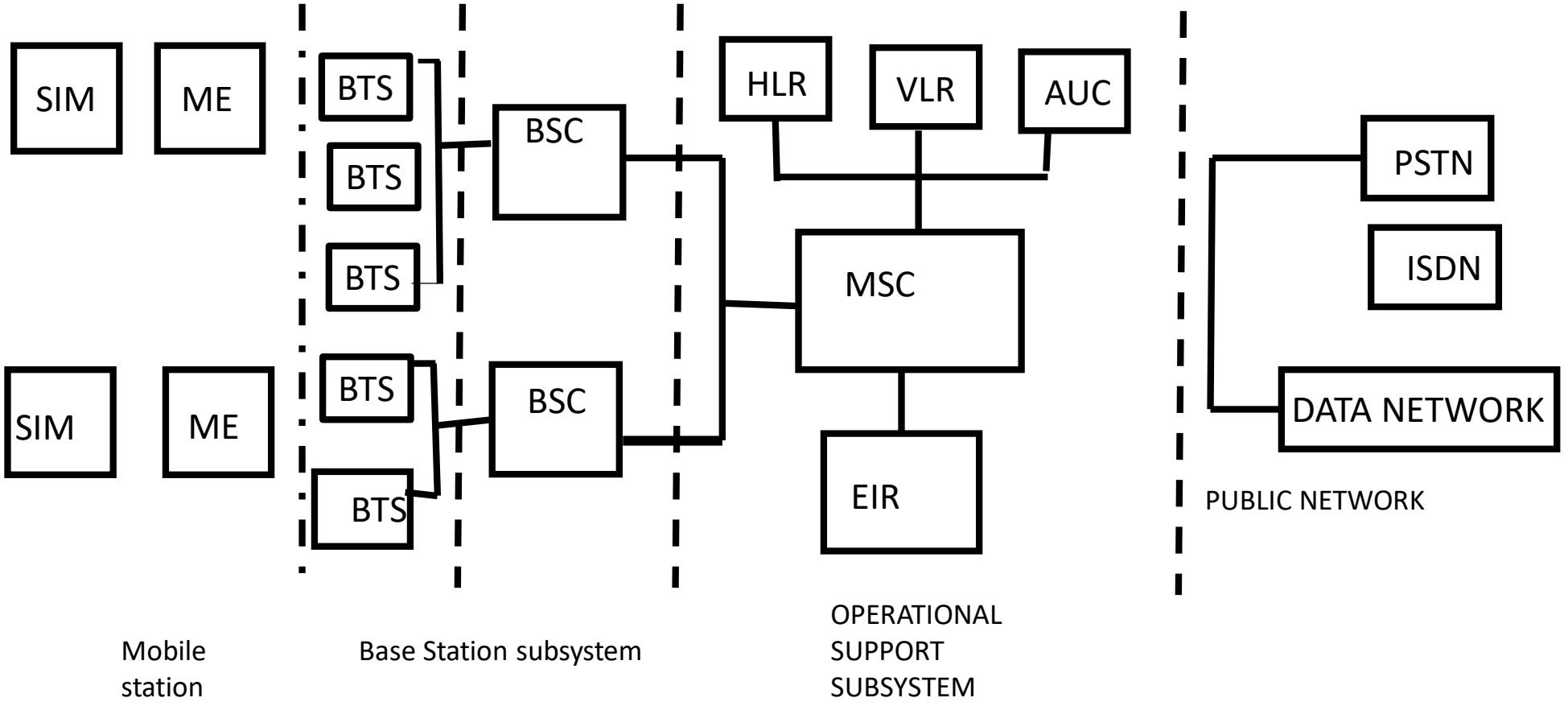
- cont.-

- Reflection. A signal may also be reflected from the surface of an obstacle, or the earth's surface e.g. A GSM 900 MHz (λ= 33 cm) signal the transmitter signal reflects from an object of size 10 m and above (much greater than λ)

GSM SERVICES

- GSM is the most successful digital mobile telecommunication system in the world today.
- It is used by over 7.26 billion people in more than 190 countries worldwide.
- GSM permits the integrates of different voice, video and data services and the interworking with existing network.
- A GSM system consist of three subsystems, the radio sub-system (RSS), the network and switching sub-system(NSS) and the operation subsystem (OSS).

GSM ARCHITECHURE



- (1) Mobile Station consists of two entities: Mobile Equipment and Subscriber Identity Module.

- A mobile station communicates across the air interface with a base transceiver in the same cell in which the mobile subscriber unit is located.

- The ME refers to the physical device, which comprise of transceiver, digital signal processor, and the antenna.

- The SIM is unique to the ME system and has a memory of 32kb.

Mobile Equipment (ME)

- It is a portable hand held device
- It is uniquely identified by an International Mobile Equipment Identity (IMEI) Number.
- It is used for voice, video and data transmission, it also monitors power and signal quality of surrounding cells for optimum handover.
- 160 characters long sms can be sent using mobile equipment

b - Subscriber Identity Module (SIM)

- It is a smart card that contains the International Mobile n Subscriber Identity (IMSI) number.
- It allows user to send and receive voice, data and other subscriber services.
- It is usually protected by password or pin.
- It contains encoded network identification details, it has key information to activate the phone.
- it can be moved from one mobile to another

- (2) Based station subsystem (BSS):
- It is also known as Radio station subsystem, it provides and manages radio transmission paths between the Mobile Station and the Mobile Switching Centre (MSC).
- BSS also manages Interface between the Mobile station and all other subsystems of GSM. It consist of Base Transceiver Station(BTS) and Base Station Controller (BSC).

a **Base Transceiver Station (BTS)**

- Each BTS defines a single cell. A cell can have a radius of between 100m to 35km.
- It encodes, encrypts, multiplexes, modulate and feeds the R/F signal to the antenna.
- It consists of transceivers Units
- It communicates with mobile stations via radio air Interface and also communicates with BSC via A-bis Interface.

b - **Based Station Controller (BSC)**

It manages radio resources for BTS. A BSC control one or more BTS

- It assigns frequency and time slots for all mobile station in its area.
- It handle call set-up, transcoding and adaption functionality handover for each MS radio and power C control.
- It communicate with MSC via A Interface and also with BTS.

- (3) Network switching subsystem (NSS). It manages the switching functions of the system and allows MSC to communicate with other Networks such as PSTN and ISDN,

a - Mobile Switching Centre. (MSC)

- It is the heart of the network. It manages communication between GSM and other Network
- It manages call set-up function, routing and basic switching.
- It performs mobility management including registration, location updating and inter BSS and inter MSC call handoff.
- It provides billing information.
- MSC does gateway function while its customers roam to other network by using HLR/VLR.

b - Home Location Registration (HLR). It is a permanent database about mobile subscribers in a large services area.

- It database contains IMSI, IMSISDN, prepaid/post-paid, roaming restriction, supplementary services.

c - Visitor Location Registers (VLR)

- It is a temporary database which updates whenever an MS enter inside the coverage area of an MSC.
- It controls mobile roaming in its area.
- It reduces number of queries to HLR.

D - Authentication Centre

- It provides protection against intruders in air interface.
- It maintains authentication Keys and algorithms and provide security triplets (RAND, SRES, KI).

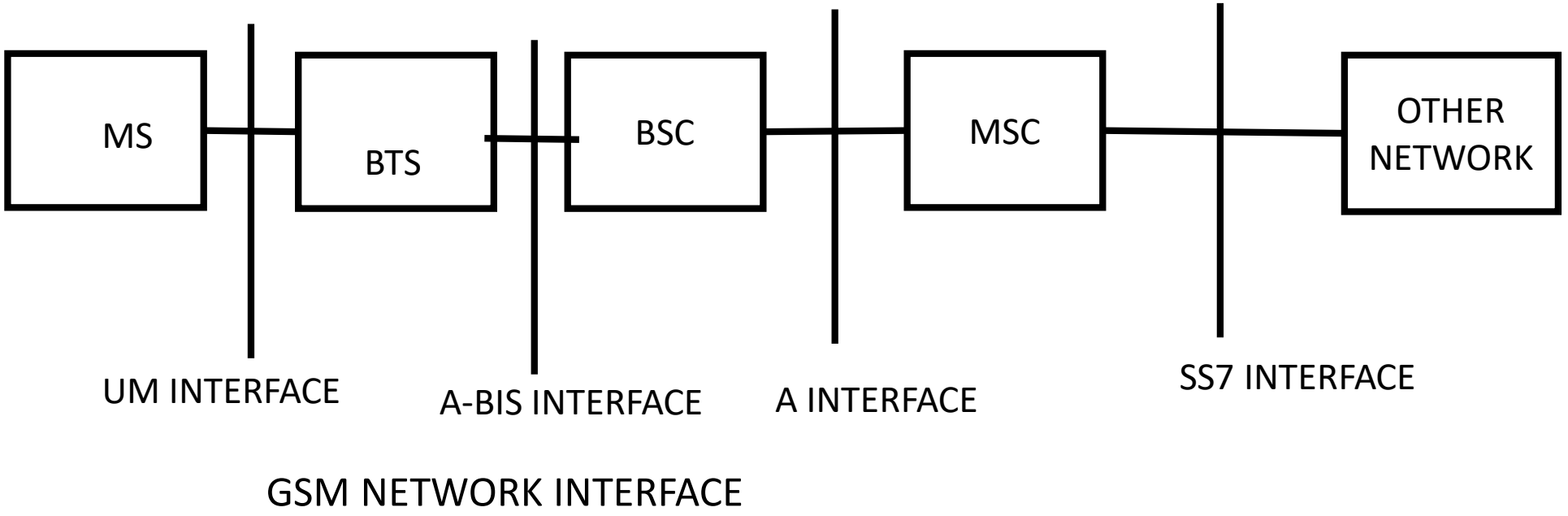
E - Equipment Identity Registry (EIR)

- It is a database that is used to track handset using the IMEI number.
- It is made up of three sub-classes, white list, black list and the grey list.

- 4 Operational Support Subsystem (OSS)
  - It supports the operation and maintenance of GSM and allows system engineers to monitor, diagnose and troubleshoot all aspects of GSM system.
  - It supports one or more Operation Maintenance Centre (OMC) which are used to monitor the performance of each MS, BTS, BSC and MSC within a GSM system.
  - It has three main functions.
  - To maintain all telecommunication hardware and network operations with a particular market.
  - To manage all charging and billing procedure.
  - To manage all mobile equipment in the system.

INTERFACES FOR GSM NETWORK

- UM Interface – used to communicate between BTS and MS
- A-bis Interface – used to communicate between BSC to BTS
- A Interface – used to communicate between BCS and MSC.
- Singing protocol SS7 – used to communicate between MSC and other network.



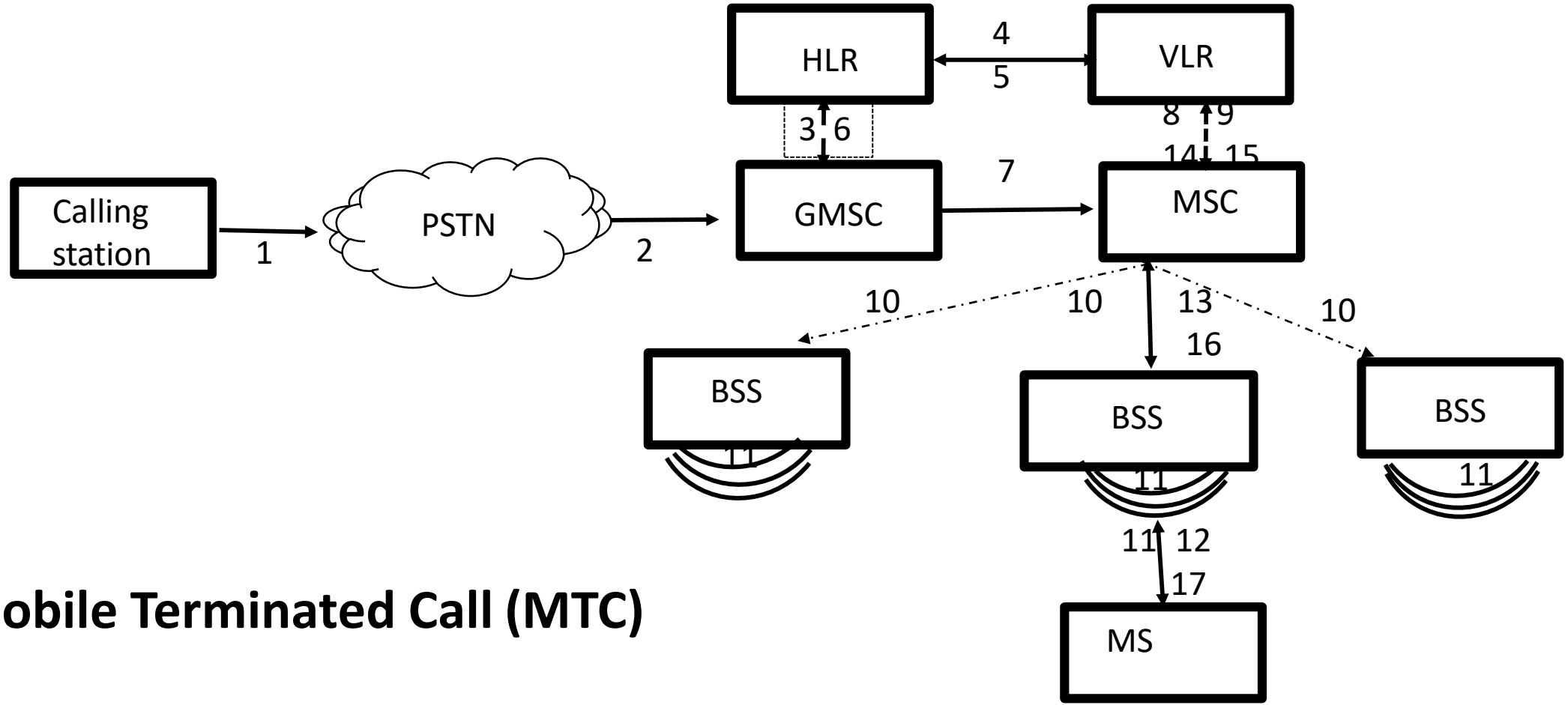
LOCATIZATION AND CALLING

- The fundamental feature of the GSM System is the automatic, worldwide localization of users for which, the system performs periodic location updates.
- The HLR always contains information about the current location and the VLR is responsible for the current MS information update to the HLR about the location changes.
- Changing the VLRs with Uninterrupted availability is called roaming. Roaming can take place within a network of one provider, between two providers a country and also between different providers in different countries.
- To locate and address an MS, several numbers are needed.

- Mobile Station International ISDN number (MSISDN) the only important number for a user of GSM is the phone number. This number consists of the country code (cc), the national destination code (NDC) and the subscriber number (SN).
- International Mobile Subscriber Identity (IMSI) GSM uses the IMSI for Internal Unique Identification of a subscriber. IMSI consists of a mobile country code (MCC), the mobile network code (MNC), and finally the mobile subscriber identification Number (MSIN).
- Temporary Mobile Subscriber Identity (TMSI) to hide the IMSI, which would give away the exact identity for the user signalling over the air interface, GSM uses the 4 byte IMSI for local subscriber identification,
- Mobile Station Roaming Number (MSRN). Another temporary address that hide the identity and location of a subscriber is MSRN. The VLR generates this address on request from the MSC, and the address is also stored in the HLR. MSRN contains the current visitor country code (VCC). The visitor National Destination Code (VNDC). The identification of the current MSC together with then subscriber number. The NISRN helps the HLR to find a subscriber for an incoming call.

A MOBILE TERMINATED CALL (MTC)

- A call originating from station (PSTN) to mobile station is refer to as a mobile terminated call.
- The following figure shows the different steps that take place:

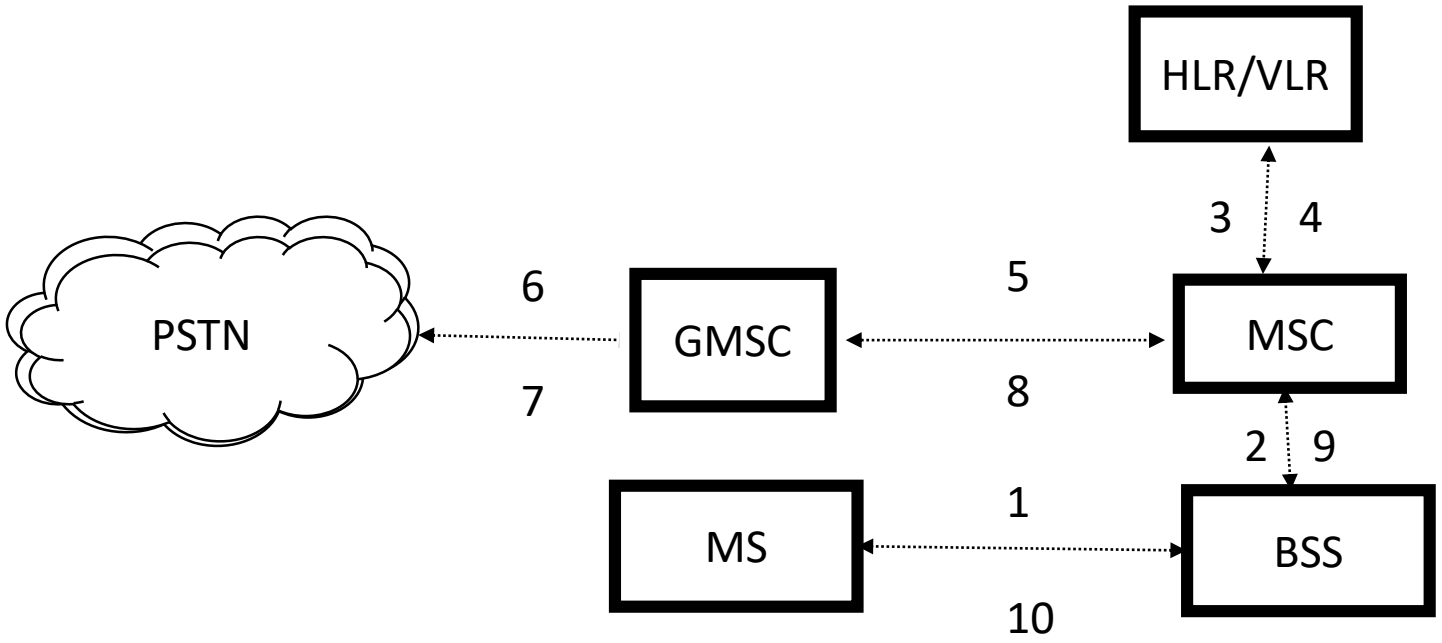


Mobile Terminated Call (MTC)

- **Step 1:** User dials the phone number of GSM subscriber
- **Step 2:** The fixed network (PSTN) identifies the number belongs to a user in GSM network and forwards the call setup to the Gateway MSC (GMSC).
- **Step 3:** the GMSC identifies the HLR for the subscriber and signals the call setup to HLR
- **Step 4:** The HLR checks for number existence and its subscribed services and requests an MSRN from the current VLR.
- **Step 5**: VLR sends the MSRN to HLR
- **Step 6**: Upon receiving MSRN, the HLR determines the MSC responsible for MS and forwards the information to the GMSC.
- **Step 7:** the GMSC can now forward the call setup request for the MSC indicated.
- **Step 8:** The MSC requests the VLR for the current status of the MS
- **Step 9:** VLR sends the requested information
- **Step 10:** if MS is available, the MSC initiates paging in all calls it is responsible for.
- **Step 11:** The BTSs of all BSSs transmit the paging signal to the MS
- **Step 12: Step 13:** if MS answers, VLR performs security checks
- **Step 15: Till step 17:** Then the VLR signals to the MSC to setup a connection to the MS

FOR A MOBILE ORIGINATED CALL (MOC).

- The following steps take place:

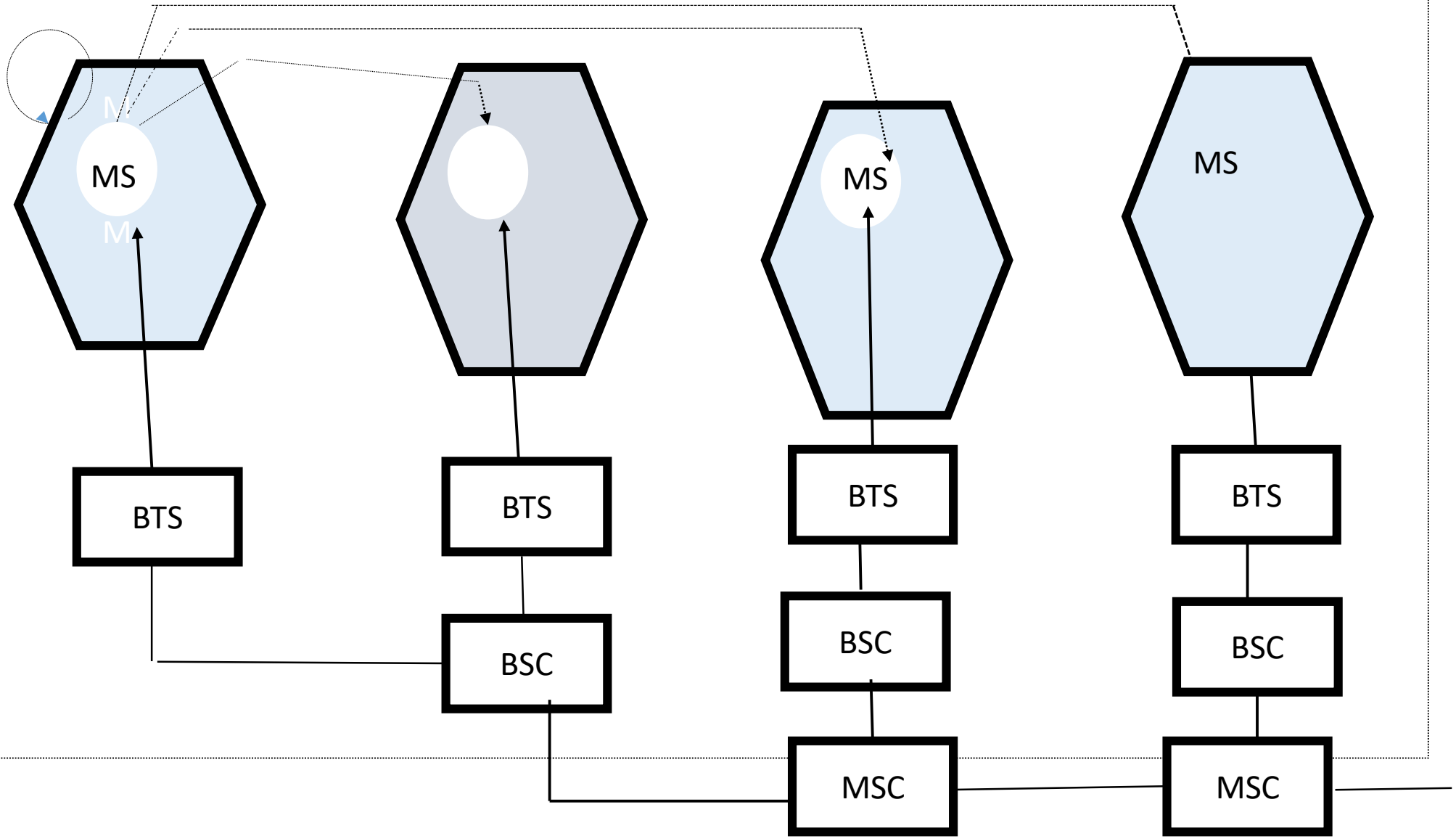


- **Step 1:** The MS transmits a request for a new connection.
- **Step 2:** The BSS forwards this request to the MSC
- **Step 3:** The MSC then checks if this user is allowed to set up a call with the request and checks the availability of resources through GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

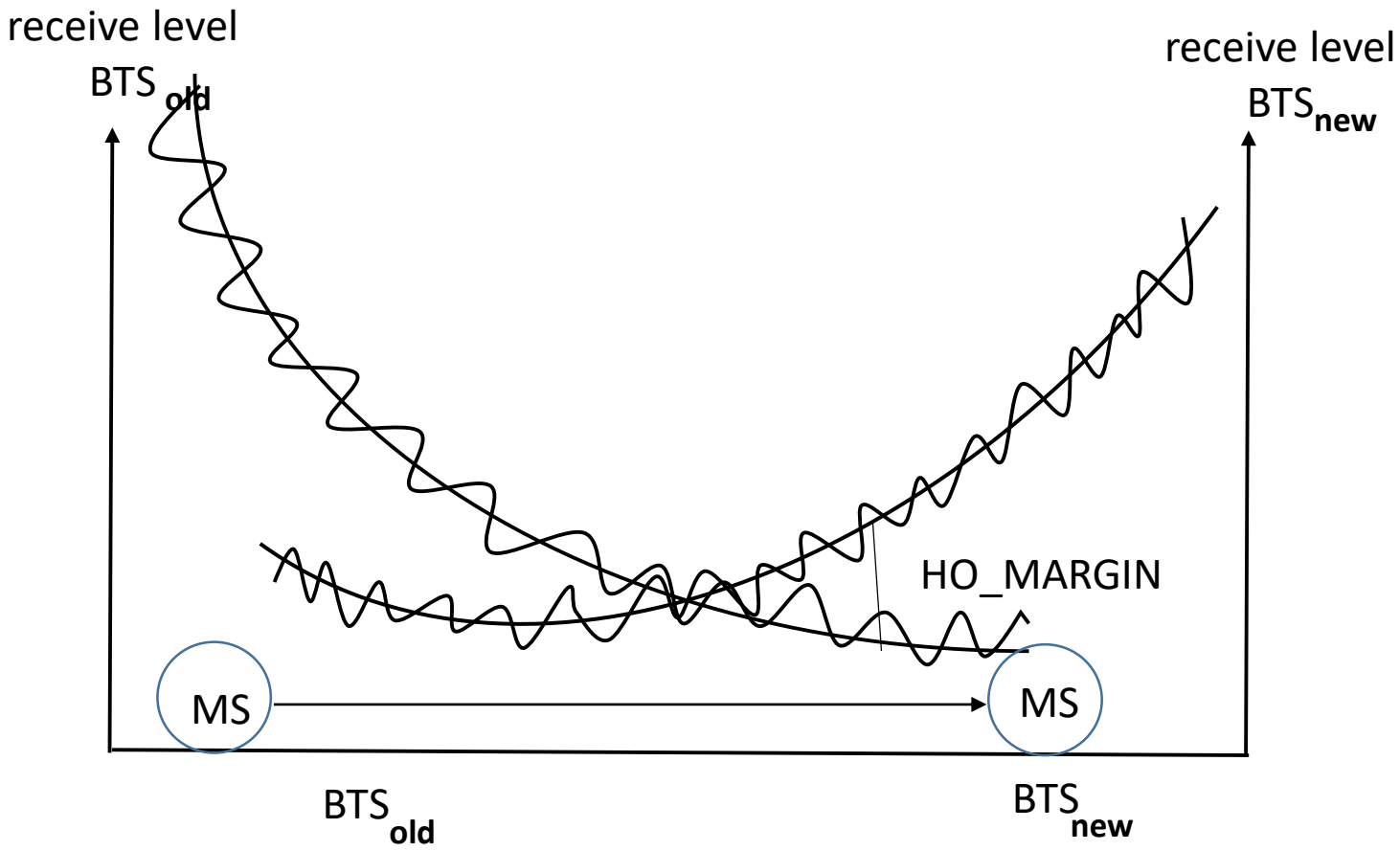
HANDOVER

- Cellular systems require **handover** procedures, as single cells do not cover the whole service area. However, a handover should not cause a cut-off, also called **call drop**. GSM aims at maximum handover duration of 60 ms. There are two basic reasons for a handover.
- 1. The mobile station **moves out of the range** of a BTS, decreasing the received **signal level** increasing the error rate thereby diminishing the **quality of the radio link.**
- 2. Handover may be due to **load balancing,** when an MSC/BSC decides the traffic is too high in one cell and shifts some MS to other cells with a lower load.

- The four possible handover scenarios of GMS are shown below:-



- **Intra-cell handover:** Within a cell, narrow-band interference could make transmission as a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario I).
- **Inter-cell, intra-BSC handover:** This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2)
- **Inter-BSC, intra-MSC handover:** As a BSC only controls a limited number of cell, GSM also has to performs a handover between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3).
- **Inter MSC handover:** A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4)



Handover decision depending on receive level

- To provide all the necessary information for a handover due to a weak link, MS and BTS both perform periodic measurements of the downlink and uplink quality respectively.
- Measurement reports are sent by the MS about every half-second and contain the quality of the current link used for transmission as well as the quality of certain channels in neighbouring cells.

WIRELESS NETWORK FOR GSM

- Space Division Multiple Access (SDMA) is used for allocating a separated space to users in wireless network. A typical application involves assigning an optimal base station to a mobile phone use. A mobile phone may receive several base stations with different quality. SDMA decide which base station is best, taking into account which frequencies, time slots or code are still available.
- Frequency Division Multiple Access (FDMS) is a method employed to permit several users to transmit simultaneously on one satellite transponder by assigning a specific frequency within the channel to each users. Each conversation gets its own, unique, radio channel. The channels are relatively narrow, usually 30KHz or less and are defined as either transmit or received channels. A full duplex. Conversation requires a transmit and receive channels pair, which is refers to uplink from MS to BTS and downlink from BTS to MS.

- FDMA in general describes schemes to subdivide the frequency dimension into several non-over-lappling frequency band.
- Time Division Multiple Access (TDMA), offers a much more flexible scheme, which comprises all technologies that allocates certain time slots for communication.

  Synchronization between sender and receiver has to be achieved in the domain, that allocating a certain time slot for a channel.
- Carrier Sense Multiple Access (CSMA) offers technology of sensing the carrier before accessing the medium. Sensing the carrier and accessing the medium only if the carrier is idle, which decreases the probability of a collision. This scheme is still used in most wireless LAWS.

INFORMATION SECURITY

- Traditionally, Computer Security refers to protection of the physical machine.

- Today, computer security is broadly, security applied to computing devices such as computers and smartphones, as well as computer network both private and public and the Internet.
- Computer Security covers all the processes and mechanisms by which digital equipment, Information and services are protected from unintended or unauthorised access, change or destruction. It is sometimes referred to as cyber security or IT security.
- Computer Crime – refers to any crime that involves a computer and a network

INFORMATION SECURITY TERMS

- Vulnerability – is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw and attacker capability to exploit the flaw.

  Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities.

- Backdoors – In computer system, a backdoor is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plan text and so on, while attempting to remain undectated.

  The backdoor may take the form of an installed program or could be a modification of an existing program or hardware device. It may also take information about disk and memory usage.

- Denial – of – Service attack – This attack is designed to render services unusable. Attacker can deny serviced to individual victims, such as by deliberately entering a wrong password so many times to cause the victim account to be lucked or overloading the capabilities of the system or network and block all users at once for example a worm Trojan horse etc.
- Direct – access attacks – An unauthorised user gaining physical access to a computer, the attacker can perform many functions, install different types of device to compromise security, including operating system modifications, software worms, key loppers and convert listening devices.
- Eaves dropping – is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For example security organisations.

- Spoofing – is where an attacker (person or program) successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- Repudiation – is where the authenticity of a signature is being challenged.
- Indirect attacks – is an attack launched by a third party computer. It usually becomes far more difficult to track down the actual attacker.

CYBERCRIME PREVENTION TIPS

- Use strong passwords: - Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.
- Secure your Computer
  - Activate Firewall – firewall are the first line of Cyber defence, they block connection to unknown or bogus sites and will keep out some types of virus and hackers.
  - Anti – Virus/Malware Software – Install and regularly update anti-virus software to prevent virus from infecting your computer.
  - Block spyware attacks – install and updating anti-spyware software to prevent spyware from infiltrating your computer.
- Be careful using social –Media – make sure your social networking profiles (eg Facebook, Twitter, Youtube, MSN, etc) are set on private. Ensure your security setting are properly configure and be careful on what information you post online.

- Secure your mobile devices – Be aware that your mobile devices is vulnerable to viruses and hackers. Download application from trusted sources only.
- Install the latest operating system update . Keep your applications and operating system (e.g Windows, Linux, Mac, etc) current with the latest system updates. Turn-on automatic updates to prevent potentials attackers on older software.
- Protect your Data – Use encryption for your most sensitive files and make regular back-up of all your important data and store it in another locations.
- Secure your Wireless network – Wifi networks at home or public places are vulnerable to intrusion if they are not properly secured. Always review and modify the defaults settings.
- Protect your e-identity – Make sure your personal information or financial information are giving only on security websites.
- Avoid being scammed – always think before you click on a link or file of unknown origin. Don’t feel pressured by e-mails, always check the source of the message. Never reply to e-mails that ask you to verify your information or confirm your sensitive information online.

PRINCIPLES OF INFORMATION SECURITY

- Confidentiality – Sometimes refer to privacy. This involve all measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching wrong people, while making sure that the right people can get it. That is, access is restricted to those only authorised. Safeguarding data confidentiality may involve special training on security risk that could threaten the information and the use of strong passwords.

- Integrity – Involve maintaining the consistency, accuracy and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorised person. This can be achieved through the use of file permission and user access control.

- Availability – is best ensure by rigorously maintaining all hardware, correctly functioning operating system environment that is free of software conflicts. It also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks
- Non – Repudiation is the assurance that someone cannot deny something. It is the presentation of unforgeable evidence that a message was sent or received. If messages or transactions can be disputed, then important identity actions can be challenged and jeopardised.
- Authentication – is the process or action of verifying the identity of a user or process. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorised user's information on a local operating system or within an authentication server.