DISTRIBUTED OPERATING SYSTEMS(SP)

CLASS : II M.Sc CS SUB CODE: 20PCS3DE3B

Unit 1

1.Fundamentals : What is a Distributed Computing System

2. Evolution of Distributed Computing Systems

3. Distributed Computing System Models

4. Why are Distributed Computing Systems gaining popularity

5.What is a Distributed Operating System

6. Issues in Designing Distributed Operating System

7. Introduction to Distributed Computing Environment.

 # Introduction to Computer Networks

–Network types – LAN –WAN #

–Communication protocols –Internetworking –ATM Technology.

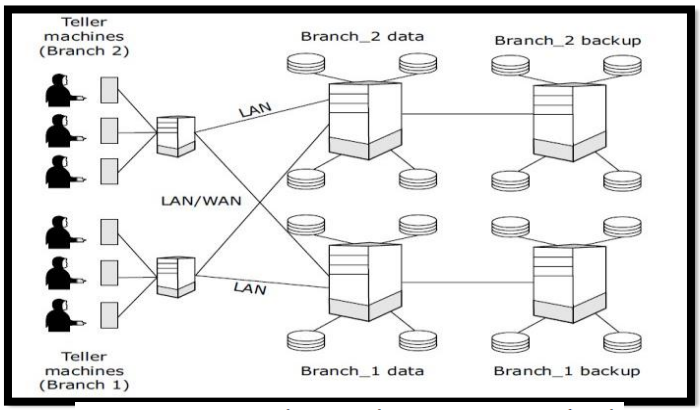
1.1 What is a Distributed System?

Tanenbaum's definition of a distributed system:

"A distributed system is a collection of independent computers that appear to the users of the system as a single coherent system."

An Example of a Distributed System

- Nationalized Bank with multiple BranchOffices



Internet connected network representing a bank

Requirements of Distributed Systems

Security and reliability

- Consistency of replicated data
- Concurrent transactions (operations which involve accounts in different banks; simultaneous access from several users, etc.)
- Fault tolerance

Architectures for Distributed Systems

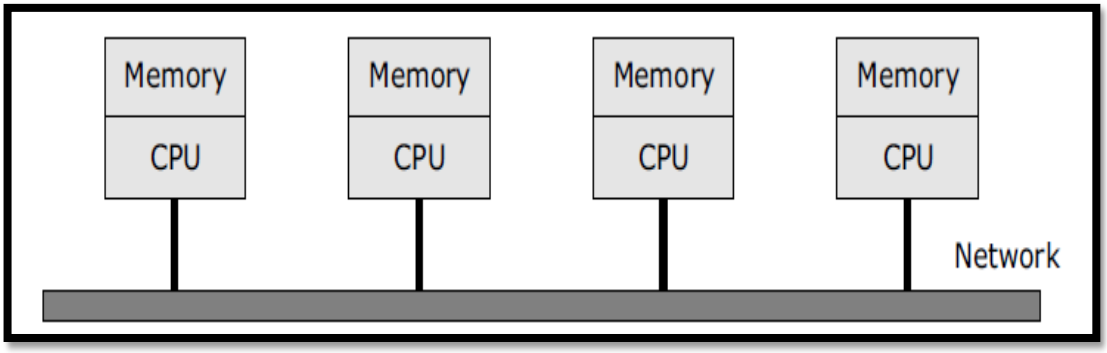
Shared memory architectures / Tightly coupled systems

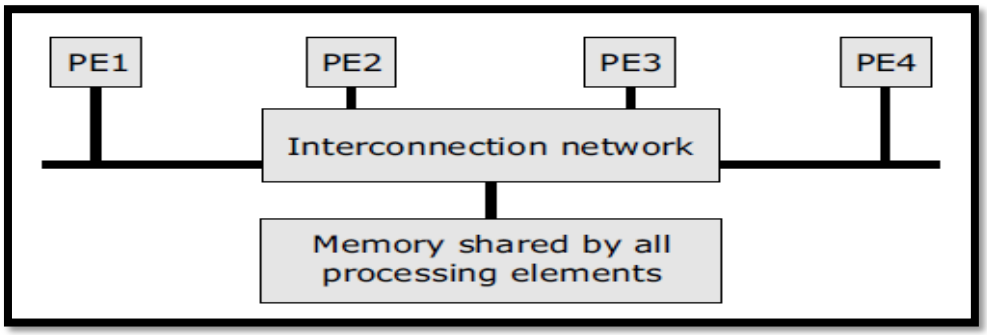
➢ easier toprogram

- Distributed memory architectures / Loosely coupled systems

- offer a superior price performance ratio andare Scalable

Architectures for Distributed Systems





Distributed memory architecture

1.2 Evaluation of DOS

In the early years of computing, mainframe-based applications were considered to be the best-fit solution for executing large-scale data processing applications.

With the advent of personal computers (PCs), the concept of software programs running on standalone machines became much more popular in terms of the cost of ownership and the ease of application use.

With the number of PC-based application programs running on independent machines growing, the communications between such application programs became extremely complex and added a growing challenge in the aspect of application-toapplication interaction.

Lately, network computing gained importance, and enabling remote procedure calls (RPCs) over a network protocol calledTransmission Control Protocol/Internet Protocol (TCP/IP) turned out to be a widely accepted way for application software communication.

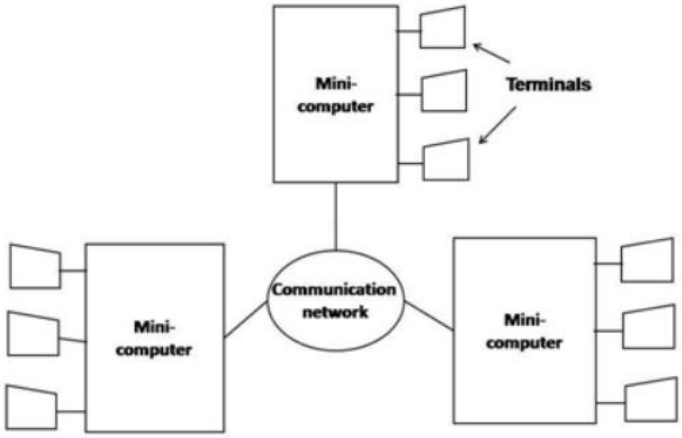
Since then, software applications running on a variety of hardware platforms, operating systems, and different networks faced some challenges when required to communicate with each other and share data. This demanding requirement lead to the concept of distributed computing applications.

As a definition, “Distributing Computing is a type of computing in which different components and objects comprising an application can be located on different computers connected to a network distributed computing model that provides an infrastructure enabling invocations of object functions located anywhere on the network. The objects are transparent to the application and provide processing power as if they were local to the application calling them.

1.3 Distributed Computing System Models

- Mini Computer
- Workstation model
- Workstation–server model
- Processor-poolmodel
- Hybrid

1.Minicomputer model



The minicomputer model is a simple extension of the centralized time-sharing system.

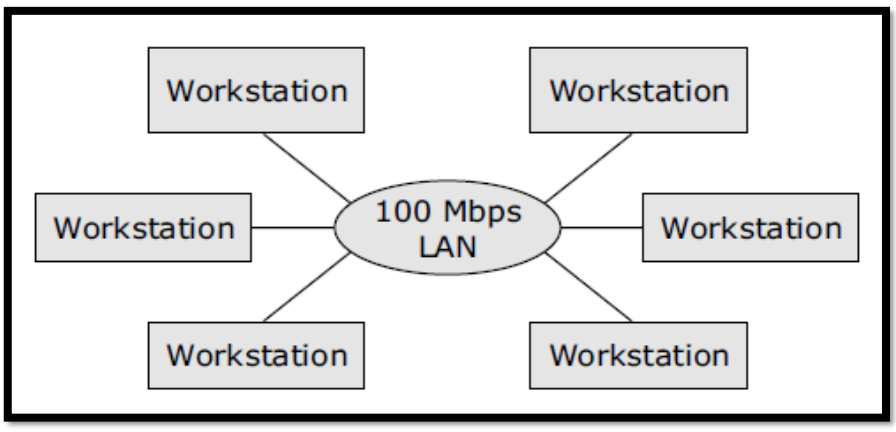
- A distributed computing system based on this model consists of a few minicomputers interconnected by a communication network were each minicomputer usually has multiple users simultaneously logged on to it.
- Several interactive terminals are connected to each minicomputer.Each user logged on to one specific minicomputer has remote access to other minicomputers.
- The network allows a user to access remote resources that are available on some machine 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.

2.Workstation Model

Consists of network of personalcomputers

Each one with its own hard disk and local filesystem

Interconnected over thenetwork



A distributed computing system based on the workstation model consists of several workstations interconnected by a communication network.

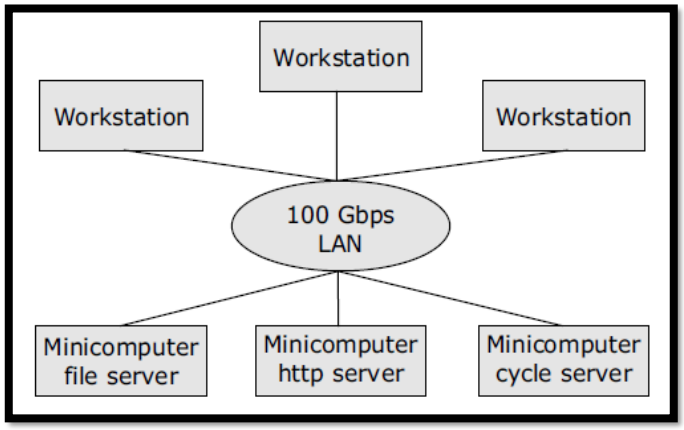
- An organization may have several workstations located throughout an infrastructure were each workstation is equipped with its own disk & serves as a single-user computer.
- In such an environment, at any one time a significant proportion of the workstations are idle which results in the waste of large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

Workstation model

- Example: Sprite system & Xerox PARC.

3. Workstation-server Mode

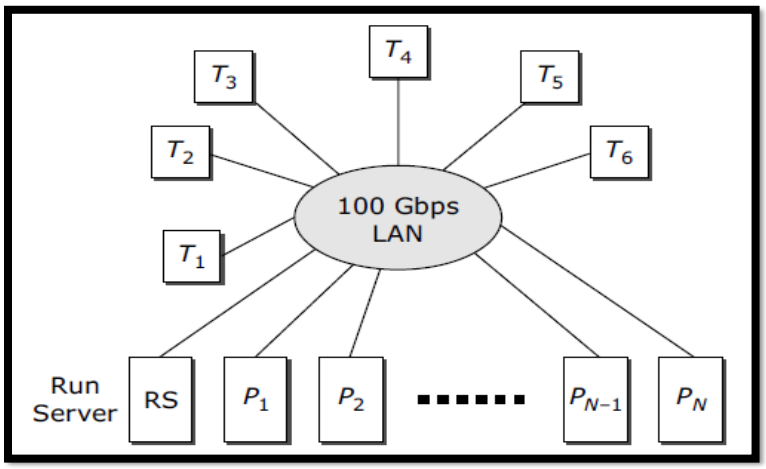
Consists of multiple workstations coupled with powerful servers with extra hardware to store the file systems and other software like databases



- The workstation model is a network of personal workstations having its own disk & a local file system.
- A workstation with its own local disk is usually called a diskful workstation & a workstation without a local disk is called a diskless workstation. Diskless workstations have become more popular in network environments than diskful workstations, 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 consists of a few minicomputers & 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 requests for services provided by special servers are sent to a server providing that type of service that performs the user's requested activity & returns the result of request processing to the user's workstation.
-
- Therefore, in this model, the user's processes need not migrated to the server machines for getting the work done by those machines.
- Example: The V-System.

4. Processor-pool Model

Consists of multiple processors: a pool of processors and a group of workstations



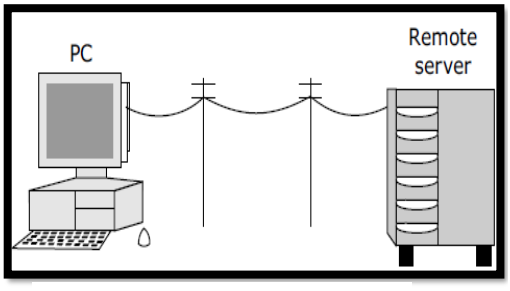
- The processor-pool model is based on the observation that most of the time a user does not need any computing power but once in a while the user may need a very large amount of computing power for a short time.
- Therefore, unlike the workstation-server model in which a processor is allocated to each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

5.Hybrid Model:

- The workstation-server model has a large number of computer users only performing simple interactive tasks &-executing small programs.
- In a working environment that has groups of users who often perform jobs needing massive computation, the processor-pool model is more attractive & suitable.
- To combine Advantages of workstation-server & processor-pool models,a hybrid model can be used to build a distributed system.
- The processors 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.

Advantages of Distributed Systems

- Inherently distributed applications
- Information sharing among



A PC connected to a remote server

geographically distributed users

- Resource Sharing, Better price performance ratio
- Shorter response time &higher throughput
- Higher reliability and vailability against component failures
- Extensibility and Incremental Growth ,Better Flexibility
- **Disadvantages of Distributed Systems**
    - Relevant software does not exist currently
    - Security poses a problem due to easy access to all data
      Networking saturation may cause a hurdle in data transfer

---

1.4 Why are Distributed computing systems gaining popularity?

i. Inherently Distributed Applications:

- Several applications are inherently distributed in nature and require distributed computing system for realization. These applications might have distributed locations for collecting, processing and accessing data resulting in need of distributed computing systems.
- Example: A computerized banking system.

ii. Information sharing among Distributed users:

- Another reason for emergence of distributed computing systems was the desire for efficient person-to-person communication facility by sharing information over distances. In distributed systems information generated by one user can be easily shared by other users for many ways.

iii. Resource Sharing:

- Sharing of software resources such as software libraries and databases can be done in an efficient way among the users of a single distributed computing system. Cloud storage can be an example.

iv. Better Price-Performance Ratio:

- This is one of the most important reasons for growing popularity as the increased power and reduced microprocessor price is combined with fast communication network that provide better price-performance ratio.
- Resource sharing is allowed in distributed computing which makes it cost-effective.

v. Shorter Response Time and higher Throughput:

- Multiplicity of processors enable distributed computing systems to have better performance. Most common performance metrics are response tine and throughput of user processes. Example is the workstation model where the users have multiple processes that run simultaneously and interact with each other.

vi. Higher Reliability:

- Reliability refers to the degree of tolerance against errors and component failures in a system. A reliable system prevents loss of information even in the event of component failure. The multiplicity of storage devices and processors in a distributed computing system allow the maintenance of multiple copies of information which still provide data if one site is down.

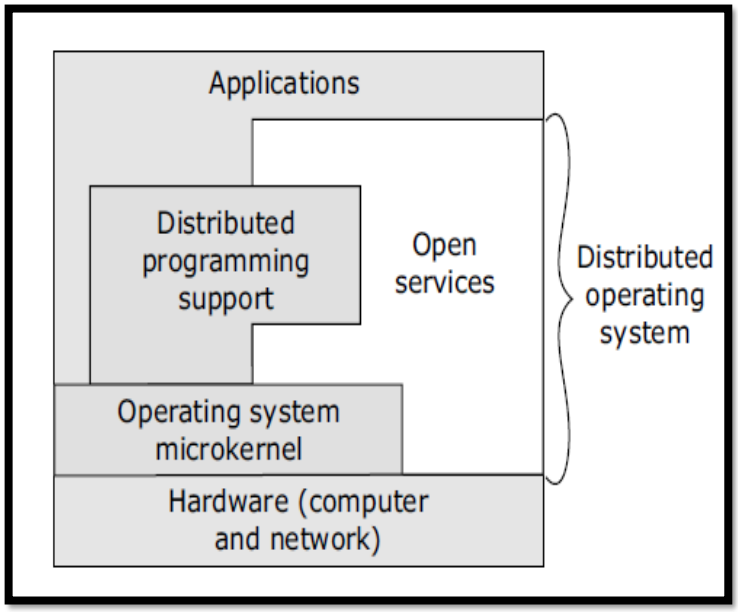
vii. Extensibility and Incremental Growth:

- It is possible to extend the power and functionality of a distributed computing system be adding additional resources to the system. Extensibility is also easier because addition of resources can be done without disruption of the normal functioning of the system.

viii. Better flexibility in Meeting Users Needs:

- A distributed computing system may have a pool of different types of computers from which the most appropriate one can be selected for processing a user's job. Hybrid model can be an example for this.

1.5 What is a Distributed operating system



Operating system as a program that controls the resources of computer system and provides its users with an interface or virtual machine that is more convenient to use than the bare machine.

According to this definition, the two primary tasks of an operating system are as follows:

1. To present users with a virtual machine that is easier to program than the underlying hardware.

2. To manage the various resources of the system. This involves performing such tasks as keeping track of who is using which resource, granting resource requests, accounting for resource usage, and mediating conflicting requests from different programs and users.

The operating systems commonly used for distributed computing systems can be broadly classified into two types

-network operating systems and distributed operating systems.

The three most important features commonly used to differentiate between these two types of operating systems are system image, autonomy, and fault tolerance capability.

1. System image.

The point of view of its users.

In case of a network operating system, the users view the distributed computing system as a collection of distinct machines connected by a communication subsystem. That is, the users are aware of the fact that multiple computers are being used. On the other hand, a distributed operating system hides the existence of multiple computers and provides a single-system image to its users. That is, it makes a collection of networked machines act as a virtual uniprocessor. The difference between the two types of operating systems based on this feature can be best illustrated with the help of examples.

Two such examples are presented below.

In the case of a network operating system, although a user can run a job on any machine of the distributed computing system, he or she is fully aware of the machine on which his or her job is executed. This is because, by default, a user's job is executed on the machine on which the user is currently logged.

If the user wants to execute a job on a different machine, he or she should either log on to that machine by using some kind of "remote login" command or use a special command for remote execution to specify the machine on which the job is to be executed.

In either case,

the user knows the machine on which the job is executed. On the other hand, a distributed operating system dynamically and automatically allocates jobs to the various machines of the system for processing. Therefore, a user of a distributed operating system generally has no knowledge of the machine on which a job is executed. That is, the selection of a machine for executing a job is entirely manual in the case of network operating systems but is automatic in the case of distributed operating systems.

With a network operating system, a user is generally required to know the location of a resource to access

it, and different sets of system calls have to be used for accessing local and remote resources. On the other hand, users of a distributed operating system need not keep track of the locations of various resources for accessing them, and the same set of system calls is used for accessing both local and remote resources.

For instance, users of a network operating system are usually aware of where each of their files is stored and must use explicit file transfer commands for moving a file from one machine to another, but the users of a distributed operating system have no knowledge of the location of their files within the system and use the same command to access a file irrespective of whether it is on the local machine or on a remote machine. That is, control over file placement is done manually by the users in a network operating system but automatically by the system in a distributed operating system.

Notice that the key concept behind this feature is "transparency." We will see later in this chapter that a distributed operating system has to support several fOnDS of transparency to achieve the goal of providing a single-system image to its users. Moreover, it is important to note here that with the current state of the art in distributed operating systems, this goal is not fully achievable. Researchers are still working hard to achieve this goal.

2. Autonomy. A network operating system is built on a set of existing centralized operating systems and handles the interfacing and coordination of remote operations and communications between these operating systems.

That is, in the case of a network operating system, each computer of the distributed computing system has its own local operating system (the operating systems of different computers may be the same or different), and there is essentially no coordination at aJI among the computers except for the rule that when two processes of different computers communicate with each other, they must use a mutually agreed on communication protocol. Each computer functions independently of other computers in the sense that each one makes independent decisions about the creation and termination of their own processes and management of localresources. Notice that due to the possibility of difference in local operating systems, the system calls for different computers of the same distributed computing system may be different in this case.

On the other hand, with a distributed operating system, there is a single systemwide operating system and each computer of the distributed computing system runs a part of this global operating system. The distributed operating system tightly interweaves all the computers of the distributed computing system in the sense that they work in close cooperation with each other for the efficient and effective utilization of the various resources of the system. That is, processes and several resources are managed globally (some resources are managed locally). Moreover, there is a single set of globally valid system calls available on all computers of the distributed computing system.

The set of system calls that an operating system supports are implemented by a set of programs called the kernel of the operating system. The kernel manages and controls the hardware of the computer system to provide the facilities and resources that are accessed by other programs through system calls, To make the same set of system calls globally valid, with a distributed operating system identical kernels are run on all the computers of a distributed computing system. The kernels of different computers often cooperate with each other in making global decisions, such as finding the most suitable machine for executing a newly created process in the system.

In short, it can be said that the degree of autonomy of each machine of a distributed computing system that uses a network operating system is considerably high as compared to that of machines of a distributed computing system that uses a distributed operating system.

3. Fault tolerance capability. A network operating system provides little or no fault tolerance capability in the sense that if 10% of the machines of the entire distributed computing system are down at any moment, at least 10% of the users are unable to continue with their work. On the other hand, with a distributed operating system, most of the users are normally unaffected by the failed machines and can continue to perform their work normally, with only a 10% loss in performance of the entire' distributed computing system. Therefore, the fault tolerance capability of a distributed operating system is usually very high as compared to that of a network operating system.

A distributed operating system is one that looks to its users like an ordinary centralized operating system but runs on multiple, independent central processing units (CPUs).

The key concept here is transparency. In other words, the use of multiple processors should be invisible (transparent) to the user. Another way of expressing the same idea is to say that the user views the system as a "virtual uniprocessor," not as a collection of distinct machines. [P.419].

A distributed computing system that uses a network operating system is usually referred to as a network system, whereas one that uses a distributed operating system is resources. Notice that due to the possibility of difference in local operating systems, the system calls for different computers of the same distributed computing system may be different in this case.

On the other hand, with a distributed operating system, there is a single systemwide

operating system and each computer of the distributed computing system runs a part of this global operating system. The distributed operating system tightly interweaves all the computers of the distributed computing system in the sense that they work in close cooperation with each other for the efficient and effective utilization of the various resources of the system. That is, processes and several resources are managed globally (some resources are managed locally). Moreover, there is a single set of globally valid system calls available on all computers of the distributed computing system.
The set of system calls that an operating system supports are implemented by a set of programs called the kernel of the operating system. The kernel manages and controls the hardware of the computer system to provide the facilities and resources that are accessed by other programs through system calls, To make the same set of system calls globally valid, with a distributed operating system identical kernels are run on all the computers of a distributed computing system. The kernels of different computers often cooperate with each other in making global decisions, such as finding the most suitable machine for executing a newly created process in the system.
In short, it can be said that the degree of autonomy of each machine of a distributed computing system that uses a network operating system is considerably high as compared to that of machines of a distributed computing system that uses a distributed operating system.

1.6 Issues in Designing Distributed Systems

- Transparency
- Flexibility
- Reliability
- Performance
- Scalability
- Security

Transparency

Transparencies required for Distributed Systems

Transparency	Description
Access	Hide the differences in data representation and how a resource is accessed
Location	Hide where a resource is physically located
Migration	Hide the movement of a resource to another location
Relocation	Hide the movement of a resource to another location while in use
Replication	Hide the fact that multiple copies of the resource exist without user's knowledge
Concurrency	Hide the fact that a resource may be shared by several users
Failure	Hide the failure and recovery of a resource
Persistence	Hide whether a resource is in memory or on disk

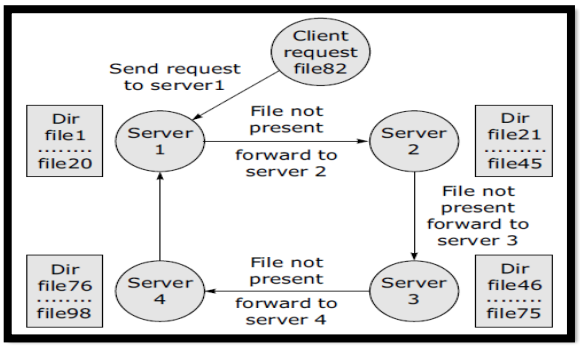
Types of transparencies

Replication Transparency

Locating Replicated File stored on any server

Flexibility

- Monolithic kernel approach
- Here kernel does all functions and provides facilities at local machine
- There is over Burdon on kernel
- Micro kernel approach

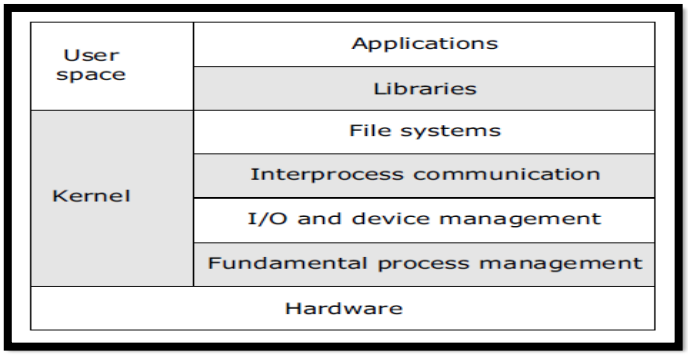


Location transparency

- It takeout as much functionality as possible from kernel And retain only essential functions.
- Provides only few functions in the kernel while uses process server to manage IPC, pager fro MM and fs management

Monolithic Kernel Approach

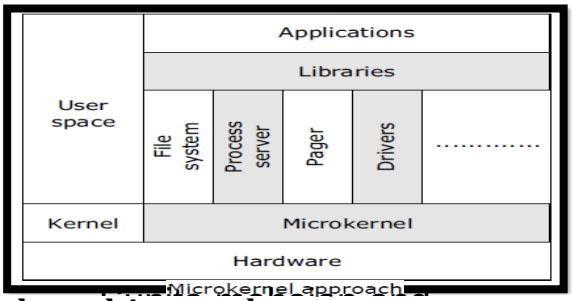
Uses the minimalist, modular approach with accessibility to other services as needed



Monolithic kernel approach

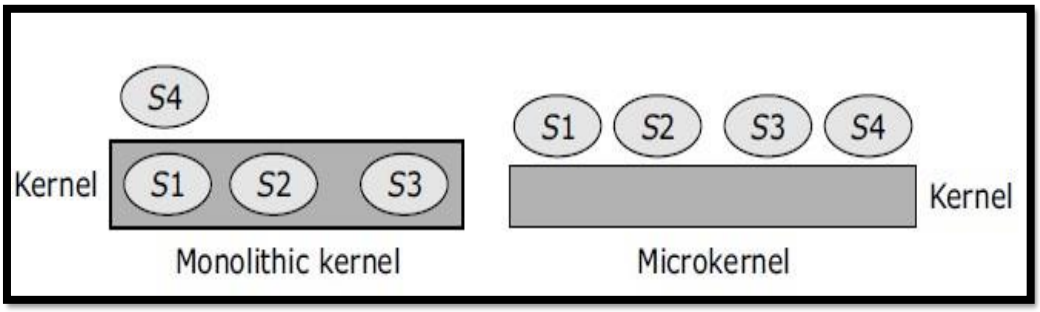
Microkernel Approach

Uses the kernel does it all approach with all functionalities provided bythekernel irrespective whether all machines use it ornot



Microkernel approach

Monolithic versus Microkernel Approach



Monolithic vs microkernel

Services (file, network)

Kernel code and data

Reliability

Availability in case of Hardware failure

- Data recovery in case of Data failure
- Maintain consistency in case of replicated data

Performance

Metrics are

Response time
Throughput
System utilization
Amount of network capacity used

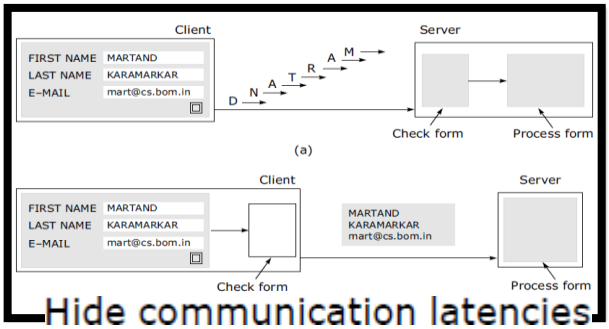
Scalability

- Techniques to handle scalability issues
  - hide communication latencies
  - hide distribution
  - hide replication

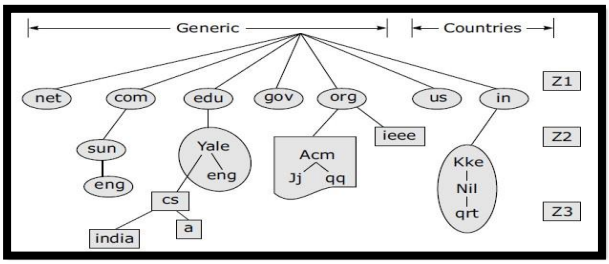
Scalability-related issues

Concept	Example
Centralized services	A single server for all users
Centralized data	A single on-line telephone book
Centralized algorithms	A single algorithm doing routing based on available information

Hide Communication Latencies



Hide Distribution



Security

Confidentiality means protection against unauthorized access
Integrity implies protection of data against corruption
Availability means protection against failure always accessible

---

1.7 Introduction to Distributed Computing Environment (DCE)

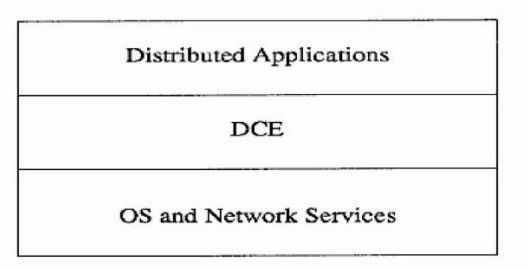
What is DCE? How was DCE created?
DCE Components DCE Cells
What is DCE?

DCE is an architecture defined by the Open Software Foundation (OSF) to provide an Open Systems platform to address the challenges of Distributed computing.

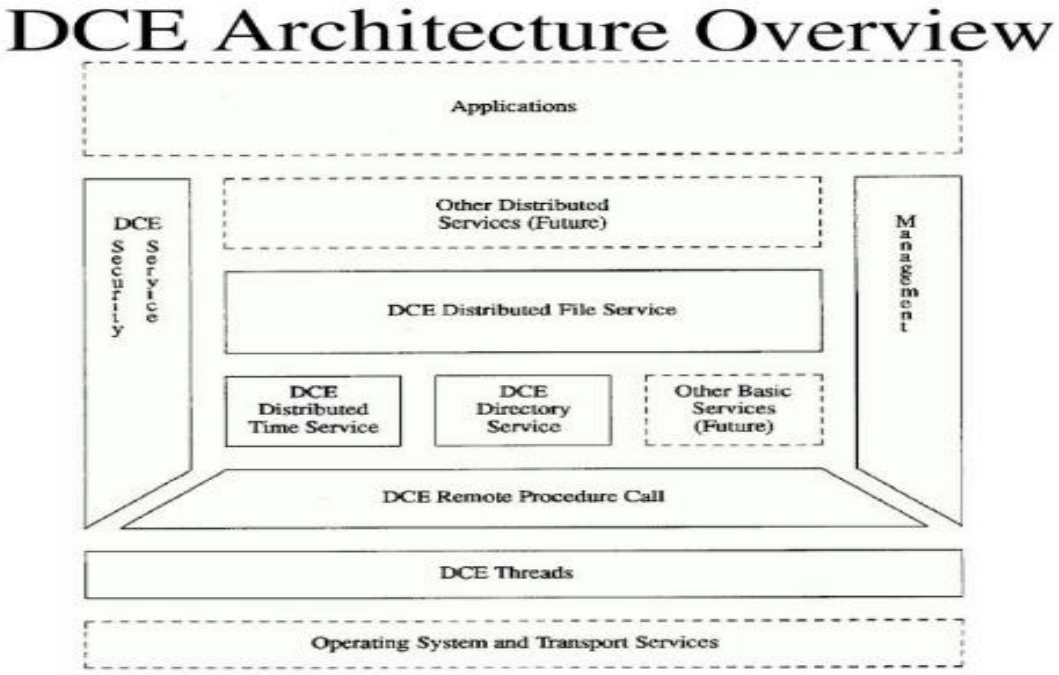
The DCE supplies a framework and toolkit for developing client/server applications.

Framework-is a re-usable design for a software system that includes support programs, code libraries, a scripting language, or other software to help develop and glue together the different components of a software project.

Position of DCE software in a DCE based distributed system



- DCE is a middleware software layered between the DCE applications layer and the OS and Networking layer.
- Idea is to take a collection of existing machines, interconnect them by communication network.
- Add DCE software platform on top lf the native operating systems of the machines and build and run distributed application.



How was DCE created?

- OSF did not create DCE from scratch instead it created DCE by taking advantage of work already done at universities and industries in the area of Distrubuted Computing.
- For this OSF issued a Request for technology.asking for tools and services needed to build a DCE.
- Then after designing it is provided to OSF employees .
- Finnaly those tools and services were selected then evaluation committee believed provided the best solutions.
- Almost entirely written in C.
- OSF produce single integrated package .

DCE Components

1. Thread package
2. RPC
3. Distributed Time Service
4. Name Services
5. Security Service

6. Distributed File Service

Threads

- DCE Threads supports the creation, management, and synchronization of multiple threads ofcontrol within a single process. This componentis conceptually a part of the operating systemlayer, the layer below DCE.
- All operating systems do not provide a threadsfacility and DCE components require threads bepresent,so this user-level threads package isincluded in DCE.

Remote Procedure Call

- A procedure call is a method of implementing the Client/Server Communication.
- The procedure call is translated into network communications by the underlying RPC mechanism.
- In DCE RPC, one or more DCE RPC interfaces are defined using the DCE interface definition language (IDL). Each interface comprises a set of associated RPC calls (called operations), each with their input and output parameters.
- The IDL when compiled generates data structure definitions and executable stubs for both the client and the server. The matching client and server executable stubs handle the necessary data transformations.

Time Service

- The DCE Time Service (DTS) provides synchronized time on the computers participating in a Distributed Computing Environment. DTS synchronizes a DCE hosts time with Coordinated Universal Time (UTC), an international time standard.
- DTS also provides services which return a time range to an application, and which compare time ranges from different machines.
- This is used to schedule and synchronize events across the network.

Directory Service

- The DCE Directory Service advertises that the server supports the new interface defined using the IDL.
- Naming provide uniquely and location transparency achieved.
- DCE Security Service also ensures that only authorized client end users can access the newly defined server function.
- The DCE Directory Service is a central repository for information about resources in the distributed system. Typical resources are Users Machines RPC-based services.

The DCE Directory Service consists of several parts

- Cell Directory Service (CDS) The CDS manages a database of information about the resources in a group of machines called a DCE cell.
- Global Directory Service (GDS) The Global Directory Service implements an international, standard directory service and provides a global namespace that connects the local DCE cells into one worldwide hierarchy.
- Global Directory Agent (GDA) The GDA acts as a go-between for cell and global directory services.

- Directory Service programming interface Both CDS and GDS are accessed using a single Directory Service application programming interface (API).

Security Service

- There are three aspects to DCE security Authentication This identifies that a DCE user or service is allowed to use the service. Secure communications Communication over thenetwork can be checked for tampering or encrypted for privacy.
- Authorization This issues the permission to access the service.
- These are implemented by several services and facilities which include the Registry Service, Privilege Service, Access Control List (ACL) Facility, and Login Facility.

File Service

- The DCE File Service (DFS) allows users to access and share files stored on a File Server any where on the network, without having to know the physical location of the file.
- The File Service achieves high performance, particularly through caching of file system data. Many users can access files that are located on a given File Server without a large amount of network traffic or delays.

DCE CELLS:

DCE can have thousands of computers and millions of users. The concept of Cells break down a large system into smaller , manageable units . In a DCE system a cell is a group of users, machines, or other resources.

The minimum configuration requires a celldirectory server, a security server, a distributed time server and one or more client machines.

A DCE cell is **a collection of machines, users, and resources managed as a group**. ... Each cell has its own namespace; the Cell Directory Service for the cell manages that namespace and its hierarchy. If DFS is present in the cell, the Distributed File Service allows remote access to files from anywhere in the cell.

Four factors for setting cell boundaries of a DCE system

1. Purpose
2. Administration
3. Security Machines
4. Overhead

Purpose: The machines of users working on a common goal should be put in the same cell, as they need easy access to a common set of system resources . same cell users interact very easily.

Eg: separate cell boundaries of product oriented approach and separate cell for function oriented approach.

Administration: All the machines and their users that are known to and manageable by an administrator should be put in a single cell. Each cell has different administrator.

Security: users of machines of a cell trust each other more than they trust the users of machines of other cells. Accessing a resource that belongs to another cell requires more sophisticated authentication.

Overhead: several DCE operations such as name resolution and user authentication, incur more overhead when they are performed between cells than when they are performed within the same cell.

Machines of users who frequently interact with each other and the resources frequently accessed by them should be placed in the same cell.

1.8 A computer network

A computer network is a communication system that links end systems by communication line and soft ware protocols to exchange data between two process running on different end systems of the network. End system referred to as nodes, sites, hosts , computers , machines etc.

Network Characteristics

Networks are broadly classified into two types: local area networks (LANs) and wide area networks (WANs). The WANs are also referred to as long-haul networks. The key characteristics that are often used to differentiate between these two types of networks are as follows:

1. Geographic Distribution:

The main difference between the two types of networks is the way in which they are geographically distributed. A LAN is restricted to a limited geographic coverage of a few kilometers, but a WAN spans greater distances and may extend over several thousand kilometers. Therefore LANs typically provide communication facilities within a building or a campus, whereas WANs may nationwide or even worldwide.

2. Data rate:

Data transmission rates are usually much higher in LANs than in WANP- transmission rates in LANs usually range from 0.2 megabit per second to 1 gigabit per second. On the other hand, transmission rates in WANs usually range from 1200 bits per second to slightly over 1 Mbps.

3. Error rate:

Local area networks generally experience fewer data transmission errors than WANs do. Typically bit error rates are in the range of 10 to the power of -8 to 10 to the power of -10 with LANs as opposed to 10 to the power of -5 to 10 to the power of -7 with WANP-

4. Communication link:

The most common communication links used in LANs are twisted pair, coaxial cable and fiber optics. On the other hand since the sites in a WAN are physically distributed over a large geographic area, the communication links used are by default relatively slow and unreliable. The communication links used in WANs are telephone lines, microwave links and satellite channels.

5. Ownership:

A LAN is owned by a single organization because of its limited geographic coverage. A WAN is usuall formed by interconnecting multiple LANs each of which may belong to a different organization.

Therefore administrative and maintenance complexities and costs of LANs are usually much lower than for WANs.

6. Communication cost:

The overall communication costs of a LAN is usually much lower than that of a WAN. The main reasons for this are lower error rates, simple routing algorithms and lower administrative and maintenance costs. The cost to transmit data in a LAN is negligible since the transmission medium is usually owned by the user organization. However with a WAN, this cost may be very high because the transmission media used are leased lines or public communication systems, such as telephone lines, microwave links and satellite channels.

1.9 LAN TECHNOLOGIES

Topology is the physical and logical arrangement of a network. The physical arrangement of the network refers to how the workstations, servers, and other equipment are joined together with cables and connectors. The logical arrangement of a network refers to how the workstations, servers, and other equipment relate to each other in terms of traffic flow. There are three primary LAN topologies: linear bus and ring.

In a linear bus topology, stations are arranged along a single length of cable, which can be extended at either end or at both ends to accommodate more nodes (Figure 65). The network consists of coaxial cable, such as the RG-58 A/U cable used with 10Base2 Ethernet LANs. The nodes are attached to the cable with a BNC (Bayonet Nut Connector) T-connector (Figure 66), the stem of which attaches to the network interface card (NIC). A BNC barrel connector attaches cable segments and a BNC terminator connector caps the cable ends. Of course, twisted pair wiring is most often used for Ethernet LANs, in which case RJ45 connectors provide the connections between devices.

A linear bus network can be further extended. For example, a tree topology is actually a complex linear bus in which the cable branches at either or both ends, but offers only one transmission path between any two stations.

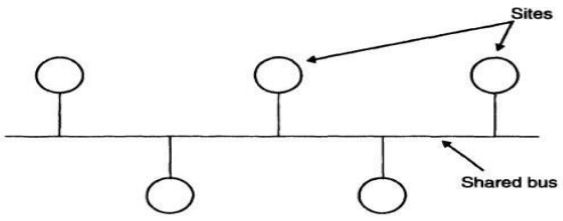


Fig. 2.1 Simple multiaccess bus network topology.

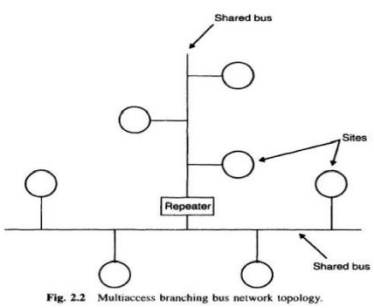


Fig. 2.2 Multiaccess branching bus network topology.

In **a ring topology**, nodes are arranged along the transmission path so data passes through each successive station before returning to its point of origin. As its name implies, the ring topology consists of nodes that form a closed circle .

In token-ring LANs, a small packet called a token is circulated around the ring, giving each station in sequence a chance to put information on the network. The station seizes the token, replacing it with an information frame. Only the addressee can claim the message. At the completion of pass through the central node, which acts as a processing and coordinating point for the network. This central node is generally referred to as a hub. Information addressed to one or more specific nodes is sent through the central node and switched to the proper receiving station(s) over a dedicated physical path.

Medium access control protocol

Special schemes are needed in a multi access environment to control the access to a shared channel. These schemes are known as medium-access control protocols. The three most important performance objectives of a medium-access control protocol are high throughput, high channel utilization, and low message delay. In addition to meeting the performance objectives, some other desirable characteristics of a medium-access control.

Several protocols have been developed for medium-access control in a multi access environment. Of these, the Carrier Sense Multiple Access with Collision Detection(CSMNCD) protocol is the one most commonly used for multi access bus networks, and the token ring and slotted ring are the two commonly used protocols for ring networks.

The CSMAlCD Protocol The CSMAl CD scheme [IEEE 1985a] employs decentralized control of the shared medium, In this scheme, each site has equal status in the sense that there is no central controller site. The sites contend with each other for use of the shared medium and the site that first gains access during an idle period of the medium uses the medium for the transmission of its own message. Obviously, occasional collisions of messages may occur when more than one site senses the medium to be idle and transmits messages at approximately the same time. The scheme uses collision detection, recovery, and controlled retransmission mechanisms to deal with this problem. Therefore, the scheme is comprised of the following three mechanisms and works as describe Computer Networks Carrier sense and defer mechanism. Whenever a site wishes to transmit a packet, it first listens for the presence of a signal (known as acarrier by analogy withradio broadcasting) on the shared medium.

1. Collision detection mechanism. Unfortunately, carrier sensing does not prevent all collisions because of the nonzero propagation delay of the shared medium.

2. Controlled retransmission mechanism. After a collision, the packets that became corrupted due to the collision must be retransmitted.

3. TheCSMNCD scheme works best on networks having a bus topology with bursty asynchronous transmissions. It has gained favor for transmission media that have relatively low speeds (around 10 Mbps) mainly because of its ease of implementation and its channel utilization efficiency. Notice that the performance ofthe CSMAlCD scheme depends on the ratio of packet length to propagation delay. The higher the ratio, the better the performance because the propagation delay is the interval during which a packet is vulnerable to collision.

Token ring protocol

A token is a special type of message (having a unique bit pattern) that entitles its holder to use the shared medium for transmitting its messages. A special field in the token indicates whether it is free or busy. The token is passed from one site to the adjacent site around the ring in one direction. A site that has a message ready for transmission must wait until the token reaches it and it is free. When it receives the free token, it sets it to busy, attaches its message to the token, and transmits it to the next site in the ring. A receiving site checks the status of the token. If it is free, it uses it to transmit its own message. Otherwise, it checks to see if the message attached to the busy token is addressed to it. If it is, it retrieves the message attached to the token and forwards the token without the attached message to the next site in the ring. When the busy token returns to the sending site after one complete round, the site removes it from the ring, generates a new free token, and passes it to the next site, allowing the next site to transmit its message (if it has any).The free token circulates from one site to another until it reaches a site that has some message to transmit.

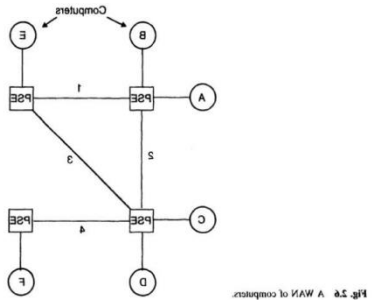
The Slotted-Ring

The Slotted-Ring Protocol :In this scheme, a constant number of fixed-length message slots continuously circulate around the ring. Each slot has two parts-control and data. The control part usually has fields to specify whether the slot is full or empty, the source and destination addresses of the message contained in a full slot, and whether the message in it was successfully received at the destination. On the other hand, the data part can contain a fixed-length message data.

1.10 WAN Technology

A WAN of computers is constructed by interconnecting computers that are separated by large distances; they may be located in different cities or even in different countries. In general, no fixed regular network topology is used for interconnecting the computers ofa WAN. Moreover, different communication media may be used for different links of a WAN.

The computers of a WAN are not connected directly to the communication channels but are connected to hardware devices can packet-switching exchanges (PSEs), which are special-purpose computers dedicated to the task of data communication.



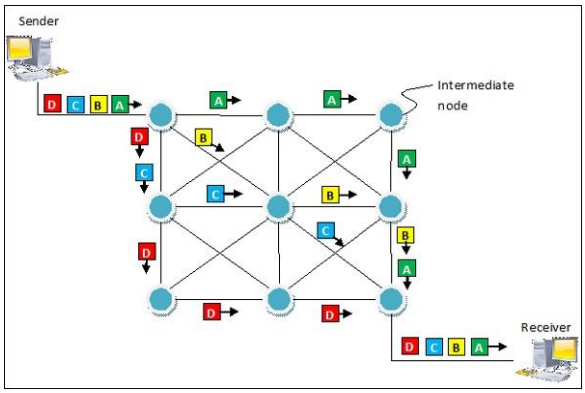
Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.

Process

Each packet in a packet switching technique has two parts: a header and a payload. The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination. The payload carries the actual data.

A packet is transmitted as soon as it is available in a node, based upon its header information. The packets of a message are not routed via the same path. So, the packets in the message arrives in the destination out of order. It is the responsibility of the destination to reorder the packets in order to retrieve the original message.

The process is diagrammatically represented in the following figure. Here the message comprises of four packets, A, B, C and D, which may follow different routes from the sender to the receiver.



Advantages

- Delay in delivery of packets is less, since packets are sent as soon as they are available.
- Switching devices don't require massive storage, since they don't have to store the entire messages before forwarding them to the next node.
- Data delivery can continue even if some parts of the network faces link failure. Packets can be routed via other paths.
- It allows simultaneous usage of the same channel by multiple users.
- It ensures better bandwidth usage as a number of packets from multiple sources can be transferred via the same link.

Disadvantages

- They are unsuitable for applications that cannot afford delays in communication like high quality voice calls.
- Packet switching high installation costs.
- They require complex protocols for delivery.

Circuit switching is a connection-oriented network switching technique. Here, a dedicated route is established between the source and the destination and the entire message is transferred through it.

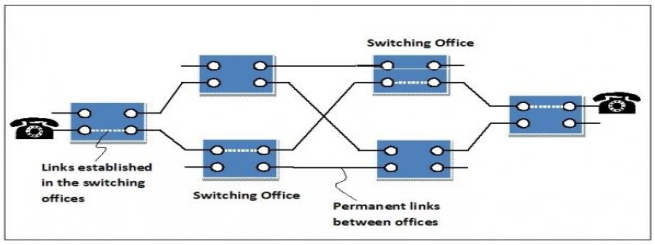
Phases of Circuit Switch Connection

- **Circuit Establishment** : In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centres. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.
- **Data Transfer** : Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate.
- **Circuit Disconnection** : When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all intermediate links from the sender to the receiver.

Diagrammatic Representation of Circuit Switching in Telephone

The following diagram represents circuit established between two telephones connected by circuit switched connection. The blue boxes represent the switching offices and their connection with other switching offices. The black lines connecting the switching offices represents the permanent link

between the offices. When a connection is requested, links are established within the switching offices as denoted by white dotted lines, in a manner so that a dedicated circuit is established between the communicating parties. The links remains as long as communication continues.



Advantages

- It is suitable for long continuous transmission, since a continuous transmission route is established, that remains throughout the conversation.
- The dedicated path ensures a steady data rate of communication.
- No intermediate delays are found once the circuit is established. So, they are suitable for real time communication of both voice and data transmission.

Disadvantages

- Circuit switching establishes a dedicated connection between the end parties. This dedicated connection cannot be used for transmitting any other data, even if the data load is very low.
- Bandwidth requirement is high even in cases of low data volume.
- There is underutilization of system resources. Once resources are allocated to a particular connection, they cannot be used for other connections.
- Time required to establish connection may be high.

1.11 Communication protocols

What is a Protocol?

A protocol is a set of rules that governs the communications between computers on a network. In order for two computers to talk to each other, they must be speaking the same language. Many different types of network protocols and standards are required to ensure that your computer (no matter which operating system, network card, or application you are using) can communicate with another computer located on the next desk or half-way around the world. The OSI (Open Systems Interconnection) Reference Model defines seven layers of networking protocols.

What is OSI Model?

The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. The Open System Interconnection (OSI Model) also defines a logical network and effectively describes computer packet transfer by using various layers of protocols.

Characteristics of OSI Model

Here are some important characteristics of the OSI model:

A layer should only be created where the definite levels of abstraction are needed. The function of each layer should be selected as per the internationally standardized protocols.

The number of layers should be large so that separate functions should not be put in the same layer. At the same time, it should be small enough so that architecture doesn't become very complicated.

In the OSI model, each layer relies on the next lower layer to perform primitive functions. Every level should able to provide services to the next higher layer

Changes made in one layer should not need changes in other lavers.

Upper and Lower layers further divide network architecture into seven different layers as below

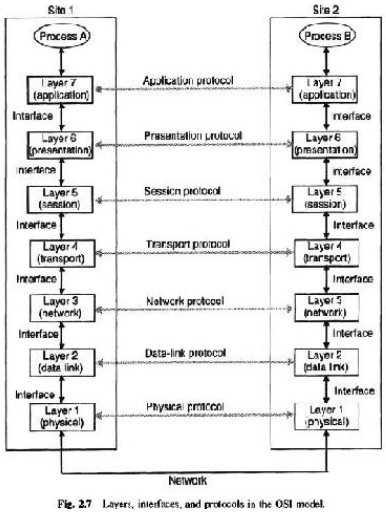


Fig. 2.7 Layers, interfaces, and protocols in the OSI model.

Layers	Protocols at each layer
Application	FTP, TFTP, TELNET, SMTP, DNS, others
Transport	TCP, UDP
Network	IP, ICMP
Data link	ARP, RARP, others
Physical	SLIP, Ethernet, Token Ring, others

Physical Layer

The physical layer helps you to define the electrical and physical specifications of the data connection. This level establishes the relationship between a device and a physical transmission medium. The physical layer is not concerned with protocols or other such higher-layer items.

Examples of hardware in the physical layer are network adapters, ethernet, repeaters, networking hubs, etc.

Data Link Layer:

Data link layer corrects errors which can occur at the physical layer. The layer allows you to define the protocol to establish and terminates a connection between two connected network devices.
It is IP address understandable layer, which helps you to define logical addressing so that any endpoint should be identified.
The layer also helps you implement routing of packets through a network. It helps you to define the best path, which allows you to take data from the source to the destination.
The data link layer is subdivided into two types of sublayers:
Media Access Control (MAC) layer- It is responsible for controlling how device in a network gain access to medium and permits to transmit data.
Logical link control layer- This layer is responsible for identity and encapsulating network-layer protocols and allows you to find the error.
Important Functions of Datalink Layer:
Framing which divides the data from Network layer into frames.
Allows you to add header to the frame to define the physical address of the source and the destination machine

Adds Logical addresses of the sender and receivers
It is also responsible for the sourcing process to the destination process delivery of the entire message.
It also offers a system for error control in which it detects retransmits damage or lost frames.
Datalink layer also provides a mechanism to transmit data over independent networks which are linked together.

Transport Layer:

The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or desegmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

Important functions of Transport Layers:

It divides the message received from the session layer into segments and numbers them to make a sequence. Transport layer makes sure that the message is delivered to the correct process on the destination machine. It also makes sure that the entire message arrives without any error else it should be retransmitted.

Network Layer:

The network layer provides the functional and procedural means of transferring variable length data sequences from one node to another connected in “different networks”.
Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.
Layer-management protocols that belong to the network layer are:
routing protocols
multicast group management
network-layer address assignment.

Session Layer

Session Layer controls the dialogues between computers. It helps you to establish starting and terminating the connections between the local and remote application.

This layer request for a logical connection which should be established on end user’s requirement. This layer handles all the important log-on or password validation.

Session layer offers services like dialog discipline, which can be duplex or half-duplex. It is mostly implemented in application environments that use remote procedure calls.

Important function of Session Layer:

It establishes, maintains, and ends a session.

Session layer enables two systems to enter into a dialog

It also allows a process to add a checkpoint to steam of data.

Presentation Layer

Presentation layer allows you to define the form in which the data is to exchange between the two communicating entities. It also helps you to handles data compression and data encryption.
This layer transforms data into the form which is accepted by the application. It also formats and encrypts data which should be sent across all the networks. This layer is also known as a syntax layer.
The function of Presentation Layers:
Character code translation from ASCII to EBCDIC.
Data compression: Allows to reduce the number of bits that needs to be transmitted on the network.
Data encryption: Helps you to encrypt data for security purposes — for example, password encryption.
It provides a user interface and support for services like email and file transfer.

Application Layer
Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means OSI application layer allows users to interact with other software application.
Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.
Example of the application layer is an application such as file transfer, email, remote login, etc.
The function of the Application Layers are:

Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
It allows users to log on to a remote host
This layer provides various e-mail services
This application offers distributed database sources and access for global information about various objects and services.

1.12 Internetworking

Internetworking stands for connectivity and communication between two or more networks.
- Internetwork (internet): a collection of communication networks interconnected by
Bridges , switches and/or routers.
- Intranet: a corporate internet that provides key Internet applications. It is usually
  Isolated and self-contained within an organization.
- End System (ES): a device attached to one of the networks.
- Intermediate System (IS): a device that connects two or more networks (e.g., switch, router). It is called sometimes an IWU (Internetworking Unit) or a relay.

Requirements for Internetworking
The overall requirements for an internetworking facility are:
1. Provide a link between networks. At minimum, a physical and link control connection is needed.
2. Provide for the routing and delivery of data between processes on different networks.
3. Provide an accounting service that keeps track of the use of the various networks and routers and maintains status information.
4. Provide the services just listed without requiring modifications to the networking architecture of constituent networks. This means accommodating the following differences:

o Different addressing schemes: e.g., naming (DNS), DHCP.
o Different maximum packet size: e.g., segmentation, ATM cells.
o Different network access mechanisms: e.g., Ethernet, FDDI, ATM.
o Different timeouts: longer with multiple networks.
Different error recovery services: some networks will have it, others won't. Internetwork error recovery should be independent of individual networks.
o Different status reporting: how and whether this information can be shared.
o Different routing techniques: may depend on fault detection and congestion control techniques. Coordination is needed.
o Different user access control: authorization for use of the network.
o Connection-oriented vs. connectionless

Components of an Internetwork

- Campus Network: locally connected users in a building or group of buildings. It generally uses LAN technologies.
- Wide Area Networks (WANs): distant campuses connected together usually through Connection providers such as a telephone company.
- Remote connections: linking branch offices and mobile users to a corporate campus.
They are generally dial-up links or low bandwidth dedicated WAN links.

Internetworking Devices

Repeaters (Hubs)

• Overcomes restrictions caused by single segment usage such as number of users, cablelength.
• Amplifies or regenerates weak signals.
• Extends cable length.
• Connects LANs of similar type, but may use different media.
• Provides simple connection between adjacent LANs at the expense of increased networkcongestion.

The bridge

The bridge was designed for interconnection of LANs that use identical protocols at the MAClayer (i.e., layer
2). However, there are bridges capable of mapping between different MACprotocols (e.g., Ethernet and Token Ring).
Characteristics of bridges
• Interconnects two or more LANs (either similar or dissimilar) at the MAC level (e.g.,Ethernet and Token Ring)
• Capable of deciding whether or not to forward a frame.
• Creates an extended network and keeps local traffic off.
• Can make minor changes to frame header.
• Does not inspect or modify the network layer packets inside frames.
Reasons for using bridges
• Reliability: fault is limited to the network where it happened.
• Performance: intra-network traffic stays within one network.
• Security: Types of traffic with different security needs are kept on physically separate media.
• Geography: LANs may need to be on separate locations.

Routers

Bridges do not stop broadcast traffic. This can lead to broadcast storms (e.g., more than 100 nonunicast frames/sec) which can be catastrophic. This can bring the network down.
Some sources of broadcast traffic:
• Address resolution (e.g., ARP, RARP, BOOTP)
• RIP (Routing Information Protocol)
• DHCP (Dynamic Host Configuration Protocol)

• IPX (Internet Packet eXchange) generates broadcast traffic to advertise servicesand routes
• Netware clients rely on broadcast to find services
• Appletalk: Route discovery protocol
To contain/reduce broadcast traffic, we need to reduce the size of the network (i.e., LAN).
Two approaches are used to do this:
• Use routers to subnet the LAN
• Use VLANs (Virtual LANs)
Characteristics
• A router separates traffic of different networks. It does not flood packets.
• Routers route packets at the network layer (layer 3)
• Routers route packets based on the contents of a routing table.
• Routing tables contain a mapping of a destination to a port. They can be static ordynamic.
• Routers "learn" their routing table entries by communicating with their routing peers.
• Routing protocols are used to implement routing (RIP, OSPF, BGP, PNNI)
• Routers perform routing decisions on the basis of the Network ID part of the destination

Switches
Switching combines advanced microprocessor technology with the concept of a layer-2 bridge.
Whatever we have said about bridges apply to switches (i.e., a switch is a bridge is a switch).
Sometime the difference between a bridge and a switch is looked at as a marketing distinctionrather than a technical one.
A switch has bridge's functionality:
¾ Learning (generally dynamic)
¾ Address table (forwarding table) including timers.
¾ Flooding when destination is unknown.
It can be said that a switch is a high-speed multi-port bridge. A large switch can have more than100 interfaces.
Brouters and Gateways
¾ Brouters: another name for layer-3 switches.
¾ Gateways: more complex as they interface between two dissimilar networks (operates above layer-3). They are necessary when two networks do not share the same network layer protocol.

1.13 ATM and ATM Networks

ATM stands for Asynchronous Transfer Mode. It is a switching technique that uses time division multiplexing (TDM) for data communications.

ATM networks are connection oriented networks for cell relay that supports voice, video and data communications. It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium.

Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.
- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

Feature

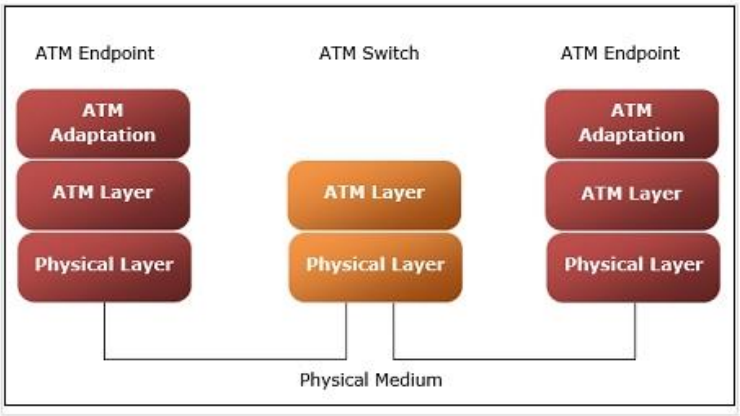
- It is scalable and flexible. It can support megabit-to-gigabit transfer speeds and is not tied to a specific physical medium.

- It efficiently transmits video, audio, and data through the implementation of several adaptation layers.
- Bandwidth can be allocated as needed, lessening the impact on and by high-bandwidth users.
- It transmits data in fixed-length packets, called cells, each of which is 53 bytes long, containing 48 bytes of payload and 5 bytes of header.
- It is asynchronous in the sense that although cells are relayed synchronously, particular users need not send data at regular intervals.
- It is connection oriented, using a virtual circuit to transmit cells that share the same source and destination over the same route.

Working of ATM:

ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consists of Virtual channel connections (VCCs) bundled together which is a basic unit carrying single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not routs the cells to a particular virtual circuit. In case of major failure all cells belonging to a particular virtual path are routed the same way through ATM network, thus helping in faster recovery.

- Switches connected to subscribers uses both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. It's basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.



ATM reference model comprises of three layers

- **Physical Layer –** This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.
- **ATM Layer –**This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.
- **ATM Adaptation Layer (AAL) –**This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers – Convergence sub layer and Segmentation and Reassembly sub layer.

- **ATM endpoints –** It contains ATM network interface adaptor. Examples of endpoints are workstations, routers, CODECs, LAN switches, etc.
- **ATM switch –**It transmits cells through the ATM networks. It accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI), updates cell header and retransmits cell towards destination.