VEERASHAIVA VIDYAVARDHAKA SANGHA'S

RAO BAHADHUR Y. MAHABALESHWARAPPA ENGINEERING COLLEGE,BALLARI
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ACCREDITED BY NATIONAL BOARD OF ACCREDITATION

Course Name : - **Network Management System**

Course Code : - **10CS834**

Sem : - **VIII**

Academic Year : - **2017-18**

Unit- 1

Introduction

Staff Name: PAMPAPATHI B M	**Semester: VIII**	**Sec: B**
Course Name: Network Management Systems	**Course Code: 10CS834**	**Total contact hours: 52**
Prerequisites: Basic Knowledge of networks ,topology, Architecture , layers and functionality protocols used etc		

COURSE OUTCOMES 2017-18

Course Outcomes	Description
C403.1	Able to understand basic knowledge of computer , telecommunication networks and basic communication architecture
C403.2	Able to identify goals, challenges of network management architecture for LAN,MAN,WAN and protocols used
C403.3	Able to understand and analyze NMS
C403.4	Ability to solve problem related to network management and applications.

CO-PO/PSO MAPPING

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
C403.1	3												3	
C403.2		3							2				3	
C403.3		3											3	
C403.4			3					1					3	
AVERAGE	3	3	3					1	2				3	

***Note:** - 1.Slight (Low) 2.Modarate (Medium) 3.Substantial (High)

Course Name : - **Network Management System**

Course Code : - **10CS834**

UNIT – 1

Introduction: Analogy of Telephone Network Management, Data and Telecommunication Network Distributed computing Environments, TCP/IP- Based Networks: The Internet and Intranets, Communications Protocols and Standards- Communication Architectures, Protocol Layers and Services; Case Histories of Networking and Management – The Importance of topology , Filtering Does Not Reduce Load on Node, Some Common Network Problems; Challenges of Information Technology Managers, Network Management: Goals, Organization, and Functions- Goal of Network Management, Network Provisioning, Network Operations and the NOC, Network Installation and Maintenance; Network and System Management, Network Management System platform, Current Status and Future of Network Management.

Unit - 1

INTRODUCTION

Network Management System: A Network Management System(NMS) is a combination of hardware and software used to monitor and administer a network.

1.1 Analogy Of Telephone Network Management

- The need for data or computer communication management is best illustrated by an analogy of telephone network management.
- The characteristics of a telephone network includes;
    a. *Reliable***-** because does what is expected of it.
    b. *Dependable***-** because always connect when we need it.
    c. *Good Quality*- we can have a conversation across the world with the same clarity that we have when we call our neighbors.
- The reason being for reliable, dependable and good quality telephone network is *good planning, design, implementation and management of network*.
- The analogy of telephone network is very well explained by the following model

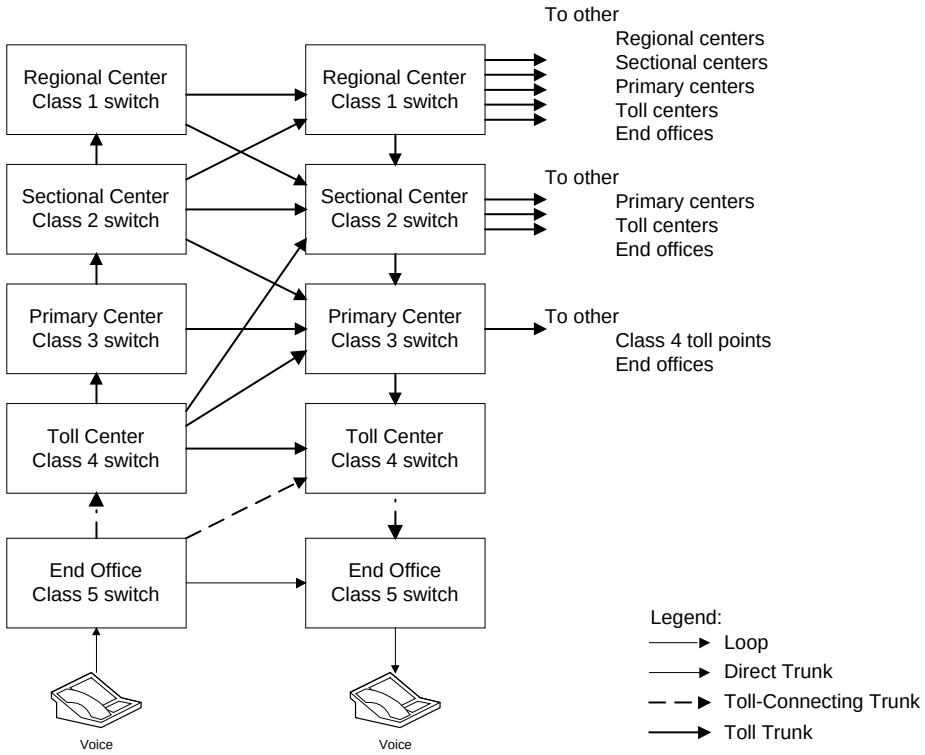


Figure 1.1 Telephone Network Model

- From the above figure 1.1 it is clear that there are *5 levels of switches and 3 types of trunks* connecting these switches.
- Trunk is a logical link between two switches that may traverse one or more physical link.
- The end office(class 5), which is lowest in the hierarchy, is the local switching office. The customer's telephone or the Private Branch Exchange(PBX) is connected to the end office via a dedicated link called "loop".
- The other four levels of switches (class 4 through class 1) are tandem or toll switches carrying toll(long distance) calls.
- From the local class 5 office to the called party's class 5 office, there are multiple routers.
- A circuit connection is set up directly using a local trunk or via higher-level switches and routers.
- Primary and secondary routers are already programmed into the switches. If the primary route is broken or facilities over the primary route are filled to capacity, an alternate route is automatically assigned.
- To ensure the quality of service in a telephone network, operations support systems are implemented. They constantly monitor the various parameters of the network.
- The quality of the call is measured in terms of signal-to-noise(S/N) ratio, is measured by a trunk maintenance system. This system accesses all the trunks in an office during the night and does a loop-back test to far end.
- For a given region, there is a network operation center(NOC) where the global status of the network is monitored.
- The NOC is the nerve center of telephone network operations.
- Telephone network is managed from the user's perspective, and not from that of the system or service provider.
- However, with emphasis on the user's point of view, first objective in operation is restoration of service and then the quality and economy of service.
- To manage a network remotely, i.e., to monitor and control network components from a central location, network management functions need to be built into the components of the network as much as possible.

1.2 Data (Computer) and Telecommunication network

- A basic network can be viewed as interconnected nodes and links as shown in below figure 1.2,

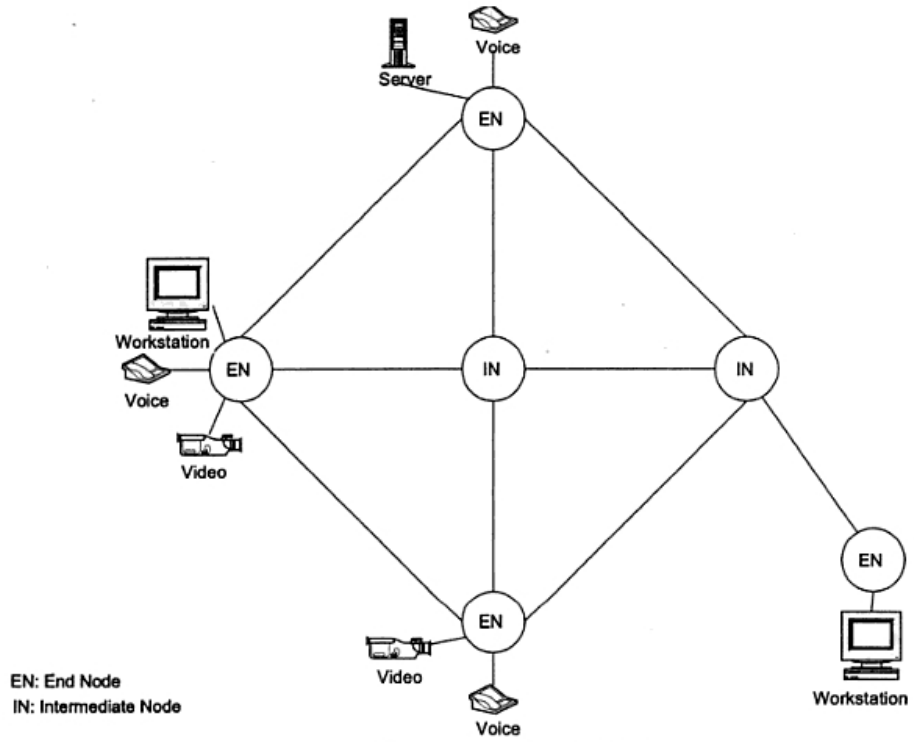


Figure 1.2 Logical Network Model

- A ***link*** carries information from one node to another that is directly connected to it.
- A ***node*** behaves as an end node or an intermediate node or both. If the node behaves as an *end node*, information either *originates or terminates* there.
- An ***intermediate*** node redirects the information from one link to another.
- Data can be transmitted in an analog or digital format.
- The analog data are sent either as a baseband(e.g., voice data from the switching office to the customer premises) or on top of a carrier(e.g., cable TV).
- Digital data are either directly generated by the user equipment (e.g., computer terminal) or as analog data and are converted to digital data (e.g., Integrated Service Digital Network(ISDN) connection to customer premises).
- Data are sent from originating to terminating node via a direct link or via a tandem of links and intermediate nodes.

- Data can be transmitted in one of the 3 modes;
  - ✓ **Circuit switched,**
  - ✓ **Message switched and**
  - ✓ **Packet switched.**

❖ **Circuit switching:**

- There is a dedicated communication path between two stations ***(end-to-end)***
- The path is a connected sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection.

❖ **Message switching:**

- With message switching there is no need to establish a dedicated path between two stations.
- When a station sends a message, the ***destination address is appended to the message.***
- The message is then transmitted through the network, in its entirety, ***from node to node.***

❖ **Packet switching:**

- In packet switching methods, a message is broken into small parts, called ***packets.***
- Each packet is tagged with appropriate ***source and destination addresses.***

Difference between message and packet switching is;

- ✓ In the message switching, data are *stored by the system and then retrieved by the user at a later time* (e.g., email).
- ✓ In the packet switching mode, packets are *fragmented and reassembled in almost real time*.

- Network communications are commonly classified as either data communications or telecommunications.
- The telephone network, which came into existence first, was known as a telecommunication network. The organization that provides this service is called a telecommunication service provider (e.g. AT&T, BSNL etc).
- With the advent of computers, the terminology data communication network came into picture. It is also called computer communication network.
- The following figure shows an early configuration of terminal-to-host and host-to-host communications, and how data and telecommunication networks interface with each other.

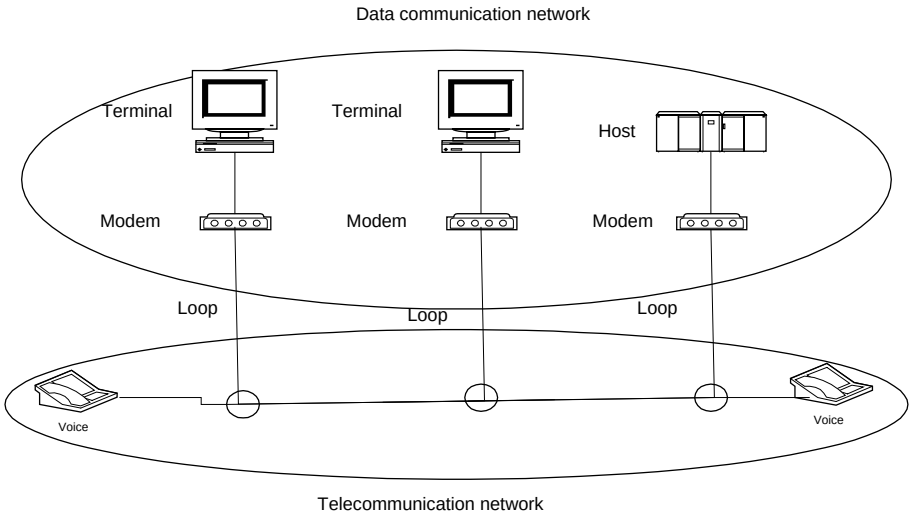


Figure 1.3 Data and Telecommunication Networks

- To interface, a terminal or host connected to an end office switch communicates with the host connected to another end-office switch by modems at each end.
- Modems transfer information from digital to analog at the source and back to digital at the destination.
- Modern telecommunication networks carry digital data.
- The following figure 1.4 shows a corporate or enterprise environment in the stage of the evolution of data and telephone communication.
- Analog signals from telephones are converted to digital signals either at the customer premises or central office.

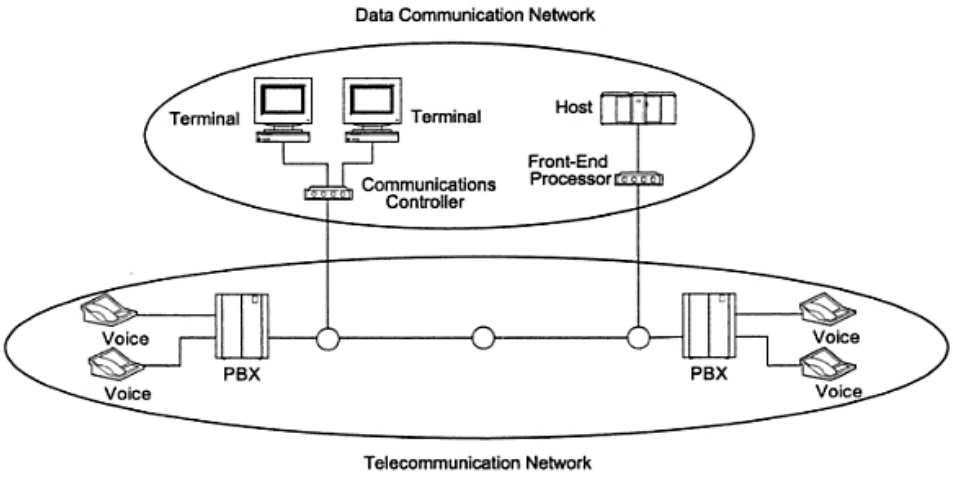


Figure 1.4 Digital Data and Telecommunication Networks

- A number of telephones and computer terminals at various corporate sites are connected by a local switch, PBX, at the customer premises, which interfaces digitally to the telephone network.
- The computer terminals are connected to a communication controller, such as a digital multiplexer, which provides a single interface to the telephone network.
- The IBM ***System Network Architecture (SNA)*** is a major step in network architecture; following figure 1.5 shows the IBM SNA structure.

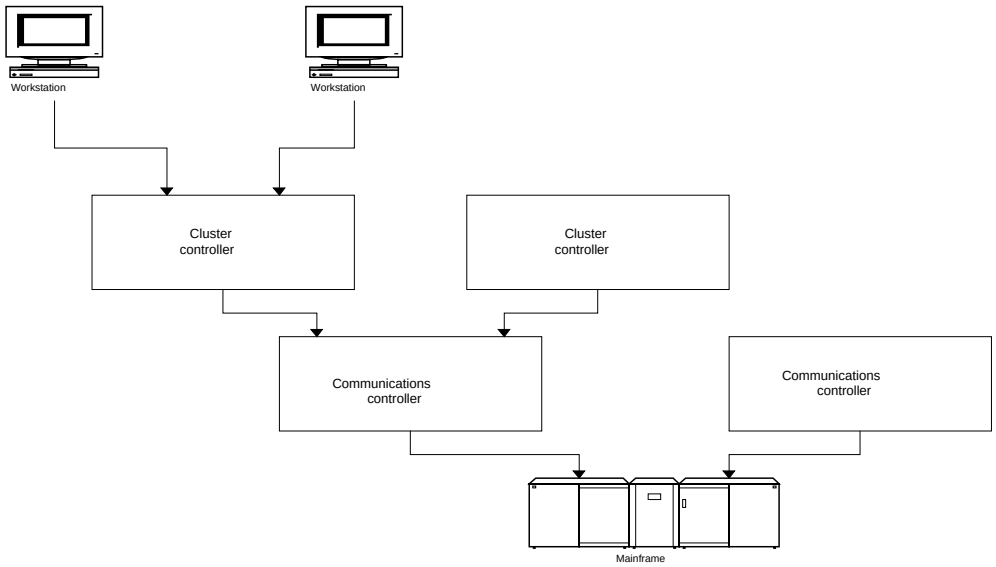


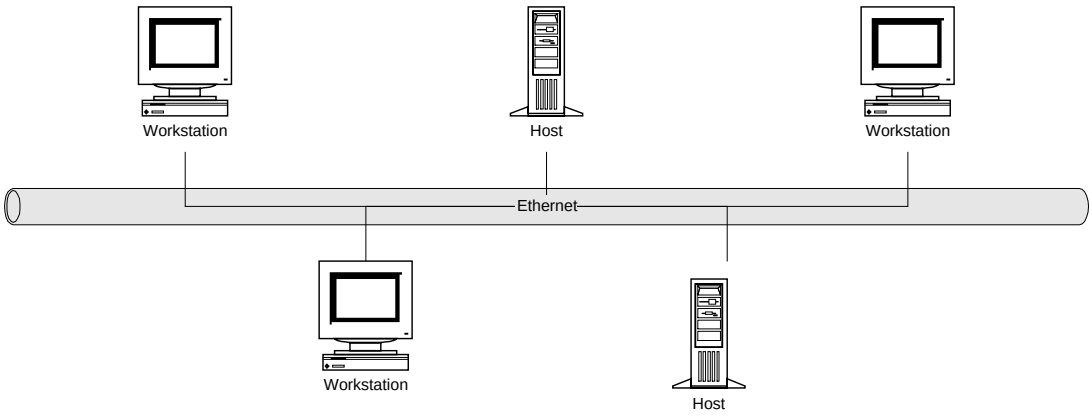
Figure 1.5 IBM Systems Network Architecture Model

- SNA is based on multitude of (dumb) terminals accessing a mainframe host at a remote location.

1.3 Distributed Computing Environment

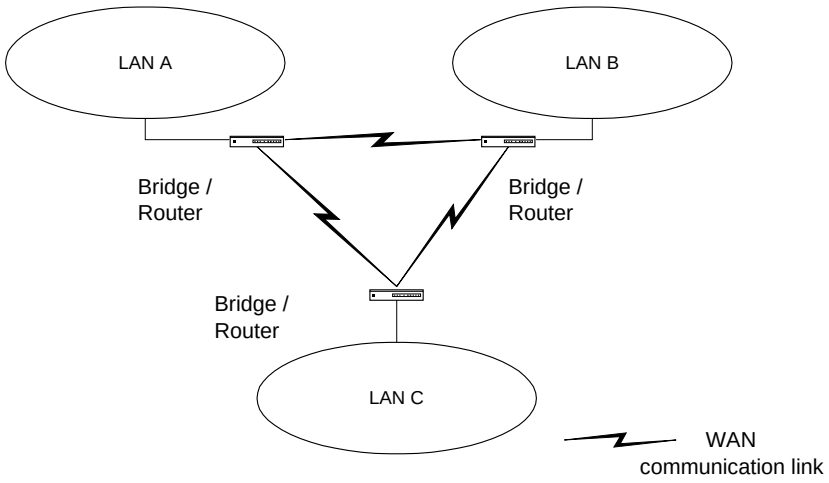
a. DCE with LAN & WAN Networks

- Following figure (a) shows a LAN with hosts and workstations.
- These workstations have a processing power rather than just acting as dump terminals.
- Any workstation can communicate with any host on the LAN. LANs that are geographically far apart can communicate via telecommunication network, either public or private switched.
- The system of links connecting remote LANs are called a WAN.



(a) Hosts and Workstations on Local LAN

- A LAN is physically connected to a WAN by a bridge or a router as shown in figure (b)



- **(b) Remote LANs Interconnected by WAN**

- In the early stage of communication network evolution, different platforms and applications running on DCE were implemented by telecommunication service

provider and computer vendors to communicate autonomously within each of their network.

- However, the telecommunication industry rapidly grew, national and international standards needed to establish for communication between equipment providers by various vendors.
- As a result *customer premises equipment(CPE)* interface, specifications are published to interface cleanly with the network.
- Thus no more monopolistic service provider is required in LAN-WAN networks.
- Also the ability of processors attached to LANs do multiple functions.

b. Client/Server Model

- The simple client/server model is as shown in below figure 1.7

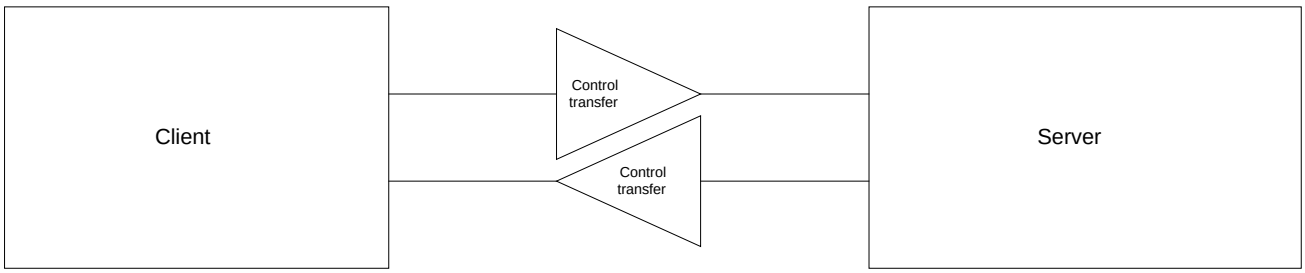


Figure 1.7 Simple Client-Server Model

- The process that initiates a transaction to run an application in either a local or a remote processor is called the **client**.
- The application process that is invoked by a client process is called the **server.** The server returns the results to the client.
- The client initiates a request to the server and waits. The server executes the process to provide the requested service and sends the results to the client.
- Note that *client cannot initiate a process in the server unless the process have already been started in the server and be waiting for requests to be processed.*
- A real-world analogy to the client-server operation is a post office. The clerk (acts as a server) behind the counter is ready and waiting for a client.
- When a customer (acts as a client) walks in and initiates a transaction the clerk responds.

- Once the clerk responds and processes the customer request, the customer leaves and the clerk, as a server goes into waiting mode until next client initiates the transaction.
- The server may be providing the service to many clients that are connected to it on a LAN, as shown in below figure 1.8

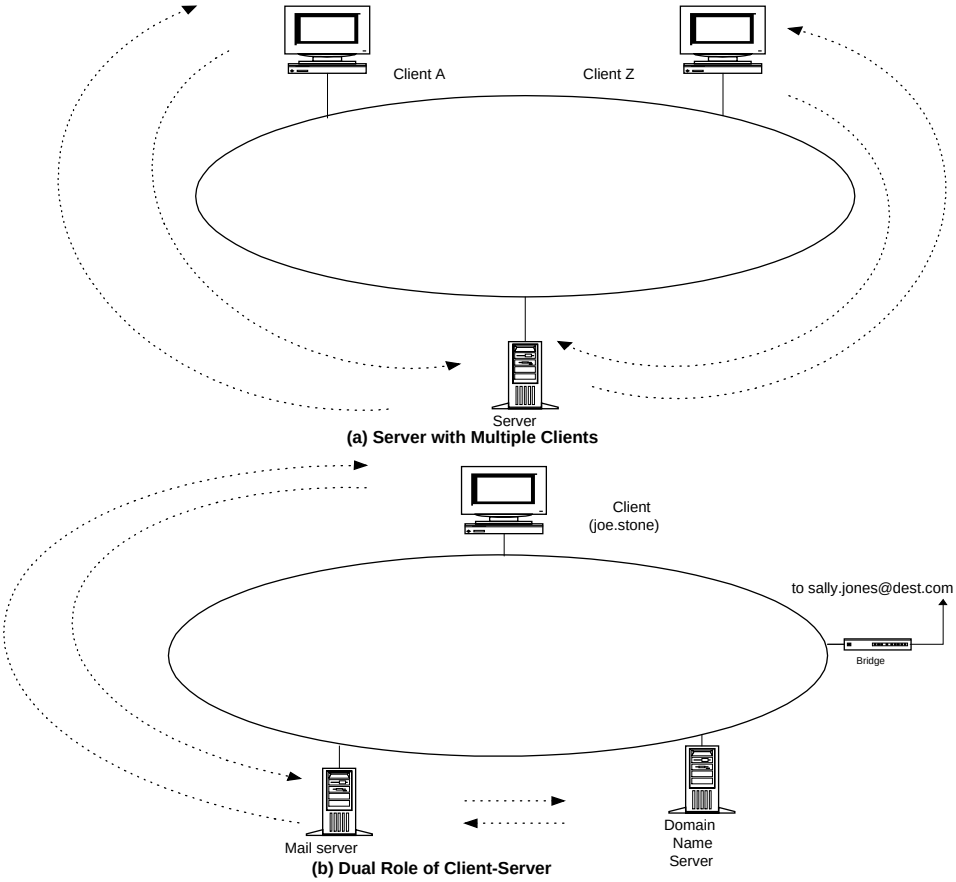


Figure 1.8 Client-Server in Distributed Computing Environment

- Each clients request is processed by a server according to the **FIFO rule**.
- The *delay could be minimized but not eliminated, by concurrent processing of the requests by the server.*
- Since the client and the server are processes running in a DCE, each of them can be designed to execute a specific function efficiently.
- As an example which is shown in figure 1.8(b), joe.stone@source.com using client in a network sends a message to sally.jones@dest.com on the network
- The message first goes to the mail server on the network.

- Before it can process the request, the mail server needs to know the network address of sally.jones, which is dest.com. Thus, it makes a request to *domain name server (DNS).*
- When it receives the information of address dest.com, the message sent by joe.stone is delivered to sally.jones via the bridge.
- Later a message is sent to joe.stone on the client stating that the message has been sent (or not sent, in failure conditions)
- The three processes in this scenario, namely the client, the mail server and the DNS, are cooperatively computing processes. Communication between these processes is called peer-to-peer communication.

1.4 TCP/IP-Based Networks: Internet and Intranet

- Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of protocols that enable networks to be connected.
- Nodes in the network route packets using network protocol, IP, a connectionless protocol. That means there is no guarantee that the packet will be delivered to the destination node.
- However, end-to-end communication can be guaranteed by using transport protocol, TCP.
- Thus, if packet is lost by IP, the acknowledgement process of TCP ensures successful retransmission of the packets.
- The internet is network of networks. Just as telecommunication network using telephone to communicate, we can also use computer network to communicate via email.
- Consider the example and visualize that Joe Stone is sending an email to Sally Jones at her home in Australia.
- Similar to unique telephone number, each person has a unique address in the computer communication network.
- Joe's email address is joe@cc.gatech.edu and Sally's address is sally@ostrich.com.au.

- Following figure1.9 shows the internet configuration for our scenario

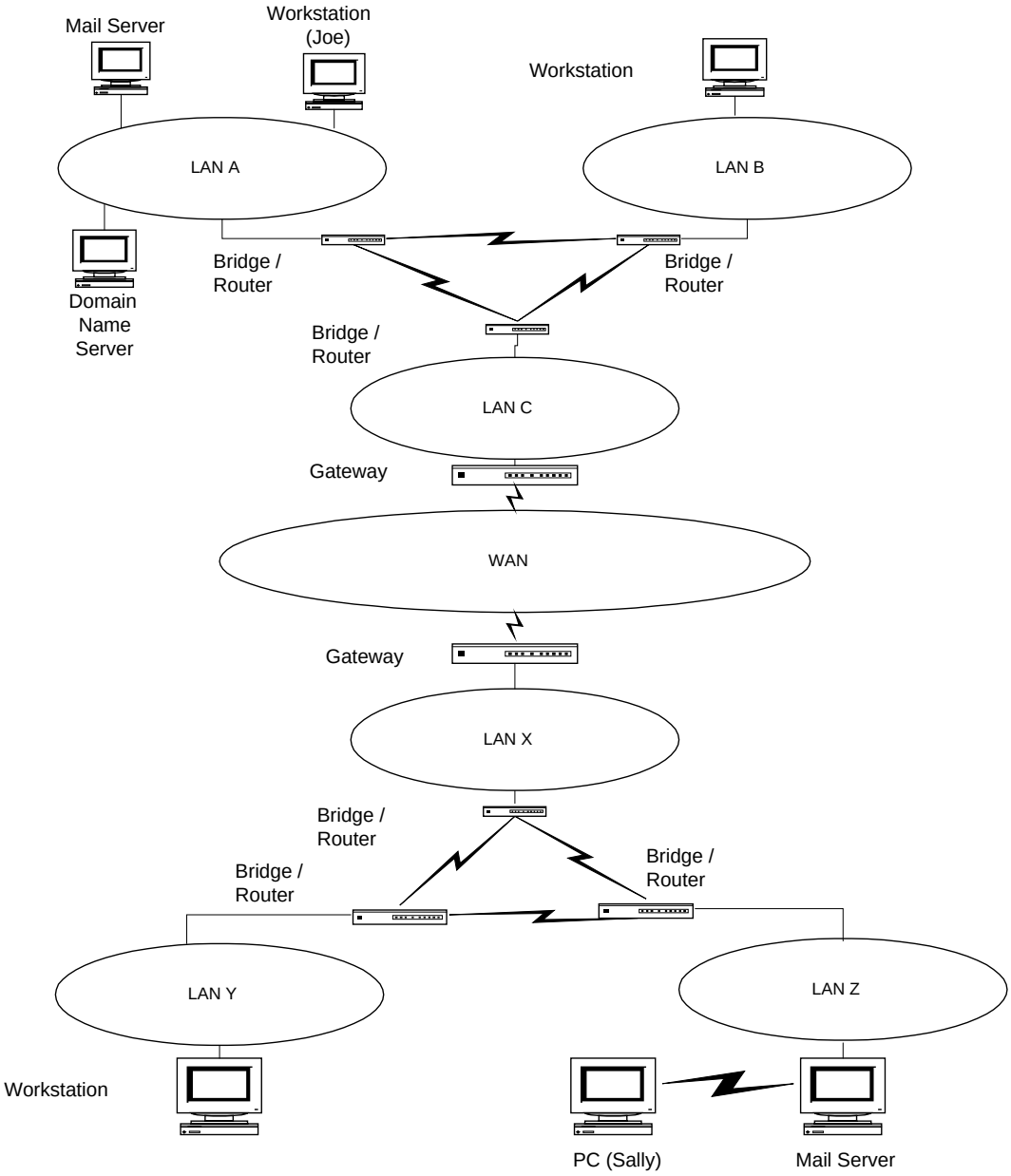


Figure 1.9 Internet Configuration

- Joe is at workstation A on LAN A sending the email to sally at workstation Z that is 'teleconnected' to her internet service provider's email server on LAN Z.
- Two servers shown on LAN A are mail server and DNS. Note that the servers need not be on the same LAN as the senders LAN, as shown above.
- The servers transmit email message to LAN C on computer network made up of bridges and routers. The link between LAN A and LAN C could be WAN.

- Information from LAN C progresses via gateways and WANs to the computer networks in Australia as shown in figure.
- Gateways between them serve as the interfaces between dissimilar and independent autonomous networks and perform many functions including protocol conversions.
- Joe's email finally reaches the email server on LAN Z in Australia and is stored there until Sally retrieves it via her internet link with an internet service provider's server.
- In fact email message are transmitted by a "store-and-forward" scheme all along the path. In addition, the final stage in the internet link uses a TCP/IP suite of protocols.
- Thus, via the internet, any user can communicate with any other user in any part of the world as long as both are connected to an Internet.

1.4.1 Internet Fabric Model/Layered Architecture of Internet:

- Internet can be visualized as a layered architecture, as shown in figure 1.9
- This architecture shows ***global Internet*** as concentric layers of workstations, LANs and WANs interconnected by fabrics of *Medium Access Control (MAC), switches and gateways.*
- **Workstations** belong to the user plane, LANs to LAN plane and WANs to WAN plane.
- The interfaces are defined as ***fabrics.*** *MAC fabric interfaces* the user plane to LAN plane.
- *LAN and WAN plane* interface through switching fabric. WANs in the WAN plane interface with each other via gateway fabric.
- Each WAN may be considered as an autonomous network and hence needs a *gateway* to communicate with another WAN.
- The physical path traverses the MAC fabric, the LAN plane, the switching fabric, the WAN planes and the gateway fabric to the core and then returns to the user plane going through all the planes and interface fabrics in reverse.

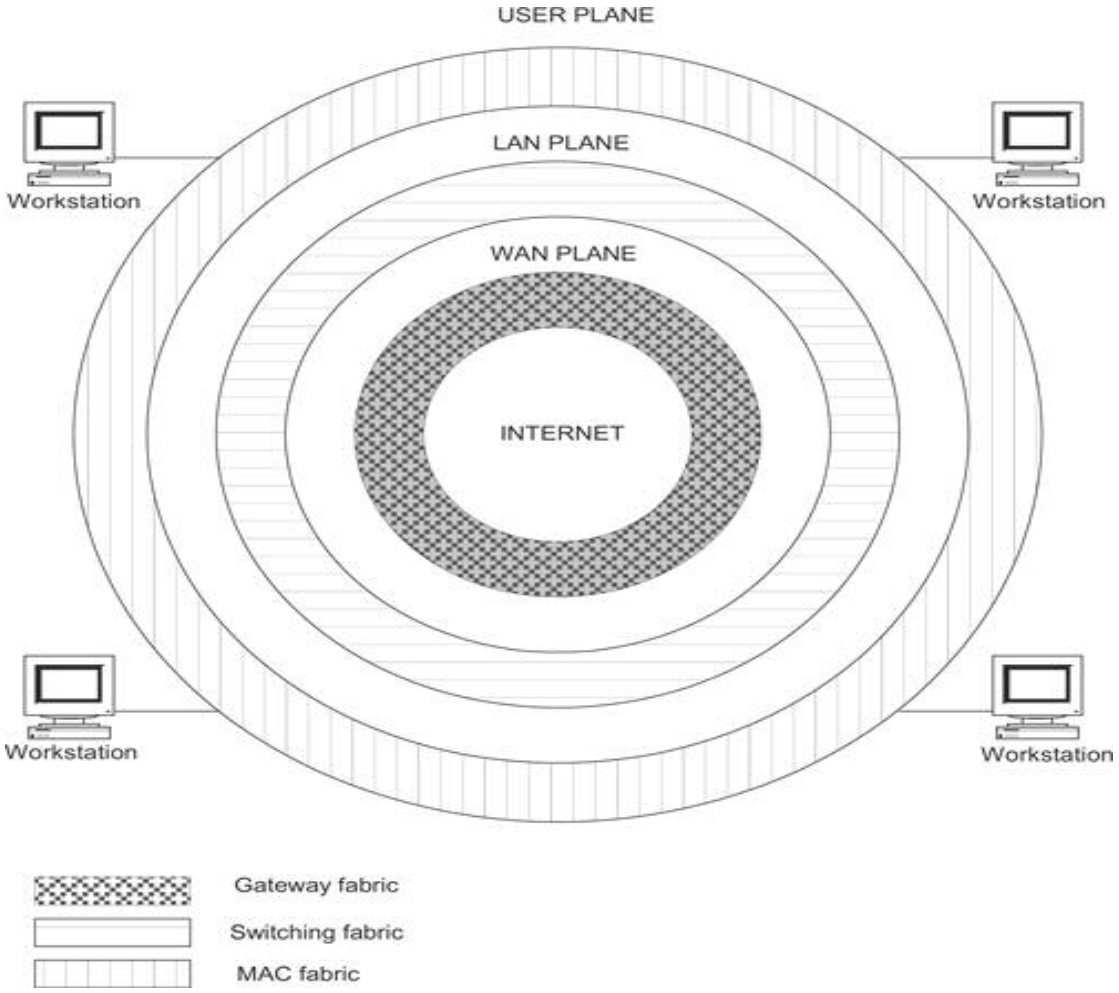


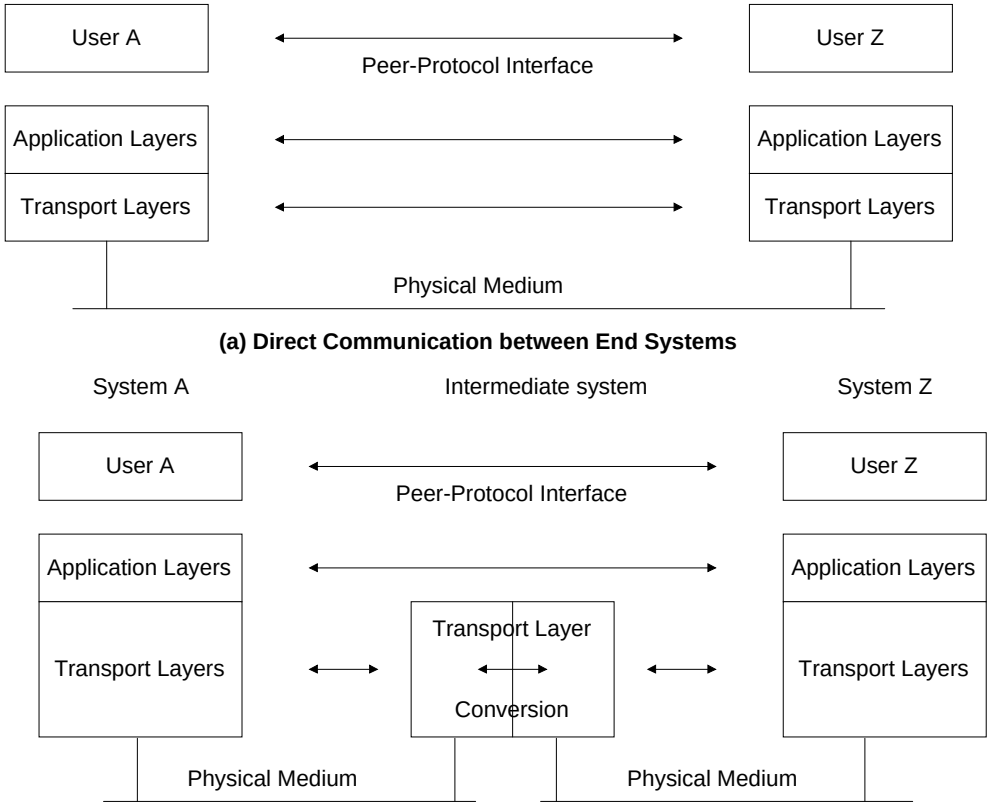
Figure 1.10. Internet Fabric Model

1.5 Communication Protocols and Standards

- The importance of communication protocols and standards can be explained with the aid of following example.
- Suppose that a fax machine and a modem brought from a local store successfully sending to a modem and fax machine anywhere in the world, even though each fax machine and attached modem were manufactured by local vendors.
- It is a miracle that two computers located anywhere in the world can transmit messages to each other as long as each is connected to internet.
- The key to the practical success of these and other such technologies is the interoperability of two end devices.
- Universal interoperability is achieved when all participants agree to establish common operational procedures.
- In communication lingo, commonality can be interpreted as standards and procedures as protocols.
- The communication can happen without any loss or error due to standardization and modular (layered) architecture of data communication protocols.
- Architecture can be defined as modeling a system into functional components and relationship among them.

1.5.1 Communication Architecture

- Communication between users and application occurs at various levels.
- They can communicate with each other at application level, the highest level of communication architecture.
- Alternatively they can exchange information at the lowest level, the physical medium.
- Each system can be subdivided into two sets of communication layers. The top set of layer consists of application layers and the bottom set transport layers.
- The users and users include application programs interface with the application level layer and the communication equipment interfaces with the physical medium.
- The basic communication architecture is as shown in below figure 1.11(a)



(a) Direct Communication between End Systems

(b) Communication between End Systems via an Intermediate System

Figure 1.11 Basic Communication Architecture

- In figure 1.11(a), the two end systems associated with the two end nodes communicate directly with each other.
- *Direct communication* occurs between the corresponding cooperating layers of each system.
- Thus, transport layers can exchange information with each other, and so can the application layers and the users.
- Figure 1.11(b) shows the end systems communicating via *intermediate system,* which enables the use of different physical media for two end systems.

- Various standard organizations propose, deliberate and establish standards.
- One of the international renowned standard organizations is *International Standard Organization (ISO).*
- ISO has developed highly modular or layered architecture for communication protocols that is called the ***Open System Interconnections (OSI)*** reference model.
- The OSI protocol architecture with all seven layers is shown in below figure 1.12

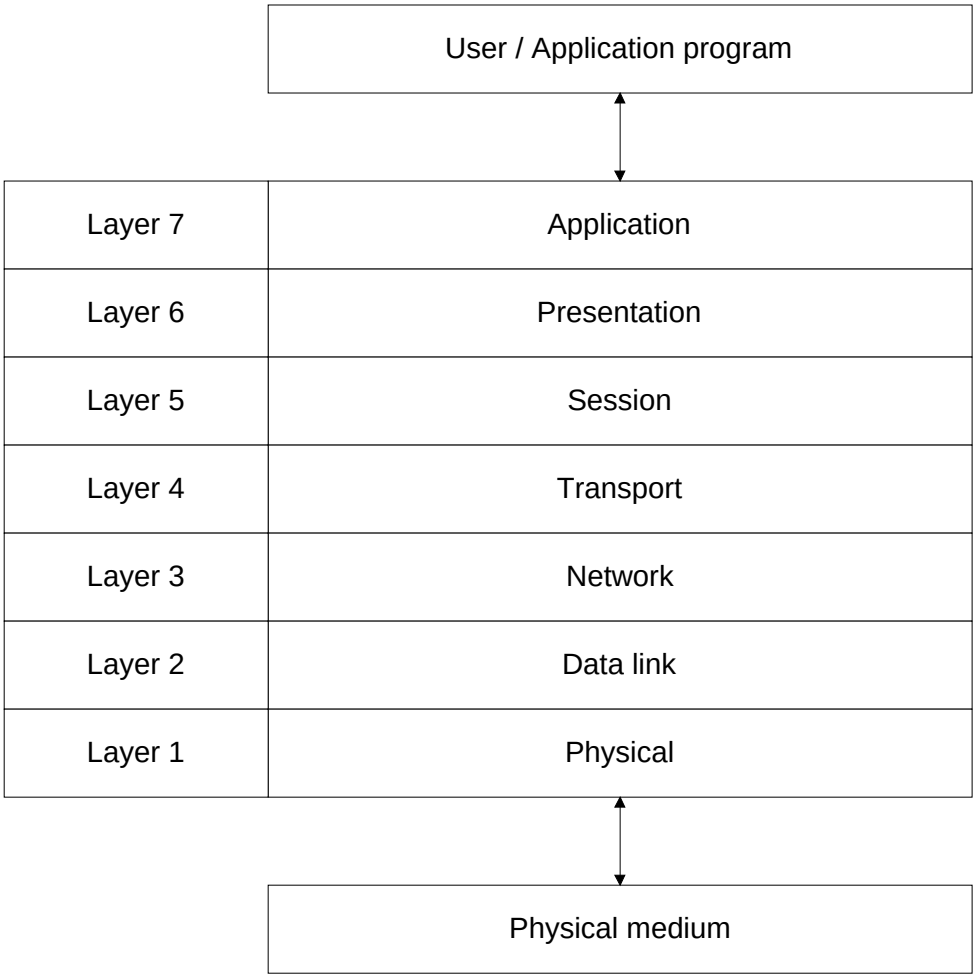


Figure 1.12 OSI Protocol Layers

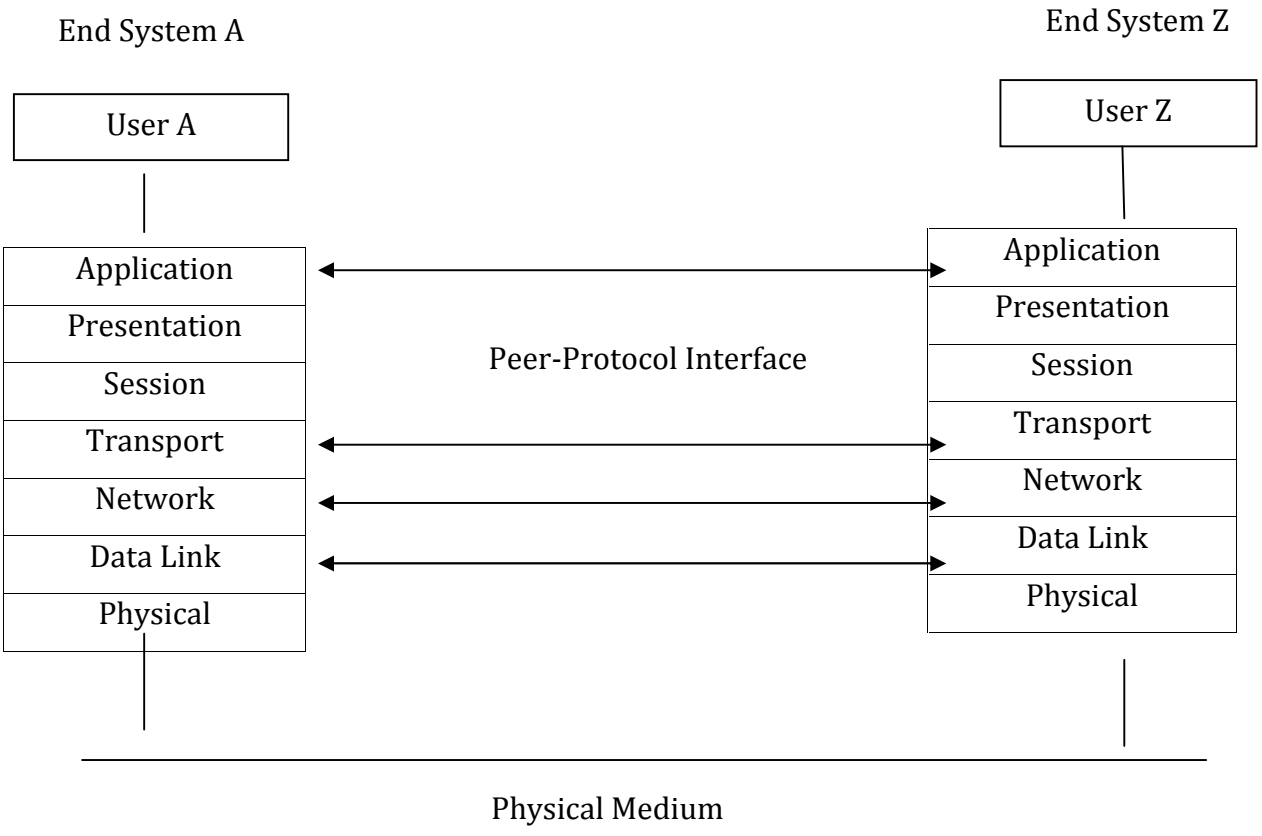
1.5.2 Protocol Layers and Services

- The salient features and services provided by each layer are as mentioned in the following table.
- **Layers 1-4** are the *transport system protocols layers* and **layers 5-7** are *application support protocol layers.*

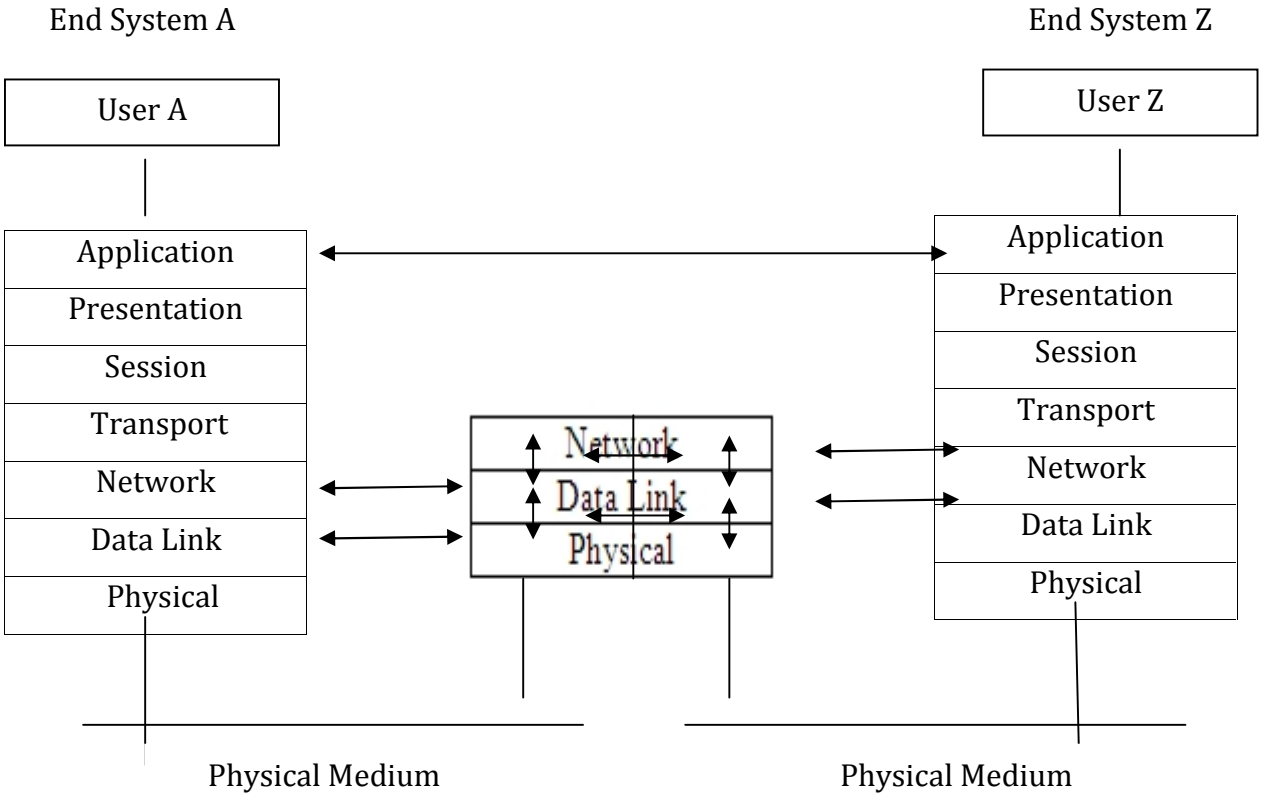
Layer No.	Layer Name	Salient services provided by the layer
1	Physical	-Transfers to and gathers from the physical medium raw bit data -Handles physical and electrical interfaces to the transmission medium
2	Data link	-Consists of two sublayers: Logical link control (LLC) and Media access control (MAC) -LLC: Formats the data to go on the medium; performs error control and flow control -MAC: Controls data transfer to and from LAN; resolves conflicts with other data on LAN
3	Network	Forms the switching / routing layer of the network
4	Transport	-Multiplexing and de-multiplexing of messages from applications -Acts as a transparent layer to applications and thus isolates them from the transport system layers -Makes and breaks connections for connection-oriented communications -Flow control of data in both directions
5	Session	-Establishes and clears sessions for applications, and thus minimizes loss of data during large data exchange
6	Presentation	-Provides a set of standard protocols so that the display would be transparent to syntax of the application -Data encryption and decryption
7	Application	-Provides application specific protocols for each specific application and each specific transport protocol system

Table 1.1 OSI Layers and Services

- The following figures expand the basic communication architecture to an OSI model, which is as shown as below.
- Figure 1.13(a) is a ***direct end to end communication model.***
- In figure 1.13(b), the ***end systems communicate with each other by going through an intermediate node/system.***
- Note that the intermediate system is involved only up to the *first three layers in the process.*
- **Layers 4-7** are not involved in the intermediate systems.



(a) Direct Communication Between End Systems



(b) Communication Between End Systems Via Intermediate Systems

Figure 1.13 OSI Communication Architecture

1.5.3 PDU communication model between end systems.

- The users message moving in each layer is contained in message units called protocol data units (PDU).
- PDU contains two parts- Protocol Control Information (PCI) and User Data (UD).
- PCI contains header information about the layer. UD contains the data that the layer acting as a service provider, receives from or transmits to the upper layer/service user layer.
- The PDU communication model between two systems A and Z, including user at the top and the transmission medium at the bottom of the PDU layers is as shown below,

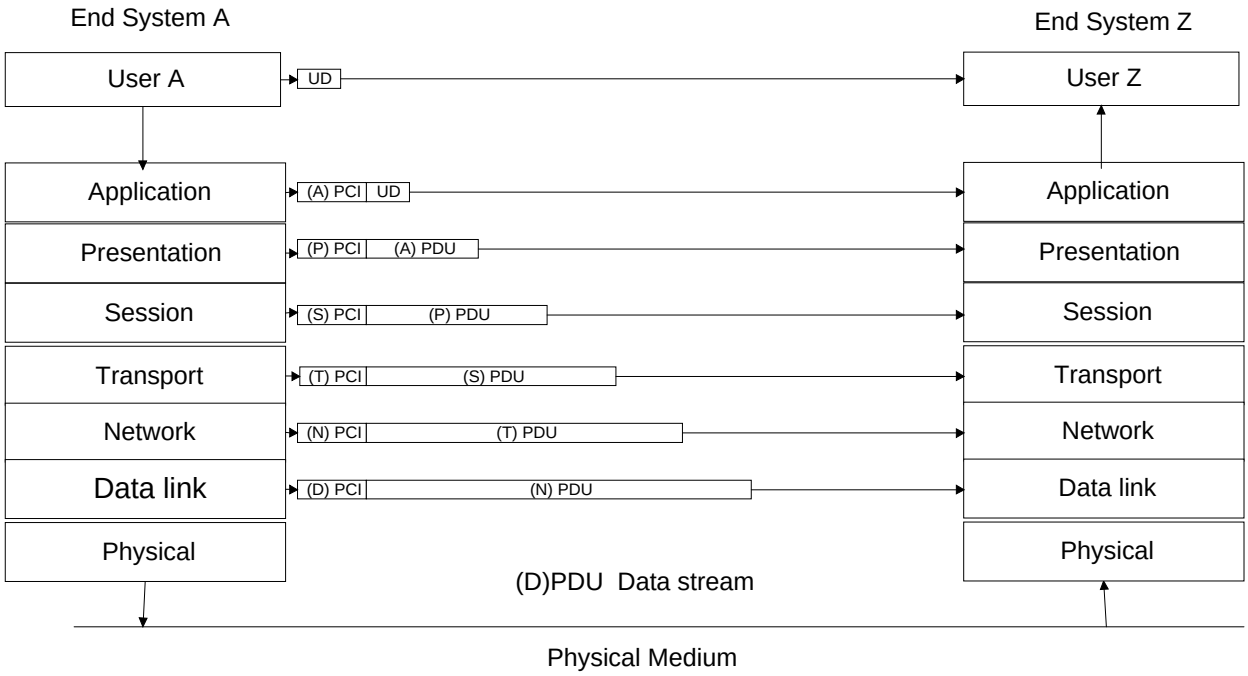


Figure 1.14 PDU Communication Model between End Systems

- Notice that the size of the PDU increases as it goes towards lower layers.
- If the size of PDU exceeds the maximum size of any layer specification, it is then fragmented into multiple packets.
- Thus, a single application layer PDU could multiply into several physical PDUs.

1.5.4 Sub layer structure of Data Link Layer

- In an OSI-layered model the data link layer is divided into two sub layers- Logical Link Control (LLC) and Media Access Control (MAC) as shown below in figure 1.15
- The ***lower MAC layer*** controls the *access and transmission of data to physical layer in an algorithmic manner.*

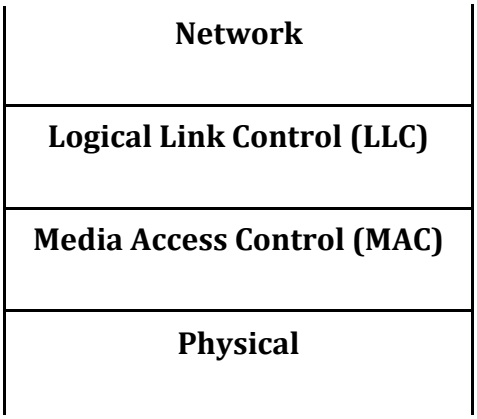


Fig 1.15 Sub layer structure of Data Link Layer

- There are three types of LANs
  - ✓ **Ethernet LAN** is a bus type and the media is accessed using a distributed probabilistic algorithm, Carrier Sensing Multiple Access with Collision Detection (CSMA/CD).
  - ✓ **A Ring Type LAN** used in Token Ring (TR) and Fiber Distributed Data Interface (FDDI).
  - ✓ **Wireless LAN or WLAN** is the third type of LAN, the probabilistic algorithm, Carrier Sensing Medium Access with Collision Avoidance (CSMA/CA) is used to access the medium.
- ***Logical Link Control (LLC)*** performs *link management and data transfer.*
- Link management includes formatting data to go on to the medium, performing error control and flow control.
- If there is security required, it could be included in the LLC sublayer.

1.5.5 Sub layer structure of Network protocol layer

- The network layer is the third layer in the OSI protocol stack. It controls and manages the switching fabric of the network.
- The network layer provides both ***connectionless network service (CLNS)*** and ***connection-oriented network service (CONS).***

- CLNS is used when lower layers are *highly reliable, such as LANs and bridges, as well as when the message are short.*
- CONS are the method for transmitting long messages, *such as file transfer. It is also used when transmission medium is not reliable.*
- The destination address of each packet is read in both *CLNS and CONS* at the network layer and routed on the appropriate link.
- *A router or routing bridge* at the nodes of a network performs the function of routing and switching data.
- The OSI architectural model divides the network layer into three sub layers as shown in below figure 1.16

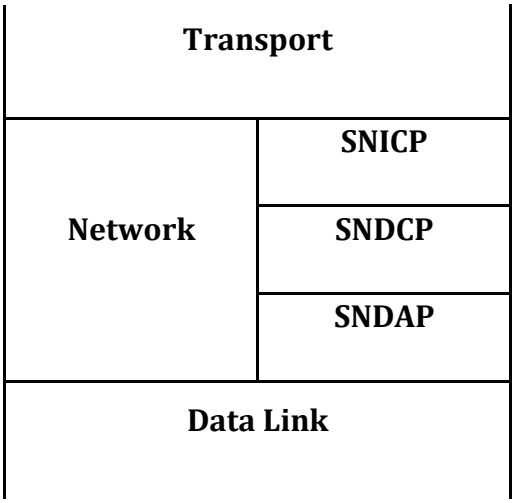


Figure 1.16 : Sublayer Structure of a Network Protocol Layer

SNICP: Subnetwork-Independent Convergence Protocol

SNDCP: Subnetwork-Dependent Convergence Protocol

SNDAP: Subnetwork-Dependent Adapter Protocol

- The top sublayer is subnetwork-Independent Convergence Protocol (SNICP) layer that *interfaces to the transport layer.*
- The internet communicates between nodes using *internet address and SNICP.*
- The nodes in turn communicate with subnetworkss using the subnetwork-*Dependent Convergence Protocol (SNDCP),* which depends on the subnetwork protocols and could be any proprietary protocol.

- The SNDCP communicates with its *Data link layer* via the third network sublayers, *Subnetwork-Dependent Access Protocol (SNDAP).*

1.5.6 Comparison of OSI and Internet Protocol Layer Model

- Following figure 1.17 shows the comparison of OSI and Internet model

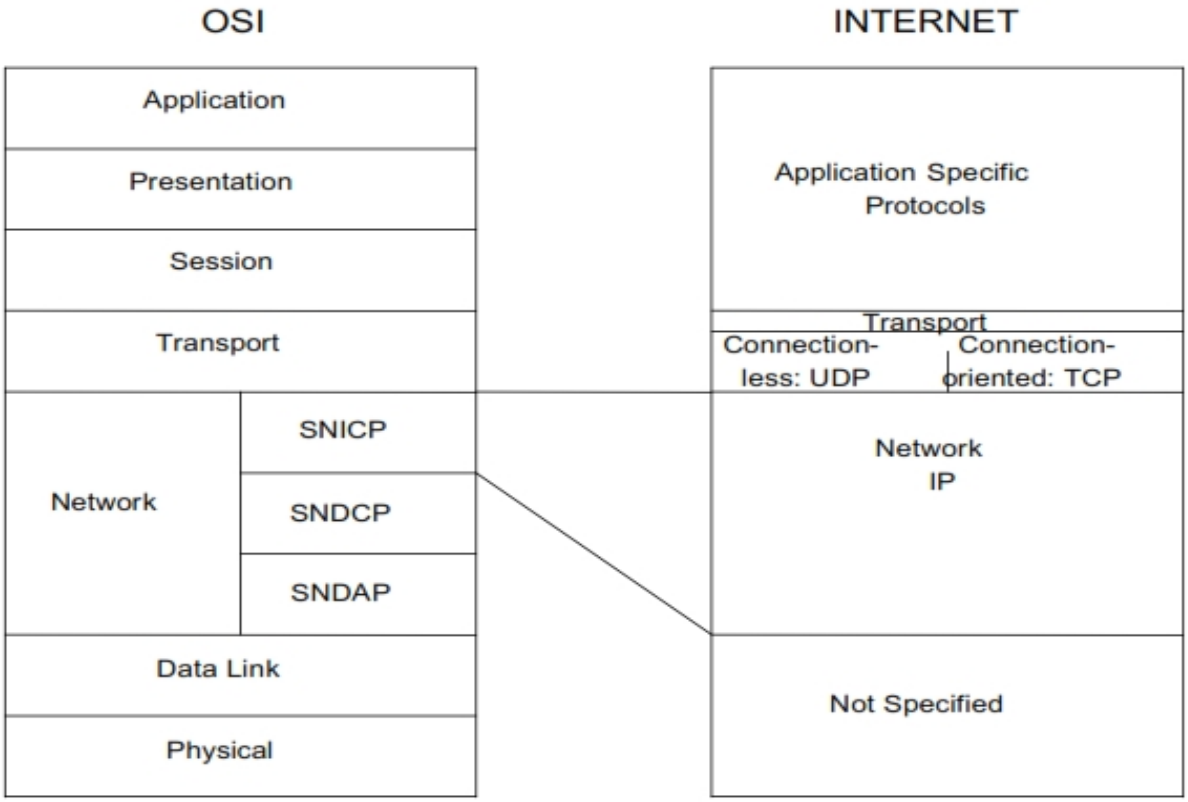


Fig 1.17 Comparison of OSI and Internet Protocol Layer Model

- Following figure 1.18 shows a comparison of four application-specific protocols in OSI and Internet models.

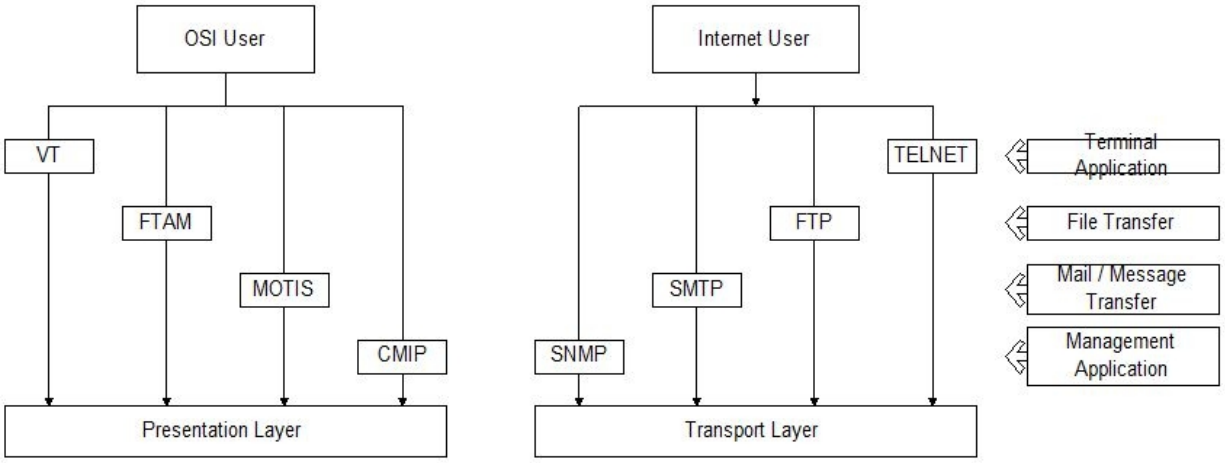


Fig 1.18 application-specific protocols in OSI and Internet models

- All application-specific protocol services in OSI are sandwiched between *user and presentation layers.*
- In Internet mode, they are sandwiched between user and transport layers.
- The boxes on the right hand side of figure 1.18 describe the comparable services offered in two layers.
- A user interfaces with a host as a remote terminal using *Virtual Terminal (VT)* in the OSI model and *TELNET* in the Internet model.
- File transfers are accomplished using *File Transfer Access and Management (FTAM)* in the OSI model and *File Transfer Protocol (FTP)* in the Internet.
- The most common used mail service function in the Internet is *Simple Mail Transfer Protocol (SMTP),* similarly *Message-Oriented Text Interchange Standards (MOTIS)* in OSI model.
- Network Management is accomplished using the *Common Management Information Protocol (CMIP)* in the OSI model and *Simple Network Management Protocol (SNMP)* in the Internet.

	OSI Model	**Internet Model**
Location	Sandwiched between user and presentation layers.	Sandwiched between user and transport layers
User interfaces	A host as a remote terminal using **Virtual Terminal (VT)**	Accomplished using **TELNET .**
File transfers	Accomplished using **File Transfer Access and Management (FTAM)**	Accomplished using **File Transfer Protocol (FTP)**
Mail service function	**Message-Oriented Text Interchange Standards (MOTIS)**	**Simple Mail Transfer Protocol (SMTP**)
Network Management	Accomplished using the **Common Management Information Protocol (CMIP)**	using **Simple Network Management Protocol (SNMP)**

Table 1.2 Comparison of application-specific protocols in OSI and Internet models

1.6 Case Histories on Network, System and Service Management

1.6.1 Case Histroy1: Importance of Topology ("Case of Footprint")

- A stable corporate network consisting of several minicomputers and about 100 desktop workstations and personal computers started crashing frequently.
- A topology used in the corporate was old-fashioned serial topology.
- Lacking sophisticated NMS tools, Information Systems, person started walking the hallways asking the users if anyone had just been doing anything out of ordinary, which might have broken the chain and caused the problem.
- When reported with no one had done anything, the Vice President (VP) of Corporate started back the halls and peeked into each office.
- Finally, he stopped and said "Let's look up the ceiling here". We found a transceiver had been fooling with and was not properly connected, which had caused the break.
- Once connected, the network segment came back up.
- When asked to VP "Why did you say-try here?", he calmly pointed to a dusty image of a sneaker footprint on the engineer's desk and the ceiling tile that was ajar above the desk and said "you need to use all the diagnostic tools at your disposal".

1.6.2 Case History 2: Centrally Managed Network Issues

- *An Integrated network management system (INMS)* was integrating alarms for *multiple element management systems (EMSs)* in a service provider network.
- Each EMS manages a domain of network elements and passes the relevant events to the INMS as shown below figure 1.19

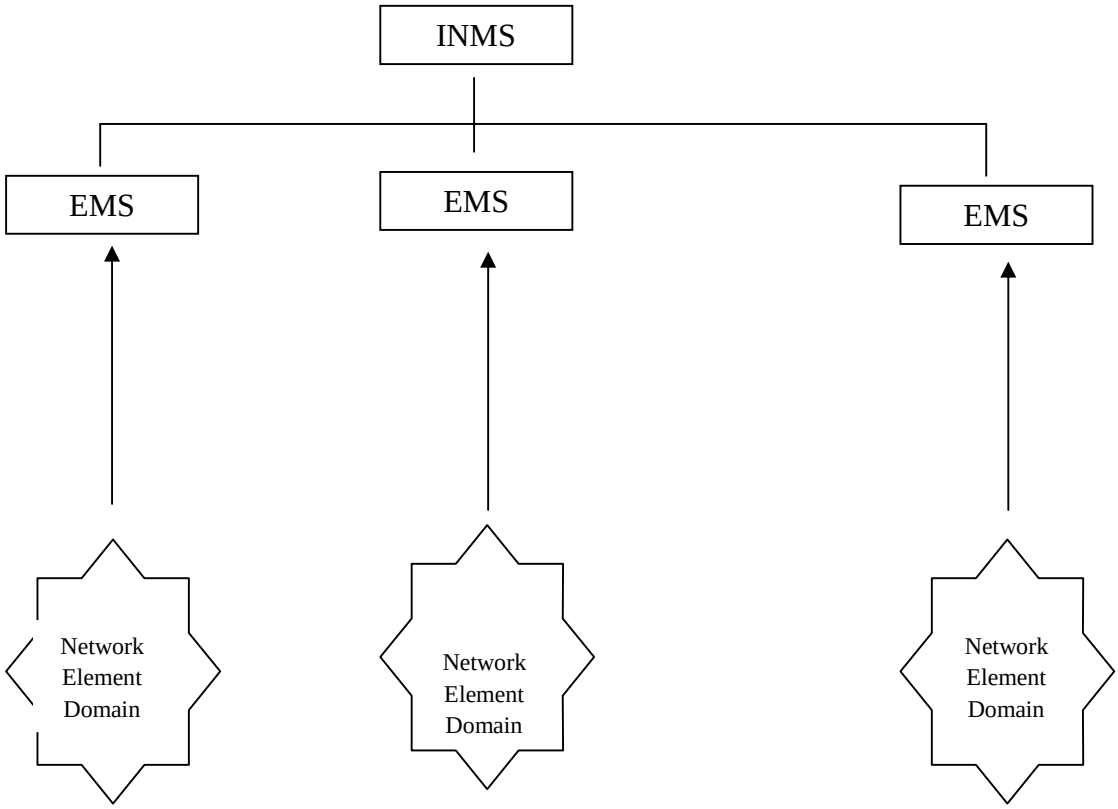


Fig 1.19: Case History 2: Centrally Managed Network Issues

- Each EMS records and displays the receipt time of the alarm. The same is transmitted to the INMS.
- It was observed that the indication of the time at which the alarm occurred was significantly different in INMS from that indicated in the EMSs that were sending the alarms.
- The alarm occurrence time was considerably delayed, sometimes by hours, in INMS.
- The challenge in a centrally managed network is to find the root cause of the problem.
- The predominant cause is the stress on NMSs, although it can be traced sometimes to network elements in the various domains.
- Transmission of unnecessary alarms also causes a stress on the network and networks have gone down due to uncontrolled generations of network management messages.

1.6.3 Some Common Network Problems

- The most common and serious problems in network are as mentioned below,
  1. Loss of Connectivity
  2. Duplicate IP address
  3. Intermittent problems
  4. Network configuration issues
  5. Non-problems
  6. Performance problems
- **Connectivity failures** are handled under the category of fault management. *Fault* is generally interpreted as *failures in accessing networks and systems by users.*
- **Network failure** is caused more often by a *node failure than failure of passive links.*
- **Network connectivity** is also based on the *IP address, which is a logical address assigned by the network administrator.*
- The IP address is uniquely associated with a physical MAC address of the network component. However, mistakes are made in assigning duplicate IP addresses.
- **Intermittent problems** could also occur *due to traffic overload causing packet loss*.
- *Power hits* could reset network component configuration, causing ***network failure***. The network has a permanent configuration (default) and a dynamic configuration (runt-time), and thus a power hit could change the configuration.
- There are few ***non-problems,*** which really mean that the cause of failure is a mystery. There is nothing else that a network manager could do except turn the system off and then on.
- ***Performance problem*** could also manifest as network delay and is more an annoyance to the network manager, who needs to separate network delay from the application program or application processes delay. Then the network manager has to convince the user and the person responsible for the application to rectify the situation.

1.8 Challenges of IT Managers

- Managing a corporate network is becoming harder as it becomes larger and more complex.
- IT managers face network administration and management problems day in and day out.
- Some of the challenges that IT managers face are as mentioned below.
  1. *Maintain reliability* in a data network as in a telephone network.
  2. *Designing, deploying and managing networks* that can handle real-time and non-real time data.
  3. *Networking with emerging technology* necessitates the need for continuing education.
  4. *Rapid advance of technology*.
  5. Manage *client-server environment* in converged networks.
  6. Providing *scalability of networks* in order to service a wide range of users.
  7. *Anticipate customer demands.*
- To manage such problems IT managers, make use of troubleshooting tools (e.g., sniffer, ping etc).
- Manages also need to predict the consequences of Troubleshooting.

1.9 Network Management: Goals, Organization and Functions

- Network Management can also defined as *Operations, Administration, Maintenance and Performance (OAMP) of network and services.*
- Figure 1.21 shows a top-down view of network management functions.
- It comprises three major groups:
  - *i. Network and service Provisioning,*
  - *ii. Network and service Operations, and*
  - *iii. Network I&M.*
- The network management functional flowchart is as shown in figure 1.22

i. Network Provisioning

- Network provisioning consists of network planning and design and is the responsibility of the Engineering group. The Engineering group keeps track of new technologies and introduces them as needed.

- What needed and when it is needed are determined from analysis of traffic and performance data provided by the network operations.
- New or modifications to network provisioning may also be initiated by management decision.

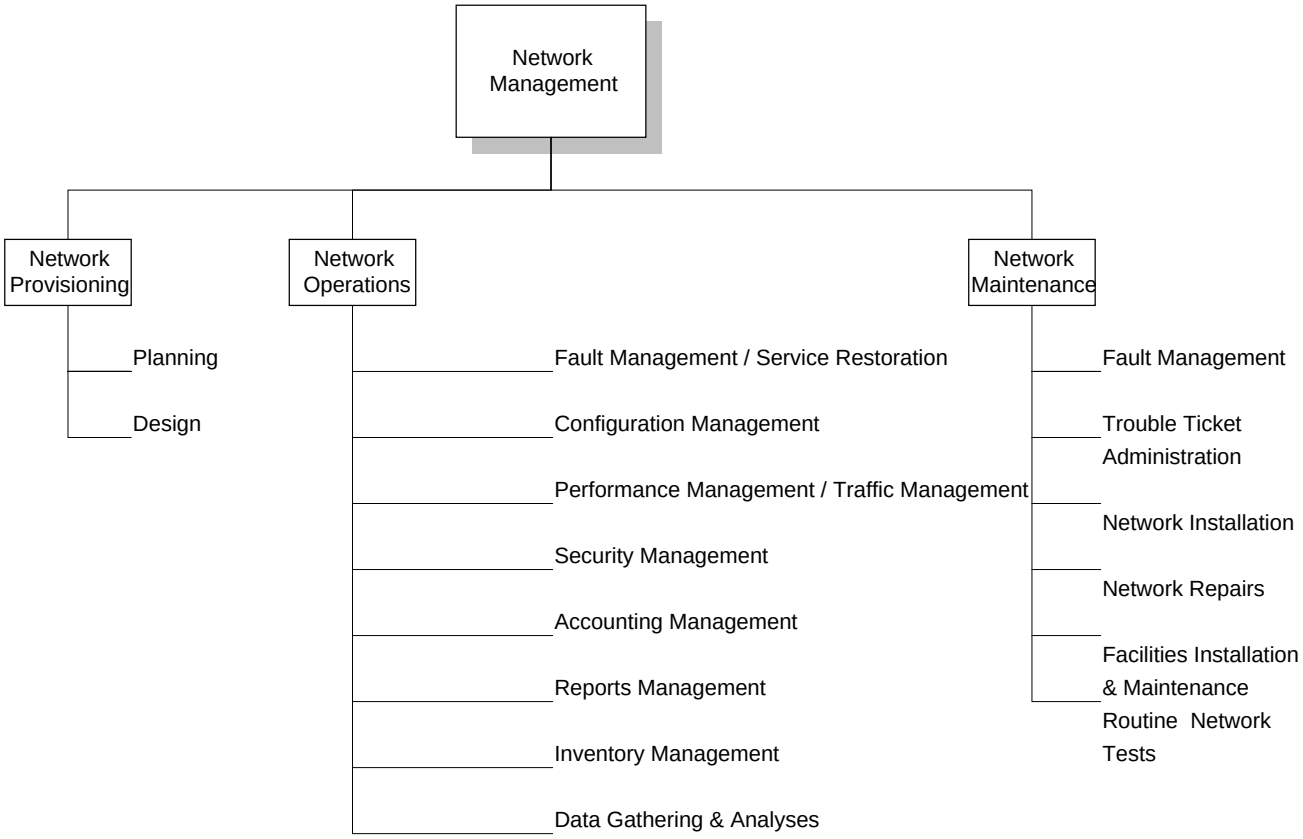


Figure 1.21 Network Management Functional Groupings

ii. Network Operations and NOC

- The functions of network operations listed in figure 1.21 are administered by the NOC.
- ISO has defined five OSI network management applications, which are fault, configuration, performance, security and accounting management.

Fault Management/Service Restoration:

- Whenever there is a service failure, it is NOC's responsibility to restore service as soon as possible.
- In several failure situations, the network will do this automatically. This network feature is called self-healing.
- In other situations, NMS can detect failure of components and indicate with appropriate alarms.

Configuration Management:

- There are three sets of configuration of the network. One is static configuration and is the permanent configuration of the network.
- The second is running configuration, which could be different from that of permanent configuration.
- The third configuration is planned configuration of the future when the configuration data will change as the network is changed.
- Any configuration changes needed in relieve temporary congestion in traffic are made by NOC and are reflected in the dynamic display at NOC.

Performance Management:

- Data need to be gathered by NOC and kept updated in a timely fashion in order to perform some of the functions, as well as tune the network for optimum performance.

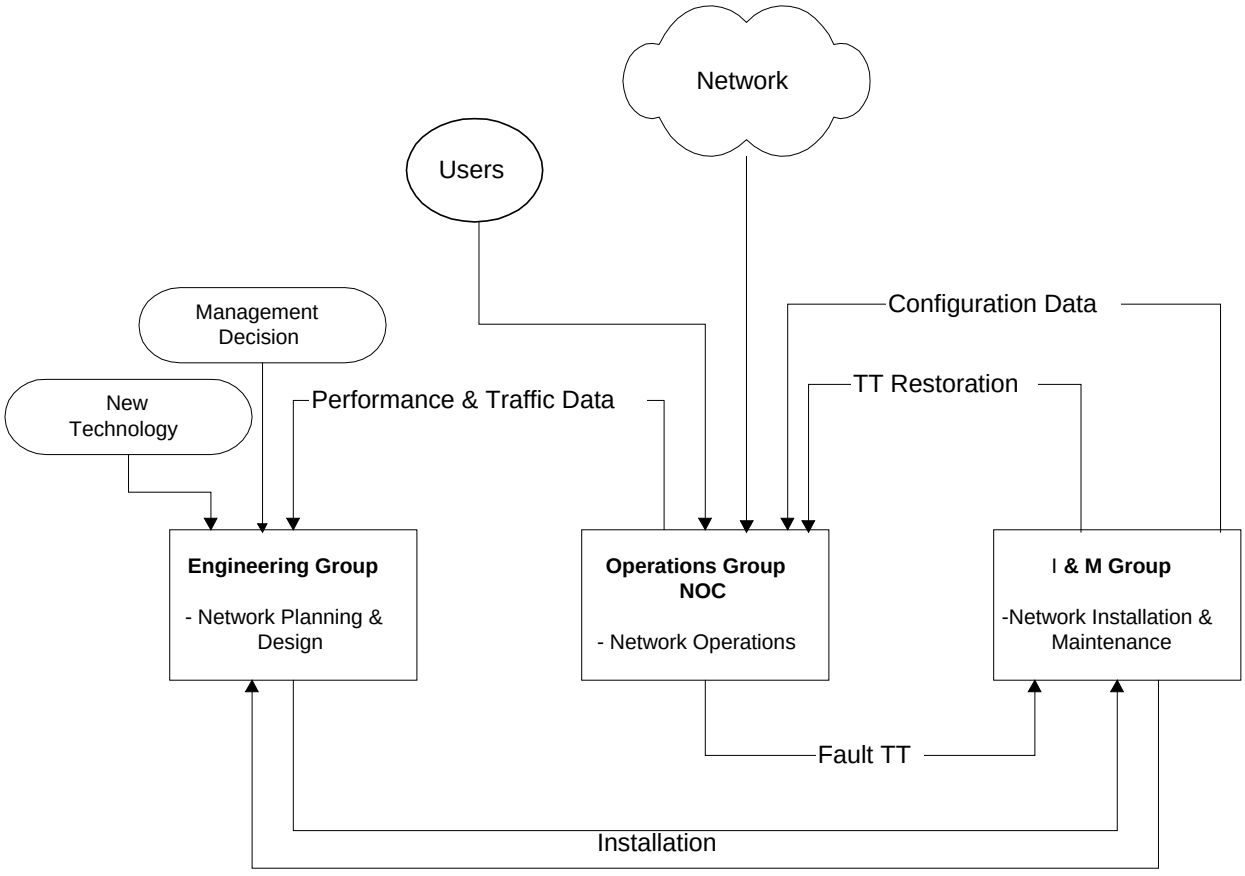


Figure 1.22. Network Management Functional Flow Chart

Security Management:

- Security management can cover broad range of security.
- It involves physically securing the network as well as access to the network by users.

Accounting Management:

- Accounting management administers cost allocation of the usage of network.
- Metrics are established to measure the usage of resources and services provided.

iii. Network Installation and Maintenance

- The network I&M group takes care of all activities of installation and maintenance of equipment and transmission facilities.
- This group is the service arm of engineering group for installation and fixing troubles for network operations.

Trouble Ticket Administration:

a. Trouble ticket administration is the administrative part of fault management and is used to track problems in the network.
b. All problems including non-problems are to tracked until resolved.
c. There are trouble-tracking systems to automate the tracking of troubles from the automatic generation of a trouble ticket by an NMS to the resolution of the problem.

1.10 Network Management Architecture and Organization

- Network management dumbbell architecture for interoperability is as shown in figure1.23(a),

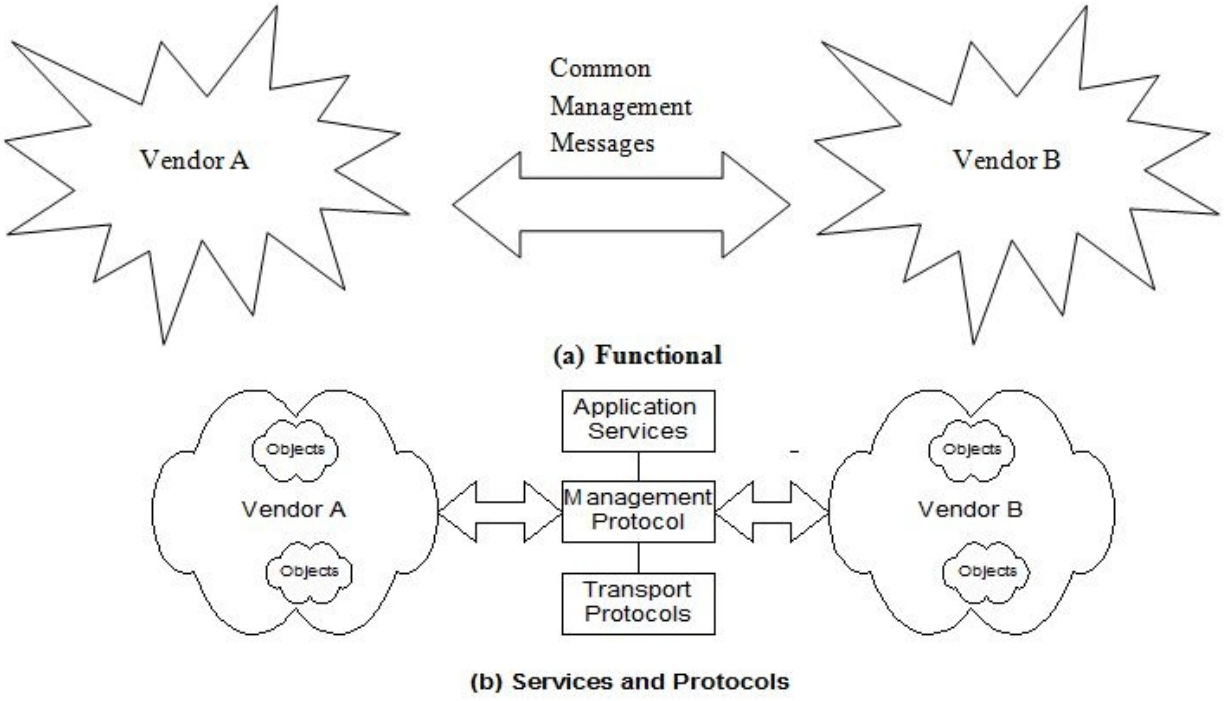


Figure 1.23 Network Management Dumbbell Architecture

- The vendor systems A and B exchange common management messages. The messages consist of **management information data** *(type, id, and status of managed objects etc)* and **management controls** *(setting and changing configuration of an object).*
- The protocols and services associated with the dumbbell architecture are presented in figure 1.23(b).
- **Application services** are the management-related applications such as *fault and configuration management.*
- **Management protocols** are *CMIP for the OSI model and SNMP for the Internet Model.*
- *Transport protocols* are the first four OSI layers for the OSI model and *TCP/IP over* any of the first two layers for the Internet model.
- Figure 1.24 models a hierarchical configuration of two network agents monitoring two sets of managed objects.

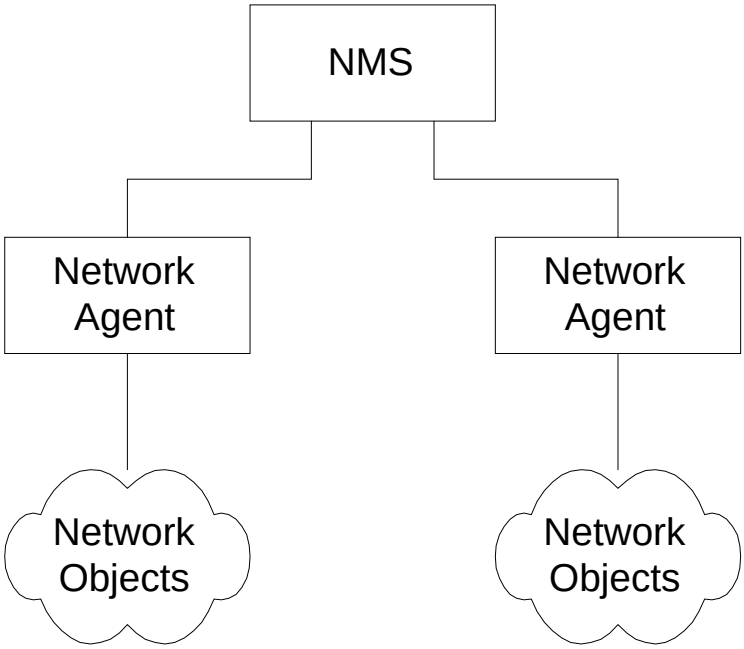


Figure 1.24 Network Management Components

- The agent could be an embedded agent in a network element or an EMS communicating with agents embedded in the network elements.
- *Peer networks can communicate network management messages and controls between them* as shown in figure 1.25
- An example where such a configuration could be implemented would be two NMSs associated with two telecommunication networks belonging to two network service provider.

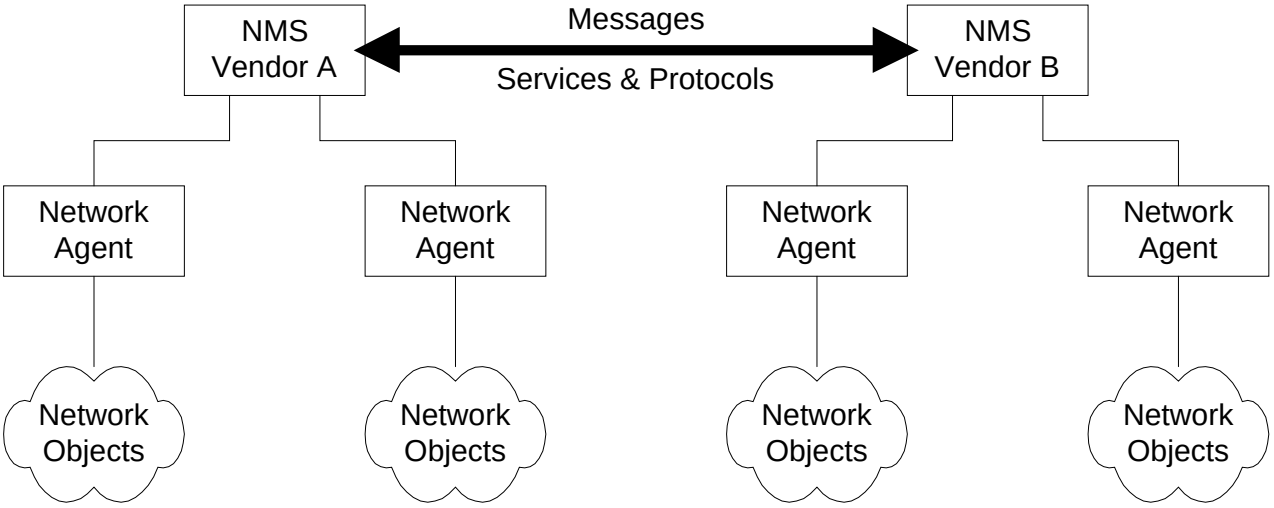


Figure 1.25 Network management Interoperability

1.11 Current Status and Future of Network Management

- The current status of Network Management are as follows-
  i. Current NMSs are based on SNMP protocol.
  ii. Limited CMIP management.
  iii. Limitation of large memory in computer system.
  iv. Poll based system, in other words NMS polls each agent as to its status or for any other data that it needs for network management.

- The above mentioned constraints on NMS have been overcome by emerging advanced network management, which are as mentioned below,
  i. Object-oriented technology has reached a matured stage, and the hardware capacity to handle object-oriented stack is now commercially available.
  ii. Service and policy management.
  iii. Business management.
  iv. Web-based management.

- Even more work on standardization of management of this technology needs to be done in this area.