NETWORK MANAGEMENT

Sub Code	**: 18CS742**	**CIE Marks**	**: 40**
Hrs/Week	**: 3:0:0**	**SEE Marks**	**: 60**
Total Hrs	**: 40**	**Exam Hours**	**: 03**

MODULE – 1 **8 Hours**

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.

MODULE- 2 **8 Hours**

Basic Foundations: Standards, Models, and Language: Network Management Standards, Network Management Model, Organization Model, Information Model – Management Information Trees, Managed Object Perspectives, Communication Model; ASN.1- Terminology, Symbols, and Conventions, Objects and Data Types, Object Names, An Example of ASN.1 from ISO 8824; Encoding Structure; Macros, Functional Model.

MODULE- 3 **8 Hours**

SNMPv1 Network Management - 1 : Managed Network: The History of SNMP Management, Internet Organizations and standards, Internet Documents, The SNMP Model, The Organization Model, System Overview **SNMPv1 Network Management – 2:** The Information Model – Introduction, The Structure of Management Information, Managed Objects, Management Information Base. The SNMP Communication Model – The SNMP Architecture, Administrative Model, SNMP Specifications, SNMP Operations, SNMP MIB Group, Functional Model **SNMP Management – RMON:** Remote Monitoring, RMON SMI and MIB, RMONI1- RMON1 Textual Conventions, RMON1 Groups and Functions, Relationship Between Control and Data Tables, RMON1 Common and Ethernet Groups, RMON Token Ring Extension Groups, RMON2 – The RMON2 Management Information Base, RMON2 Conformance Specifications; ATM Remote Monitoring, A Case Study of Internet Traffic Using RMON.

MODULE- 4 **8 Hours**

Broadband Network Management: Broadband Access Networks and Technologies – Broadband Access Networks, roadband Access Technology; HFCT Technology – The Broadband LAN, The Cable Modem, TheCable Modem Termination System, The HFC Plant, The RF Spectrum for Cable Modem; Data Over Cable Reference Architecture; HFC Management – Cable Modem and CMTS Management, HFC Link Management, RF Spectrum Management, DSL Technology; Asymmetric Digital Subscriber Line Technology – Role of the ADSL Access Network in an Overall Network, ADSL Architecture, ADSL Channeling Schemes, ADSL Encoding Schemes; ADSL Management – ADSL Network Management Elements, ADSL Configuration Management, ADSL Fault Management, ADSL Performance Management, SNMP-Based ADSL Line MIB, MIB Integration with Interfaces Groups in MIB-2, ADSL Configuration Profiles.

MODULE- 5 **8 Hours**

Network Management Applications: Configuration Management- Network Provisioning, Inventory Management, Network Topology, Fault Management- Fault Detection, Fault Location and Isolation Techniques, Performance Management – Performance Metrics, Data Monitoring, Problem Isolation, Performance Statistics; Event Correlation Techniques – Rule-Based Reasoning, Model-Based Reasoning, Case-Based Reasoning, Codebook correlation Model, State Transition Graph Model, Finite State Machine Model, Security Management – Policies and Procedures, Security Breaches and the Resources Needed to Prevent Them, Firewalls, Cryptography, Authentication and Authorization, Client/Server Authentication Systems, Messages Transfer Security, Protection ofNetworks from Virus Attacks, Accounting Management, Report Management, Policy-Based Management, Service Level Management.

Text Books:

1. Mani Subramanian: Network Management- Principles and Practice, Pearson Education, 2003.

UNIT 1: DATA COMMUNICATION & NETWORK MANAGEMENT OVERVIEW

ANALOGY OF TELEPHONE NETWORK MANAGEMENT

Why Telephone Network is popular?

- This is reliable
- This is dependable
- The Qos is generally good

Telephone Network Model

- A *trunk* is a logical link between two switches that may traverse one or more physical links (Figure: 1.1).
- The customer's telephone which is a switch on the customer premises, is connected to the end office via a dedicated link called a *loop*.
- The direct distance dialing (DDD) network, which enables us to dial far-end telephone w/o an operator's assistance, comprises following 3 transmission trunks:
  1) a direct trunk connects 2 end offices
  2) a toll connecting trunk connects an end office to any toll office
  3) a toll trunk connects any 2 toll offices
- A circuit connection is set up either directly using a local trunk or via the higher level switches & routes.
- Primary & secondary routes are already programmed into the switch. If the primary route is broken or the facilities over the primary route are filled to capacity, an alternative route is automatically assigned.
- Operations support systems ensure the quality of service in the telephone network.
- For a given region, there is a *NOC (Network Operations Center)* where the global status of the network is monitored. The NOC is the nerve center of telephone network operations.

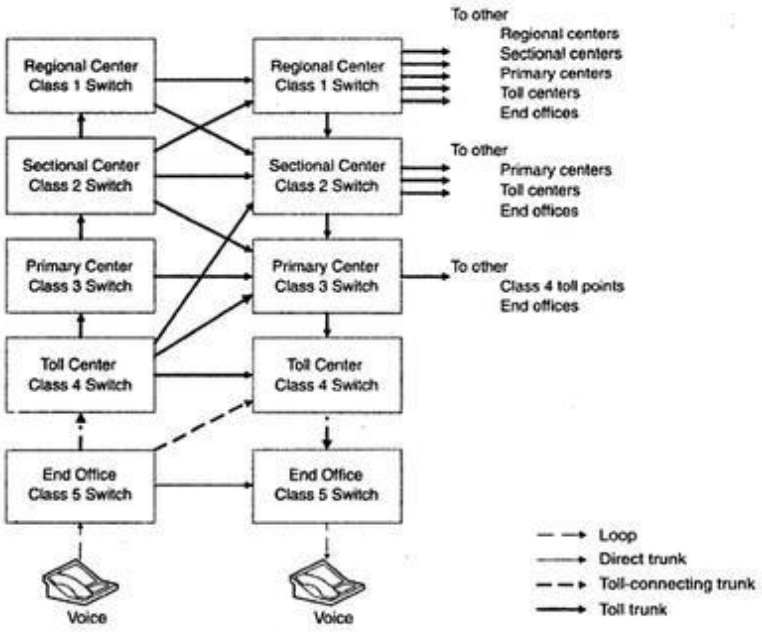


Figure 1.1 Telephone Network Model

DATA (COMPUTER) & TELECOMMUNICATION NETWORKS

THREE MODES OF DATA TRANSMISSION

- The data can be transmitted in one of 3 modes:
    1) Circuit switched
    2) Message switched or
    3) Packet switched.
- In the circuit switched mode, a physical circuit is established between the originating & terminating ends before the data is transmitted. The circuit is disconnected after completion of transmission.
- In message-switched & packet-switched modes, the data is broken into packets & each packet is enveloped with the destination & originating addresses.
- Message-switched mode is used to send long messages such as email. Whereas ,Packet switched mode is used to transmit small packets used in applications such as interactive communication.
- In message switched mode, the data is stored by the system & then retrieved by the user at a later time. In packet switched mode, the packets are fragmented & reassembled in almost real time.
- The bridges & routers open each packet to find the destination address & switch the data to the appropriate output links.

DATA & TELECOMMUNICATION NETWORKS

- Telecommunication network is a circuit-switched network that is structured as a public network accessible by any user (Figure: 1.3).
- The organization that provides service is called a telecommunication service provider E.g. BSNL, Airtel.
- 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 the information from digital to analog at source & back to digital at destination.

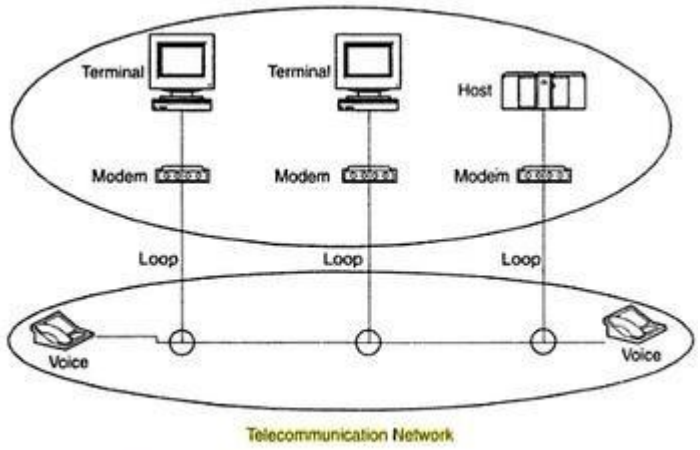


Figure 1.3 Data and Telecommunication Networks

INTERIM CORPORATE DATA & TELECOMMUNICATION NETWORK

- A number of telephones & computers terminals at various corporate sites are connected by the telecommunication network (Figure: 1.4).
- The telephone are connected locally by a local switch, PBX, which interfaces to the telephone network.
- The computer terminals are connected to onsite communication controllers, which manages the local terminals & provides a single interface to the telephone network.
- In the above corporate environment, the computer terminals communicate directly with the host.
- This communication system architecture is expensive & inefficient because the user has to pay for the data traffic over the public or leased telecommunications line.
- To reduce the cost & improve the performance, the computer terminals can communicate with a local communications processor, which can then communicate with remote hosts.
- Processor-to-processor communications over the telecommunications lines takes less time & therefore are less expensive.

IBM SYSTEMS NETWORK ARCHITECTURE MODEL

- In SNA, the host is connected to the terminals via the communications controllers & cluster controllers.
- Cluster controllers manage the DTEs at the peripheral nodes & the communication controllers manage the traffic

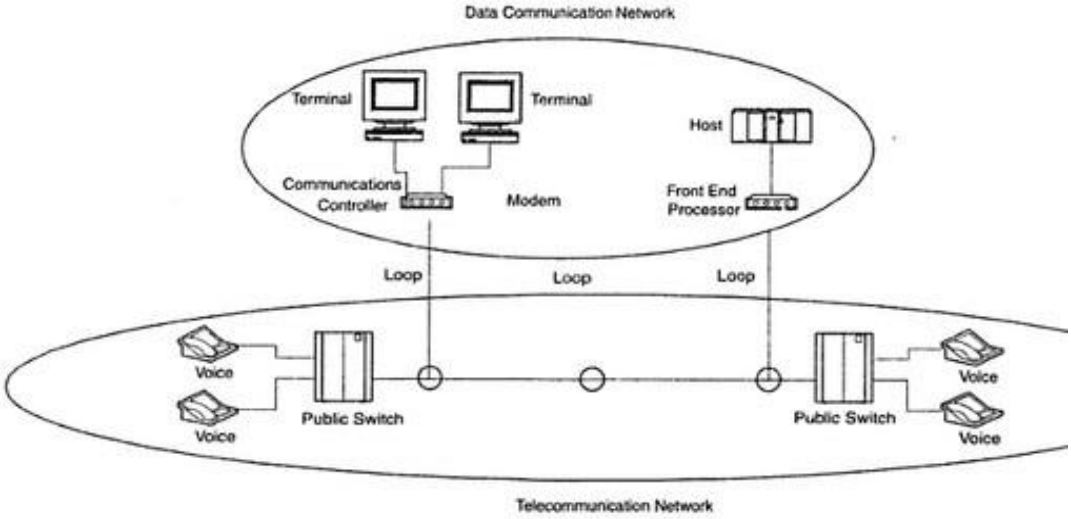


Figure 1.4 Interim Corporate Data and Telecommunication Networks

at the subnetwork levels (Figure: 1.5).

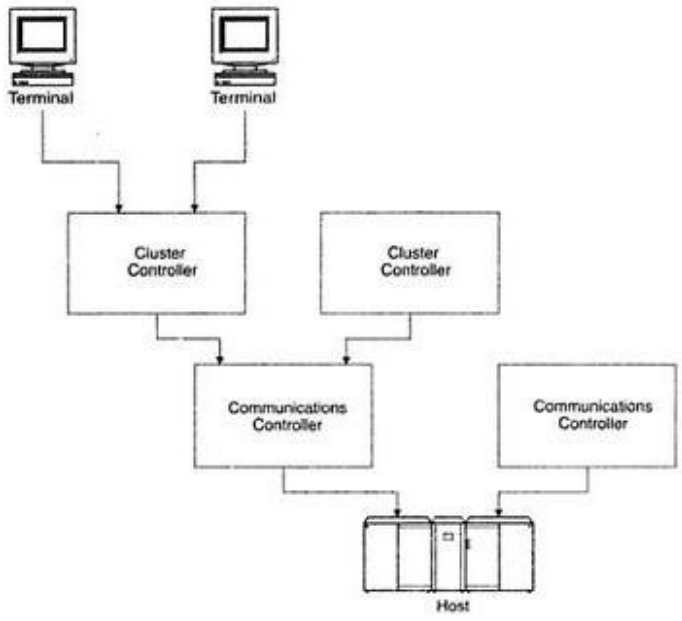


Figure 1.5 IBM Systems Network Architecture Model

DCE (DISTRIBUTED COMPUTING ENVIRONMENT)

SIMPLE CLIENT/SERVER MODEL

- The client initiates a request to the server & waits (Figure: 1.7).
- The server executes the process to provide the requested service & sends the results to the client.
- The client cannot initiate a process in the server. Thus, the process should have already been started in the server & be waiting for requests to be processed.

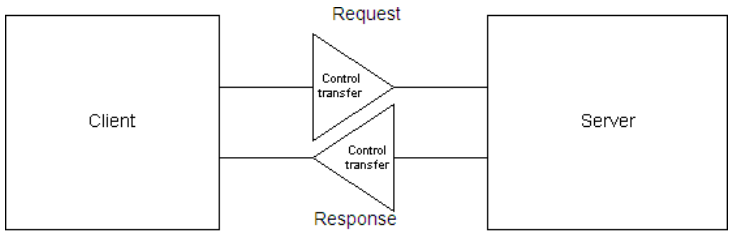


Figure 1.7 Simple Client-Server Model

MODEL OF CLIENT/SERVER NETWORK IN A DCE

- Each client's request is normally processed by the server according to the FIFO rule (Figure: 1.8,). This delay could be minimized, but not eliminated by concurrent processing of requests by the server.
- Since the client & application processes are running in a distributed computing environment, each of them can be designed to execute a specific function efficiently.
- For example, joe.stone using a 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 dept.com.. Therefore, it makes a request to the DNS on the network for the routing information for the address of dept.com
- When it receives that information, it sends out joe.stone's message via the bridge to the network.
- In this example, the mail server behaves both as a server & as a client.
- The 3 processes in this scenario, namely the client, the mail server and the DNS are considered cooperative computing processes & may be running in 3 separate platforms on remote LANs connected by a WAN. The communication between these processes is called peer-to-peer communication.

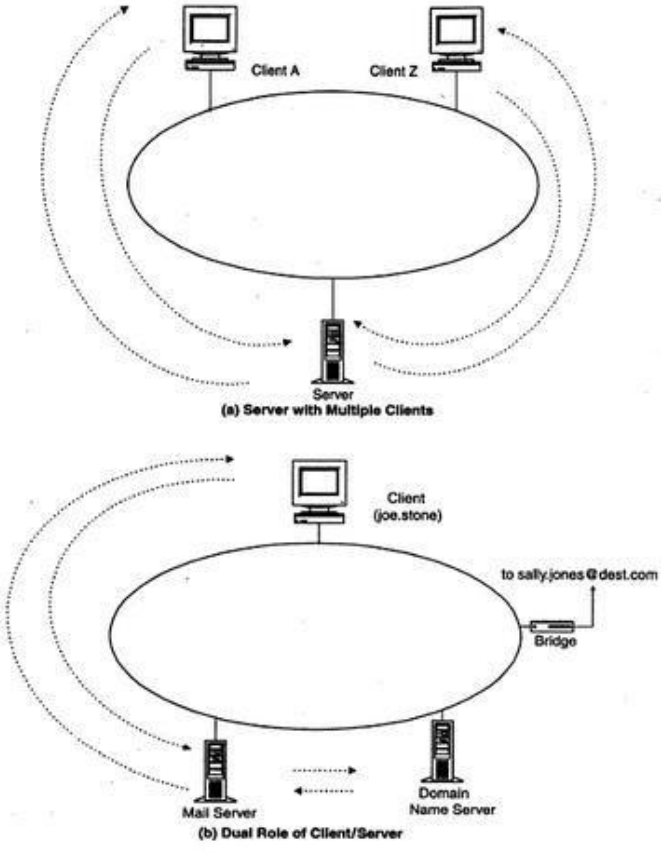


Figure 1.8 A Model of a Client/Server Network in a Distributed Computing Environment

TCP/IP-BASED NETWORKS: THE INTERNET AND INTRANET

- TCP/IP is a suite of protocols that enable networks to be interconnected.
- TCP/IP forms the basic foundation of the Internet(Figure:1.9).
- The nodes in the network use network protocol named IP to route packets.
- IP is a connectionless protocol. That means there is no guarantee that the packets will be delivered to the destination node. However, end-to-end communication can be guaranteed by using the transport protocol, TCP.
- TCP is connection-oriented protocol. Whereas , UDP is a connectionless protocol.
- Much of Internet traffic really uses UDP/IP, because of the reliability of data transmission.
- The Internet is a network of networks. Whereas, An intranet is a private network & access to it is controlled by the enterprise that owns it, whereas the Internet is public.
- Gateways between LANs serve as the interfaces between dissimilar & independent, autonomous networks & perform many functions including protocol conversions.

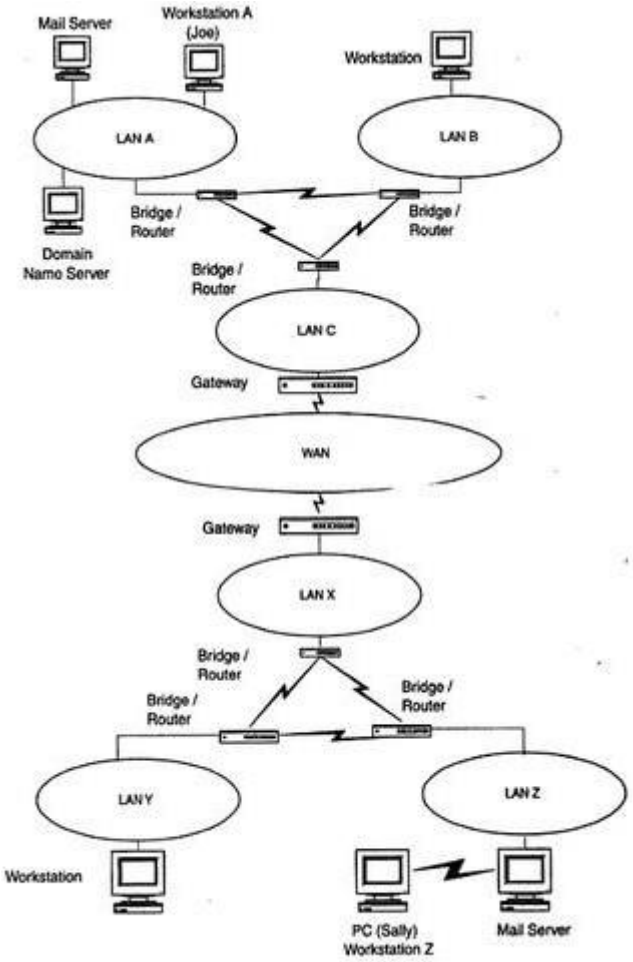


Figure 1.9 Internet Configuration

INTERNET FABRIC MODEL

- The workstations belong to the user plane, the LANs to the LAN plane, & WANs to the WAN plane.
- The interfaces are defined as the fabrics (Figure: 1.10).
- MAC fabric interfaces the user plane & the LAN plane. The user's workstation interfaces to a LAN via a MAC
- LANs interface to a WAN by a switching fabrics of bridges, routers & switches.
- Each WAN can be considered an autonomous network, & hence needs a gateway to communicate with another WAN. Gateway fabric interconnects different WANs.

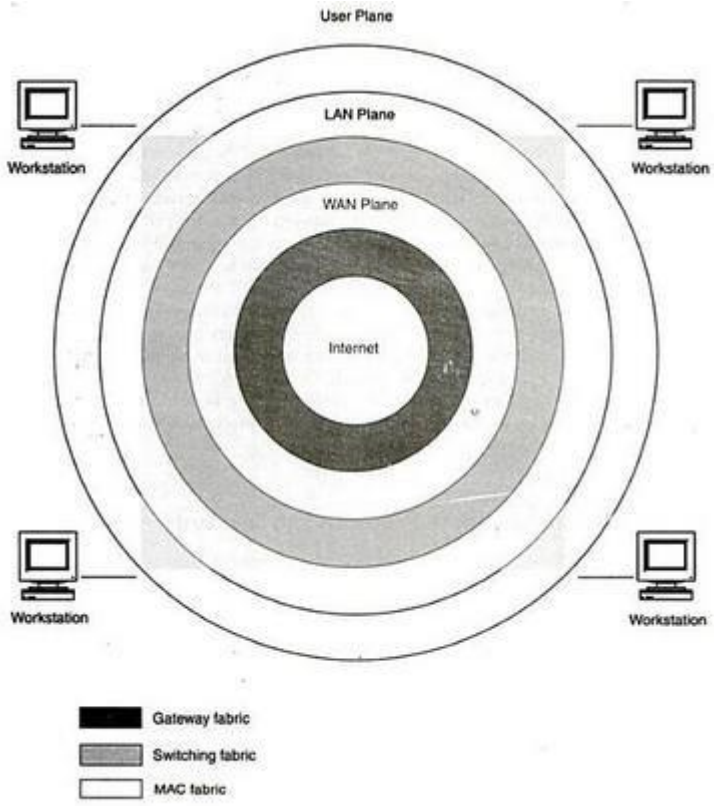
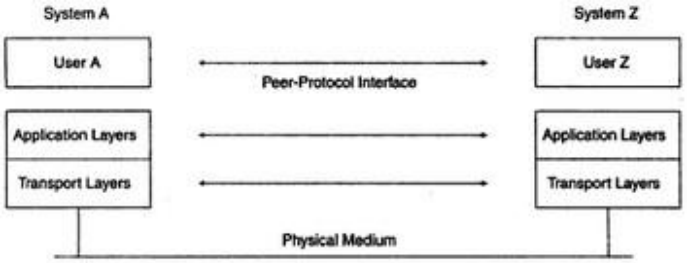


Figure 1.10 Internet Fabric Model

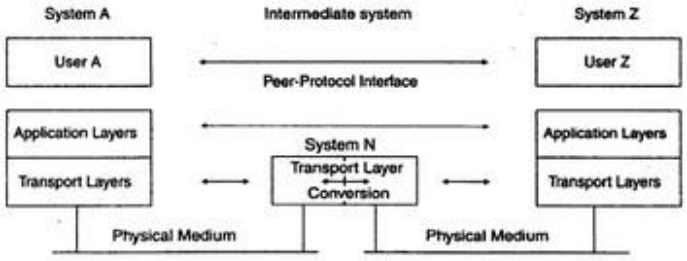
COMMUNICATION PROTOCOLS AND STANDARDS

COMMUNICATION ARCHITECTURE

- Communication between users occurs at various levels.
- Each system can be divided into 2 broad sets of communication layers. The top set of layers consists of the application layers & the bottom set of the transport layers.
- The users interface with the application level layer & the communication equipment interfaces with the physical medium.
- In Figure:1.11a, direct communication occurs between the corresponding cooperating layers of each system.
- In Figure:1.11b, the end systems communicating via an intermediate system N, which enables the use of different physical media for the 2 end systems.
- System N converts the transport layer information into the appropriate protocols.



(a) Direct Communication between End Systems



(b) Communication between End Systems via an Intermediate System

Figure 1.11 Basic Communication Architecture

OSI COMMUNICATION ARCHITECTURE

- OSI model was developed based on the premise that the different layers of protocol provide different services, and that each layer can communicate with only its own neighboring level (Figure: 1.12).
- Two systems can communicate on a peer-to-peer level i.e. at the same level of the protocol.

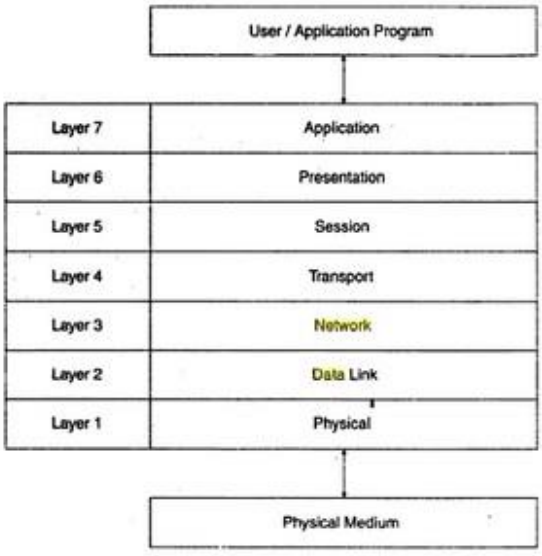


Figure 1.12 The OSI Protocol Layers

PDU COMMUNICATION MODEL BETWEEN END SYSTEMS

- The message in each layer is contained in message units called protocol data units (PDUs), which consists of two parts-- PCI(protocol control information) & UD(user data) (Figure:1.14).
- 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 size of the PDU increases as it goes toward lower layers.
- If the size of the PDU exceeds the maximum size of layers specifications, it is fragmented into multiple packets. Thus, a single application-layer PDU could multiply into several physical PDUs.

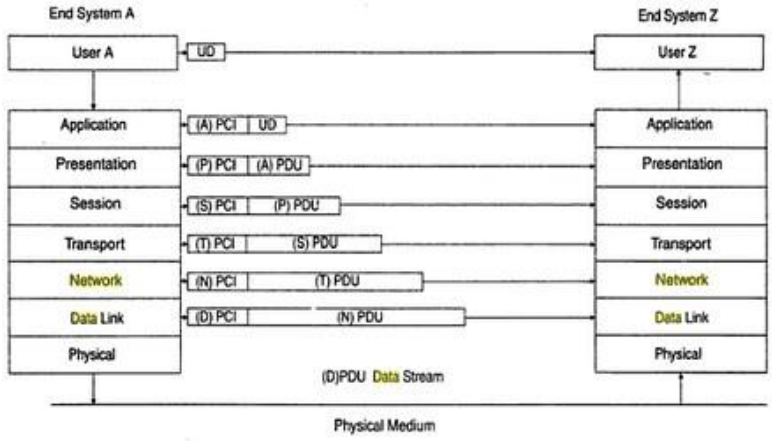


Figure 1.14 PDU Communication Model between End Systems

OSI LAYERS & SERVICES

Physical layer

- Transfers to & gathers from the physical medium raw bit data (Figure: 1.13).
- Handles physical & electrical interfaces to the transmission medium.

Data link layer

- Consists of two sublayers: LLC(Logical link control) & MAC(Medium access control).
- LLC formats the data to go on the medium, performs error control & flow control.
- MAC controls data transfer to & from LAN, resolves conflicts with other data on LAN.

Network layer

- Forms the switching/routing layer of the network.

Transport layer

- Multiplexes & demultiplexes messages from applications.
- Acts as a transparent layer to applications & thus isolates them from the transport system layers.
- Makes & breaks connections for connection-oriented communications.
- Controls flow of data in both directions.

Session layer

- Establishes & clears sessions for applications, and thus minimizes loss of data during large data exchange.

Presentation layer

- Provides a set of standard protocols so that the display would be transparent to syntax of the application.
- Data encryption & decryption.

Application layer

- Provides application-specific protocols for each application & each transport protocol system.

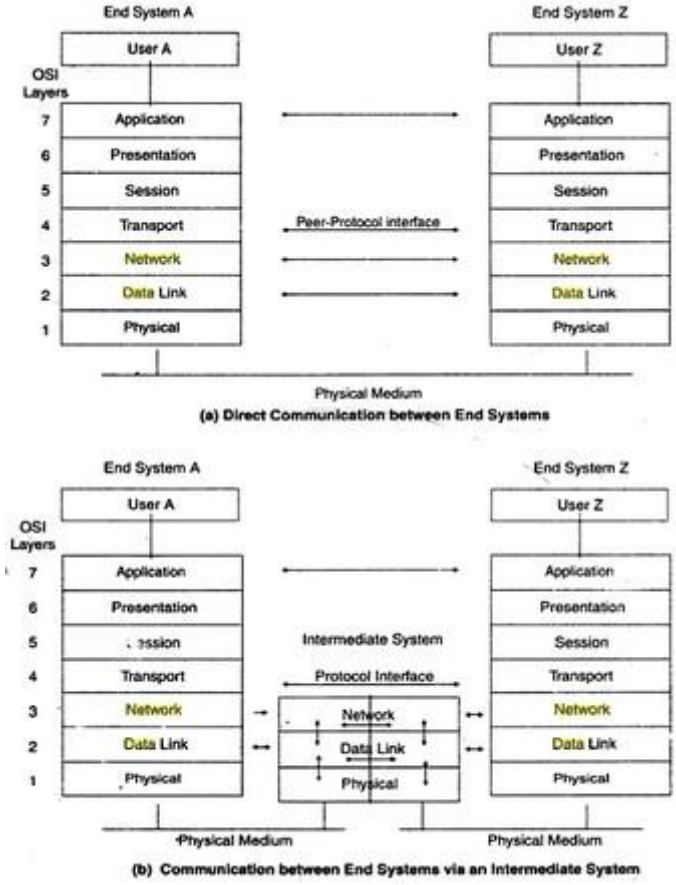


Figure 1.13 OSI Communication Architecture

PHYSICAL LAYER

- This is responsible for physically placing the electrical signal on the physical medium & picking up the signal from it.
- This controls & manages the physical & electrical interfaces to the physical medium, including the connector or transceiver.
- The physical medium could be copper, optical fiber or wireless media.
- The signal could be either digital or analog.

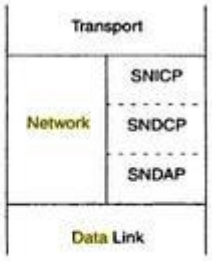
DATA LINK LAYER

- The data communication between 2 DTEs is controlled & managed by this layer.
- The data communication is a serial bit-oriented stream.
- The data link layer needs to do basic functions:
    1) Establish & clear the link, and
    2) Transmit the data.
- This does error control & data compression. Flow control is done on a hop-to-hop basis.
- This is divided into two sublayers--LLC & MAC (Figure: 1.15). The lower MAC layer controls the access & transmittal of data to the physical layer in an algorithmic manner. LLC performs the link management & data transfer.
- There are two basic forms of LANs--Ethernet LAN is a bus type & the media is accessed using a distributed probabilistic algorithm, CSMA/CD The second type of LAN is a ring type used in token ring & FDDI.A deterministic token-passing algorithm is used in this case.

Figure 1.15 The Sublayer Structure of a Data Link Protocol Layer

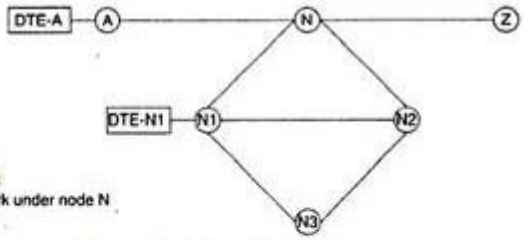
NETWORK LAYER

- This controls & manages the switching fabric of the network (Figure: 1.16).
- This provides both CLNS (connectionless network services) & CONS (Connection oriented network service). CLNS is used when the lower layers are highly reliable such as LANs & bridges as well as when the messages are short. CONS is the method for transmitting long messages such as file transfer. This is also used when the transmission medium is not reliable.
- The OSI architecture model handles this by dividing the network layer into 3 sublayers:
    1) SNICP (Subnetwork Independent Convergence Protocol)
    2) SNDCP (Subnetwork Dependent Convergence Protocol)
    3) SNDAP (Subnetwork Dependent Access Protocol) (Figure: 1.17)
- The Internet communicates between nodes using a Internet address and the SNICP. The nodes in turn communicate with subnetworks using the SNDCP, which depends on the subnetwork protocol & could be any proprietary protocol. In such a situation, the SNDCP communicates with its data link layer via the SNDAP.



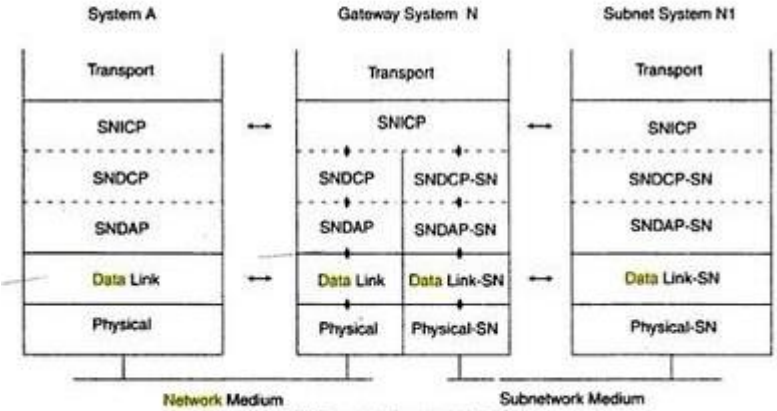
SNICP = Subnetwork Independent Convergence Protocol
SNDCP = Subnetwork Dependent Convergence Protocol
SNDAP = Subnetwork Dependent Adapter Protocol

Figure 1.16 The Sublayer Structure of a Network Protocol Layer



A–N–Z Standard network
N–N1–N2–N3 Subnetwork under node N

(a) Network Configuration



(b) Protocol Communication

Figure 1.17 Gateway Communication to a Proprietary Subnetwork

PRESENTATION LAYER

- This is the medium of presentation of the message's context to the user or application program.
- This is context sensitive layer.
- This can be interpreted as the common languages & image that the users at both end systems use & understand.

COMPARISON OF SNA, OSI AND INTERNET PROTOCOL LAYER MODELS

- The transport & network layers form the suite of TCP/IP protocols. The application layers are combined into application-specific protocols (Figure: 1.18).
- In the 7-layered SNA model, the physical, data link & application layers have one-to-one correspondence with the OSI layers.
- Much of the SNA transport & session layer functions equivalent to those of the OSI model are done in the data flow control & transmission control layers. The combination of these 2 services is also called *the SNA transmission subsystem.*
- The presentation services, which are known as SNA high level services, combine the presentation services & functions with some of the session control functions.

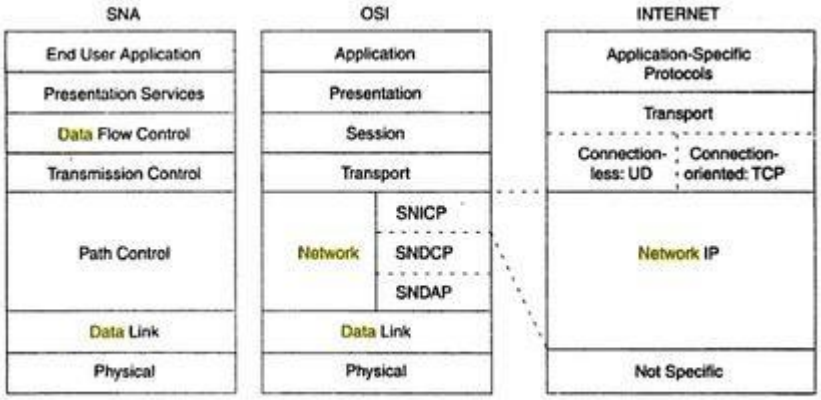


Figure 1.18 Comparison of SNA, OSI, and Internet Protocol Layer Models

APPLICATION SPECIFIC PROTOCOLS IN THE ISO & INTERNET MODELS

- All application specific protocol services in OSI are sandwiched between the user & presentation layers. In the Internet model, they are sandwiched between the user and the transport layers (Figure: 1.19).
- A user interfaces with a host at a remote terminal using virtual terminal in the OSI model & TELNET in the Internet model.
- File transfers are accomplished using FTAM (File Transfer Access & Management) in the OSI model and FTP (File transfer protocol) in the Internet.
- The most common mail service function in the Internet is the SMTP.A similar protocol in the OSI model is the MOTIS (message oriented text interchange standard).
- Network management is accomplished using CMIP (Common Management Information protocol) in the OSI model and SNMP in the Internet.

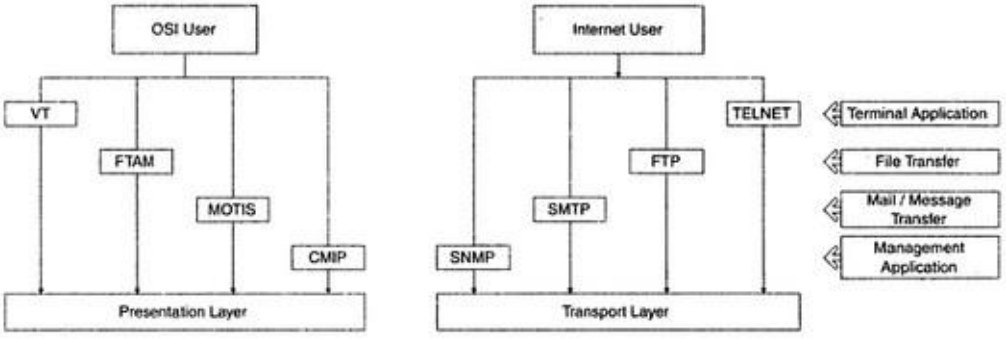


Figure 1.19 Application-Specific Protocols in the ISO and Internet Models

CHALLENGES OF INFORMATION TECHNOLOGY MANAGERS

- IT manager needs to maintain both computer & telecommunication networks because both types are slowly merging in function.
- They are responsible for management of information because of the explosion of information storage & transfer in the modern information era.
- They have to keep up with the new technologies because the technology is moving fast & the corporate growth is enormous.
- They need to make provisions for contingencies to change direction when the IT industry does
- They face network & administrative & management problems day in & day out because most of the corporate networks run 24/7.

WHAT ARE TOP CHALLENGES IN MANAGING THE NETWORK?

- Analyzing problems, which requires intuition & skill
- Anticipating customers' demands
- Acquiring resources
- Managing the client/server environment
- Networking with emerging technology as part of continuing education
- Collaborative research between academic institutions & industry
- Maintaining reliability
- Diagnosing problems or outrages in a non-disruptive manner
- Estimating value of a technology transition
- Maintaining a secure firewall between the internal network & the Internet
- Sustainable network that is scalable & maintainable
- Staying abreast of the rapid advance of technology
- Determining responsibility for outages to the WAN

NETWORK MANAGEMENT: GOALS, ORGANIZATIONS & FUNCTIONS

- This can be defined as OAM&P of network & services.
- The goal of network management is to ensure that the users of a network receives the information technology services with the quality of service that they expect.

Network Management Functions

Network Provisioning

- The engineering group keep track of new technologies & introduces them as needed. (Figure: 1.21).
- Determination of what is needed & when is made through analysis of the traffic and performance data provided by the network operations.
- Network management tools are helpful to the engineering group in gathering statistics and studying the trends of traffic patterns for planning purposes.

Network Operations & the NOC

- They are concerned with daily operations of the network & providing network services.

Fault Management/Service Restoration

(Check detailed FM in next page).

Trouble Ticket Administration

- This is the administrative part of fault management & is used to track problems in the network. All problems, including nonproblems, are to be tracked until resolved.

Configuration Management

- There are 3 configurations of the network:

1) One is the static configuration & is the permanent configuration of the network. The static configuration is on that would come up if the network is started from idle status.

2) The second configuration of a network is the current running configuration.

3) The third configuration is the planned configuration of the future when the configuration data will change as the network is changed. This information is useful for planning & inventory management.

Security management

(Check detailed SM in next page).

Performance Management

(Check detailed PM in next page).

Accounting Management

- The NOC administers costs & allocates the use of the network.
- Metrics are established to measure the usage of resources & services.
- There are 3 classes of reports: systems, management & user.

Network Installation & Maintenance

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

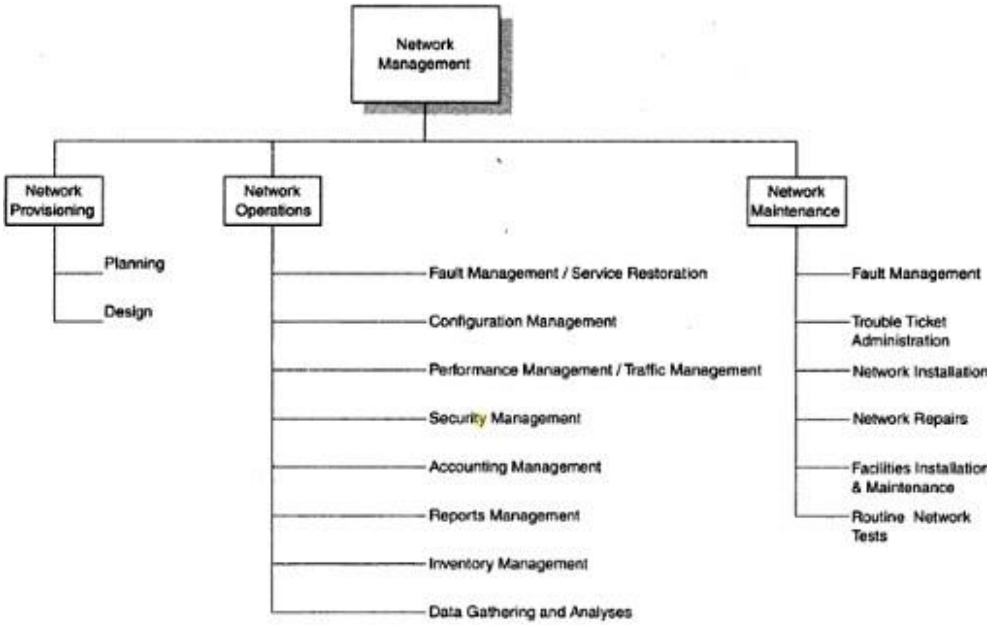


Figure 1.21 **Network Management Functional Groupings**

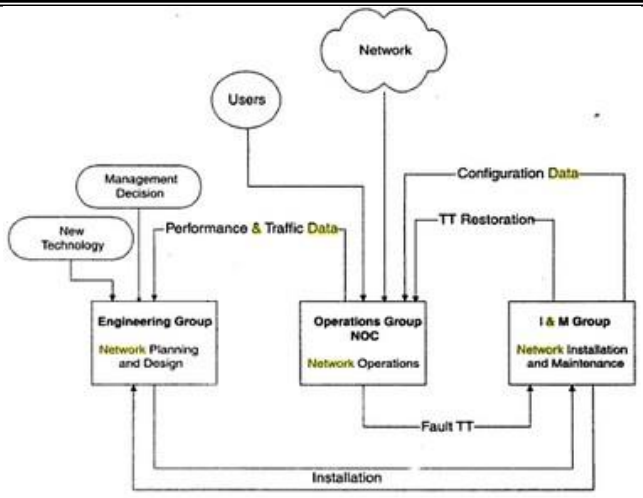


Figure 1.22 Network Management Functional Flowchart

NETWORK OPERATIONS & THE NOC (in detail)

FAULT MANAGEMENT

- This involves detection & isolation of the problem that caused the failures, and restoration of the service.
- 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*.
- An NMS can also detect failures of components & indicate them with appropriate alarms.
- The responsibility to fix the problem usually rests with the I&M group.
- A trouble ticket is generated manually by a source engineer at NOC using a trouble-ticket system or automatically generated by an NMS.
- The information on the trouble ticket includes
  - → a tracking number assigned by the system
  - → time at which problem occurred
  - → the nature of the problem
  - → affected user
  - → the responsible group/engineer to resolve the problem
- The tracking of a trouble involves several groups and the administration of it generally belongs to the network maintenance group.

SECURITY MANAGEMENT

- This involves physically securing network, access to network resources & secured communication over network.
- Access privilege to application software is not the responsibility of the NOC unless the application is either owned or maintained by the NOC.
- A security database is established & maintained by the NOC for access to the network & network information.
- Unauthorized access to the network generates an alarm on the NMS at the NOC.
- Firewalls protect corporate networks & network resources from being accessed by unauthorized personnel & programs including virus programs.
- Secured communication prevents tampering of information as it traverses the network, so that is cannot be accessed or altered by unauthorized personnel. Cryptography plays a vital part in security management.

PERFORMANCE MANAGEMENT

- This is concerned with the performance behavior of the network.
- The status of the network is displayed by a NMS that measures the traffic & performance of the network.
- The NOC gathers data & keeps them up to date to tune the network for optimum performance.
- The network statistics include data on traffic, network availability& network delay.
- The traffic data can be captured based on volume of traffic in the various segments of the network.
- Performance data on availability & delay is useful for tuning the network to increase the reliability & to improve its response time.
- Traffic statistics are helpful in detecting trends & planning future needs.

ACCOUNTING MANAGEMENT

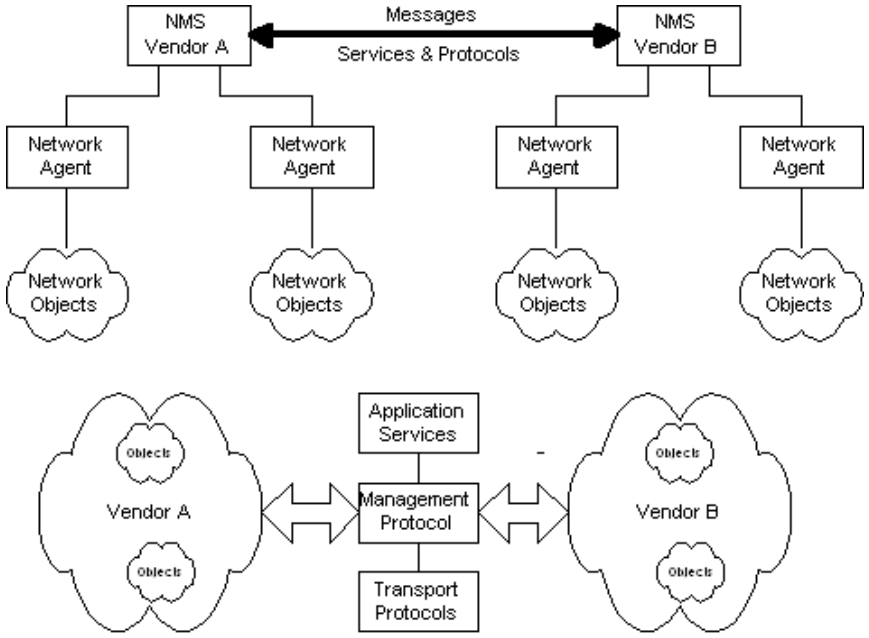
- The NOC administers costs & allocates the use of the network.
- Metrics are established to measure the usage of resources & services.
- There are 3 classes of reports: systems, management & user.
- System reports are needed for network operations to track the activities. Management reports go to the management of the network management group to keep them informed about the activities & performance of the NOC & the network. The user reports are distributed to the users on a periodic basis to let them know the status of network performance.

NETWORK & SYSTEM MANAGEMENT

- The problem in the application program is a system problem & falls under the category of system management. On the other hand, the transport problem from the client's workstation to the server platform is a system problem & falls under network management.
- System management is concerned with management of systems & system resources in the network. Whereas, Network management is concerned with network resources such as hubs, switches, bridges, routers & gateways, and the connectivity among them via a network.
- Network management also addresses end-to-end connectivity between any two processors in the network. System management also addresses logging & archiving events.

Network Management Dumbbell Architecture

- In fig:1.23 , the messages consist of management information data & management controls.
- Application services are the management-related applications such as fault & configuration management.
- The management protocols are CMIP for the OSI model & SNMP for the Internet model.
- Transport protocols are first 4 layers of OSI model & TCP/IP over any of first 2 layers of the 7-layer OSI model.



(b) Services and Protocols

Figure 1.23 Network Management Dumbbell Architecture

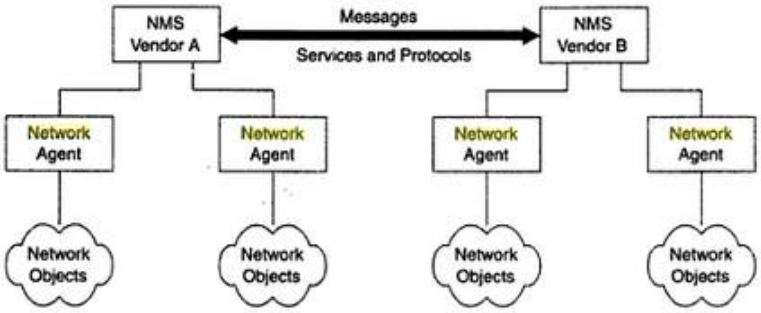


Figure 1.25 Network Management Interoperability