DATA THROUGH TELEPHONE NETWORKS

- Data transmission in PSTNs,
- Switching technique for Datatransmission,
- Data communication Architecture,
- Link-to-Link Layers,
- End-to-End Layers,
- Satellite Based Data Network.

Data Networks

In the last few decades, computer and communication technologies have been coming together to support many new applications and developments. One of the early examples of such a development is data networks. Data

In the beginning, data transmission was organised using telegraph or telex networks as they could carry digital signals directly. There were, however, two limitations. First, the speeds were limited to 50 bauds in the case of switched circuits or to 110 bauds in the case of leased lines. Secondly, these networks did not provide a wide coverage of the population. The possibility of carrying signals at higher speeds in telephone networks and their wide coverage led to the serious consideration of public switched telephone network (PSTN) as a candidate system for data transmission. As remote computing was maturing, the idea of sharing data, information and other resources among computers emerged. The focus shifted from terminal-to-computer communication to computer-to-computer communication. Early efforts were confined to interconnecting homogeneous computer systems from the same vendor. Soon, the advantages of interconnecting computers from different vendors were realised and the progress made in this direction has led to evolution of modern **public data networks** (PDNs).

Data networks are classified according to their geographical coverage:

- Wide area networks (WANs)
- Metropolitan area networks (MANs)
- Local area networks (LANs).

Intercity, intercountry and intercontinental networks are known as WANs. Based on the communication infrastructure used, they may be classified as **terrestrial data networks (TDNs)** or **satellite based data networks (SBDNs)**. In TDNs, data communication is organised using cables, fibre optic lines or radio links. A geostationary or a geosynchronous satellite is used for communication in SBDNs.

A metropolitan area network interconnects computers within a metropolitan city. Community antenna television (CATV) cables, twisted pair wires or shielded lines, optical fibres, radio links or line-of-sight (LOS) optical communication links provide the communication medium for MAN. The broadband capability of CATV cables permits carrying voice, data and video simultaneously. Thus MANs are usually multimedia networks.

Local area networks are confined to a single building or a group of buildings generally belonging to the same organisation. Optical fibres, twisted pair and coaxial cables are used as the communication media for LANs. Fibre optic networks (FONs) are suitable for both LANs and MANs. Synchronous optical networks (SONET) are designed to operate at high speeds.

LANs, MANs and WANs are generally interconnected in a hierarchical manner to form a global network as shown in Fig. 10.1. LANs are often

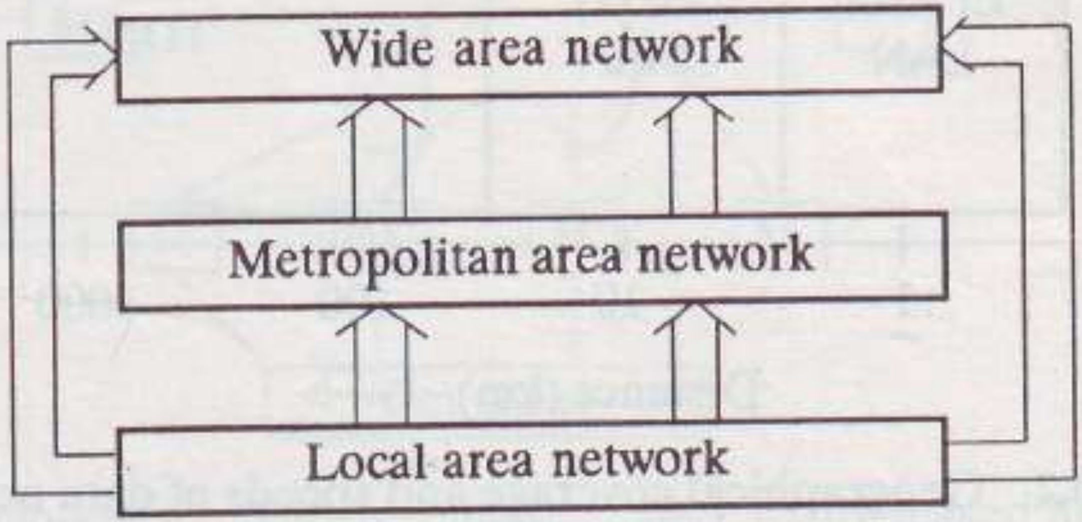


Fig. 10.1 Data network hierarchy.

connected directly to WANs, particularly in places where MANs are not installed or have not developed well. Apart from the different geographical coverages, the range of data rates supported on these networks also differs widely. Figure 10.2 summarises the typical data rates and geographical coverages for these networks.

Data Transmission in PSTNs

Public switched telephone networks and electronic PABXs are designed to carry analog voice signals. They can, however, be used for data transmission by employing suitable interfaces. As seen from Fig. 10.2, LANs can be designed around PABXs, and MANs around PSTNs. In these cases, the data rates are usually limited to a maximum of 64 kbps. Terrestrial data networks and the upcoming integrated services digital networks can, however, support data rates of 1.544 or 2.048 Mbps.

Transmission of digital data signals over PSTN networks demands that the digital signals be converted to analog form at the transmitting end and vice versa at the receiving end. A modulator translates the data pulses into voice band analog signals at the transmitting end. At the receiving end, the analog signals are demodulated to recover the digital information. A combined modulator/demodulator unit is called a **modem**.

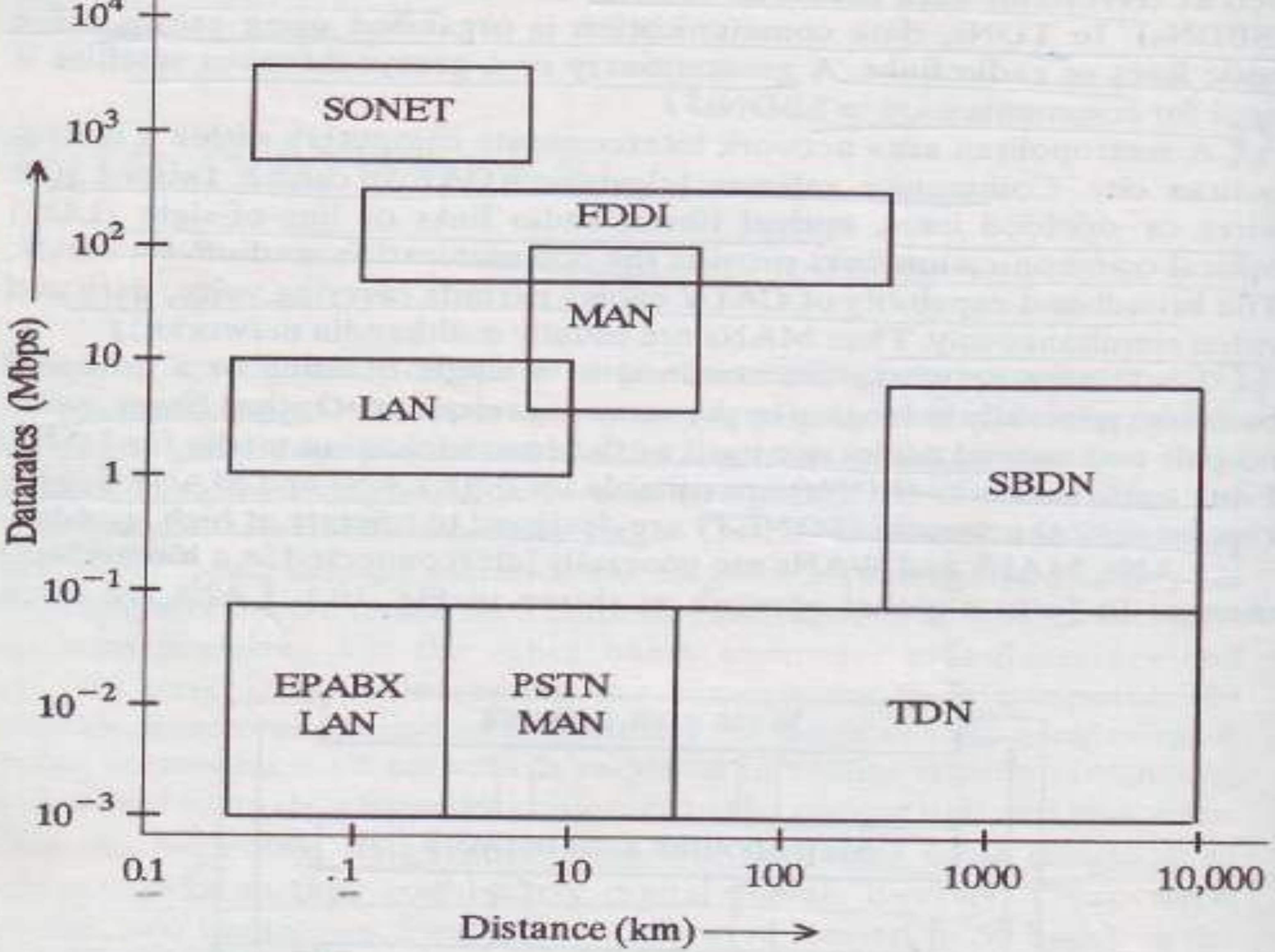
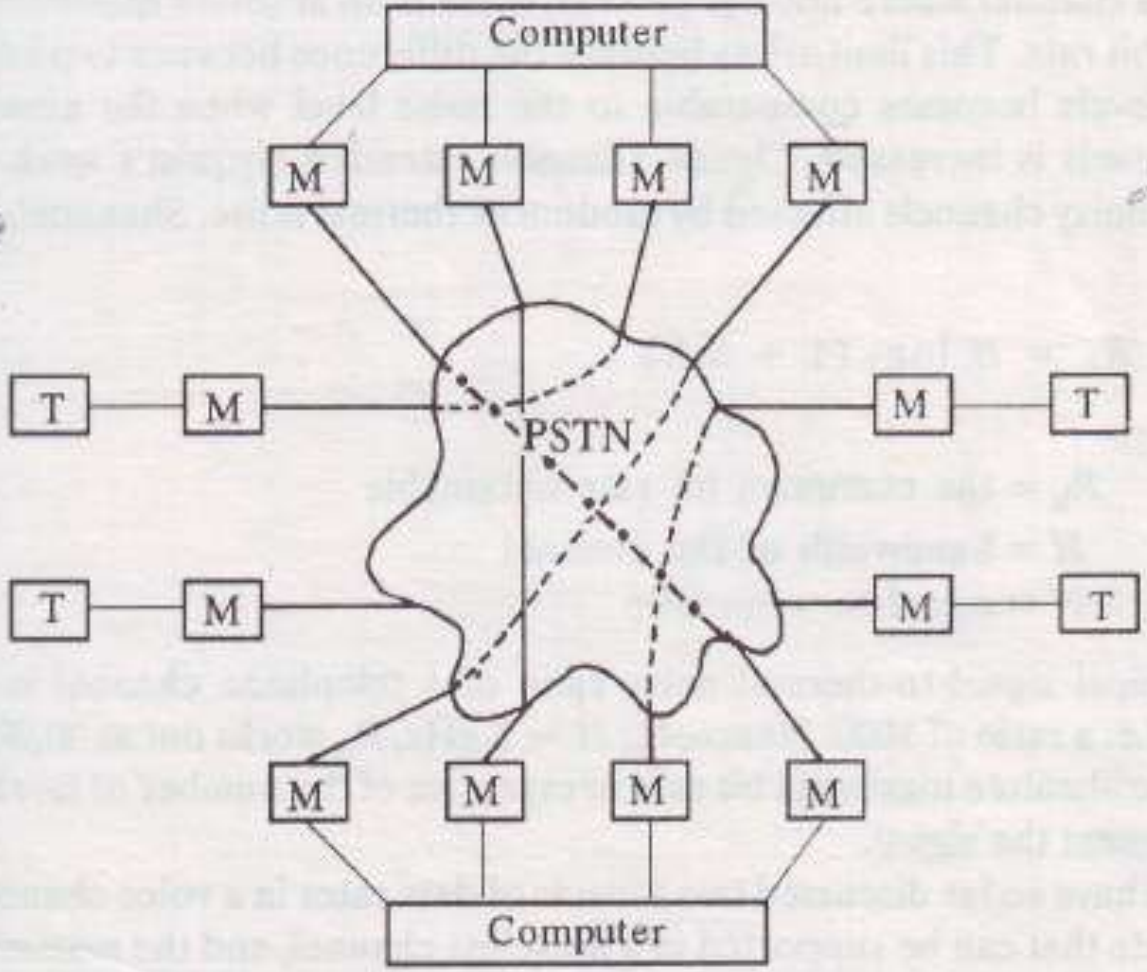


Fig. 10.2 Geographical coverage and speeds of data networks.

was established using modems and PSTNs. A data communication scheme using modems and a PSTN is shown in Fig. 10.3. The digital interface of a modem is connected to the computer and the analog interface to the telephone network. In addition to data exchange, the digital interface perm-

In a PSTN, a connection may be established using a dial-up facility or a dedicated nonswitched leased line. A 2-wire or 4-wire leased line may be used. The modems usually have automatic dialling and answer facility which is useful when working with dial-up line.Modems are driven by a communication software package that runs on the terminal or the personnel computer of the user. The transmission may be half-duplex or full-duplex. In Fig.10.3, both terminal-to-computer and computer-to-computer connections are shown.



M = modem   T = terminal   —— 4-wire leased line
– – dial-up line   – · – 2-wire leased line

Fig. 10.3 Data communication using PSTN.

Data Rates in PSTNs

A voice channel in a PSTN is band limited with a nominal bandwidth of 3.1 kHz. What is the maximum data rate that a voice channel can support with its limited bandwidth? A first-cut estimate of this can be obtained from Nyquist's theorem which applies to noiseless channels and states:

$$R = 2H \log_2 V \text{ bps} \tag{10.1}$$

where

R = maximum data rate
H = bandwidth of the channel
V = number of discrete levels in the signal

Switching techniques in data network

The recognition of the diverse characteristics of voice and data traffic has led to the development of a switching technique other than the one used for voice transmission. This technique is better suited for transmitting data traffic. Hence, two switching techniques are prevalent for data trans mission:

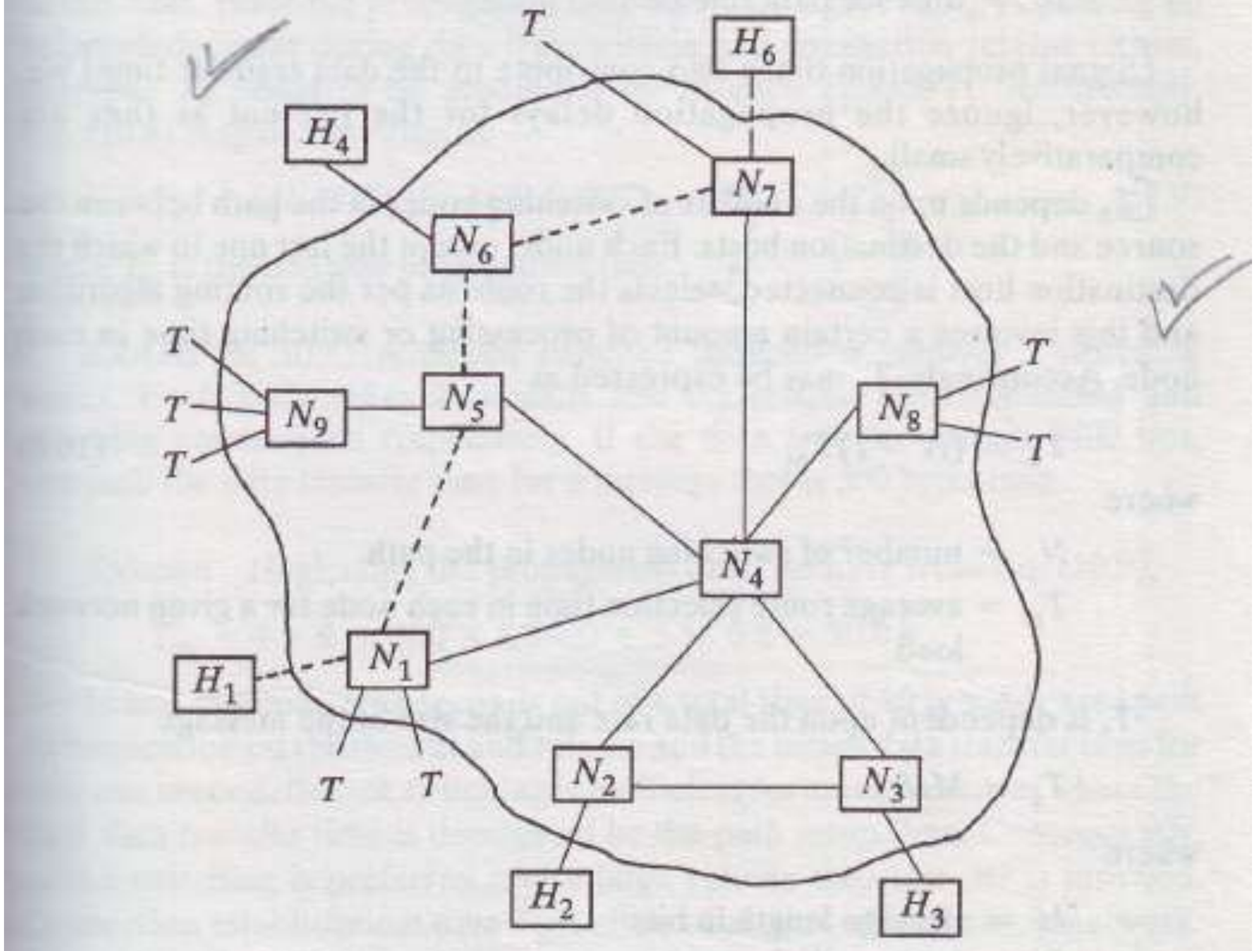
- Circuit switching
- Store and forward (S&F) switching.

Circuit switching is entirely analogous to the telephonic switching. S&F switching functions in a fashion that is analogous to the postal or telegraph system. In fact, a comparison of the characteristics of the postal system and the telephone system applies equally well to the comparison of S&F switching and circuit switching.

Circuit Switching

In circuit switching, an electrical path is established between the source and the destination before any data transfer takes place. The electrical path may be realised by physical wires or coaxial cables or radio or satellite links. It remains dedicated to the communicating pair for the entire duration of the transmission irrespective of whether data is actually transferred or not. No other potential user can use the path even if it is idle. The connection is released only when specifically signalled so by either of the communicating entities. Data transmission using a PSTN connection is a typical example of a circuit switched data transfer.

Figure 10.7 illustrates the principle of circuit switching. When the host computer H_1 wants to transfer data to the host computer H_6, a connection



H = host N = node T = terminal

Fig. 10.7 Circuit switched network.

Circuit switching has certain disadvantages for transmitting data traffic. The path set up time which is typically of the order of 20–30 s or more turns out to be an excessive overhead for bursty computer traffic which typically lasts for a few seconds or less. The entire line quality is affected if there is one

Similarly, the speed of operation of the circuit is limited by the slowest link in the circuit. This leads to poor utilisation of high capacity lines. In circuit switched connection, the required bandwidth is statically allocated and the unused bandwidth is wasted. The network provides no error control facilities which are to be handled by the end systems.

Store and Forward Switching

A store and forward (S&F) network configuration is shown in Fig. 10.9. In S&F switching, the switching nodes have the ability to store user messages and forward the same towards the destination as and when the links become available. For this purpose, each node is equipped with a processor and some buffer storage. No end-to-end link is set up prior to data transmission. The user deposits his/her message to the nearest switching node and then on, the network takes the responsibility for delivering the message to the destination user or host. (Observe the analogy to the postal system.)

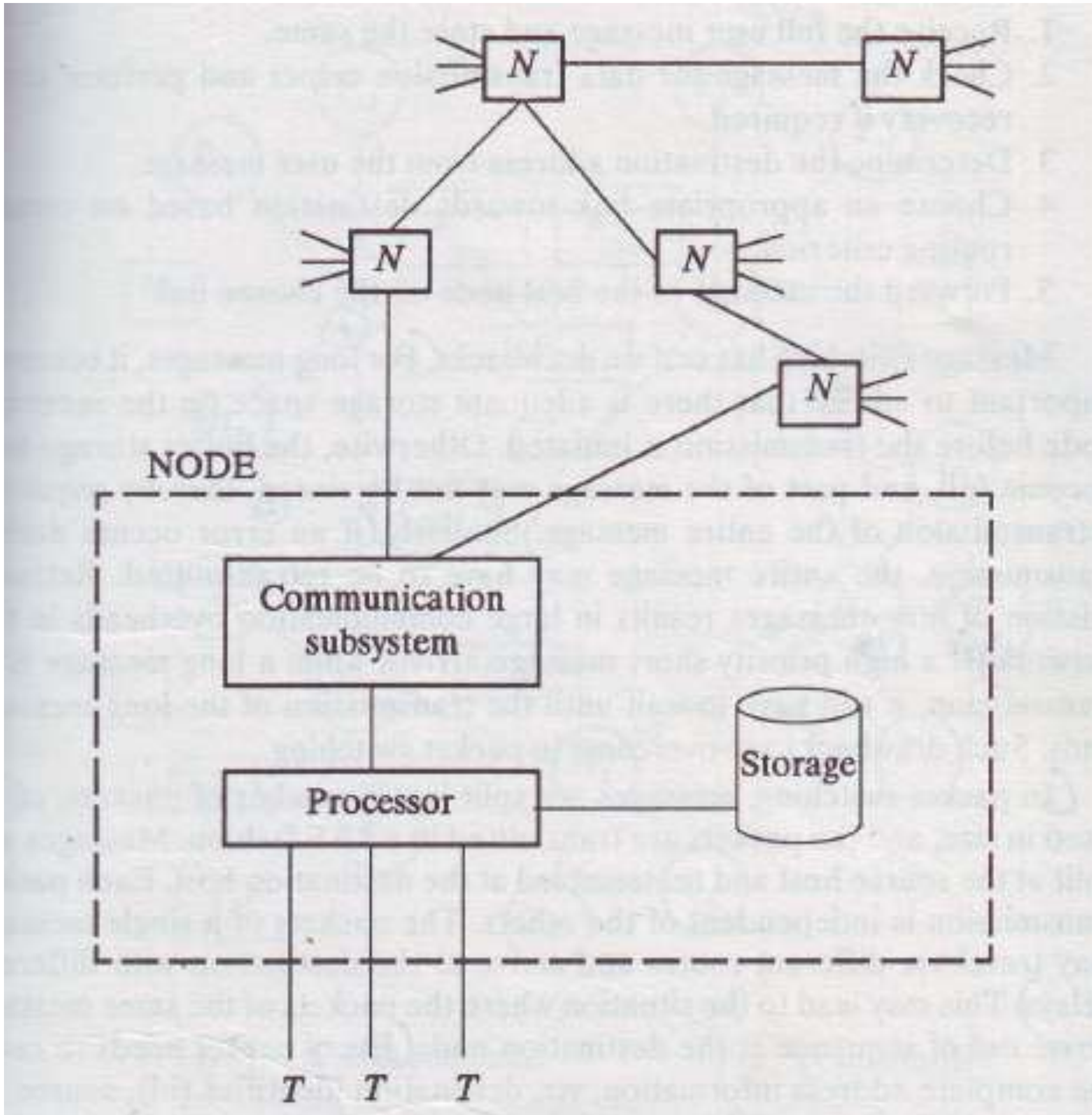


Fig. 10.9 Store and forward network.

The network moves the user information from node to node. One such movement is called a hop. Since the communication links are used one at a time between any two nodes, line speeds can be utilised efficiently. S&F switching may be classified as:

- Message switching
- Packet switching.

In message switching, once the transmission is initiated, a message is transmitted in its entirety without a break from one node to another. The node processor performs the following functions:

1. Receive the full user message and store the same.
2. Check the message for data transmission errors and perform error recovery if required.
3. Determine the destination address from the user message.
4. Choose an appropriate link towards destination based on certain routing criterion.
5. Forward the message to the next node on the chosen link.

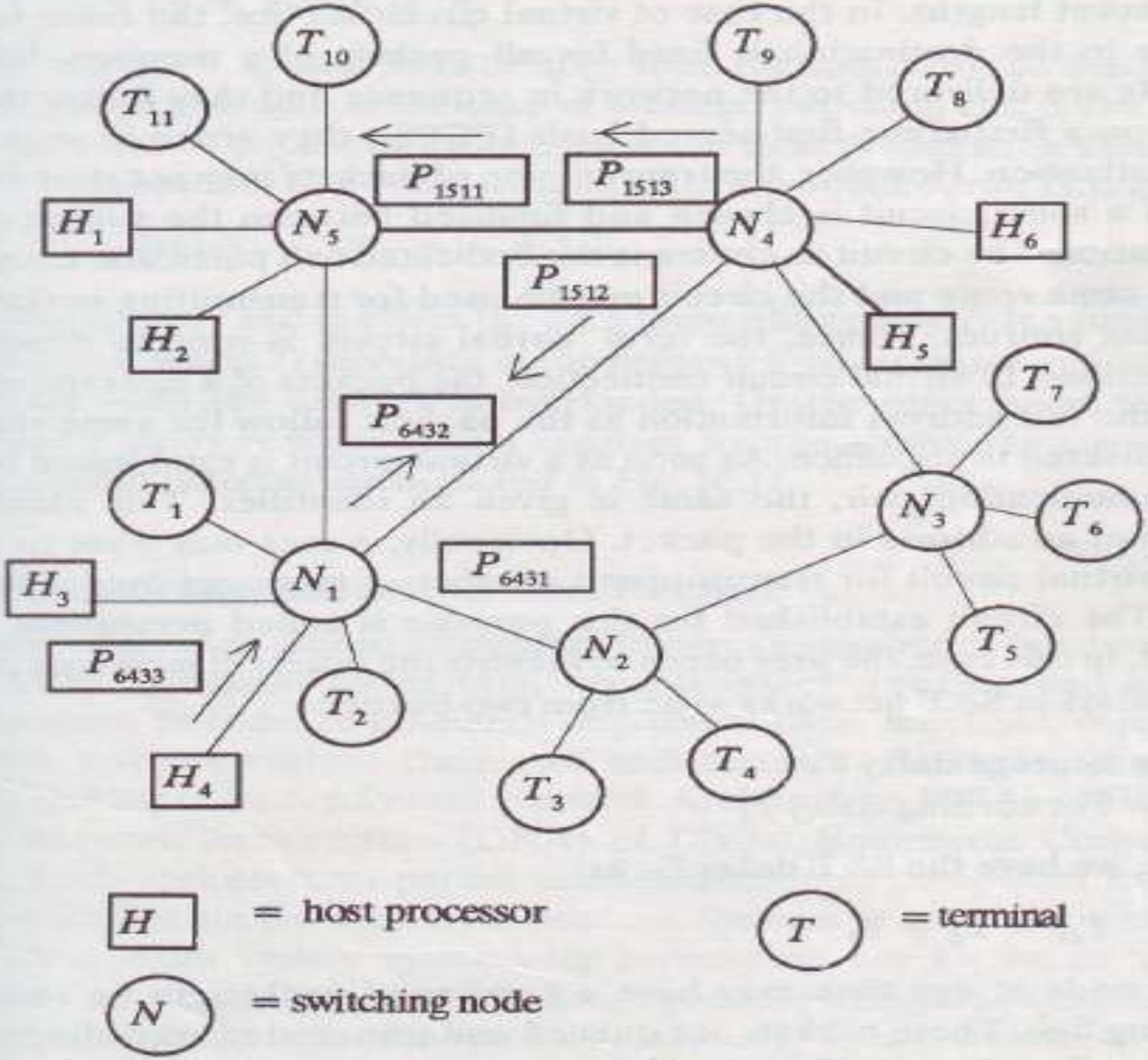
Message switching has certain drawbacks. For long messages, it becomes important to ensure that there is adequate storage space on the receiving node before the transmission is initiated. Otherwise, the buffer storage may become full, and part of the message may not be stored, thereby requiring retransmission of the entire message. Similarly, if an error occurs during transmission, the entire message may have to be retransmitted. Retransmission of long messages results in large communication overheads in the network. If a high priority short message arrives while a long message is in transmission, it will have to wait until the transmission of the long message ends. Such drawbacks are overcome in packet switching.

In packet switching, messages are split into a number of packets, often fixed in size, and the packets are transmitted in a S&F fashion. Messages are split at the source host and reassembled at the destination host. Each packet transmission is independent of the others. The packets of a single message may travel via different routes and arrive at the destination with different delays. This may lead to the situation where the packets of the same message arrive out of sequence at the destination node. Every packet needs to carry the complete address information, viz. destination identifier (id), source id, message id, and packet id, in addition to the actual user data. A typical

A packet switching schematic is shown in Fig. 10.10(b). In this schematic, a packet is numbered using a four subscript quantity where the first subscript is the destination host id, the second the source host id, the third the message id, and the fourth the packet id of the message. For example, P_{6432} indicates that this is the second packet of the third message originating from the host 4 and destined to host 6. It may be observed that the source host delivers the packets of a message in sequence to the network node and it is natural to

Header					User data
Destination id	Source id	Message id	Packet id	Control	

(a) A typical packet format



(b) Packet switching network (PSN)

Fig. 10.10 Packet switching.

Data Communication Architecture

Data communication among computers involves a number of functions such as physical transmission of bits, error control, routing and session establishment. In order to efficiently implement these functions, vendors of computer systems evolved their own architectures. Examples of vendor specific architectures are System Network Architecture (SNA) of IBM and Digital Network Architecture (DNA) of Digital Equipment Corporation (DEC). Such architectures permit interconnection of computers from the same vendor but not from different vendors. Systems or networks, which are not open to other vendor systems for networking, are known as 'closed' systems or networks. In order that heterogeneous computer systems from different vendors be interconnected as a network, an architecture which is used as a standard by all the vendors is required. The heterogeneity covers the following aspects:

1. Systems of different vendors
2. Systems under different managements
3. Systems of different complexities
4. Systems of different technologies.

1. ISO-OSI Reference Model

Before we discuss this model, a few definitions are in order.

System: A system is one or more autonomous computers and their associated software, peripherals and users, which are capable of information processing and/or transfer.

Subsystem: A logically independent smaller unit of a system. A succession of subsystems make up a system as shown in Fig. 10.12.

Layer: A layer is composed of subsystems of the same rank of all the interconnected systems. The concept of a layer is illustrated in Fig. 10.12, which shows a five-layer network. The subsystems and the layers are numbered starting with one at the bottom level.

Entity: The functions in a layer are performed by hardware subsystems and/or software packages. These are known as entities.

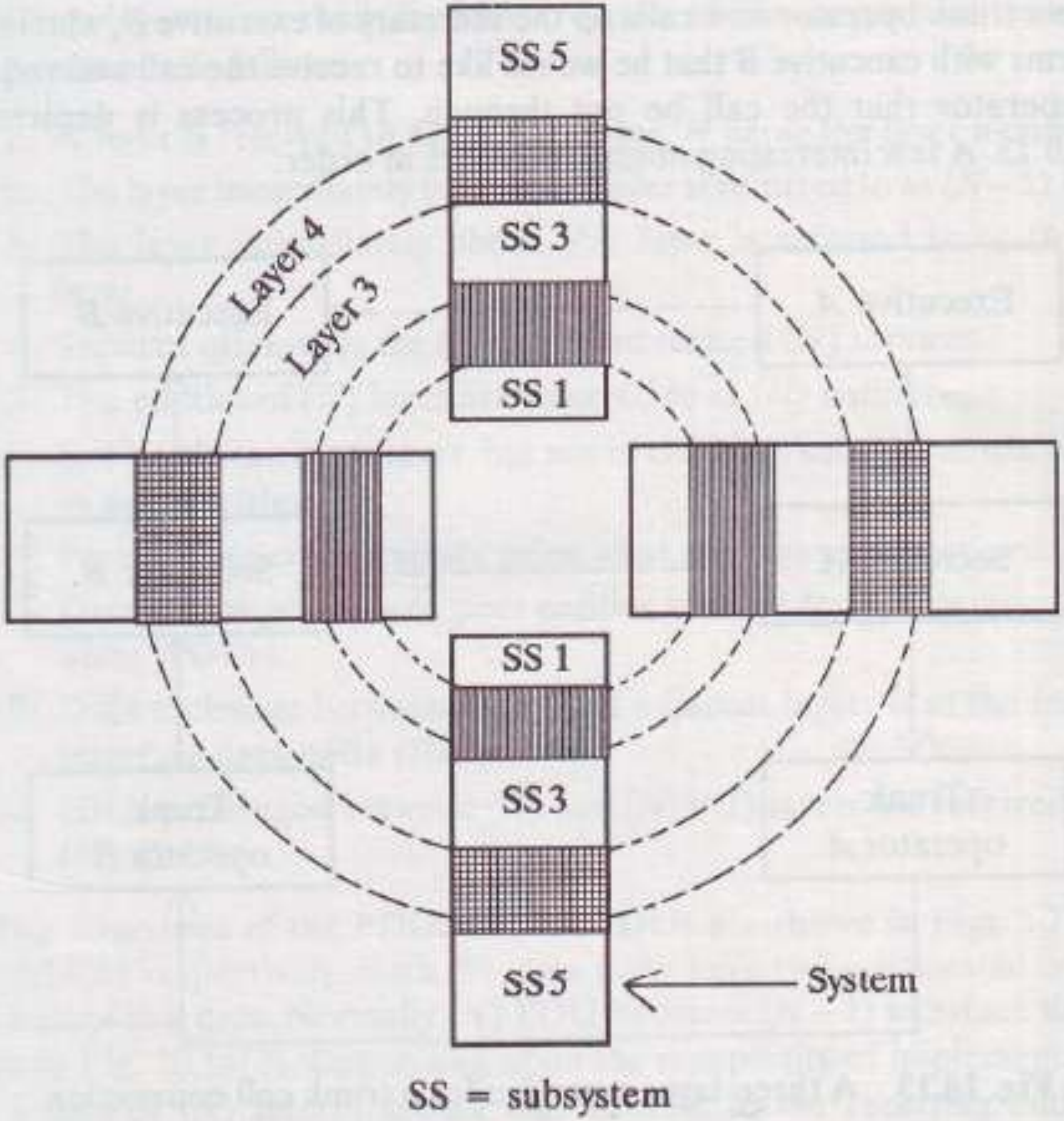


Fig. 10.12 Systems, subsystems and layers in ISO-OSI model.

ISO-OSI architecture is a layered one. Layering is a natural choice for communication architectures. This is well illustrated by an example.

Consider the activities that are involved when executives *A* and *B* of two companies in different cities want to converse over a trunk telephone connection. For the sake of illustration, let us assume that there is no subscriber trunk dialling (STD) facility between the two cities. Let executive *A* be the calling party. As a first step, he requests his secretary to connect him to executive *B*. His secretary in turn calls up the trunk operator and communicates the calling number, called number, nature of the call, the name of the particular person called etc. Then, the local trunk operator calls up the other trunk operator in the other city and communicates the details. Remote trunk operator now calls up the secretary of executive *B*, who in turn confirms with executive *B* that he would like to receive the call and requests the operator that the call be put through. This process is depicted in Fig. 10.13. A few interesting observations are in order:

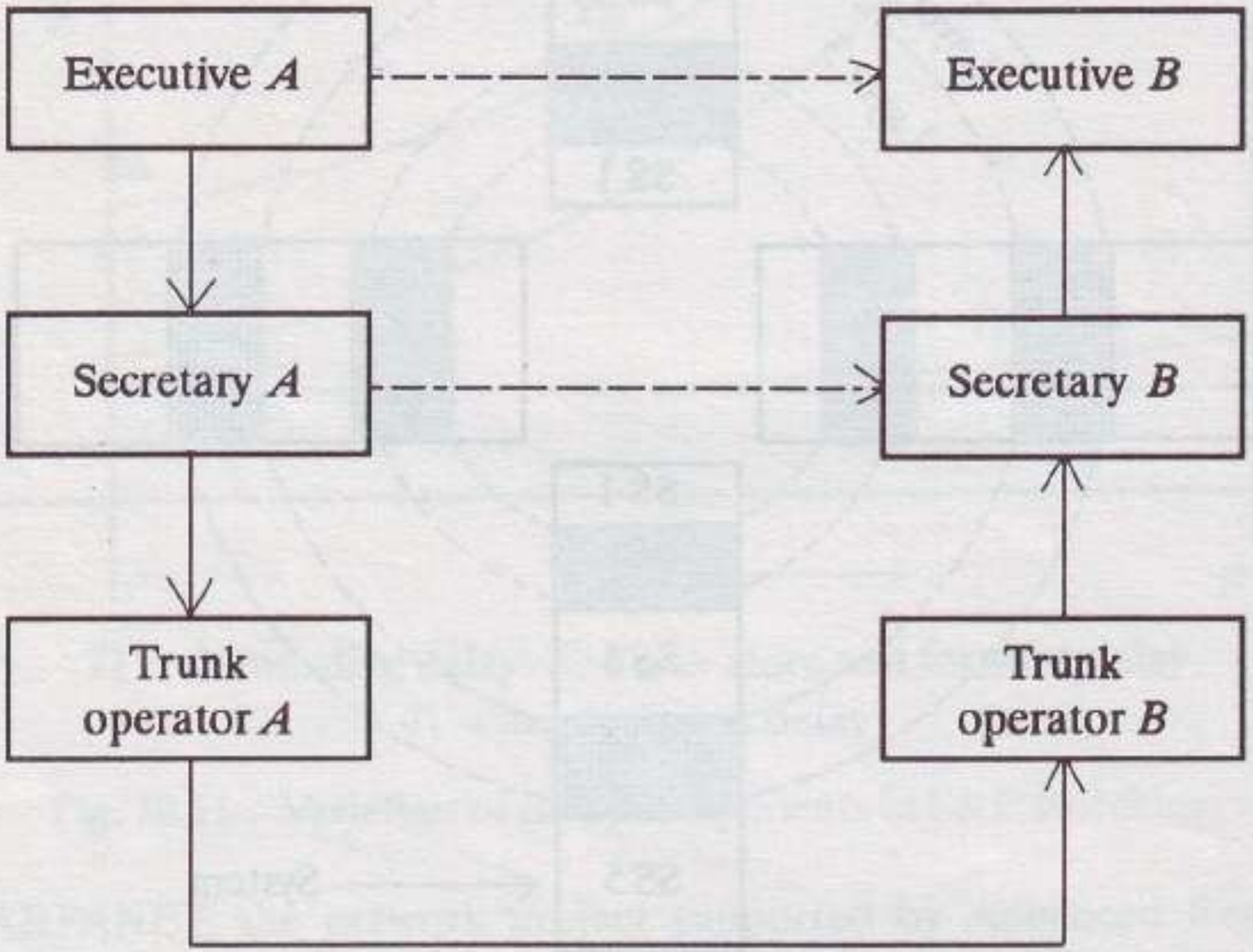


Fig. 10.13 A three-layer structure for a trunk call connection.

1. A three-layer structure is used in this communication process.
2. The conversation between an upper and lower layer is strictly business like.
3. There is generally a little private conversation between the trunk operators and the two secretaries on account of their familiarity. In other words, entities in the same level or layer exchange information using their own private protocols.
4. A layer obtains services from its immediate lower layer and provides services to its immediate upper layer. In this sense, a layer acts both as a user as well as a service provider.
5. There are fairly well defined functions to be performed by each layer.
6. It is immaterial as to how the functions of each layer are implemented. For example, the secretary may ask his assistant to book the call and as far as the executive is concerned, it is immaterial who books the call as long as the call is booked.

In fact, the above observations regarding a simple telephone conversation are some of the stated important layering principles of OSI reference model. IS 7498 recommends standard reference conventions when discussing layers and their functions. Some of the important reference conventions are as follows:

1. A layer is referred to as the (*N*) layer, *N* being the layer number.
2. The layer immediately below (*N*) layer is referred to as (*N* – 1) layer.
3. The layer immediately above (*N*) layer is referred to as (*N* +1) layer.
4. Services offered by the (*N*) layer are termed (*N*) services.
5. The entities of (*N*) layer are referred to as (*N*) entities.
6. Entities in the same layer, but not in the same subsystem, are known as **peer entities.**
7. Peer entities communicate using what are known as **peer protocols.**
8. Data exchange between peer entities is in the form of **protocol data units (PDUs).**
9. Data exchange between entities of adjacent layers is in the form of **interface data units (IDUs).**
10. IDUs exchanged between (*N*) and (*N* + 1) layers are referred to as (*N*) IDUs.

Link-to-link Layers

The first three layers, viz. physical, data link and network layers, form the link-to-link layers of OSI reference model. Entities in an OSI layer perform certain functions to fulfill the stated purpose of the layer. They obtain services from the immediate lower layer and provide services to the immediate upper layer. OSI services may be placed under two broad categories:

- Connection oriented services
- Connectionless services.

In connection oriented services, a connection is first established between the sender and the receiver before data transfer can commence. The connection may be virtual (logical) or physical, depending upon the network

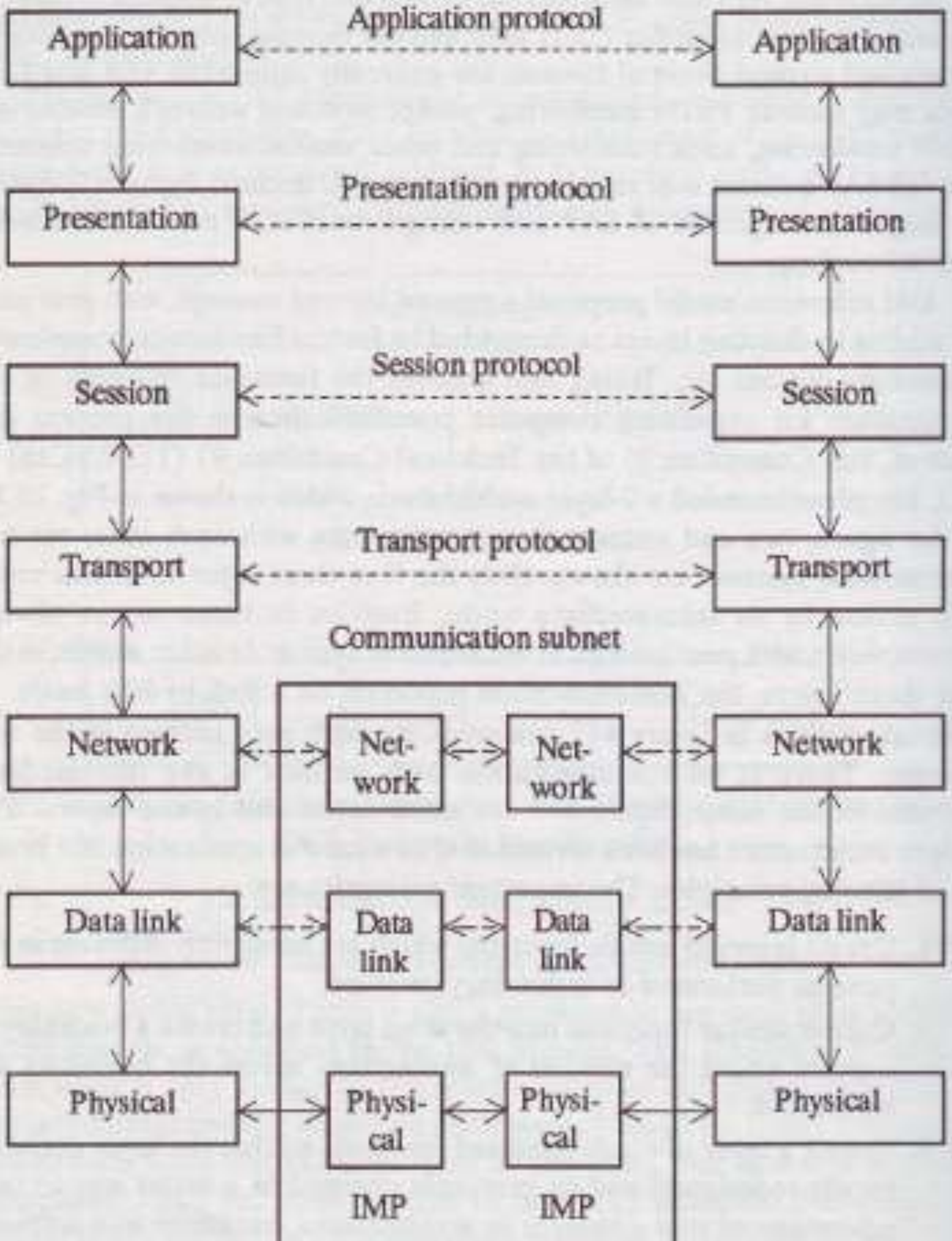
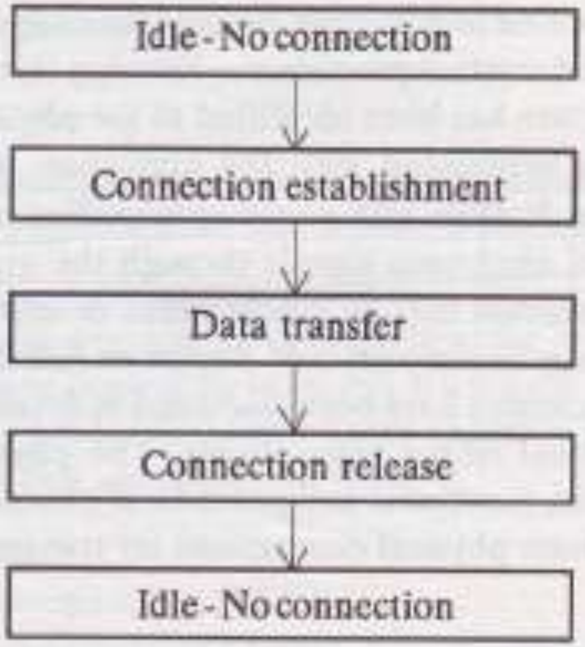
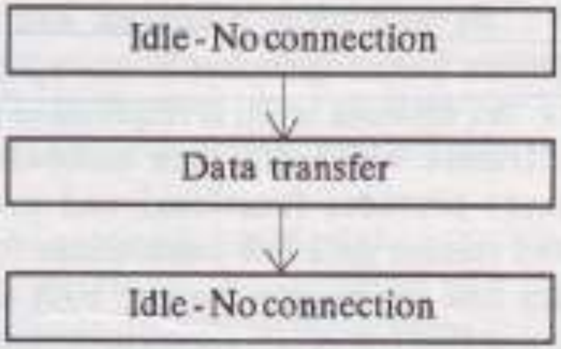


Fig. 10.17 ISO OSI reference model.

capabilities and facilities. The essence of a connection oriented service is that a connection acts like a tube or a pipe delivering the data to the receiver strictly in the same order in which the data was put into the connection by the sender. Connection oriented service is modelled after the telephone system. In contrast, connectionless service is modelled after the postal system. Each submission by the sender is treated independently of others and is self-contained with the full address of the destination and the source indication which may be the full address too. In connectionless service, when two messages are sent to the same destination one after another, it is possible that the first one is delayed and the second one arrives first. Datagram service and the virtual circuit service discussed in Section 10.2 are examples of connectionless and connection oriented services respectively. The operation of the two categories of services is shown in Figs. 10.18(a) and (b).



(a) Connection oriented service



(b) Connectionless service

Operation of connection oriented and connectionless networks.

A connection oriented service has provision for acknowledgements, flow control and error recovery, whereas a connectionless service does not generally have such provisions.

Peer entities of OSI layers communicate using peer protocols. Protocols are strict procedures and sequence of actions to be followed in order to achieve orderly exchange of information among peer entities. Corresponding to the two categories of services, there are two sets of protocols; one set for the connection oriented services and the other for connectionless services. It is important to recognise that layer protocols relate to the implementation of services of the layer and therefore are not visible to the users or other layers. This separation of services and the protocols provides complete freedom to change protocols at will without affecting the services.

10.4.1 Physical Layer

It is essential that the OSI architecture permits the usage of a realistic variety of physical media and control procedures. Keeping this in mind, the lowest layer of the architecture has been identified as the physical layer. This layer performs functions associated with the activation and deactivation of physical connections. It deals with encoding/decoding of signals and the bit level transmission of electronic signals through the available transmission medium. The transmission may be synchronous or asynchronous. Mode of data transmission may be simplex, half duplex or full duplex. Transmission and data encoding schemes have been discussed in detail in Chapters 5 and 7 for cables and optical fibres respectively. The physical layer provides mechanical, electrical, functional and procedural characteristics to activate, maintain and deactivate physical connections for transmission of bits.

10.4.2 Data Link Layer

Some physical communication media like telephone lines have error rates that are not acceptable for the great majority of data network applications. Special techniques are required to ensure error free transmission of data. The data link layer deals with error detection, and automatic recovery procedures required when a message is lost or corrupted. For this purpose, a user of this layer, i.e. the network layer, is required to break up the data to be transmitted into frames which are then numbered and transmitted sequentially. The layer provides functional and procedural means to establish, maintain and release data link connections for the entities in the network layer. A data link connection may be built upon one or several physical connections. Another important function performed by the data link layer is the link level flow control of frames. Flow control is essentially a traffic regulation mechanism that will have to be enforced when the receiver is unable to accept frames as fast as the transmitter is able to send.

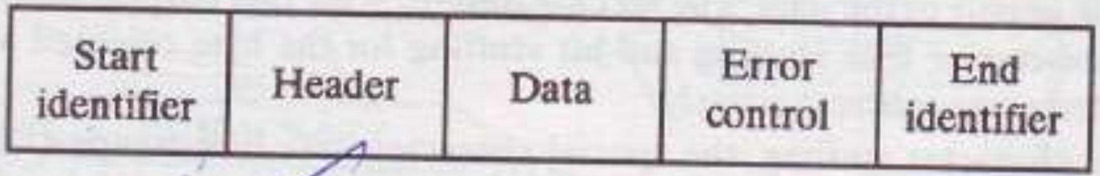
A data link may be of point-to-point type as in the case of terrestrial networks or broadcast type as in the case of SBDNs, LANs or MANs. In the case of broadcast type channels, the data link layer will have to perform an additional function of acquiring or accessing the channel before data transmission can begin. Media access techniques for satellite channels are

The main sources of error in a system are:

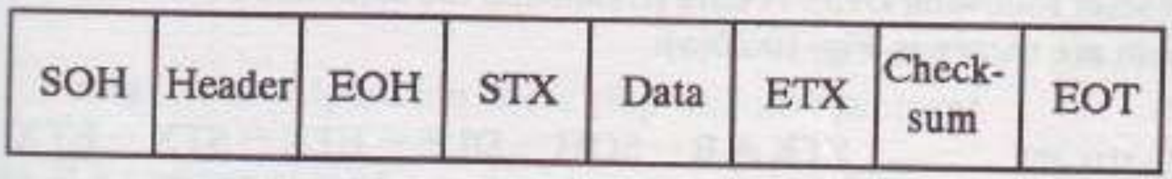
1. Thermal noise which is internal to the system
2. Impulse or spike noise which originates from man-made sources like automobiles or signalling in telephone systems, and from natural sources like lightning
3. Crosstalk which occurs through electromagnetic radiation from parallel and adjacent wires which behave like an antenna.

Errors are of two types: isolated and bursty. Errors due to thermal noise are generally isolated, whereas errors due to spike noise or crosstalk are bursty in nature. Error control mechanisms are chosen depending upon the type of error that is predominant in a given system. There are three error control mechanisms that are commonly used:

1. Echo checking
2. Forward error correction (FEC)
3. Automatic repeat request (ARQ).



(a) General structure of a frame



EOH = end of header ETX = end of text EOT = end of transmission
SOH = start of header STX = start of text

(b) structure of a character oriented frame

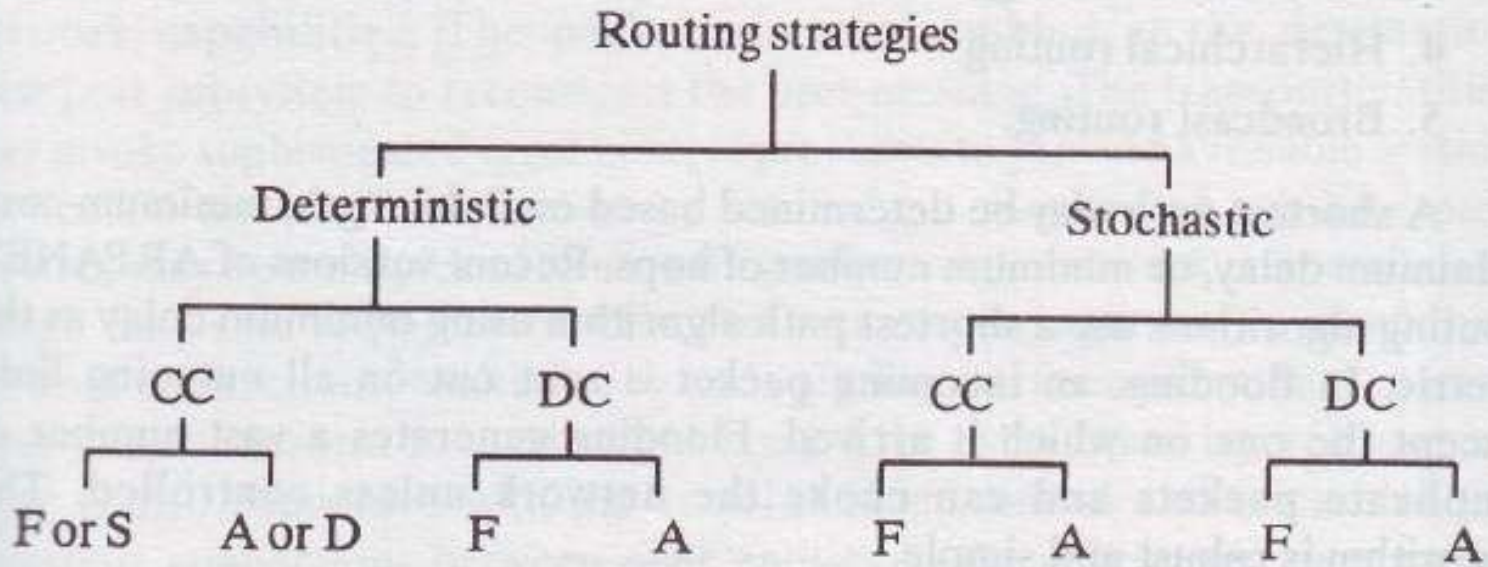
(c) Structure of a bit oriented frame

Fig. 10.19 Data link frame structure.

10.4.3 Network Layer

The highest link-to-link layer in the OSI model is the network layer. Although this layer functions on a link-to-link basis, it is concerned with transmission of packets from the source node to the destination node. It deals with routing and switching considerations that are required in establishing a network connection which may involve the use of several transmission resources in tandem, including a number of intermediate switching nodes of different subnetworks. The network layer makes invisible to the transport layer, the details of the underlying communication media and the different characteristics of the transmission and network technologies. It only assures a certain quality of service to the upper layers. Since an end-to-end connection may involve routing through a number of different networks, internetworking is an important function of the network layer. Addressing schemes, network capabilities, protocol differences, and accounting and billing are all issues to be handled in internetworking. Network congestion, which may occur due to too many messages on a particular route, is also tackled by the network layer.

There is a wide variety of routing and congestion control algorithms. However, OSI network layer specifications do not recommend and discuss any routing or congestion control algorithms and they are left as implementation dependent features. We briefly discuss some of the generic routing and congestion control strategies here. Routing strategies may be classified as shown in Fig. 10.24. Routing algorithms may be deterministic or.



CC = centralised control DC = distributed control F = fixed
S = static A = adaptive D = dynamic

Fig. 10.24 Classification of routing algorithms.

A number of measures may be used in assessing the performance of a routing algorithm:

1. Minimum delay
2. Minimum number of intermediate nodes or hops
3. Processing complexity
4. Signalling capacity required on the network
5. The rate of adaption in the case of adaptive algorithms
6. Fairness to all types of traffic
7. A reasonable response time over a range of traffic intensities
8. Robustness: the ability to reach the destination even when parts of the network fail
9. Stability: the ability to reach the destination quickly without wandering.

Some examples of the widely used algorithms are:

1. Shortest path
2. Flooding
3. Flow based routing
4. Hierarchical routing
5. Broadcast routing.

End-to-End Layers

Many data networks were operational before the OSI model was designed. These networks were well thought out up to the network layer, but little had been done about the transport layer and above. As a consequence, the design of the bottom three layers of OSI was highly influenced by pre-OSI developments. In contrast, OSI design is expected to dominate the upper four layers in the years to come except for the influence of transmission control protocol (TCP) of ARPANET at the transport layer, which has come to be accepted widely.

Transport Layer

Transport layer is the first end-to-end layer in the OSI architecture. It is responsible for matching user message characteristics and service requirements with that of the network capabilities. In a packet switched network, the transport entity breaks up a long user message into packets to match the network capabilities. The packets are reassembled at the destination transport subsystem to reconstruct the user message. The transport entities may invoke sophisticated error control protocols to provide a reliable session service on an unreliable network. Similarly, a number of low rate user services may be multiplexed to use efficiently a single network connection, or a high data rate requirement from the user may be split into a number of network connections. Multiplexing and splitting, performed by the transport layer are transparent to the sessions layer. Like every other layer, transport layer is also concerned with the establishment, control and release of the transport connections between peer entities in the source and destination systems. End-to-end flow control and error recovery are also functions of the transport layer. The need for flow control arises when the speed or the buffer space of the destination machine does not match with that of the source machine. Similarly, end-to-end error recovery becomes necessary when the

As far as a user is concerned, it is the transport layer that offers transport services regardless of the underlying subnetwork. The user makes his service requests to this layer by specifying certain 'quality of service' (QOS) parameter values. Some QOS parameters that are of direct interest to the users are:

1. Transit delay
2. Residual error rate
3. Protection
4. Transfer failure probability
5. Priority
6. Throughput.

10.5.2 Session Layer

The main function of the session layer is to organise different sessions between cooperating entities and perform all related functions like synchronisation, failure management, control, etc. for the successful execution of a session. Online search of databases, remote job entry, remote login to a time sharing system and file transfer between two systems are all examples of sessions. Different sessions have different requirements. For example, a dialogue session may be two-way simultaneous, or one-way alternate. A large file transfer session may call for rollback points being established in order to recover from system crashes. An online transaction processing session calls for semaphore management, and file, record and sometimes even item level lock mechanisms. A quarantine service is one which enables a specified number of presentation layer SDUs to be transported to the destination system but not actually deliver them unless explicitly so requested by the sender. The session layer may also offer a directory service.

10.5.3 Presentation Layer

The purpose of the presentation layer is to represent information to the communicating application entities in a way that preserves the meaning while resolving syntax differences. Syntax differences are resolved by encoding application data into a standard abstract notation that is valid throughout the network. Thus, file format differences (e.g. IBM or DEC format), data representation differences (e.g. ASCII or EBCDIC) or data structure differences are all resolved by using a standard notation. Data transformation and formatting may include data compression, encryption etc. There are two aspects associated with network wide handling of a variety of data in a standard form. First, the representation of the data in a standard form, and second, the transmission of the data as a bit stream across the network.

10.5.4 Application Layer

As the highest layer in the OSI reference model, the application layer provides services to the users of OSI environment. The layer provides all services that are directly comprehensible by the users, which include

1. Electronic mail or message handling services
2. Directory services
3. Cost allocation
4. Determination of quality of service
5. File transfer and management
6. Editors and terminal support services
7. Telematic services like videotex.

In general, every application requires its own software which in turn uses a number of generic supporting packages. These generic packages and the application specific packages are part and parcel of the application layer. What is listed above is a set of generic applications and support packages. For example, file transfer or remote file access may be used by airlines reservation system, banking applications etc. Similarly, electronic mail may be used in order placement and processing systems. There is yet another level of support packages that are used by some of these generic applications packages. They include connection establishment, transaction processing, database crash recoveries etc. Two such packages are:

- Association control service element (ACSE)
- Commitment, concurrency and recovery (CCR).

Satellite Based Data Networks