Unit 17 □ Network Architecture and Services

Structure

17.0 Objectives

The objectives of the Unit are to :

- Explain the concept of network architecture
- Study OSI models

17.1 Introduction

Networks are connections between groups of computers and associated devices that allow users to transfer information electronically. It implies techniques, physical

connections, and computer programmes used to link two or more computers. Network users are able to share files, printers and other resources; send electronic messages; and run programmes on other computers. A network has three layers of components : application software, network software and network hardware. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams. In effect, computer network may be considered as a communication channel. The basic reasons for the growth of computer networks are :

- Resource sharing
- Data sharing
- Communication and data exchange.

17.2 Network Connections

A network has two types of connections : Physical connections and Logical or Virtual Connections.

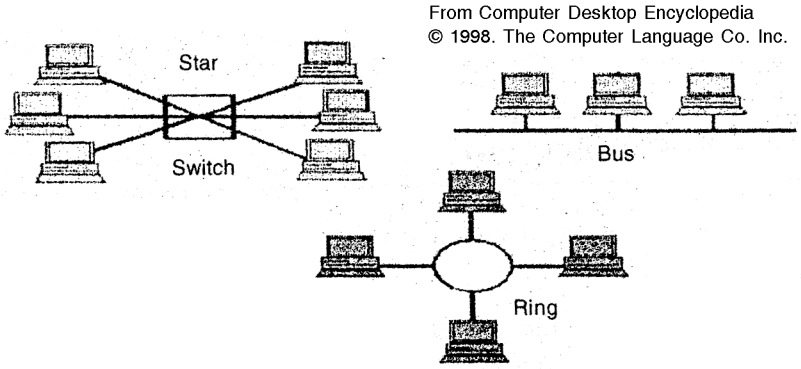
- Physical connections that let computers directly transmit and receive signals. Physical connections are defined by the medium used to carry the signal, the geometric arrangement of the computers (topology) and the method used to share information.
- Logical, or virtual, connections that allow computer applications, such as word processors, to exchange information. Logical connections are created by network protocols and allow data sharing between applications of different types of computers, such as an Apple Macintosh and an IBM personal computer (PC), in a network. Some logical connections use client-server application software and are primarily for file and printer sharing. The Transmission Control Protocol/Internet Protocol (TCP/IP) suite is the set of logical connections used by the Internet. TCP/IP, based on peer-to-peer application software creates a connection between any two computers.

17.3 Network Architecture (Topology)

Computers communicate with other computers via networks. The simplest network is a direct connection between two computers. However, computers can also be connected over large networks, allowing users to exchange data, communicate via electronic mail, and share resources such as printers. Computers can be connected in

serveral ways. The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology (Protocol) which is the method used to pass information between workstations. Main types of physical topologies are :

- Linear Bus
- Star
- Star-Wired Ring
- Tree



17.3.1.1 Linear Bus

A linear bus topology consists of a main run of cable with a terminator at each end. All nodes (file server, workstations, and peripherals) are connected to the linear cable. Ethernet and Local Talk networks use a linear bus topology.

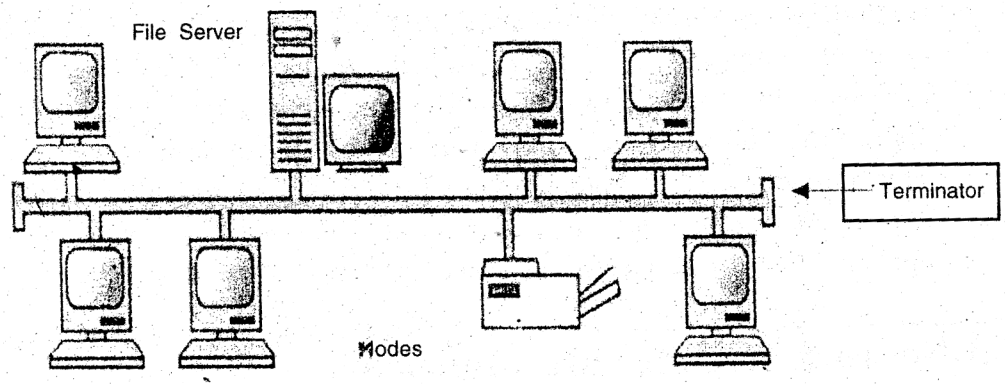


Figure : Linear Bus topology

In a bus configuration, computers are connected through a single set of wires, called a bus. A bus requires a full duplex medium (one which signals can flow in either direction). One computer sends data to another by broadcasting the address of the receiver and the data over the bus. All the computers in the

network look at the address simultaneously and the intended recipient accepts the data. A bus network, unlike a ring network, allows data to be sent directly from one computer to another. However, only one computer at a time can transmit data. The others must wait to send their messages. Messages are detected by all nodes but are accepted only by the node(s) to which they are addressed. Because a bus network relies on a common data "highway," a malfunctioning node simply ceases to communicate; it doesn't disrupt operation.

Advantages of a Linear Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.
- Lack of routing and the lack of centralized control provide substantial reliability.

Disadvantages of a Linear Bus Topology

- Entire network shutsdown if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shutsdown.
- Not meant to be used as a stand-alone solution in a large building.
- Segmenting the network for maintenance is difficult.
- The impedance irregularities caused by the installation of taps cause signal reflections that can interfere data transmission if nodes/taps are placed too closed to each other.

17.3.1.2 Star

In a star configuration, computers are linked to a central computer called a hub. A computer sends the address of the receiver and the data to the hub, which then links the sending and receiving computers directly. A star network allows multiple messages to be sent simultaneously, but it is more costly because it uses an additional computer, the hub, to direct the data.

A star topology is designed with each node(file server, workstations and peripherals) connected directly to a central network hub or concentrator. Data on a star network passes through the hub or concentrator before continuing to its destination. The hub or concetrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

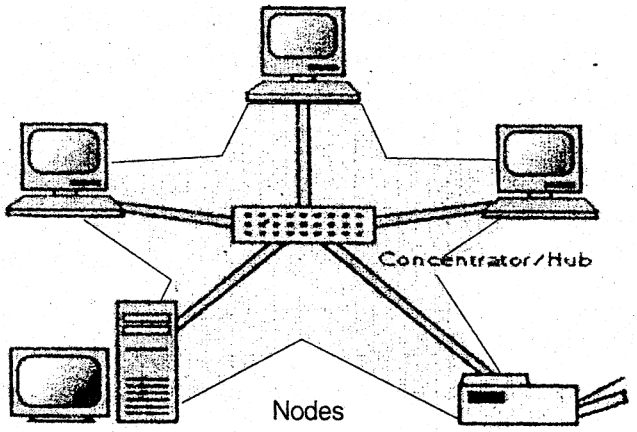


Figure : Star topology

A star network is reliable in the sense that a node can fail without affecting any other node on the network. Its weakness, however, is that failure of the central computer results in a shutdown of the entire network. And because each node is individually wired to the hub, cabling costs can be high.

Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

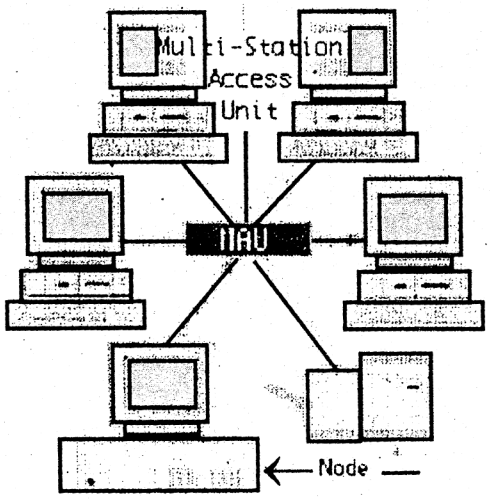
- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.

The protocols used with star configurations are usually Ethernet or LocalTalk. Token Ring uses a similar topology, called the star-wired ring.

17.3.1.3 Star-Wired Ring

In a ring configuration, data are transmitted along the ring and each computer in the ring examines this data to determine if it is the intended recipient. If the data are not intended for particular computer, the computer passes the data to the next computer in the ring. This process is repeated until the data arrive at their intended destination. A ring network allows multiple messages to be carried simultaneously, but since each computer checks each message; data transmission is slow. A star-wired ring topology may appear (externally) to be the same as a star topology. Internally, the MAU (multi

station access unit) of a star-wired ring contains wiring that allows information to pass from one device to another in a circle or ring. The Token Ring protocol uses a star-wired ring topology.



17.3.1.4 Tree

A tree topology combines characteristcs of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable. Tree topologies allow for the expansion of an existing network and enable organizations to configure a network to meet their needs.

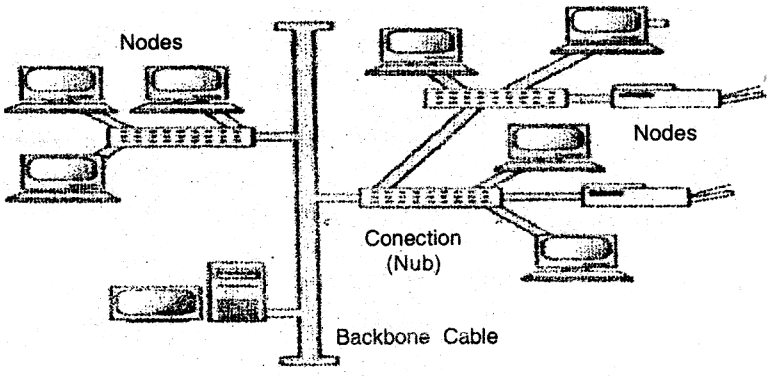


Figure : Tree topology

Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software vendors.

Disadvantages of a Tree Topology

- Overall the type of cabling used limits length of each segment.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

17.3.1.5 5-4-3 Rules

A consideration in setting up a tree topology using Ethernet protocol is the 5-4-3 rule. One aspect of the Ethernet protocol requires that a signal sent out on the network cable reach every part of the network within a specified length of time. Each concentrator or repeater that a signal goes through adds a small amount of time. This leads to the rule that between any two nodes on the network there can only be a maximum of 5 segments, connected through 4 repeaters/concentrators. In addition, only 3 of the segments may be populated (trunk) segments if they are made of coaxial cable. A populated segment is one, which has one, or more nodes attached to it. In Figure (Tree Topology), the 5-4-3 rules is adhered to. The furthest two nodes on the network have 4 segments and 3 repeaters/concentrators between them. This rule does not apply to other network protocols or Ethernet networks where all fiber optic cabling or a combination of a fiber backbone with UTP cabling is used. If there is a combination of fiber optic backbone and UTP cabling, the rule simply translated to 7-6-5 rule.

Summary Chart :

Physical Topology	Common Cable	Common Protocol
Linear Bus	Twisted Pair Coaxial Fiber	Ethernet LocalTalk
Star	Twisted Pair Fiber	Ethernet LocalTalk
Star-Wired Ring	Twisted Pair	Token Ring
Tree	Twisted Pair Coaxial Fiber	Ethernet

17.3.2 Protocol

Networks use protocols, or rules, to exchange information through a single shared connection. These rules include guidelines that regulate the following characteristics of a network :

- Access method,
- Allowed physical topologies,
- Types of cabling, and
- Speed of data transfer.

These protocols prevent collisions of data caused by simultaneous transmission between two or more computers. Computers on most LANs use protocols known as Ethernet or Token Ring. An Ethernet-linked computer checks if a shared connection is in use. If not, the computer transmits data. Since computers can sense an idle connection and send data at the same time, transmitting computers continue to monitor their shared connection and stop transmitting if a collision occurs. Token Ring protocols pass a special message called a token through the network. A computer that receives the token is given permission to send a packet of information or if the computer has no packet to send, it passes the token to the next computer. The most common protocols are :

- Ethernet
- LocalTalk
- Token Ring
- FDDI
- ATM

17.3.2.1 Ethernet

The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.

17.3.2.2 LocalTalk

LocalTalk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by LocalTalk is called CSMA/CA (Carrier sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except

that a computer signals its intent to transmit before it actually does so. LocalTalk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established. The LocalTalk protocol allows for linear bus, star or tree topologies using twisted pair cable. A primary disadvantage of LocalTalk is speed. Its speed of transmission is only 230 Kbps.

17.3.2.3 Token Ring

IBM developed the Token Ring protocol in the mid-1980s. The access method used involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the receiving computer captures the data. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring has decreased.

17.3.2.4 FDDI

Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. A major advantage of FDDI is speed. It operates over fiber optic cable at 100 Mbps.

17.3.2.5 ATM

Asynchronous Transfer Mode (ATM) is a network protocol that transmits data at a speed of 155 Mbps and higher. ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.

Protocol Summary

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair,	10 Mbps	Linear Bus, Star,
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4Mbps-16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

17.3.2.6 TCP/IP

TCP/IP is a layered protocol, which means that after an application initiates the communication, the message (data) to be transmitted is passed through a number of stages or layers, until it actually moves out onto the wire. The data are packaged with a different header at each layer. At the receiving end, the corresponding programmes at each protocol layer unpackage the data, moving it "back up the stack" to the receiving application.

TCP/IP is composed of two parts : TCP (Transmission Control Protocol) and IP (Internet Protocol). TCP is a connection-oriented protocol that passes its data to IP, which is connectionless. TCP sets up a connection at both ends and guarantees reliable delivery of the full message sent. TCP tests for errors and requests retransmission if necessary, because IP does not. Although the OSI model is widely used and often cited as the standard, most Unix workstation vendor have used TCP/IP protocol. TCP/IP is designed around a simple four layer scheme. It does omit some features found under the OSI model. Also it combines the features of some adjacent OSI layers and splits other layers apart. The four network layers defined by TCP/IP model are as follows.

1. Layer 1 - Link : This layer defines the network hardware and device drivers.
2. Layer 2 - Network : This layer is used for basic communication, addressing and routing. TCP/IP uses IP and ICMP protocols at the network layer.
3. Layer 3 - Transport : Handles communication among programmes on a network. TCP and UDP falls within this layer.
4. Layer 4 - Application : End-user applications reside at this layer. Commonly used applications include NFS, DNS, arp, rlogin, talk, ftp, ntp and traceroute.

17.4 Standard Sayered Framework for Network Design (Open System Interconnection)

The Open Systems Interconnection (OSI) reference model has been an essential comoponent of computer network design model since its inception in 1984. OSI is an abstract model, meaning that actual network implementations need not to adhere to it strictly. The ISO (International Standards Organization) has created a layered model, called the OSI (Open Systems Interconnect) model, to describe defined layers in a network operating system. The purpose of the layers is to provide clearly defined functions that can improve inter-network connectivity between "computer" manufacturing companies. Each layer has a standard defined input and a standard defined output.

This is a top-down explanation of the OSI Model. It starts with the user's PC and it follows what happens to the user's file as it passes though the different OSI Model layers. The top-down approach was selected specifically (vs. starting at the Physical Layer and working up to the Application Layer) for ease of understanding. It is used here to show how the user's files are transformed (through the layers) into a bit stream for transmission on the network. These are the 7 Layers of the OSI model :

7. Application Layer (Top Layer)
6. Presentation Layer
5. Session Layer
4. Transport Layer
3. Network Layer
2. Data Link Layer
1. Physical Layer (Bottom Layer)

The OSI model divides the complex task of host-to-host networking, traditionally called internetworking, into layers. Layers in the OSI model are ordered from lowest level to highest in a stack. The OSI contains seven layers in two groups :

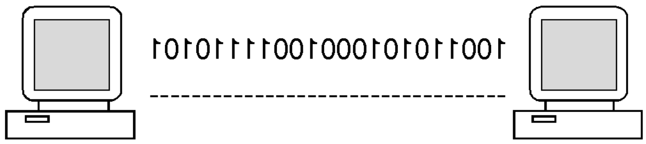
Upper Layers

OSI designates the application, presentation and session layers as "upper" layers. Generally speaking, software in these layers performs application specific functions like data formatting, encryption, and connection management. Higher layers cover network requests and responses, representation of data and network protocol as seen from a user's point of view.

The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data. For example, in a Web browser application, the Application layer protocol HTTP packages the data needed to send and receive Web page content. The Application layer provides data to (and obtained data from) the Presentation layer.

Lower Layers

The remaining lower layers provide more primitive network-specific functions like routing, addressing, and flow control. The lower layers deal with electrical signals, chunks of binary data, and routing of these data across networks.



The physical layer is responsible for the ultimate transmission of data over network communications media. It operates with data in the form of bits that are sent from the physical layer of the sending (source) device and received at the physical layer of the destination device. Ethernet cabling, Token Ring network technology and SCSI all function at the Physical Layer. Hubs and Repeaters are standard network devices that function at the Physical layer. At the physical layer, data are transmitted using the type of signaling supported by the physical medium :

- Electric Voltage
- Radio Frequencies
- Pulses of infrared or ordinary light

The OSI Model of computer Networks

Upper Layers	Application	HTTP, FTP, SMTP
	Presentation	GIF, MPEG
	Session	AppleTalk, WinShock
Lower Layers	Transport	TCP, UDP, SPX
	Network	IP, IPX
	Data Link	Ethernet, ATM
	Physical	Ethernet, Token Ring, Hub, Repeater

Layer 7-Application Layer

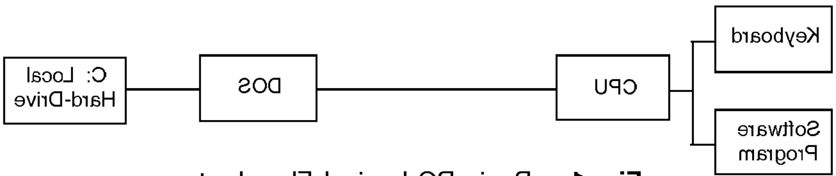


Fig. 1. : Basic PC Logical Flowchart

A basic PC logic flowchart is shown in Fig. 1. The keyboard & application are shown as inputs to the CPU (requesting access to the hard disk). The keyboard requests accesses through user inquiries and the application seeks access through "File Openings" and "Saves". The CPU, through the Disk Operating System, sends and receives data from the local hard disk ("C:" in this example).

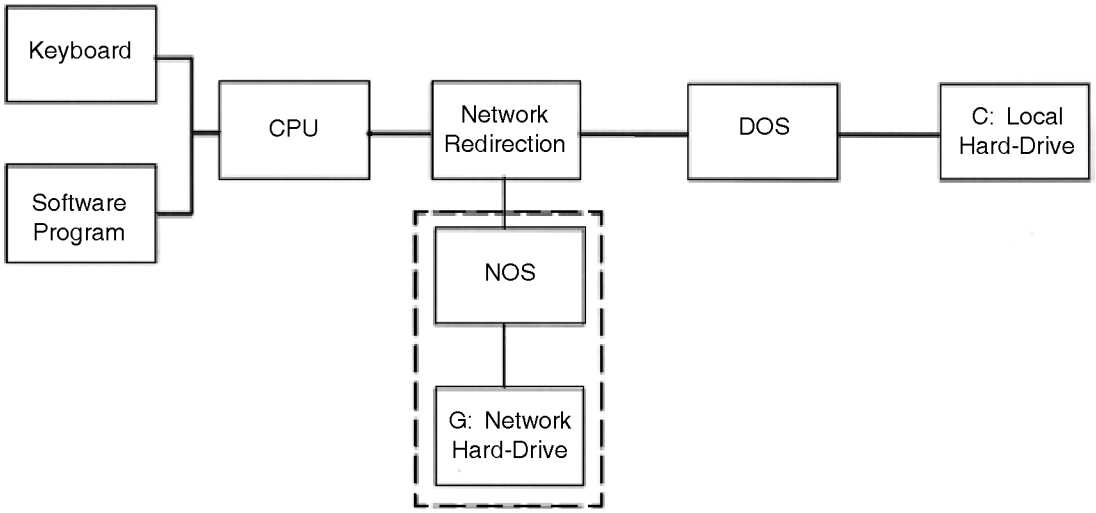


Fig. 2. : Simple Network Redirection

A PC setup as a network workstation has a software "Network Redirector" (the actual name depends on the network-we will use a generic term here) placed between the CPU and DOS (as shown in Fig 2.). The Network Redirector is a TSR (Terminate and Stay Resident) Programme : it presents the network hard disk as another local hard disk ("G:" in this example) to the CPU. The "Network Redirector" intercepts all CPU requests. The Network Redirector Checks to see if either a local or a network drive is requested. If a local drive is requested, the request is passed on to DOS. However, if a network drive is requested, the request is then passed onto the network operating system (NOS).

Electronic mail (E-Mail), client-server databases, games played over the network, print and file servers, remote logons, and network management programmes (or any "network aware" applications) are all aware of the network redirector. They have the ability to communicate directly with other "network applications" on the network. The "Network Aware Applications" and the "Network Redirector" make up Layer 7 (the Application layer of the OSI MOdel, as shown in Fig. 3).

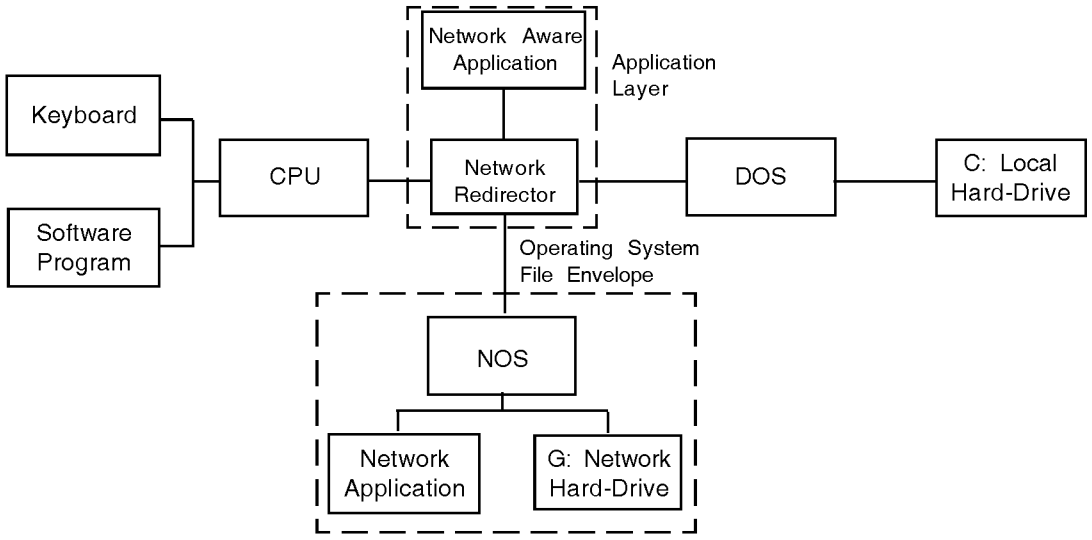
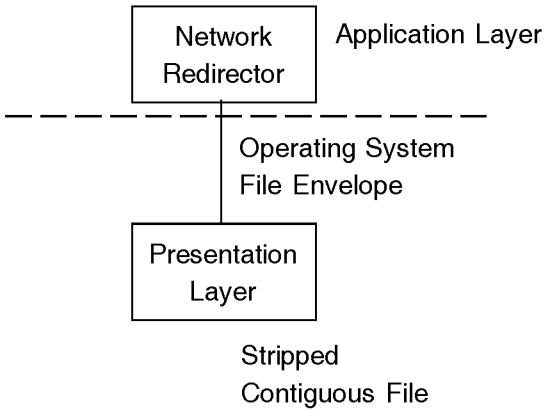


Fig. 3. : PC Workstation with Network Aware Software

Layer 6 - Presentation Layer

The Network Redirector sends CPU operating system native code to the network operating system : the coding and format of the data is not recognizable by the network operating system. The data consists of file transfers and network calls by network aware programmes.

For example, when a dumb terminal is used as a workstation (in a mainframe or minicomputer network), the network data is translated into (and from) the format that the terminal can use. The Presentation layer presents data to and from the terminal using special control characters to control the screen display (LF-line feed, CR-carriage return, cursor movement, etc..). The presentation of data on the screen would depend on the type of terminal that's used : VT100, VT52, VT420, etc.



Similarly, the Presentation layer strips the pertinent file from the workstation operating system's file envelope. The control characters, screen formatting, and workstation operating system envelope are all stripped or added to the file (if the workstation is receiving or transmitting data to the network). This could also include translating ASCII file characters from a PC world to EBCDIC in an IBM Mainframe world.

The Presentation Layer also controls security at the file level : this provides both file locking and user security. The DOS Share programme is often used for file locking. When a file is in use, it is locked from other users to prevent 2 copies of the same file from being generated. If 2 users both modified the same file, and User A saved it, then User B saved it, then User A's changes would be erased! At this point, the data is contiguous and complete (i.e. one large data file).

Layer 5-Session Layer

The Session layer manages the communication between the workstation and the network. The Session layer directs the information to the correct destination, and identifies the source to the destination. The Session layer identifies the type of information as data or control. The Session layer manages the initial start-up of a session, and the orderly closing of a session. The Session layer also manages Logon procedures and Password recognition (See Fig. 5).

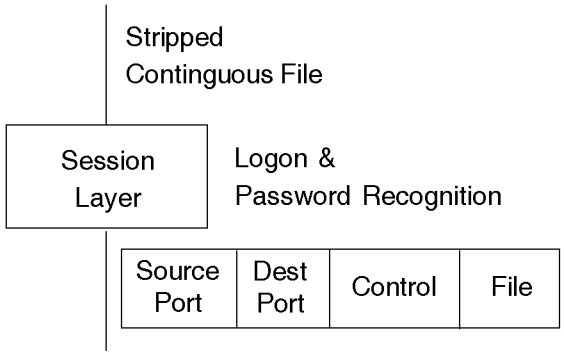
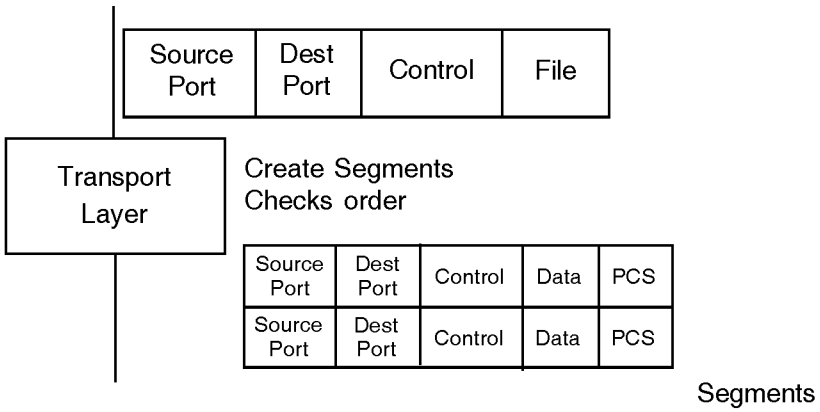


Fig. 5. : Session Layer

Layer 4-Transport Layer

In order for the data to be sent across the network, the file must be broken up into usable small data segments (typically 512-18K bytes). The Transport layer breaks up the file into segments for transport to the network, and combines incoming segments into a contiguous file. The Transport layer does this logically, not physically, and it is done in software as opposed to hardware.



The Transport layer provides error checking at the segment level (frame control sequence). This makes sure that the datagrams are in the correct order : the Transport layer will correct out of order datagrams. The Transport layer guarantees an error-free host-to-host connection. It is not concerned with the path between machines.

Layer 3-Network Layer

The Network layer is concerned with the path through the network. It is responsible for routing, switching, and controlling the flow of information between hosts. The Network layer converts the segments into smaller datagrams than the network can handle : network hardware source and destination addresses are also added. The Network layer does not guarantee that the datagram will reach its destination.

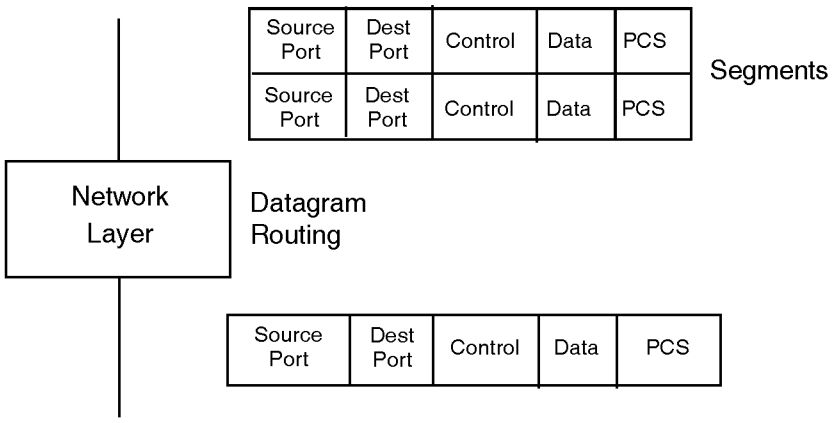


Fig. 7. : Network Layer

Layer 2 - Data Link Layer

The Data Link layer is a firmware layer of the network interface card. The data link layer puts the datagrams into packets (frames of bits : 1s & 0s) for transmission,

and assembles received packets into datagrams. The Data Link layer works at the bit level, and adds start/stop flags and bit error checking (CRC or parity) to the packet frame. Error checking is at the bit level only : packets with errors are discarded and a request for re-transmission is sent out. The Data Link layer is primarily concerned with bit sequence.

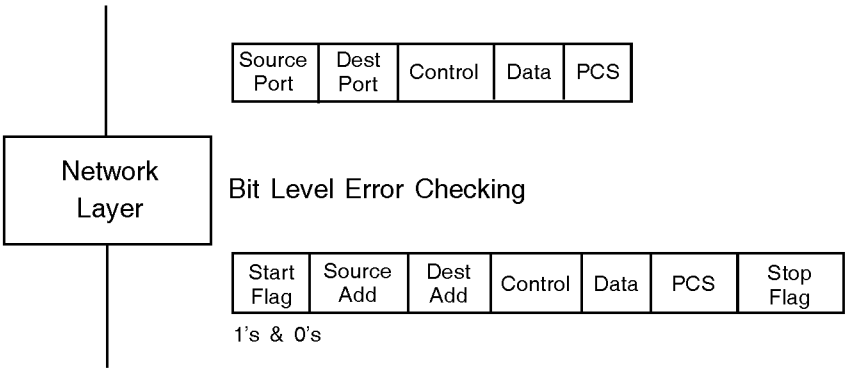


Fig. 8. : Data link Layer

Layer 1 - Physical Layer

The Physical layer concerns itself with the transmission of bits. It also manages the network card's hardware interface to the network. The hardware interface involves the type of cabling (*coax*, twisted pair, etc.), frequency of operation (1 Mbps, 10 Mbps, etc.), voltage levels, cable terminations, topography (star, bus, ring, etc.), etc. Examples of Physical layer protocols are as follows : 10 Base5- Thicknet, 10Base2- Thinnet, 10BaseT - twisted pair, ArcNet, FDDI, etc. (see Fig. 9).

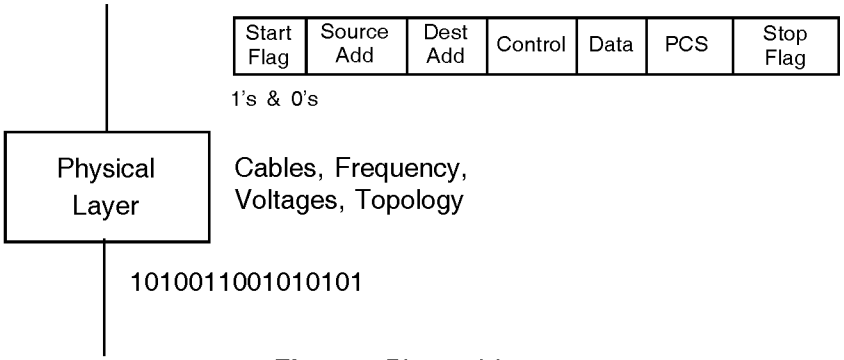
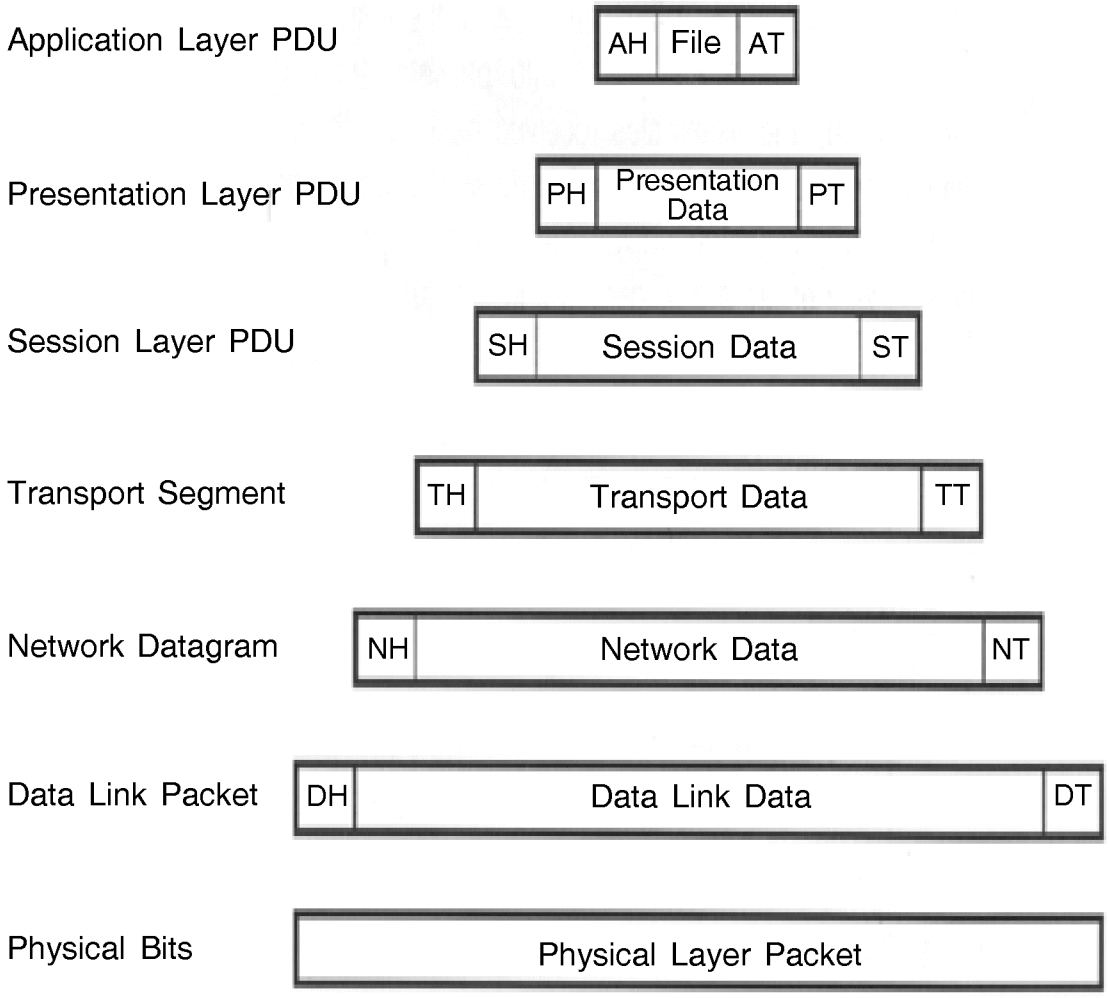


Fig. 9. : Physical Layer

Layer-Specific Communication

Each layer may add a Header and a Trailer to its Data (which consists of the next higher layer's Header, Trailer and Data as it moves through the layers). The Headers

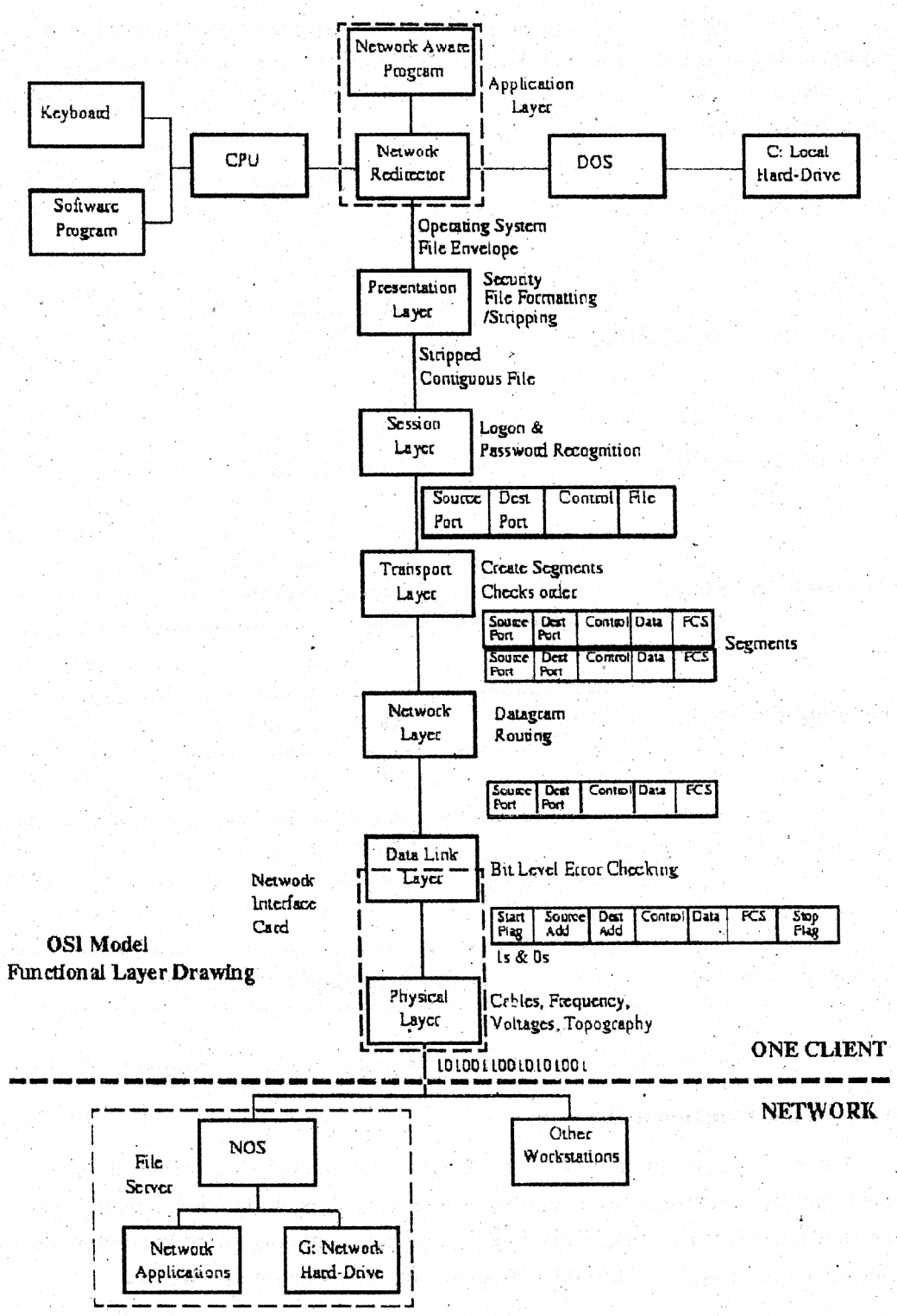
contain information that specifically addresses layer-to-layper communication. For example, the Transport Header (TH) contains information that only the Transport layer sees. All other layers below the Transport layer pass the Transport Header as part of their Data.



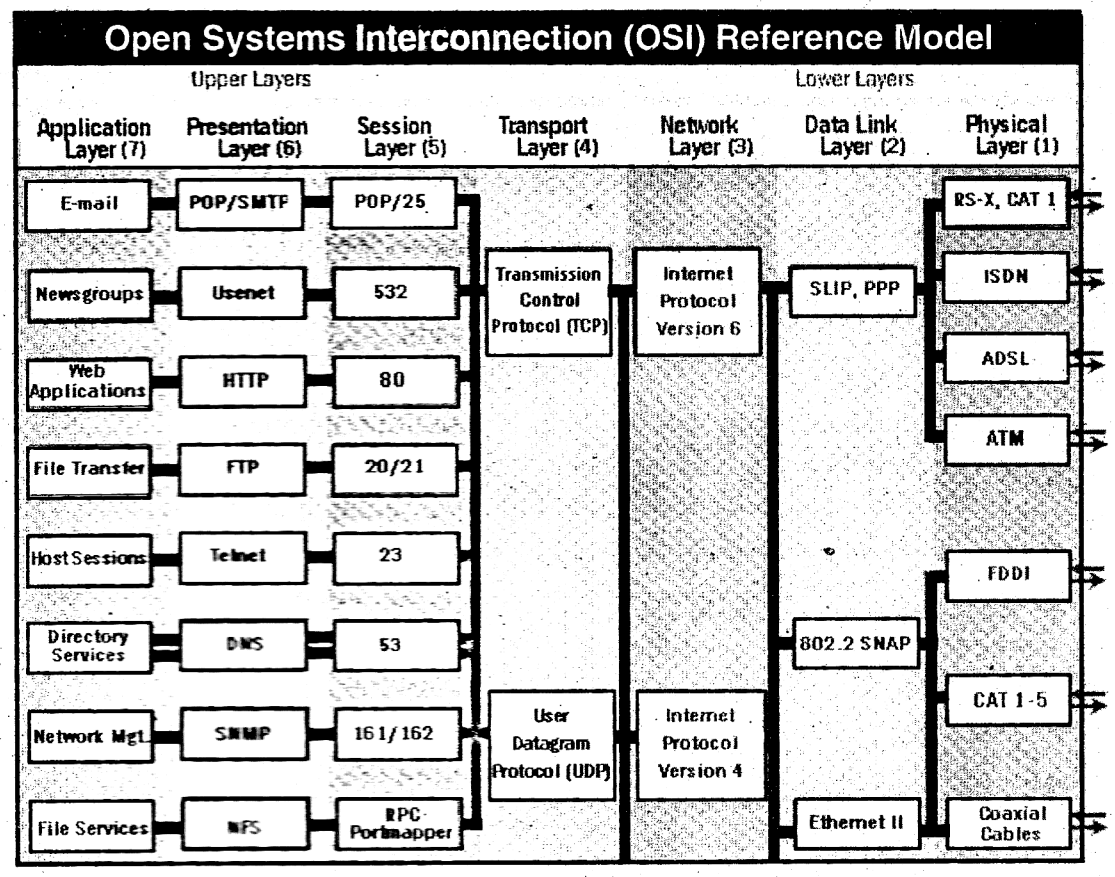
PDU-Protocol Data Unit (a fancy name for Layer Frame)

OSI Model Functional Drawing

Open Systems Interconnection (OSI) is a standard reference model for communication between two end users in a network. It is used in developing products and understanding networks. This figure shows how commonly used Internet products and services fit within the model. Also see the notes below the figure.



OSI Model
Functional Layer Drawing



Benefits

The layered approach in the OSI model offers several advantages to system implementations. By design into logical smaller pieces, vendors can more easily solve network design problems. A product from one vendor that implements OSI Layer 2 functionality, for example, will likely to interoperate with another vendor's OSI Layer 3 product because both vendors are following the OSI model.

References and Further Readings

1 2001 Blanchard (Eugene). Introduction to the ISO-OSI model (http://www.linuxports.com/howto/intro_to_networking/c4412.htm). Visited last : 12/10/2005

2 2005 OSI Reference Model illustrated (http://searchnetworking.techtarget.com/sDefinition/0,,sid7gci523729,00.html

3 2001 Computer Desktop Encyclopedia. 9th ed. Osborne-McGraw-Hill, 2001

17.5 Exercise

1. Discuss different network topologies.
2. Discuss different major network protocols.
3. Discuss OSI model.