Chapter 2:
Reference Model

Network Software

Network Software is a set of primitives that define the protocol between two machines. The network software resolves an ambiguity among different types of network making it possible for all the machines in the network to connect and communicate with one another and share information.

Network Software is the information, data or programming used to make it possible for computers to communicate or connect to one another.

Network software is used to efficiently share information among computers. It encloses the information to be sent in a "package" that contains a "header" and a "trailer". The header and trailer contain information for the receiving computer, such as the address of that computer and how the information package is coded. Information is transferred between computers as either electrical signals in electric wires, as light signals in fiber-optic cables, or as electromagnetic waves through space.

Protocols

A protocol is used for communication between entities in different systems. The terms 'entity' and 'system' are used in a very general sense. Examples of entities are user application programs, file transfer package, database management systems, electronic mail facilities, and terminals. Examples of systems are computers, terminals, and remote sensors. Note that in some cases the entity and the system in which it resides are coextensive (*e.g.* terminal).

In general, an entity is anything capable of sending or receiving information, and a system is physically distinct object that contains one or more entities. For two entities to communicate successfully, they must 'speak the same language'. What is communicated? How it is communicated and when it is communicated? Must conform to some mutually acceptable conventions between the entities involved. The conventions are referred to as a protocol.

Protocol may be defined as a set of rules governing the exchange of data between two entities. It also may be conceived as a set of agreement between two communicating processes. The key elements of protocol are:

- **Syntax:** Includes such things as data format and signal levels.
- **Semantics:** Includes control information for co-ordination and error handling.
- **Timing:** Includes speed matching and sequencing, create new paragraph.

Functions of protocols

Some of the numerous functions served by network protocol are as follows:

- Orderly exchange of data messages.
- Management of priorities at both the network entry and transmission levels within the network.
- Process synchronization.
- Session establishment between network users
- Session termination between network users.

- Means for protocol validation.
- Routing establishment and assignment of message routes and routing information.
- Flow control and congestion prevention.
- Sequencing—sequenced transmission and delivery of messages.
- Addressing of network components and users.
- Efficient network resources utilization.
- Resource management, monitoring and protection.
- Layered transparency between networks users and nodes.
- Reliable message transmission, including error, control and recovery.
- Testing of network resources, such as links and routes.
- Security and privacy.
- Optional packet switching through message segmenting and pipelining.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufactures and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communication. Data communication standards fall into two categories: by fact and by law.

Layered Approach

Some of the key design issues that occur in computer networking are present in several layers.

I. Every layer needs a mechanism for identifying senders and receivers. Since network normally has many computers, some of which have multiple processors means is needed for a process on one machine to specify with whom it wants to talk. As a consequence having multiple destinations, some form of addressing is needed in order to specify a Specific destination.

II. Another set of design decision concerns the rules for data transfer, such as. Simplex, Half duplex, Full duplex.

III. Error control is an important issue because physical communication circuits are not perfect. Many error-detecting and error-correcting codes are known, but both ends of the connection must agree on which one is being used. Also the receiver must have some way of telling the sender which messages have been correctly received and which has not.

IV. Not all communication channels preserve the order of messages sent on them. To deal with a possible loss of sequencing the protocol must make explicit provision for the receiver to allow the pieces to be put back together properly.

V. An issue that occurs at every level is how to keep a fast sender from swamping a slow receiver with data.

VI. Another problem that must be solved at several levels is the inability of all processes to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting and then reassembling messages.

When there are multiple paths between source and destination, a route must be chosen sometimes this decision must be split over two or more layers.

Services

Layers offer two types of services.

I. **Connection Oriented Service**

This is modeled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk and then hang up. Similarly, to use a connection oriented network services, the services user first establishes a connection, uses the connection and then releases the connection. The essential aspect of connection is that it acts like a tube. The sender pushes objects (bits) in at one end and the receiver takes them out in the same order at the other end.

Connection oriented services are of following:

- Reliable message stream service.
  e.g. sequence of pages.
- Reliable byte stream.
  e.g. remote login.
- Unreliable connection.
  e.g. Digitized voice.

II. **Connectionless Services**

This is modeled after the postal system. Each message carries the full destination address and each one is routed through the system independent of all the (users) others. Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive. However, it is possible that the first one sent, can be delayed so that the second one arrives first. With connection oriented service this is impossible.

Connectionless services are of the following:

- Unreliable datagram.
  e.g. Electronic junk mail.
- Acknowledged datagram.
  e.g. Registered mail.
- Request reply service.
  e.g. Database query.

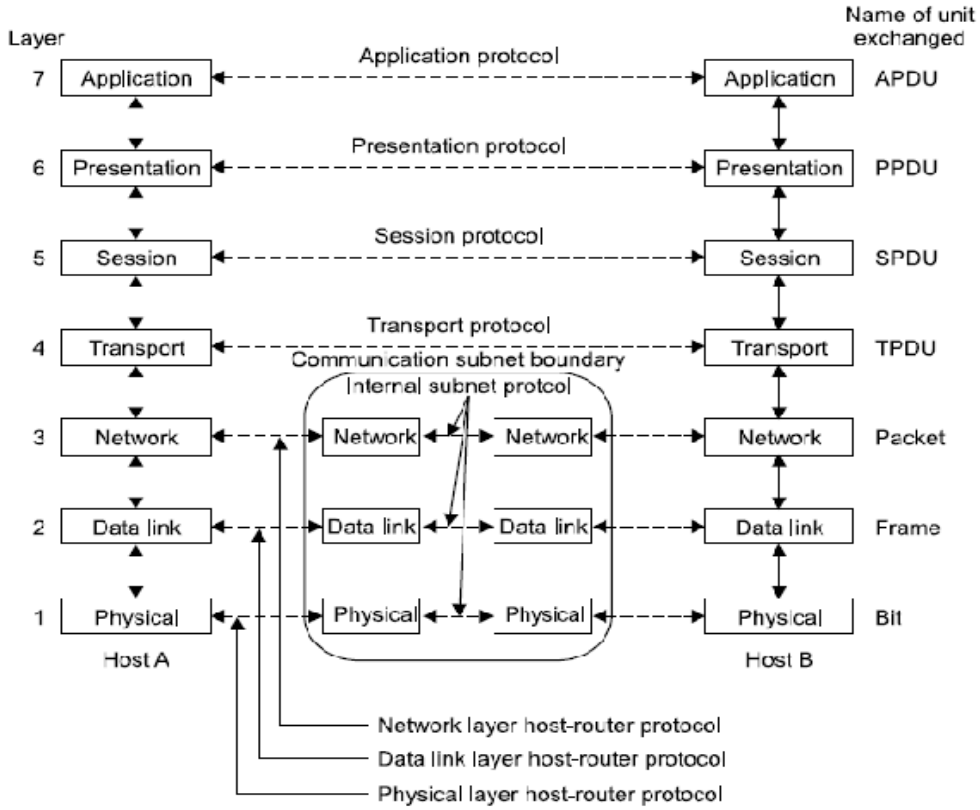
The OSI Reference Model

The OSI model is shown in the figure. This model is based on a proposal developed by the **International Standards Organization (ISO)** as a first step towards international standardization of the protocols used in the various layers, (Day & Zimmerman, 1983). The model is called the **ISO OSI (Open Systems Interconnection)** Reference Model because it deals with connecting open systems, *i.e.*, the systems that are open for communication with other systems.

The OSI Model has seven layers. The **principles that were** applied to arrive at the seven layers are as follows.

I. A layer should be created where a different level of abstraction is needed.
II. Each layer should perform a well defined function.
III. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
IV. The layer boundaries should be chosen to minimize the information flow across the interfaces.

V. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become widely.



Benefits of OSI Model:

- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

1. Physical Layer:

Physical layer is the bottom layer of the OSI reference model. The physical layer has four important characteristics.

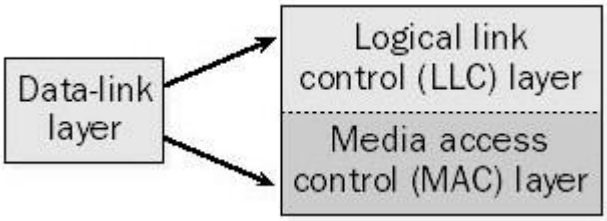
Mechanical: Relates to the physical properties of the interface to a transmission medium. Typically, the specification is of a pluggable connector that joins one or more signal conductors, called circuits.

Electrical: Relates to the representation of bits (e.g., in terms of voltage levels) and the data transmission rate of bits. It defines the voltage, current, modulation, bit synchronization, connection activation and deactivation, and various electrical characteristics for the transmission media (such as unshielded or shielded twisted-pair cabling, coaxial cabling, and fiber-optic cabling).

Functional: Specifies the functions performed by individual circuits of the physical interface between a system and the transmission medium.
Procedural: Specifies the sequence of events by which bit streams are exchanged across the physical medium.

2. Data Link Layer:

The physical layer provides only a raw bit-stream service, the data link layer attempts to make the physical link reliable while providing the means to activate, maintain, and deactivate the link . For LANs, the Project 802 standards of the Institute of Electrical and Electronics Engineers (IEEE) separate the data-link layer into two sub layers:



- The logical link control (LLC) layer, the upper of the two layers, which is responsible for flow control, error correction, and resequencing functions for connection-oriented communication, but which also supports connectionless communication
- The media access control (MAC) layer, the lower of the two layers, which is responsible for providing a method for stations to gain access to the medium

Functions:

- **Framing:** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing:** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control**: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control:** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access control:** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time

Examples of data-link protocols for local area networking include the following:

- IEEE 802.3, which provides the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method for baseband Ethernet networks

- IEEE 802.5, which provides the token-passing access method for baseband token ring implementations

For WANs, data-link layer protocols encapsulate LAN traffic into frames suitable for transmission over WAN links. Common data-link encapsulation methods for WAN transmission include the following:

- Point-to-point technologies such as Point-to-Point Protocol (PPP) and High-level Data Link Control (HDLC) protocol
- Multipoint technologies such as frame relay, Asynchronous Transfer Mode (ATM), Switched Multimegabit Data Services (SMDS), and X.25

3. Network Layer:

The network layer is responsible for functions such as the following:

- Logical addressing and routing of packets over the network
- Establishing and releasing connections and paths between two nodes on a network
- Transferring data, generating and confirming receipts, and resetting connections

The network layer also supplies connectionless and connection-oriented services to the transport layer above it. The network layer functions closely with the physical layer (layer 1) and data-link layer (layer 2) in most real-world network protocol implementations.

On TCP/IP-based networks, IP addresses and network numbers are used at the network layer, and IP routers perform their routing functions at this layer. An example of an OSI model network layer protocol is the X.25 packet-switching network layer protocol, which is built on the X.21 physical layer protocol.

4. Transport Layer:

The transport layer is responsible for providing reliable transport services to the upper-layer protocols. These services include the following:

- Flow control to ensure that the transmitting device does not send more data than the receiving device can handle. Packet sequencing for segmentation of data packets and remote reassembly.
- Error handling and acknowledgments to ensure that data is retransmitted when required.
- Multiplexing for combining data from several sources for transmission over one data path.
- Virtual circuits for establishing sessions between communicating stations.

The Transmission Control Protocol (TCP) of the TCP/IP protocol suite resides at the transport layer

The connection between two devices that acts as though it's a direct connection even though it may physically be circuitous. The term is used most frequently to describe connections between two hosts in a packet-switching network. In this case, the two hosts can communicate as though they have a dedicated connection even though the packets might actually travel very different routes before arriving at their destination. An X.25 connection is an example of a virtual circuit. Virtual circuits can be either permanent (called PVCs) or temporary (called SVCs).

5. Session Layer:

Layer 5 of the Open Systems Interconnection (OSI) reference model, which enables sessions between computers on a network to be established and terminated. The session layer does not concern itself with issues such as the reliability and efficiency of data transfer between stations because these functions are provided by the first four layers of the OSI reference model.

Functions:

Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half- duplex (one way at a time) or full-duplex (two ways at a time) mode.
Synchronization: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

6. Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems .
Specific responsibilities of the presentation layer include the following:

Translation: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption: To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7. Application layer:

Layer 7 of the Open Systems Interconnection (OSI) reference model, in which network-aware, user-controlled software is implemented—for example, e-mail, file transfer utilities, and terminal access. The application layer represents the window between the user and the network. Examples of protocols that run at the application layer include File

Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), telnet, and similar protocols that can be implemented as utilities the user can interface with.

File transfer, access, and management: This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
Mail services: This application provides the basis for e-mail forwarding and storage.
Directory services: This application provides distributed database sources and access for global information about various objects and services.

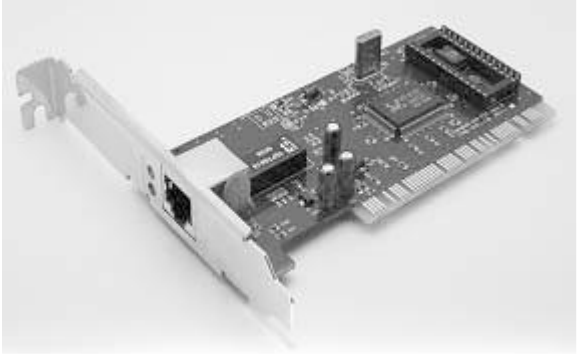
Comparison between OSI model and TCP/IP model

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical mode
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard
Protocols are not strictly defined	Stricter boundaries for the protocols

Networking Hardware:

NIC (Network Interface Card)

A NIC is a hardware board or card that you put into an empty slot in the back of your client computer or server. NIC is the interface between the PC and the physical network connection. This card physically connects to the cable that links network.



In addition to providing the physical connection to the networks, they also perform the following:

- **Prepare data**
  NIC prepare data so that it can transmit through the cable. The card translates data bit back and forth as they go from the computer to the cable and back again.
- **Address data**
  Each NIC has its own unique address that it imparts to the data stream. The card provides the data with an identifier. When it goes out on to the net and enables data seeking a particular computer to know where to exit the cable.
- **Control data flow**
  The card has RAM on it to help it, place the data so that it doesn't overwhelm the receiving computer on the cable.
- **Make (and agree on) the connection to another computer**
  Before it actually sends data, the NIC an electronic dialog with the other PC on the network that wants to communicate. They agree on thing like the maximum size of data groups to be sent. The total maximum size of data (amount), the time interval between data checks the amount of time that will elapse before confirmation that the data has arrived successfully and how much data each card hold before it overflows. NIC is an especially useful place to implement IP sec. technology. This is the place where end station data is turned into useful security management information where data can be queued in order of priority before transport and where hardware acceleration can be used to the greatest advantage to help facilitate encryption. An encrypted audio/video stream from a server to its clients provides a good example of the benefits of hardware acceleration. Users would experience much better network performance, if the stream were decrypted on an IP. (see enabled NIC). Instead of via decryption software only hardware acceleration in the NIC can help to improve network performance by accelerating the many math cycle required by encryption and decryption algorithms by offloading the process onto a NIC problems are avoided. Data transfers between the interfaces or nodes takes using this hardware address.

Hub

Hub is a basic networking component used in traditional 10-Mbps Ethernet networks to connect network stations to form a local area network (LAN). Hubs can be used for

- Connecting about a dozen computers to form a work-group or departmental LAN
- Connecting other hubs in a cascaded star topology to form a larger LAN of up to roughly a hundred computers

How It Works

Hubs are the foundation of traditional 10BaseT Ethernet networks. The hub receives signals from each station and repeats the signals to all other stations connected to the hub. In active hubs (which all of today's hubs are), the signal received from one port is regenerated (amplified) and retransmitted to the other ports on the hub. Hubs thus perform the function of a repeater and are sometimes called multiport repeaters. From a logical cabling point of view, stations wired into a hub form a star topology.

Hubs generally have RJ-45 ports for unshielded twisted-pair (UTP) cabling, and they range in size from 4 to 24 or more ports for connecting stations to the hub, plus one or more uplink ports for connecting the hub to other hubs in a cascaded star topology. Hubs generally have various light-emitting diode (LED) indicator lights to indicate the status of each port, link status, collisions, and so on. Hubs with several different types of LAN connectors such as RJ-45, BNC, and AUI are commonly called combo hubs.

Repeater

Networking components that extend a network by boosting the signal so that it can travel farther along the cabling.

How It Works

Digital signals traveling on cables weaken with distance—a phenomenon known as attenuation. A repeater is a form of digital amplifier that works at the physical layer (layer 1) of the Open Systems Interconnection (OSI) reference model for networking to regenerate (amplify) the signal so that it can travel farther. Repeaters also perform other functions such as filtering out noise caused by electromagnetic interference (EMI), reshaping the signal, and correcting timing to remove signal jitter so that the signal can travel farther. Repeaters can also be used to join dissimilar media such as unshielded twisted-pair (UTP) cabling and thinnet, but they cannot be used to join dissimilar network architectures such as Ethernet and Token Ring. Repeaters are an inexpensive way to extend a network.

Repeaters can be used in Ethernet and Token Ring local area networks (LANs) to extend signal transmission to remote nodes and over long fiber-optic cabling runs to connect LANs. Repeaters can also be used in mainframe environments for boosting signals for serial transmission to remote terminals.

Other uses for repeaters include the following:

- Joining two 16-Mbps Token Ring networks in different buildings over distances up to 3000 meters over multimode fiber-optic cabling or up to 20 kilometers over single-mode fiber
- Increasing the lobe length between a Token Ring main ring and a remote node
- Joining dissimilar 10Base2 and 10Base5 segments to form a single Ethernet LAN
- Boosting signals from mainframe controllers to 3270 terminals over coaxial or UTP cabling to support distances up to 2500 meters
- Extending the operating distance of T1 lines by placing G.703 repeaters at 2.2-kilometer intervals
- Extending backbone fiber-optic cable runs in campus wide LANs or metropolitan area networks (MANs)

Repeaters are also used in fiber-optic networks to amplify and regenerate light signals for long-distance cable runs. Repeaters come in various types for different network architectures and data communication technologies.

Bridge:

A networking component used either to extend or to segment networks. Bridges work at the OSI data-link layer. They can be used both to join dissimilar media such as unshielded twisted-pair (UTP) cabling and fiber-optic cabling, and to join different network architectures such as Token Ring and Ethernet. Bridges regenerate signals but do not perform any protocol conversion, so the same networking protocol (such as TCP/IP) must be running on both network segments connected to the bridge. Bridges can also support Simple Network Management Protocol (SNMP), and they can have other diagnostic features.

How it works?

Bridges operate by sensing the source MAC addresses of the transmitting nodes on the network and automatically building an internal routing table. This table is used to determine which connected segment to route packets to, and it provides the filtering capability that bridges are known for. If the bridge knows which segment a packet is intended for, it forwards the packet directly to that segment. If the bridge doesn't recognize the packet's

destination address, it forwards the packet to all connected segments except the one it originated on. And if the destination address is in the same segment as the source address, the bridge drops the packet. Bridges also forward broadcast packets to all segments except the originating one.

Switch:

Switch is essentially a multi-port bridge. Switches allow the segmentation of the LAN into separate collision domains. Each port of the switch represents a separate collision domain and provides the full media bandwidth to the node or nodes connected on that port. With fewer nodes in each collision domain, there is an increase in the average bandwidth available to each node, and collisions are reduced.

Why Switches:

In a LAN where all nodes are connected directly to the switch, the throughput of the network increases dramatically. The three primary reasons for this increase are:

- Dedicated bandwidth to each port
- Collision-free environment
- Full-duplex operation

Routers

Routers are internetwork connectivity devices. An internetwork may consists of two ormore physical connected independent network. These networks can be of different type. For example, they can be Ethernet and Token ring network. Each network is logically separate and is assigned an address. Routers can use network address to assists efficient delivery of message. Delivering packets according to logical network address is called routing. Routers perform routing. Routing is the process of finding a path from a source to every destination in the network. Routers are intelligent. They can use algorithms to determine most efficient path for sending a packet to any given network. Routers can also be used to divide large busy LANs into smaller segments. The protocols like IP, IPX and DDP are used to support routing functions. Routers are also employed to connect LAN to wide area network (WAN).

Routers are of two types.

1. *Static routers:* Static routers do not determine paths, but need to specify them.
2. *Dynamic routers:* Dynamic routers have capacity to determine routes.