Introduction to Computer Networks

- A network may be defined as a set of two or more computers connected by a physical link (subnet) or as two or more networks connected by one or more subnets.

- Obviously, a network must provide connectivity among a set of computers. This connectivity may be limited in that connects only a few select machines for reasons of privacy and security (corporate Intranets), or can span the globe (Internet).

- A network that is designed to support growth to an arbitrarily large size is said to **scalable**.

- Network connectivity occurs at many different levels. At the lowest level, a network can consist of two or more computers directly connected by some physical medium, such as a coaxial cable or an optical fiber, as well as specialized computers such as routers, bridges, etc.

- The physical medium that provides the connectivity is called the **subnet**. The physical links are sometimes limited to a pair of nodes (**point-to-point**), or in other cases, several nodes may share a single physical link (multiple-access).

- Current networks use a wide variety of computers and communication technologies to carry out useful tasks. These might include mainframes, LANs, workstations, personal computers, and proprietary and standards-based networking platforms.

- The main issue is that not all of these products are interoperable (at least, not easily), and it may be difficult to exchange data across different systems and applications.

- **Open systems** aim at resolving the issues underlying the difficulty in enabling any two computers of any size, regardless of the operating system and hardware platforms, to communicate.

- An open system may be defined as one for which the specification of the architecture is in the public domain and is readily available to others who want to design and develop products for the platform. The definition applies equally well to both hardware and software.

- **Linux** is an excellent example of an open software platform. Linux is an open source implementation of classic **UNIX** that has been around for 30 years. Its source code is available to anyone who wants to modify and use it.

- Linux can be ported to run on many hardware platforms, eliminating proprietary dependencies.

The OSI Reference Model

- The ISO (International Standards Organization) proposed a standard as a first step towards standardization various protocols and functions used in data communications and networking.

- This model is called the ISO OSI (Open Systems Interconnection) reference model because it deals with connecting open systems – that is, systems that are open for communication with other systems.

The Physical layer

- Implements functions for transmitting raw bits over a communication channel.

- The design issues here concern the physics of signal transmission such as bandwidth, modulation, frequency spectrum, transmission rates, etc.

The Data Link Layer

- Error Detection/Correction.

- Packetizes data

- Flow control

- Acknowledgements and handshaking.

The Network Layer

- Routing issues

- Congestion control algorithms.

- Internetworking issues.

The Transport Layer

- Provides reliable "end-to-end" user connection

- Routing (naming) issues

The Session Layer

- Establishes sessions between two machines.
- Duplex or simplex traffic.
- Synchronization of data transfers.

The Presentation Layer

- Character representation (ASCII or EBCDIC).
- Data format conversion.
- Data Compression and Encryption.

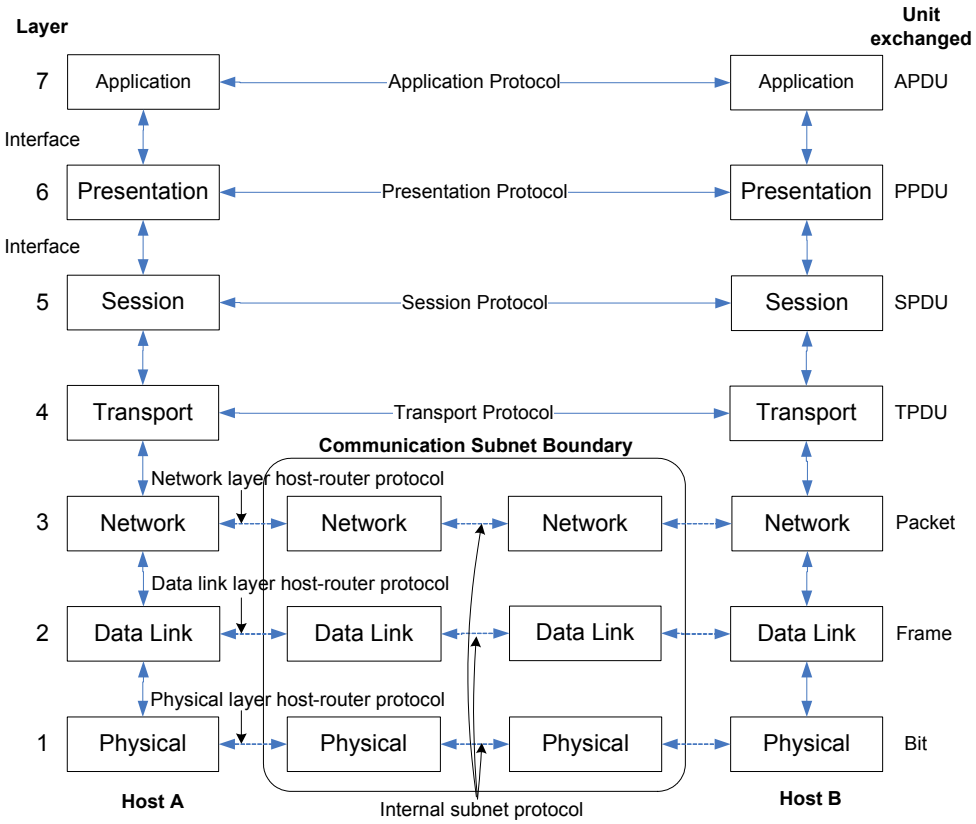
The Application Layer

Applications:

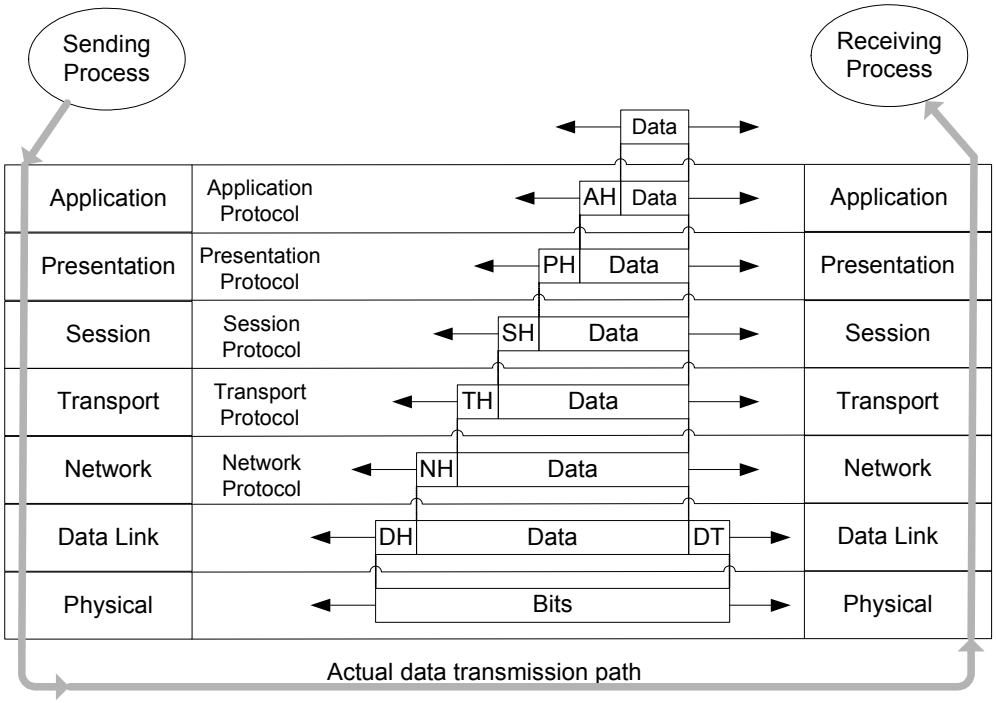
- Web Browsers
- E-Mail
- Electronic Funds Transfer
- File Transfer
- Data Base Query, etc.

Data Transmission in the OSI Model

- Data propagates from the Application to the Physical layer.
- Each layer attaches its own header to the data.
- At the receiving machine the data propagates upward with each layer stripping of its header until it reaches the receiving process.
- Peer-to-peer communication between layers
- The diagrams provided illustrate this process.



The OSI Reference Model



LAN Protocols

- LAN data transmissions fall into three classifications: **unicast**, **multicast**, and **broadcast**. In each type of transmission, a single packet is sent to one or more nodes.

- In a **unicast** transmission, a single packet is sent from the source to a destination on a network.

- First, the source node addresses the packet by using the **address** of the **destination node**. The package is then sent onto the network, and finally, the network passes the packet to its destination.

- A **multicast** transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network.

- First, the source node addresses the packet by using a **multicast address**. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

- A **broadcast** transmission consists of a single data packet that is copied and sent to all nodes on the network.

- In these types of transmissions, the source node addresses the packet by using the **broadcast address**.

- The packet is then sent into the network, which makes copies of the packet and sends a copy to every node on the network.

- LAN protocols function at the lowest two layers of the OSI reference model between the physical layer and the data link layer.

- In any broadcast network, the key issue is how to determine who gets to use the channel when multiple nodes wish to transmit.

- The **Medium Access Control** (**MAC**) sublayer implements the channel access algorithm in networks that use a multi-access channel as the basis of their communication.

MAC Sublayer

- Consists of various schemes for controlling access to LAN channels:
    - ALOHA
    - Slotted ALOHA
    - Persistent and Non-Persistent CSMA
    - CSMA/CD

- LAN protocols typically use one of two methods to access the physical network medium: **Carrier Sense Multiple Access** with **Collision Detect** (**CSMA/CD**) and token passing.

- In the CSMA/CD media-access scheme, network devices contend for use of the same physical network medium.

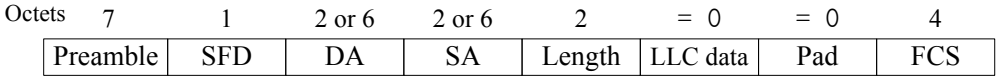
- CSMA/CD is therefore sometimes called **contention control**. Examples of LANs that use the CSMA/CD media-access scheme are **Ethernet/IEEE 802.3** networks, including **100BaseT**.

- In the token-passing media-access scheme, network devices access the physical medium based on possession of a token.

- Examples of LANs that use the token-passing media-access scheme are **Token Ring/IEEE 802.5** and **FDDI**.

CSMA/CD and IEEE 802.3

- The most widely used implementation of CSMA/CD is found in the Ethernet specification.
- The Ethernet system was developed partly from the ALOHA concepts.
- In 1980, Xerox, Intel and DEC created a standard for a 10 Mbps Ethernet.
- This standard formed the basis for the IEEE 802.3 standard.
- The 802.3 specification covers rules for configuring LANs, the type of media that can be used, and how the elements should be networked together.
- The Ethernet protocol provides the services called for in the Physical and Data Link Layers of the OSI reference model.
- One element of the 802.3 specification states that Ethernet networks run at a data rate of 10 Mbps or at a rate of 100Mbps which is commonly referred to as fast Ethernet.
- Another important element defined by the 802.3 specification is the channel access method to be used by stations connected to an Ethernet LAN, CSMA/CD.
- The **Data Link layer** provides the actual logic to the control the CSMA/CD network. It is medium independent, i.e., broadband or baseband.
- The **Physical layer** is responsible for such services as injecting the signals into the channel, providing the timing on the channel, and data encoding/decoding.
- The 802.3 frame format is shown below:



SFD = Start Frame Delimiter
DA = Destination Address
SA = Source Address
FCS = Frame Check Sequence

IEEE 802.3 Frame Format

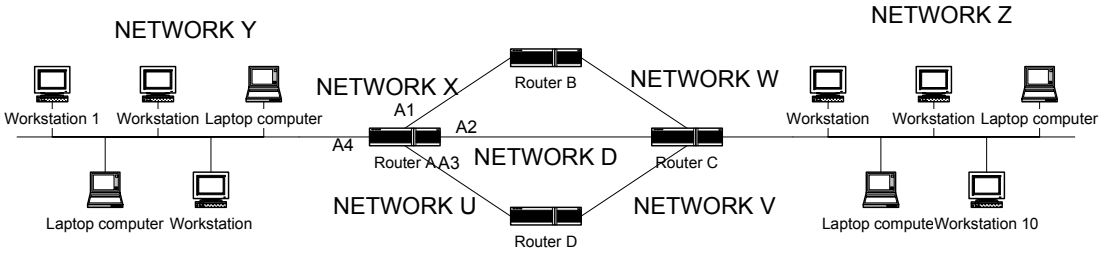
- The source and destination addresses are also know as MAC addresses, the addresses assigned and hard coded into each NIC.
- 802.3 specifies that valid frames must be at least 64 bytes long from Destination Address to the Frame Check Sum.
- If the data portion (LLC) is less than 46 bytes, the Pad field is used to fill out the frame to the minimum size.

Routing

- As networks grow in size, so does the traffic imposed on the subnet, which in turn impacts the overall network throughput and performance.

- In order to maintain network performance at optimal levels, a large network is partitioned into multiple smaller networks that are interconnected by specialized devices, including routers, bridges, and switches.

- The diagram below depicts an internetworked scenario. The two autonomous networks are internetworked via four routers and five possible paths.



- Assuming that Workstation 1 on Network Y wants to send a message to Workstation 10 on Network Z, the main issue is how the intermediate routers handle this data.

- The routing from source to destination uses various co-operative processes, in both routers and workstations, whose main concern is to allow for the intelligent delivery of data to its ultimate destination.

- Data exchange can take place between any two workstations, whether or not both belong to the same network. The key elements required in this process are the **MAC**, **network**, and **complete addresses**.

Network Addresses and the Complete Addresses

- In addition to a unique MAC address all workstations must have a **network address**. The MAC and network addresses are analogous to street names and house numbers respectively.

- Thus a **complete address** designating a workstation on the network must include enough information to lead to the actual MAC address and the network address of that workstation.

- Unlike data link addresses, which are hardwired on the NIC, network addresses are software-configurable as part of the network administrator's responsibilities.

- For the purposes of our discussion we will assume that a complete address is represented as: ***network address: MAC address*** notation.

- A data frame originating from **Workstation 1** on **Network Y** going to **Workstation 10** on **Network Z** will have ***Y:1*** as its source address and ***Z:10*** as its destination address.

- Also note that Workstation 1 is using Router A to help in the delivery of data to Workstation 10 on Network Z.

Routing Tables

- Each router maintains a **routing table** that includes routing information for every known network, how far the network is, and how it can be reached. The routing process builds and maintains the routing table by employing a route discovery process known as the **Routing Information Protocol** (**RIP**).

- Consider the table below that is an example of a routing table that would be maintained by the routing process in Workstation 1.

Destination Network	Distance	Next Router
Z	3	A
V	2	A

- Now consider a table maintained by Router A. The table includes the destination network address, the distance (number of routers) of the destination in question from the workstation or router, the next router, and the output port (network interface) from which the data should be delivered to the next router.

Destination Network	Distance	Next Router	Output Port
Z	1	C	A2
X	0	A	A1
V	1	D	A3
Y	0	A	A4
(etc)			

- Although the routing table of Workstation 1 provides different information about the reachability of Network Z, it remains consistent with the information maintained by Router A.

Routing Algorithms

- Routing algorithms strive to select the shortest path connecting two networks. We can see that more than one route connects Networks Y and Z. Router A's routing table, as shown in the figure, includes only one path, the shortest path.

- Routers create and maintain routing tables by either dynamically exchanging routing information among themselves or by being statically configured by network administrators or both.

- The dynamic exchange of routing information is handled by yet another process besides the routing process itself. In the case of TCP/IP, IP (Internet Protocol) handles the routing process, whereas RIP (Routing Information Protocol) handles the route discovery process.

- The table shown below illustrates the previous concepts and the interaction that takes place between the various components of the routing process.

- The table depicts the changes in the frame (MAC) addresses and the packet level (complete network) addresses as data emerges from Workstation 1 and crosses Routers A and C to be delivered to Workstation 10

- Note that the first column refers to the address of the actual network that the packet is crossing as part of the path leading to Workstation 10.

Data on Network	MAC Dest. Address	MAC Source Address	Complete Dest. Address	Complete Source Address
Y	A	1	Z:10	Y:1
D	C	A	Z:10	Y:1
Z	10	C	Z:10	Y:1

Data Multiplexing/Demultiplexing

- What we have discussed so far is how data can be communicated between computers rather than with processes that are representative of user applications.
- Recall that the ultimate purpose of data communications is the exchange of data between user processes.
- This is especially of concern on multitasking environments where more than one process might be communicating with its counterparts on the network.
- This issue is handled at a protocol level and in the case of the TCP/IP protocol suite it is handled by port numbers.
- Both TCP and UDP define a group of well-known ports to identify well-known services running on a server. For example, FTP is assigned the well-known port number 21.
- Clients on the other hand use so called ephemeral ports. These are short-lived ports that are assigned automatically to clients by TCP or UDP.