KASNEB

DICT

Computer Networking

Level II Paper No 5

Contents

TOPIC 1

INTRODUCTION TO COMPUTER NETWORKS

Definition

A **computer network** is a set of **computers** connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server.

Advantages of Computer Network

- ✓ Networks allow data transmission among far areas also within local areas.
- ✓ Networks allow different users share the processing characteristics of different computers.
- ✓ Network allows users to share common set of data files and software stored in a main system.
- ✓ Network allows users to share common hardware resources such as printers, fax machines, modem etc.
- ✓ The cost of computing is reduced to each user as compared to the development and maintain of each single computer system.

Role of computer networks

Describes why and how computer networks support successful work

Information and communication are two of the most important strategic issues for the success of every enterprise. While today nearly every organization uses a substantial number of computers and communication tools (telephones, fax, personal handheld devices), they are often still isolated. While managers today are able to use the newest applications, many departments still do not communicate and much needed information cannot be readily accessed.

To overcome these obstacles in an effective usage of information technology, computer networks are necessary. They are a new kind (one might call it paradigm) of organization of computer systems produced by the need to merge computers and communications. At the same time they are the means to converge the two areas; the unnecessary distinction between tools to process and store information and tools to collect and transport information can disappear. Computer networks can manage to put down the barriers between information held on several (not only computer) systems. Only with the help of computer networks can a borderless communication and information environment be built.

Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities. Because of these optimal information and communication possibilities, computer networks may increase the organizational learning rate, which many authors declare as the only fundamental advantage in competition.

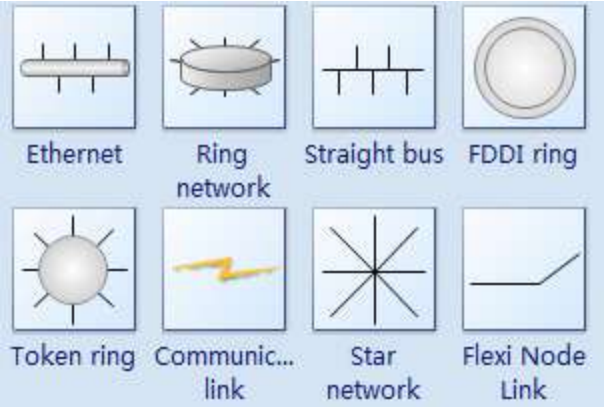
TOPIC 3

SETTING-UP A NETWORK

Introduction to protocols

Protocols are a set of rules whose main purpose is to govern communications amongst computers sharing the same network. The rules are inclusive of guidelines, which are known to regulate network characteristics such as cabling types, access method, data transfer speed and allowed physical topologies. There are five most common types of protocols found on networks; ATM, Token Ring, Local Talk, FDDI and Ethernet.

The followings are some commonly used network symbols to draw different kinds of network protocols.



Ethernet protocol's is the most common of the protocols. It uses the Carrier Sense Multiple Access/Collision Detection abbreviated as CMMA/CD access method. The system works by the letting every computer to listen to the cable before it is able to send something via the network; a clear network will boost transmission. If a separate node is transmitting already the computer waits until the line is clear before transmission can take place. Should two computers try to transmit at the same time there will be a collision occurring. In such a case, the computers each back off and then wits for random amounts of time before it can try to transmit again; this method of access is known to collisions but it should be noted that the delay that is as a result of retransmitting and collisions is small and will not affect the speed of the network transmission. This protocol supports tree, star or bus topologies. Data is transmitted over the fiber optic cable, wireless access points, coaxial or twisted pair at speeds of 10 Mbps and up to 1000 Mbps.

Fast Ethernet - To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the application of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary. Fast Ethernet is becoming common in schools that have been recently wired.

Local Talk uses the Carrier Sense Multiple Access with Collision Avoidance method. Specially twisted pair cables and the Local Talk adapters are used to connect computer series through a serial port. Macintosh operating system facilitates the creation of peer-to-peer networks even without additional software. This protocol allows for tree, star, or linear bus topologies by the use of a twisted pair cable. It has a speed of 230 Kbps of transmission, which is a great disadvantage. Also known as Asynchronous Transfer Mode, ATM is a network protocol that facilitates the transmission of data at 155 Mbps speeds and more. It works by the transmission of data in small packets with a fixed size.

The Token Ring protocol was developed by IBM 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 data is captured by the receiving computer. 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 in school environments has decreased.

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 high speed. It operates over fiber optic cable at 100 Mbps.

Asynchronous Transfer Mode (**ATM**) is known to support various media like imaging, video and CD-quality audio. Fiber Distributed Data Interface network protocol interconnects two or more local area networks on large distances and involves a token passing using a dual ring type of physical topology. The Token Ring protocol uses the token passing access method in Token Ring, the computer connection is done in such a way to let the signal travel on the network smoothly between the computers in a logical ring. It is vital to note that the various network protocols call for different specifications although some might be similar.

Gigabit Ethernet The most latest development in the Ethernet standard is a protocol that has a transmission speed of 1 Gbps. Gigabit Ethernet is primarily used for backbones on a network at this time. In the future, it will probably also be used for workstation and server connections. It can be used with both fiber optic cabling and copper. The 1000BaseTX, the copper cable used for Gigabit Ethernet, became the formal standard in 1999.

Compare the Network Protocols

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

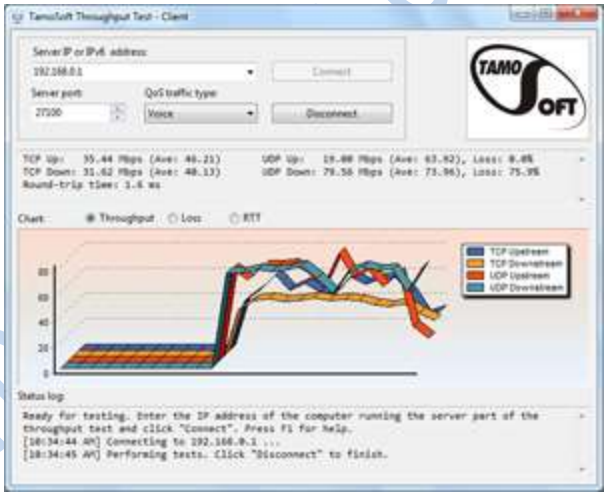
Tools in networking

Protocol analyzer: This protocol analyzer is called as a network sniffer. It will be huge troubleshooting asset. This protocol analyzer will be a software running or a standalone device on the laptop or computer. It is used to capture the traffic, which is flowing via the network switch, with the help of port mirroring features of the switch. By checking the captured packets, it is easy to grasp the information about the

communication flow, as they are being maintained, torn down and set up. The examination of those captured packets is considered as traffic analysis, this offers the administrators with sufficient insights on the nature of the traffic flowing via veins of a network.

This protocol analyzer is available in a wide range of costs and features, the Wireshark is the free software program that will make the laptop to act as the protocol analyzer. This software Based analyzer which is similar to powerful electron microscope as well as interpreters for the network traffic. By using this protocol analyzer, an administrator can find the failed NIC- network interface card which is getting a constant data stream onto the networks. This also referred as the chatty network interface card. The administrator can able to identify the NIC based MAC address source, which can be gotten in the output of the packet sniffers. For each packet. The other uses of the protocol analyzer include obtaining an IP destination and source, examining the data and network scanning for intrusion.

Throughput tester: The throughput is the data delivery rate through the communication channel. For that, this tester will test the data delivery rate through the network. The throughput can be measured in bps - bits per second. Testing this throughput is necessary for the administrators and to make aware of what exactly the networks are doing. It is specially designed to gather information more quickly about the network functionality and especially the network overall average throughput.



TOPIC 6

TRANSMISSION MEDIA

Introduction to Transmission medium

A **transmission medium** is a material substance (solid, liquid, gas, or plasma) that can propagate energy waves. For example, the transmission medium for sounds is usually air, but solids and liquids may also act as transmission media for sound.

The absence of a material medium in vacuum may also constitute a transmission medium for electromagnetic waves such as light and radio waves. While material substance is not required for electromagnetic waves to propagate, such waves are usually affected by the transmission media they pass through, for instance by absorption or by reflection or refraction at the interfaces between media.

The term transmission medium also refers to a technical device that employs the material substance to transmit or guide waves. Thus, an optical fiber or a copper cable is a transmission medium. Not only is this but also able to guide the transmission of networks.

A transmission medium can be classified as a:

- *Linear medium*, if different waves at any particular point in the medium can be superposed (**i.e.** when two waves meet they overlap and interact. Sometimes they add to make a wave bigger, sometimes they cancel each other)
- *Bounded medium*, if it is finite in extent, otherwise *unbounded medium*;
- *Uniform medium* or *homogeneous medium*, if its physical properties are unchanged at different points;
- *Isotropic medium*, if its physical properties are the same in different directions.

Transmission and reception of data is performed in four steps.

1. The data is coded as binary numbers at the sender end
2. A carrier signal is modulated as specified by the binary representation of the data
3. At the receiving end, the incoming signal is demodulated into the respective binary numbers
4. Decoding of the binary numbers is performed

Telecommunications

A physical medium in data communications is the transmission path over which a signal propagates.

Many transmission media are used as communications channel.

For telecommunications purposes in the United States, Federal Standard 1037C, transmission media are classified as one of the following:

- Guided (or bounded)—waves are guided along a solid medium such as a transmission line.
- Wireless (or unguided)—transmission and reception are achieved by means of an antenna.

Bounded/Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of Bounded/ Guided are discussed below.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 µs/km.
- Repeater spacing is 2km.

Twisted Pair is of two types :

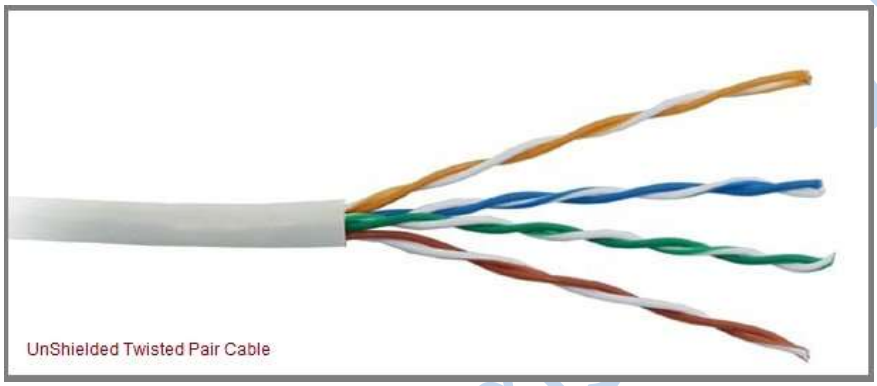
- **Unshielded Twisted Pair (UTP)**

- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.



It can be either voice grade or data grade depending on the condition. UTP cable normally has an impedance of 100 ohm. UTP cost less than STP and easily available due to its many use. There are five levels of data cabling

TOPIC 8

TYPES OF COMPUTER NETWORKS

Introduction to computer network types

Different types of (private) networks are distinguished based on their size (in terms of the number of machines), their data transfer speed, and their reach.
Private networks are networks that belong to a single organization.

There are usually said to be three categories of networks:

- LAN (**local area network**)
- MAN (**metropolitan area network**)
- WAN (**wide area network**)

There are two other types of networks:

- **TANs (Tiny Area Network)**, which are the same as LANs but smaller (2 to 3 machines),
- and **CANs (Campus Area Networks)**, which are the same as MANs (with bandwidth limited between each of the network's LANs).

***LAN* stands for *Local Area Network*.**
It's a group of computers which all belong to the same organization, and which are linked within a small geographic area using a network, and often the same technology (the most widespread being Ethernet).

A local area network is a network in its simplest form. Data transfer speeds over a local area network can reach up to 10 Mbps (such as for an Ethernet network) and 1 Gbps (as with FDDI or Gigabit Ethernet).
A local area network can reach as many as 100, or even 1000, users.

Note
Ethernet (also known as *IEEE 802.3 standard*) is a data transmission standard for local area networks based on the following principle:

- All machines on an Ethernet network
- are connected to the same communication line,
- made up of cylindrical cables

FDDI (*Fiber Distributed Data Interface*) technology is network access technology over *fibre optic* type lines.

By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined:

TOPIC 9

NETWORKING PROTOCOLS

Network Models (Data Communications and Networking)

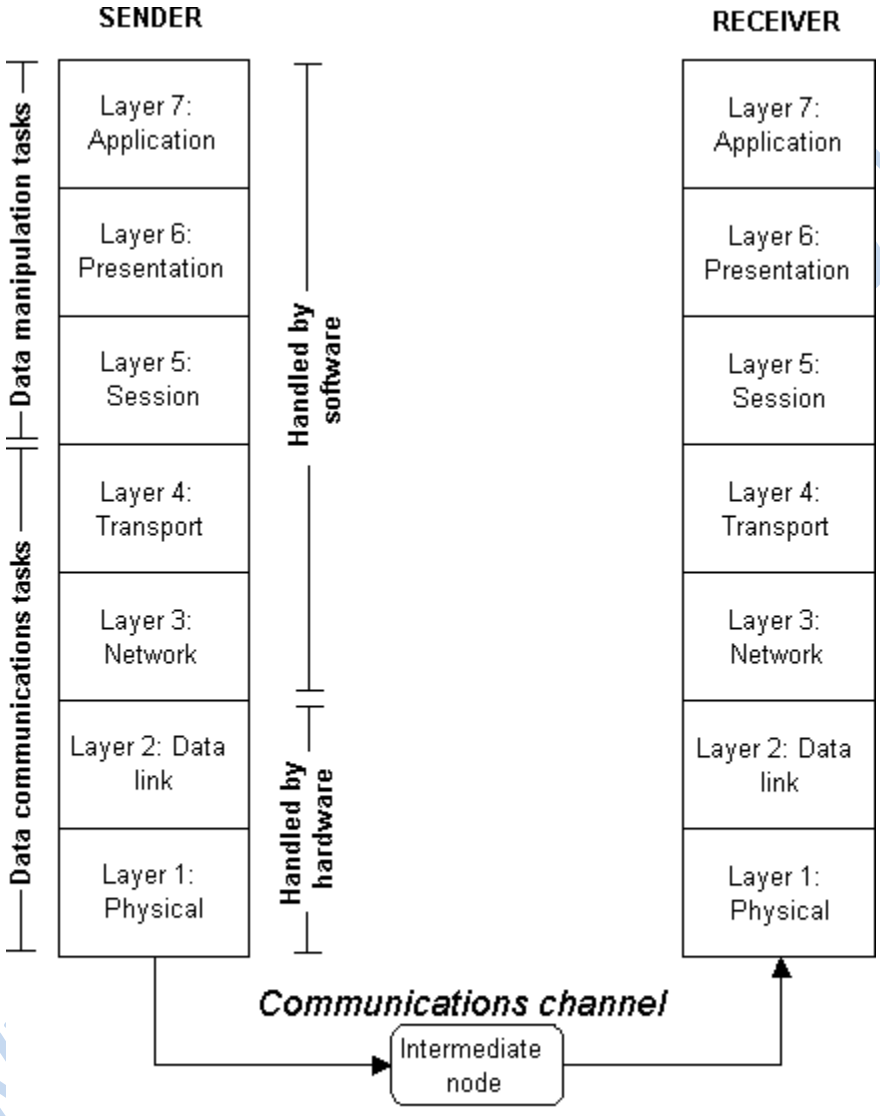
There are many ways to describe and analyze data communications networks. All networks provide the same basic functions to transfer a message from sender to receiver, but each network can use different network hardware and software to provide these functions. All of these hardware and software products have to work together to successfully transfer a message.

One way to accomplish this is to break the entire set of communications functions into a series of layers, each of which can be defined separately. In this way, vendors can develop software and hardware to provide the functions of each layer separately. The software or hardware can work in any manner and can be easily updated and improved, as long as the interface between that layer and the ones around it remain unchanged. Each piece of hardware and software can then work together in the overall network.

There are many different ways in which the network layers can be designed. The two most important network models are the Open Systems Interconnection Reference (OSI) model and the Internet model.

Open Systems Interconnection (OSI) model

While many hardware and software vendors have attempted to promote their own protocols, the International Standards Organization (ISO) has set forth a reference model for networking called the Open Systems Interconnection (OSI) model. The OSI model consists of seven interconnected layers, as shown in the figure on the next page.



The Open Systems Interconnection (OSI) Model

The application layer (Layer7) is the highest layer in the OSI model and is what the user sees (at both the sending and receiving ends of the communication network). It defines the way the user's application program interacts with the network. The application program could be either electronic mail, database management, or a terminal emulation program (for connecting to a mainframe computer system). It is in the application layer that the user's message is converted from human readable form to computer readable form with the message header indicating the sender and intended receiver of the message.

The presentation layer (Layer6) defines the way that data is formatted, presented, converted, and coded. In essence, the presentation layer ensures that the message is transmitted in a language that the receiving computer can understand (often ASCII -- American Standard Code for Information Interchange). If necessary, or as directed by the user, the message is also compressed and encrypted at this stage.

The session layer (Layer5) coordinates communication between the sender and receiver. In essence, this layer maintains the session for as long as it is needed, performing security, logging, and any administrative functions that are needed. It is in the session layer that the mode of communication is established -- either full duplex where both parties in the communication can send and receive messages simultaneously, or half duplex where the parties must take turns communicating. All of these details are recorded and placed into a "session header" for the session.

The transport layer (**layer 4)**, defines protocols for message structure and supervises the validity of the transmission by performing error checking. In effect, the transport layer protects the data being transmitted. The protection comes from *checksum* tests -- mathematically calculated sums based on the contents of the data being sent. The "transport header" records each segments checksum and its position in the message.

The network layer (Layer3), defines protocols for data routing to ensure that the data arrives at the correct destination node. It is the network layer that essentially selects a route for the message, using protocols such as TCP/IP (transmission control protocol/internet protocol), or IPX/SPX which is the protocol for Novell networks. Routers, discussed above, are used at the network layer. The data are formed into packets and a header is added that contains the sequence and number of packets and the network address of the destination.

The data-link layer (Layer2), validates the integrity of the flow of data between nodes. This validation is performed by synchronizing blocks of data and controlling the flow of data. In this manner, the data-link layer supervises the transmission. It confirms the checksum and then addresses and duplicates the packets. The data-link layer keeps a copy of each packet until it receives confirmation from the next point along the transmission route that the packet has been received. Bridges, discussed above, are used at the data-link layer.

Finally, the physical layer (Layer1), is the actual transmission hardware or link along which the messages physically pass. It is only along layer 1 that messages physically move from the origin to the destination. If phone lines are being used, then it is the physical layer that actually converts the digital signals into analog signals so that they can be carried on the phone line. Intermediate nodes along the transmission path verify the checksum and might reroute the message in light of congestion in the network.

At the receiving end, the message passes through the same seven layers, in reverse. The physical layer reconverts the analog signals into digital form (bits). The data-link layer recomposes the checksum, confirms arrival, and logs in the packets. The network layer recounts each packet for security and billing purposes. The transport layer again recalculates the checksum and rebuilds the message segments. The session layer holds the parts of the message until the message is complete and then sends it to the next layer. If the message was compressed, the presentation layer expands it, and if the message had been encrypted it is decrypted at this stage. Finally, the application layer reconverts the bits into readable characters and directs the data to the appropriate application (e.g., email).

A few comments about the seven layer OSI model are appropriate. First, each layer is independent allowing protocols for each layer to be defined and developed independent of other layers. Second,

communication is possible only between adjacent layers. Layer 3 can communicate only with layer 2 and layer 4. Finally, the model makes a distinction between data communication tasks and data manipulation tasks. Layers 1 through 4 (physical through transport) perform data communications tasks which interact primarily with hardware devices. Layers 1 and 2 interact *only* with hardware devices, whereas Layers 3 and 4 interact with both hardware and software devices. For data transmissions over the Internet, it is layers 1 through 4 that handle the necessary tasks for physically transmitting packets of data over the Internet. As we will see a little later, there can literally be hundreds of "intermediate nodes" that come into play when data is transmitted over the Internet. Layers 5, 6, and 7 which perform data manipulation tasks interact primarily with software -- the operating system and the specific application program being used. Thus, when you use a Web browser such as Netscape, layers 5 through 7 are responsible for the necessary translations between the network transmission (e.g., Novell Netware or Windows NT), the operating system (e.g., Windows 9x), and the browser (e.g., Netscape 4.x).

Open Systems Interconnection Reference Model elaborated Details……..

The Open Systems Interconnection Reference model (usually called the OSI model for short) helped change the face of network computing. Before the OSI model, most commercial networks used by businesses were built using non-standardized technologies developed by one vendor (remember that the Internet was in use at the time but was not widespread and certainly was not commercial). During the late 1970s, the International Organization for Standardization (ISO) created the Open System Interconnection Subcommittee, whose task was to develop a framework of standards for computer-to-computer communications. In 1984, this effort produced the OSI model. **The OSI model is the most talked** about and most referred to network model. If you choose a career in networking, questions about the OSI model will be on the network certification exams offered by Microsoft, Cisco, and other vendors of network hardware and software. However, you will probably never use a network based on the OSI model. Simply put, the OSI model never caught on commercially in North America, although some European networks use it, and some network components developed for use in the United States arguably use parts of it. Most networks today use the Internet model, which is

THIS IS A SAMPLE

TO GET COMPLETE NOTES,

CALL|TEXT|WHATSAPP 0728 776 317