COURSE CODE: CSC 426
COURSE TITLE: Computer Communication System
NUMBER OF Units: 3 Units

Course Duration: Two Hours lecture, One Hour practical

COURSE DETAILS:
Course Lecturer: Dr. O. Folorunso
B.Sc. (Abeokuta), M.Sc. (Lagos), PhD (Abeokuta), MNCS, MCPN
Email: folorunsolusegun@yahoo.com
Office Location: Room B201, COLNAS Building
Consultation hours: 12-2pm, Wednesdays & Fridays
Lecture Note developed by: The Department of Computer Science, University of Agriculture, Abeokuta
Head of Department: DR. A.F. ADEKOYA

Course Content: Information and encoding, basic concepts of interactive computing, interactive terminal devices, protocol, direct links, communication channels, telecommunication links, simplex, Duplex, and half-duplex, multiplexer, concentrator, computer networks, operating systems for online processing, scheduling algorithm, response time, reliability and security.

Course Description: The course is designed to describe the fundamental concepts of computer communication system, data communication, basic issues in computer networking, examining its nuts and bolts, communication channels, protocols, topologies, principles of congestion control, security in computer networks and the internet.

Course Justification:
Any serious study of computer communication requires an examination of some related topics. Today's internet is arguably the largest engineered system ever created by mankind, with hundreds of millions of connected computers, communication links, and switches, hundreds of millions of users who connect intermittently via cell phones and PDAs; and devices such as sensors, webcams, game consoles, picture frames and even washing machines being connected to the internet. Given that the internet is so large and has so many diverse components and uses, is there any hope to understand how it (and more generally computer networks) works? Are there guiding principles and structure that can provide a foundation of understanding such an amazingly large and complex system? The answer to all these questions is a resounding yes! The lecture note will provide you with a modern introduction to the dynamic field of computer communication system, with emphasis on computer networking and its management, giving you the principles and practical insights you will need to understand.

Course Objectives:
The general objective of the course as an integral part of the Bachelor Degree for Computer Science Students in University of Agriculture, Abeokuta, is to:

- To increase capacity of computer science students to express ideas
- Improve their background in the area of Information and Communications Technology.
- Increase the ability to identify various Networking components, its installation and configuration
- To better understand how to secure a communication system.

Course Requirements:
This is a compulsory course for all computer science and Electrical/Electronic Engineering students in the University. In view of this, students are expected to participate in all the course activities and have minimum of 75% attendance to be able to write the final examination.

EXAM	70%
PRATICAL	20%
QUIZ	10%
	100%

Reading List:

1. Marian Cole (2002) Introduction to Telecommunications- Voice, Data and the Internet 2^{ND} EDITION Published by Prentice Hall, U.S.A.
2. 3comcorp “white paper: understanding IP addressing; everything you ever wanted to know”, http://www.3com.com/other/pdfs/infra/corpinfo/en_us/501302.pdf.
3. D. Bertsekas, R. Gallagher (1991), Data Networks, 2^{ND} EDITION, Prentice Hall, Englewood Cliffs, NJ.
4. Bishop. M (2003), computer security: Art and science, Boston: Addison Wesley, BOSTON MA.
5. D. Chiu and R. Jain (1989): Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks, “Computer Networks and ISDN systems, vol.17, No1 pp. 1-14: http://www.cs.wustl.edu/jain/papers/cong_av.htm.
6. S.M Bellovin, Security problems in the TCP/IP protocol suite, computer communication review, 1989.
7. Tamara Dean, Network+ in depth, Stacy L. Hiquet, 2005.
8. Matt Curtin, Introduction to Network Security, Kent information Inc. 1997.

LECTURE CONTENT

WEEK 1:

Data communication, DTE and DCE, serial and parallel transmission of data, Asynchronous and synchronous Transmission, Error Detection and Correction, Flow Control, Baud Rate.

OBJECTIVES

1. Understanding the basics of communication
2. Understanding the fundamental principles of Data communication
3. Identifying errors in transmission and there corrections.

LECTURE NOTE:

DATA COMMUNICATION

Data communication is the transmission of characters, numbers, graphics, and symbols using digital signals. The public switched telephone network (PSTN) is used to carry both voice and data communication. Data communication is closely related to voice communication, both communication systems are concerned with transmitting information over some distance. The primary difference between voice and data lies in the signal used to convey information. Voice is converted by the transmitter of a telephone into an analog electrical signal having many different voltage levels. Data is converted into an electrical signal that has two different voltage level represented by the binary 0 and 1.

The public switched telephone network started as an analog network designed to handle analog voice signals but it has gradually been converted from an analog to a digital network because nowadays most signals are two-state digital signals. Several digital technologies have been developed for voice communication that move the codec from the line circuit to the customer's premises example include

i. Integrated Services Digital Network (ISDN)
ii. Asymmetric Digital Subscriber Line (ADSL)

DTE AND DCE

The personal computer belongs to the category of equipment called Data Terminal Equipment. A DTE device is used to transmit and receive data in the form of digital signals.

Data Communication Equipment (DCE) which is also refers to as data circuit termination equipment is a device that interfaces Data Terminal Equipment (DTE) to the PSTN. A modem is a DCE used to interface a DTE to analog line circuit on the PSTN. A channel service unit /data service unit (CSU/DSU) is a DCE device used to interface a DTE device to a leased digital line in the public switched telephone network.

The most common connection used to connect DTE to DCE is an EIA-232 interface. This interface is also called a recommended standard 232 (RS-232) which is approved as the CCITT standard V.24. The EIA-232 interface cable comes in a 25-conductor and 9-conductor cable. The 25-conductor cable uses a DB-25 connector attached to each end of the cable and the 9-conductor cable uses DB-9 connectors. A cable for connecting data terminal equipment (DTE) to data communication equipment (DCE) will have a female connector on one end and a male connector on the other end.

SERIAL AND PARALLEL TRANSMISSION OF DATA.

Data can be transmitted one bit or several bits at a time. When data is transmitted one bit at a time, it is transmitted over one wire, where each bit is transmitted one after the other onto the same wire the type of transmission is termed Serial Transmission.
Parallel transmission is the type of transmission where data is transmitted several bits at time; each bit is transmitted over its own wire. The bits are transmitted over wires that are parallel. The most common form of parallel transmission is to transmit 8 bits at one time. Example includes the seven level ASCII coding with an eighth bit used as a parity bit to check the validity of the code. By transmitting 8bits at once we can transmit a character at a time instead of a bit at a time. Most printers connected to a personal computer are parallel printers transferring 8 data bits at a time. It is apparent that parallel transmission is much faster than serial transmission, but serial transmission is most often used in data communication because only one circuit is needed for the transmission of data. Parallel data transmission is used when the transmission distance is less than 25ft.

ASYNCHRONOUS AND SYNCHRONOUS TRANSMISSION.

Asynchronous transmission also called start and stop transmission. The transmitting device sends a start bit prior to each character and sends a stop bit after each character. The receiving device will synchronize from the received start bits. Thus, synchronization occurs at the beginning of each character. Data is sent between two devices as a serial bit stream. In asynchronous transmission each character has it own synchronizing information. The start bit is a bit whose value is 0 and is refers to as space and a stop bit with value 1 refers to as Mark bit.
Synchronous transmission involves the transmission of data as blocks of bytes. Synchronization of the receiver occurs from a special bit pattern called a sync signal placed in front of the block of data information. A typical block contains 128, 256, 512, or 1024 characters. A header is placed in front of the data sent and a trailer is placed after the data. The header will contain the destination address of the message, a synchronization signal and control information. The trailer contains parity checking information and the address of the sender. The header usually contains about 32bits and the header 8 to 16 bits. Synchronous data transmission is obviously faster than asynchronous transmission because fewer bits are needed to send the same data.

ERROR DETECTION AND CORRECTION

ASYNCHRONOUS TRANSMISSION ERROR CHECKING

The simplest error checking method is parity checking. This technique is used for asynchronous transmission. ASCII uses 7 bits for coding and does not use the 8th bit allowing the use of the 8th bit for parity checking. There are five types of parity namely: odd, even, mark, space, and no parity. In odd parity each character has an odd number of 1s, for odd a 0 is placed in the 8th bit position. An even parity is the error checking protocol ensures each transmitted byte has an even number of 1s.

SYNCHRONOUS TRANSMISSION ERROR DETECTION AND CORRECTION

The use of synchronous transmission between the two modems allows the use of sophisticated error detection and control techniques. Modems use a synchronous error detection technique called cyclic redundancy checking (CRC).
There are two types of CRC; CRC-16 and CRC-32. The block of data is divided by a 17-bit divisor for CRC-16 or a 33-bit divisor for CRC-32. The CRC calculation is done at the transmitting modem and the remainder is placed in the trailer behind the block of data and trailer behind the block of data transmitted. The receiving modem receives the block of data and trailer. It then calculates a remainder using the same CRC protocol used by the transmitting modem, comparing it with the sent remainder. Error conditions are handled by requesting that the originating modem retransmit the data. This technique is called Automatic Retransmission Request (ARQ). There are two types of error correction namely;
Discrete ARQ also called stop and wait ARQ, an error control protocol that requires an acknowledgement from the receiver after each block of data sent. The transmitting modems sends a block of data and then waits for an acknowledgement before sending the next block of data.
Continuous ARQ also known as sliding window ARQ, continuous ARQ eliminates the need for a transmitting device to wait for acknowledgement after each block of data. The device continuously returns positive acknowledgement to the transmitter until otherwise.

FLOW CONTROL

Controlling the flow of data from one device to another is usually via hardware flow control; Request to send and clear to send (RTS/CTS) or by software flow control (XON/XOFF). A modem contains a memory buffer to allow it to compress data before transmitting and to allow it to convert asynchronous data to synchronous data. It must be able to stop the transmitting personal computer when this memory buffer approaches a near full condition some modems contain a very large memory buffer, which negates the need for flow control

BAUD RATE

Baud rate is defined as the number of times a signal changes. Baud rate is one of the components determining the physical line speed of a modem. The other component is the number of bits represented by one signal change. For example if the amplitude of a signal changes 2400 times a second the signal changes states 2400 times per second or at 2400 baud.

WEEK 2:

Data Networking via LANs, Putting a LAN together, Connecting Two LANs to each other, The LAN Medium, Communication within the LAN.

OBJECTIVE:

The objective of the week lecture is for the student to be able to understand LAN topology and how networking is performed in the LAN environment.

LECTURE NOTE:

DATA NETWORKING VIA LANS

In linking many computers that are physically closed together such as within one building, or on one floor of a building, we can utilize a LAN. Two LANs can be connected together using a device called a bridge. LANs within a larger geographical region such as a city are connected using a metropolitan area network (MAN) and LANs separated by any distance are connected using WAN.

DEFINITION

A LAN is a data communication system allowing a number of independent devices such as computer and printers that are usually located within 500m of each other to communicate directly with each other over a common physical medium. The distance can be more or less than 500m depending on the type of cable used for the medium.

ADVANTAGES OF USING LANs.

1. The use of a LAN allows data, applications, printers, and other resources to be shared efficiently and economically.
2. It enhances communication
3. Sharing of resources reduces the cost of computing.
4. Allows business to gain economics of scale in the purchase of application of software.
5. Allows installation of groupware applications software.

PUTTING A LAN TOGETHER.

A LAN consists of the transmission medium used to connect workstation and servers together. To connect workstations, servers and printers together using a LAN the following are to be decided;

1. Determine the quantity and types of devices that need to be connected to the LAN and what features the LAN will be providing.

2. Determine the type of Network operating system software that the LAN will use. If the connection is between two computers windows can be use for the workgroups and a network card supported by this software might be used. Dos-based LANs can support up to 300 users, but LANs of this size will usually opt for a Novell or Windows NT-based LAN. The Network operating systems software contains an applications program interface (API) that handles the interpretation of messages to allow different PC operating systems to exist on the LAN.
3. Deciding the architecture for the LAN setup. There are two predominant architectures for LAN; the Token ring and the Ethernet.

ARCHITECTURE	LAN STANDARD	TOPOLOGY
Ethernet	IEEE 802.3	Bus
Token Ring	IEEE 802.5	Ring

Though the token ring employs a ring topology it is implemented by wiring the computers in a star arrangement. The central point of the star is a wiring HUB called a medium access unit (MAU).

4. Another decision that needs to be made is the type of transmission medium to use. There are different choices they include coaxial cable, thin coaxial cable, twisted pair copper wire and fiber optic cable. The Ethernet based LAN use the thick coaxial cable.

CONNECTING TWO LANS TO EACH OTHER.

Repeaters can be used to extend LANs. The repeater is a layer 1 device; it simply regenerates new signals based on the signal received. LANs of similar or dissimilar architectures can be connected together by a bridge. The bridge is a device that uses both layers 1 and 2 but is usually described as operating at the layer 2 level. It has the intelligence necessary to be able to determine which addresses resides on which side of the bridge. Special bridges known as remote bridges can be used on each end of a leased transmission facility to connect LANs that are distant from each other together. Each LAN is connected to a remote bridge and the remote bridges are connected to a CSU/DSU bridges exist that allows the connection of an Ethernet LAN to a token ring LAN these bridges are often called translating bridges, intelligent bridges or encapsulating bridges.

THE LAN MEDIUM

The LAN medium is a shared medium. Users takes turn using the medium and each user is granted a brief period when they can use it. Thus, the medium is used in a time division multiplexing (TDM) arrangement. Ethernet controls the size of each frame of data that a user can send. Ethernet limits the user's data to 1500 bytes at a time. This ensures that one user cannot hog the medium for extended periods.

COMMUNICATION WITHIN THE LAN

For devices to communicate with each other across a LAN, they must know the hardware address (physical or MAC address) of the device they wish to communicate with. This is why the Ethernet frame contains MAC addresses. If a higher level protocol is being used on a LAN such as TCP/IP, higher level network addresses will be used by applications that wish to converse across the LAN or across networks. The higher level addresses must be resolved to hardware addresses when the two devices reside on the sane network.

WEEK 3:

Communication channels, examples of communication channels, Types of communication channels, Transmission Directions: Simplex, Duplex, Half Duplex.

OBJECTIVE:

The objective of the week lecture is for the student to be able to understand Communication channels, examples of communication channels, Types of communication channels.

LECTURE NOTE:

COMMUNICATION CHANNEL

In telecommunications and computer networking, a communication channel, or channel, refers either to a physical transmission medium such as a wire, or to a logical connection over a multiplexed medium such as a radio channel. A channel is used to convey an information signal, for example a digital bit stream, from one or several senders (or transmitters) to one or several receivers. A channel has a certain capacity for transmitting information, often measured by its bandwidth in Hz or its data rate in bits per second.

EXAMPLES OF COMMUNICTION CHANNELS

A channel can take many forms. Examples of communications channels include:

1. A connection between initiating and terminating nodes of a circuit.
2. A single path provided by a transmission medium via either
    - physical separation, such as by multipair cable or
    - Electrical separation, such as by frequency-division or time-division multiplexing.
3. A path for conveying electrical or electromagnetic signals, usually distinguished from other parallel paths.
    - A storage which can communicate a message over time as well as space
    - The portion of a storage medium, such as a track or a band, that is accessible to a given reading or writing station or head.
    - A buffer from which messages can be 'put' and 'got'. See Actor model and process calculi for discussion on the use of channels.
4. In a communications system, the physical or logical link that connects a data source to a data sinks.

5. A specific radio frequency, pair or band of frequencies, usually named with a letter, number, or code word, and often allocated by international agreement.
6. A room in the Internet Relay Chat (IRC) network, in which participants can communicate with each other.

All of these communications channels share the property that they transfer information. The information is carried through the channel by a signal.

TYPES OF COMMUNICATIONS CHANNELS

- Digital (discrete) or analog (continuous) channel
- Baseband and passband channel
- Transmission medium, for example a fibre channel
- Multiplexed channel
- Computer network virtual channel
- Simplex communication, duplex communication or half duplex communication channel
- Return channel
- Uplink or downlink (upstream or downstream channel)
- Broadcast channel, unicast channel or multicast channel

TRANSMISSION DIRECTION

Data transmission, whether analog or digital, may also be characterized by the direction in which the signals travel over the media.

SIMPLEX, HALF-DUPLEX, AND DUPLEX

In cases in which signals may travel in only one direction, the transmission is considered simplex. In simplex, communication is possible in only one direction that is there is only one sender. An example of simplex communication is a football coach calling out orders to his team through a megaphone. In this example, the coach’s voice is the signal, and it travels in only one direction—away from the megaphone’s mouthpiece and toward the team. Simplex is sometimes called one-way, or unidirectional, communication.

In half-duplex transmission, signals may travel in both directions over a medium but in only one direction at a time. Half-duplex systems contain only one channel for communication, and that channel must be shared for multiple nodes to exchange information. Communication is possible in both direction but one at a time. For example, the walkie talkie operates in this way; an apartment’s intercom system that requires someone to press a “talk” button to allow the voice to be transmitted over the wire uses half-duplex transmission. If you visit a friend’s apartment building, you press the “talk” button to send your voice signals to his apartment. When your friend responds, he presses the “talk” button in his apartment to send his voice signal in the opposite direction over the wire to the speaker in the lobby where you wait. If you press the “talk” button while he’s talking, you will not be able to hear his voice transmission. In a similar manner, some networks operate with only half-duplex capability.

When signals are free to travel in both directions over a medium simultaneously, the transmission is considered full-duplex. Full-duplex may also be called bidirectional transmission or, sometimes, simply duplex. When you call a friend on the telephone, your connection is an example of a full-duplex transmission, because your voice signals can be transmitted to your friend at the same time your friend's voice signals are transmitted in the opposite direction to you. In other words, both of you can talk and hear each other simultaneously

WEEK 4:

Protocols.

OBJECTIVE:

To understand the fundamentals of network protocols, the different types of protocols and IP addressing.

LECTURE NOTE:

PROTOCOLS

A protocol is a rule that governs how networks communicate. Protocols define the standards for communication between network devices. Without protocols, devices could not interpret the signals sent by other devices, and data would go nowhere.
Protocols vary according to their purpose, speed, transmission efficiency, utilization of resources, and ease of setup, compatibility, and ability to travel between different LANs. In choosing protocols, it is important to consider these characteristics, plus network interconnection and data security requirements. Networks running more than one protocol are called Multiprotocol networks.

TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP)

TCP/IP is not simply one protocol, but rather a suite of specialized protocols—including TCP, IP, UDP, ARP, and many others—called sub protocols. Most network administrators refer to the entire group as "TCP/IP," or sometimes simply "IP." TCP/IP's roots lie with the U.S. Department of Defence, which developed TCP/IP for its Advanced Research Projects Agency network (Arpanet, the precursor to today's Internet) in the late 1960s.TCP/IP has grown extremely popular thanks to its low cost, its ability to communicate between a multitude of dissimilar platforms, and its open nature. "Open" means that a software developer, for example, can use and modify TCP/IP's core protocols freely. TCP/IP is a de facto standard on the Internet and has become the protocol of choice on LANs and WANs. TCP/IP would not have become so popular if it weren't routable. Protocols that can span more than one LAN (or LAN segment) are routable, because they carry Network layer addressing information that can be interpreted by a router. It popularity is also due to its flexibility; it can run on virtually any combination of network operating system or network media.

TRANSMISSION CONTROL PROTOCOL (TCP)

TCP (Transmission Control Protocol) operates in the Transport layer of the OSI Model and provides reliable data delivery services. TCP is a connection-oriented sub protocol, which means that a connection must be established between communicating nodes before this protocol will transmit data. TCP further ensures reliable data delivery through sequencing and checksums. Without such measures, data would be transmitted indiscriminately, without checking whether the destination node was offline, for example, or whether the data became corrupt during transmission. Finally, TCP provides flow control to ensure that a node is not flooded with data. TCP has 10 header fields.

USER DATAGRAM PROTOCOL (UDP)

UDP (User Datagram Protocol), like TCP, belongs to the Transport layer of the OSI Model. Unlike TCP, however, UDP is a connectionless transport service. In other words, UDP offers no assurance that packets will be received in the correct sequence. In fact, this protocol does not guarantee that the packets will be received at all. Furthermore, it provides no error checking or sequencing. Nevertheless, UDP's lack of sophistication makes it more efficient than TCP. It can be useful in situations where a great volume of data must be transferred quickly, such as live audio or video transmissions over the Internet. In these cases, TCP—with its acknowledgments, checksums, and flow control mechanisms—would only add more overhead to the transmission. UDP is also more efficient for carrying messages that fit within one data packet. UDP contains only four header fields the source port, destination port, length and checksum.

INTERNET PPROTOCOL (IP)

IP (Internet Protocol) belongs to the Network layer of the OSI Model. It provides information about how and where data should be delivered, including the data's source and destination addresses. IP is the subprotocol that enables TCP/IP to internetwork that is, to traverse more than one LAN segment and more than one type of network through a router. At the Network layer of the OSI Model, data is formed into packets. In the context of TCP/IP, a packet is also known as an IP datagram. The IP datagram acts as an envelope for data and contains information necessary for routers to transfer data between different LAN segments. IP is an unreliable, connectionless protocol, which means that it does not guarantee delivery of data. Higher-level protocols of the TCP/IP suite, however, use IP to ensure that data packets are delivered to the right addresses. Note that the IP datagram does contain one reliability component, the Header checksum, which verifies only the integrity of the routing information in the IP header. If the checksum accompanying the message does not have the proper value when the packet is received, then the packet is presumed to be corrupt and is discarded; at that point, a new packet is sent.

Some other examples of protocols include;

1. INTERNET CONTROL MESSAGE PROTOCOL (ICMP)
2. INTERNET GROUP MANAGEMENT PROTOCOL (IGMP)
3. ADDRESS RESOLUTION PROTOCOL (ARP)
4. REVERSE ADDRESS RESOLUTION PROTOCOL (RARP

IP ADDRESSING

The IP protocol provides an address field for the address of the originator of an IP packet that is called the source address. The IP protocol also contains an address field for the destination of an IP packet that is called Target address. In IP version 4 both of these addresses are 32 bits long. The 32 bits field consists of 4 bytes; each byte can contain a number from 1 to 255. Address possibility ranges between 0.0.0.0 to 255.255.255.255.

Instead of specifying a particular user's computer, the IP address is used to specify a network and then a host on the network. Host is a term used to refer to a workstation, server or other computer attached to a network. A network containing many hosts is classified as a class A network, medium size networks are class B networks, and a small network is a class C network. There are not many very large class A networks but there are a lot of small class C networks. There are more than 255 medium size networks. In addition class D and class E addresses exist but are rarely used.

Although 8 bits have 256 possible combinations, only the numbers 1 through 254 can be used to identify networks and hosts in an IP address. The number 0 is reserved to act as a placeholder when referring to an entire group of computers on a network for example, "10.0.0.0" represents all of the devices whose first octet is "10."The number 255 is reserved for broadcast transmissions. For example, sending a message to the address 255.255.255.255 will send a message to all devices connected to your network segment.

Dotted decimal notation, the most common way of expressing IP addresses, refers to the "shorthand" convention used to represent IP addresses and make them easy for people to read. In dotted decimal notation, a decimal number between 0 and 255 represents each binary octet (for a total of 256 possibilities).A period, or dot, separates each decimal. An example of a dotted decimal IP address is 131.65.10.18.

NETWORK CLASS	BEGINNING OCTET	NUMBER OF NETWORKS	MAXIMUM ADDRESSABLE HOST PER NETWORK
A	1-126	126	16,2777,214
B	128-191	>16,000	65,534
C	192-223	>2,000,000	254

SUBNET MASK

In addition to an IP address, every device on a TCP/IP-based network is identified by a subnet mask. A subnet mask is a special 32-bit number that, when combined with a device's IP address, informs the rest of the network about the segment or network to which the device is attached. That is, it identifies the device's subnet. Like IP addresses, subnet masks are composed of four octets (32 bits) and can be expressed in either binary or dotted decimal notation. Subnet masks are assigned in the same way that IP addresses are assigned—either manually, within a device's TCP/IP configuration, or automatically, through a service such as DHCP.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP).

This is an automated means of assigning a unique IP address to every device on a network. DHCP like BOOTP belongs to the application layer of the OSI model. Reasons for implementing DHCP include the following:

- To reduce the time and planning spent on IP address management
- To reduce the potential for errors in assigning IP address.
- To enable users to move their workstations and printers without having to change their TCP/IP configuration
- To make IP addressing transparent for mobile users.

WEEK 5:

Networking hardware: Network Interface Card, Repeaters and Hubs, Bridges, Routers. Hardware devices involved in networking and their roles in managing data traffic, more about network interface cards, which serve as the workstation's link to the network and are often the source of connectivity problems.

OBJECTIVE:

1. Name some hardware involved in networking systems and their functions.
2. Identify problems associated with connectivity hardware.
3. Describe the factors involved in choosing a NIC, hub, switch, or router

LECTURE NOTE:

NETWORKING HARDWARE

For effective communication of computers, some hardware are required which helps in the transmission of data. This hardware has different functionality which will be reviewed briefly.

NICs (Network Interface Cards)

Network interface cards (also called NICs, network adapters, or network cards) are connectivity devices that enable a workstation, server, printer, or other node to receive and transmit data over the network media.

NICs belong to both the Physical layer and Data Link layer of the OSI Model, because they apply data signals to the wire and assemble or disassemble data frames. They also interpret physical addressing information to ensure data is delivered to its proper destination. In addition, they perform the routines that determine which node has the right to transmit data over a network at any given instant.

TYPES OF NICs

NICs come in a variety of types depending on:

The access method (for example, Ethernet versus Token Ring)
Network transmission speed (for example, 100 Mbps versus 1 Gbps)
Connector interfaces (for example, RJ-45 versus SC)
Type of compatible motherboard or device (for example, PCI)
Manufacturer (popular NIC manufacturers include 3Com, Adaptec, D-Link, IBM, Intel, Kingston, Linksys, and so on)

Internal Bus Standards

A computer’s bus is the circuit, or signalling pathway, used by the motherboard to transmit data to the computer’s components, including its memory, processor, hard disk, and NIC. Buses differ according to their capacity. The capacity of a bus is defined principally by the width of its data path (expressed in bits) and its clock speed (expressed in MHz). The most popular expansion board NIC is one that uses a PCI bus. PCI (Peripheral Component Interconnect) is a 32- or 64-bit bus with a 33- or 66-MHz clock speed whose maximum data transfer rate is 264 Mbps.

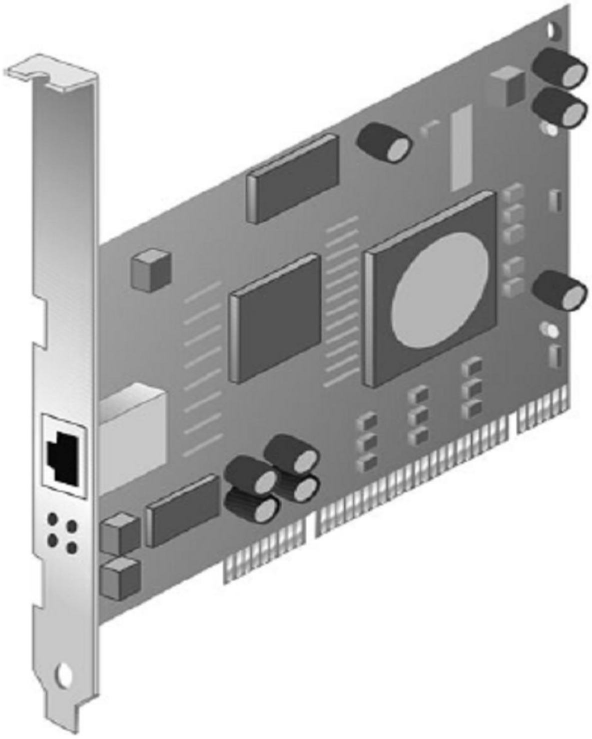

Figure 1. A PCI NIC

Peripheral Bus Standards

Some peripheral devices, such as modems or NICs, are attached to the computer's bus externally rather than internally. Typically, an externally attached adapter needs only to be plugged into the port to be physically installed. An expansion board NIC, on the other hand, requires the user to turn off the computer, remove its cover, insert the board into an expansion slot, fasten the board in place, replace the cover, and turn on the computer.

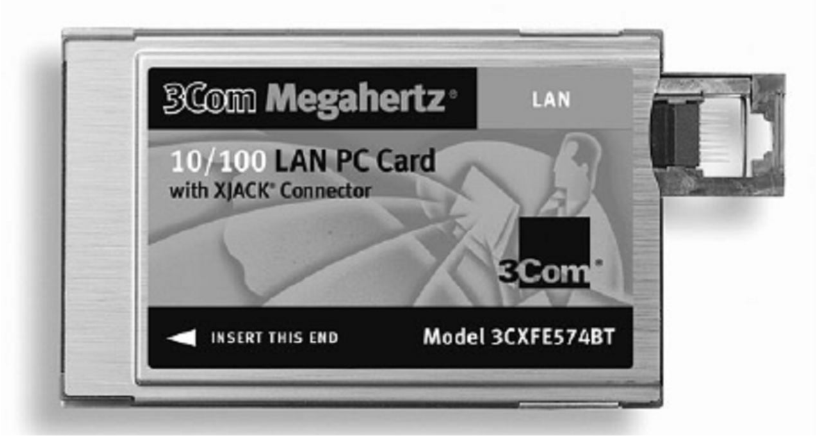

Figure 2. A Card Bus NIC

Another type of externally attached NIC is one that relies on a USB (universal serial bus) port. USB is a standard interface used to connect multiple types of peripherals, including modems, mice, audio players, and NICs.

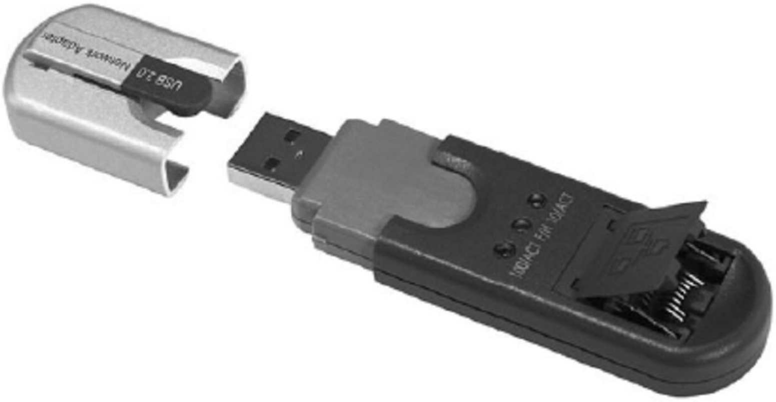

Figure 3. A USB NIC

On-Board NICs

Not all peripheral devices are connected to a computer’s motherboard via an expansion slot or peripheral bus. Some are connected directly to the motherboard using on-board ports. For example, the electrical connection that controls a computer’s mouse operates through an onboard port, as does the connection for its keyboard and monitor.

Wireless NICs

NICs are designed for use with either wire-bound or wireless networks. As you have learned, wireless NICs use an antenna (either internal or external) to exchange signals with a base station transceiver or another wireless NIC.

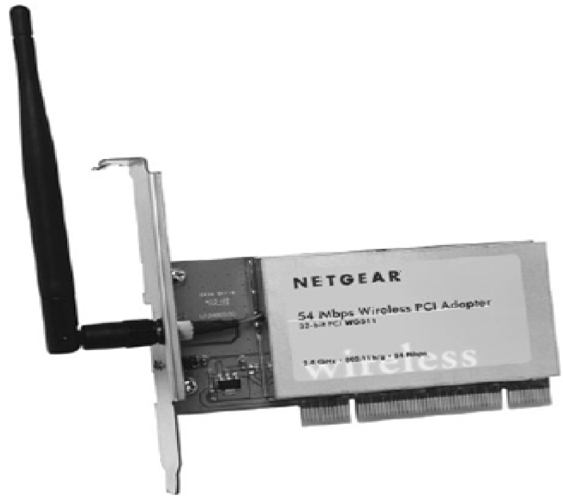

Figure 4. A wireless NIC

HUB

To make data transmission more extensible and efficient than a simple peer-to-peer network, network designers use specialized network devices, such as hubs, switches, routers, and wireless access points, to send data between network devices. The type of connection that is needed determines the device that is used.

Hubs are devices that extend the range of a network by receiving a signal on one port, then regenerating the signal and sending it out to all other ports. This process means that all traffic from a device connected to the hub is sent to all the other devices connected to the hub every time the hub transmits data. This causes a great amount of network traffic. Hubs are also called concentrators, because they serve as a central connection point for a LAN. The following are some of the properties of the hub;

- Extend the range of a signal by receiving then regenerating it and sending it out all other ports
- Traffic is sent out all ports of the hub
- Allow a lot of collisions on the network segment and are often not a good solution

- Also called concentrators because they serve as a central connection point for a LAN

Figure 5. A Hub

BRIDGES AND SWITCHES

Files are broken up into small pieces of data, called packets, before they are transmitted over a network. This allows for error checking and easier retransmission if the packet is lost or corrupted. Address information is added to the beginning and to the end of packets before they are transmitted over the network. The packet, along with the address information, is called a frame.

LANs are often divided into sections called segments bounded by bridges. A bridge has the intelligence to determine if an incoming frame is to be sent to a different segment, or dropped. This improves traffic flow of data by keeping frames from entering the wrong segment. A bridge has two ports.
Switches are sometimes called multiport bridges. A typical bridge may have just two ports, linking two segments of the same network. A switch has several ports, depending on how many network segments are to be linked. A switch is a more sophisticated device than a bridge. A switch maintains a table of the MAC addresses for computers that are connected to each port. When a frame arrives at a port, the switch compares the address information in the frame to its MAC address table. The switch then determines which port to use to forward the frame.

Figure 6. Bridge

ROUTERS

While a switch connects segments of a network, routers are devices that connect entire networks to each other. Switches use MAC addresses to forward a frame within a single network. Routers use IP addresses to forward frames to other networks. A router can be a computer with special network software installed, or a router can be a device built by network equipment manufacturers. Routers contain tables of IP addresses along with optimal destination routes to other networks.

Figure 7 Router.

WIRELESS ACCESS POINTS

Wireless access points provide network access to wireless devices such as laptops and PDAs. The wireless access point uses radio waves to communicate with radios in computers, PDAs, and other wireless access points. An access point has limited range of coverage. Large networks require several access points to provide adequate wireless coverage.

STUDY QUESTION

1. List 5 hardware used in networking and their functions.
2. State the difference between a hub and a repeater.
3. Explain the routing protocols.

WEEK 6:

Transmission media; Coaxial cable, Twisted-pair cabling, fibre – optic cable.

OBJECTIVES:

To encourage the students to Identify names, purposes, and characteristics of the common network cables

LECTURE NOTE:

TRANSMISSION MEDIA

Until recently, cables were the only medium used to connect devices on networks. A wide variety of networking cables are available. Coaxial and twisted-pair cables use copper to transmit data. Fiber-optic cables use glass or plastic to transmit data. These cables differ in bandwidth, size, and cost. As a technician, you need to know what type of cable to use in different situations so that you are able to install the correct cables for the job. You will also need to be able to troubleshoot and repair problems that you encounter.

COAXIAL CABLE

Coaxial cable, called "coax" for short, was the foundation for Ethernet networks in the 1970s and remained a popular transmission medium for many years. Over time, however, twisted-pair and fiber-optic cabling have replaced coax in modern LANs.
Coaxial cable is a copper-cored cable surrounded by a heavy shielding. Coaxial cable is used to connect computers in a network. There are several types of coaxial cable, including the following:

Thicknet or 10Base5 - Coax cable that was used in networks and operated at 10 megabits per second with a maximum length of 500 meters.

Thinnet or 10Base2 - Coax cable that was used in networks and operated at 10 megabits per second with a maximum length of 185 meters.

RG-59 - Most commonly used for cable television in the US

RG-6 - Higher quality cable than RG-59 with more bandwidth and less susceptibility to interference

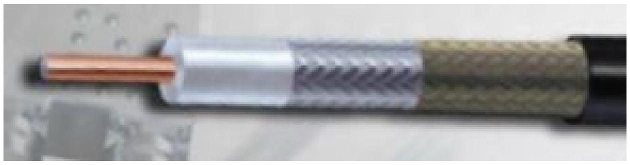

FIGURE 8 coaxial cable.

TWISTED-PAIR CABLING

Twisted-pair is a type of copper cabling that is used for telephone communications and most Ethernet networks. A pair of wires forms a circuit that can transmit data. The pair is twisted to provide protection against crosstalk, which is the noise generated by adjacent pairs of wires in the cable. Pairs of copper wires are encased in color-coded plastic insulation and twisted together. An outer jacket protects the bundles of twisted pairs called poly-vinyl chloride (PVC). PVC will produce hazardous fumes when burned. Most network cables are installed in the plenum space, or areas in the ceiling, in the walls, and under the floor. If cables with the PVC jackets do burn in the plenum space, hazardous fumes can spread quickly through a building. To avoid this danger, only install plenum-grade fire resistant cabling in the plenum space.

When electricity flows through a copper wire, a magnetic field is created around the wire. A circuit has two wires, and in a circuit, the two wires have oppositely charged magnetic fields. When the two wires of the circuit are next to each other, the magnetic fields cancel each other out. This is called the cancellation effect. Without the cancellation effect, your network communications become slow due to the interference caused by the magnetic fields.

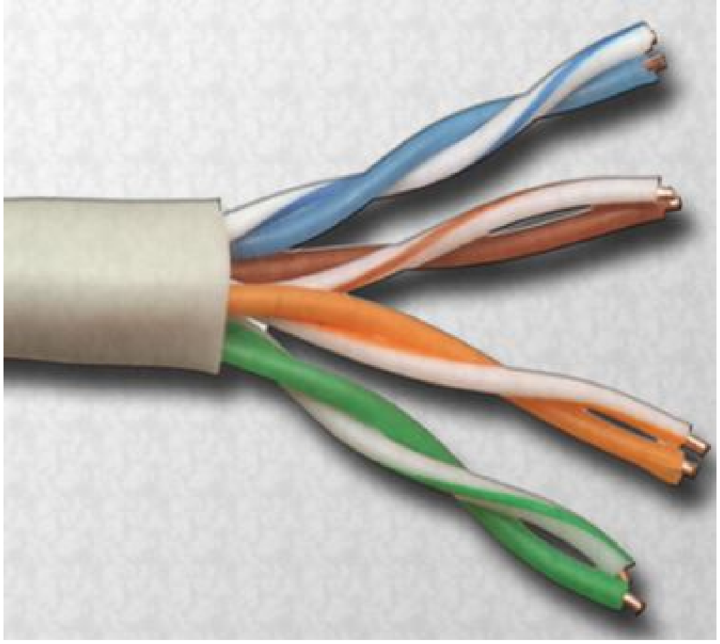

Figure 9 Twisted pair cable

TWO BASIC TYPES OF TWISTED-PAIR CABLES

1. **UNSHIELDED TWISTED-PAIR (UTP)**

- Has two or four pairs of wires
- Relies on the cancellation effect for reduction of interference caused by electromagnetic interface (EMI) and radio frequency interference (RFI)
- Most commonly used cabling in networks
- Has a range of 328 ft (100 meters)

2. **SHIELDED TWISTED-PAIR (STP)**

Each pair is wrapped in metallic foil to better shield the wires from electrical noise. Four pairs of wires are then wrapped in an overall metallic braid or foil. STP reduces electrical noise from within the cable. It also reduces EMI and RFI from outside the cable.

Facts about STP

- Prevents interference better than UTP.
- Primarily used outside North America.

Disadvantages of STP

- More expensive because of extra shielding.
- More difficult to install because of the thickness.
- Metallic shielding must be grounded at both ends. If not, shield acts like an antenna picking up unwanted signals.

CATEGORY RATING

UTP comes in several categories that are based on two factors:

1. The number of wires in the cable
2. The number of twists in those wires

The following are the categories of unshielded twisted-pair cable;

- Category 3 is the wiring used for telephone connections. It has four pairs of wires and a maximum data transmission rate of up to 16 Mbps.
- Category 5 and Category 5e have four pairs of wires with a maximum data transmission rate of up to 100 Mbps. Category 5 and 5e are the most common network cables used.
- Category 5e has more twists per foot than Category 5 wiring. These extra twists further prevent interference from outside sources and the other wires within the cable.
- Category 6 cable uses a plastic divider to separate and maintain the position of the pairs of wires relative to each other. This prevents interference. The pairs also have more twists than Category 5e cable.

FIBER-OPTIC CABLE

A fiber optic cable is a glass or plastic strand that transmits information using light and is made up of one or more optical fibers enclosed together in a sheath or jacket. It has the following properties;

- Not affected by electromagnetic or radio frequency interference.
- All signals are converted to light pulses to enter the cable, and converted back into electrical signals when they leave it.
- Signals are clearer, can go farther, and have greater bandwidth than with copper cable.
- Signal can travel several miles or kilometres before the signal needs to be regenerated.
- Usually more expensive to use than copper cabling and the connectors are more costly and harder to assemble.
- Common connectors for fiber-optic networks are SC, ST, and LC. These three types of fiber-optic connectors are half-duplex, which allows data to flow in only one direction. Therefore, two cables are needed.

Two types of glass fibre-optic cable:

Multimode - Cable that has a thicker core than single-mode cable. It is easier to make, can use simpler light sources (LEDs), and works well over distances of a few kilometres or less.
Single-mode - Cable that has a very thin core. It is harder to make, uses lasers as a light source, and can transmit signals dozens of kilometers with ease.

WEEK 7:

Computer networks, types of network, elements that constitute the most popular type, networking standards and the OSI model

OBJECTIVES:

- To list the advantage of networked computing relative t standalone computing.
- Distinguish between types of networks.
- Describe several specific uses for a network.
- List element of Clients/Server network.
- Identify different types of network topologies.

LECTURE NOTE

COMPUTER NETWORK

WHY USE A NETWORK?

Simply defined, a network is a group of computers and other devices (such as printers) that are connected by some type of transmission media. All networks offer advantages relative to using a standalone computer. Most importantly, networks enable multiple users to share devices (for example, printers) and data (for example, spread sheet files), which are collectively known as the network's resources.

TYPES OF NETWORK

Computers can be positioned on a network in different ways relative to each other. They can have different levels of control over shared resources. They can also be made to communicate and share resources according to different schemes. The following sections describe two fundamental network models: peer-to-peer and client/server.

PEER – TO – PEER NETWORKS

It is the simplest form of a network, in this type of network, every computer communicate with each other directly with no computer having more authority than another.

ADVANTAGES OF PEER – TO – PEER NETWORK

1. They are simple to configure.
2. They are less expensive to set up and to maintain.

DISADVANTAGES

1. They are not very flexible to change in network growth.
2. They are not practical for connecting more than a handful of computer.

A common way to share resources on a peer-to-peer network is by modifying the file – sharing controls via the computer's operating system.

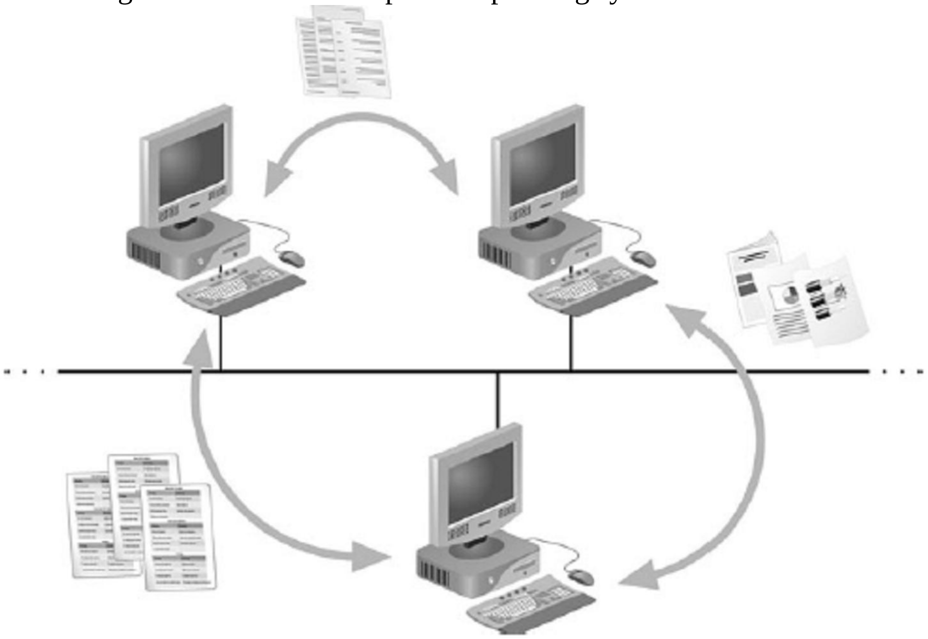

Figure 10. Resource sharing on a simple peer-to-peer network

CLIENT/SERVER NETWORKS

Another way of designing a network is to use a central computer, known as a server, to facilitate communication and resource sharing between other computers on the network, which are known as clients also known as work stations.
The computer functioning as the server must be running a network operating system (NOS), which is specially designed to; Manage data and other resources for a number of clients, Ensure that only authorized users' access the network, Control which types of files a user can open and read.

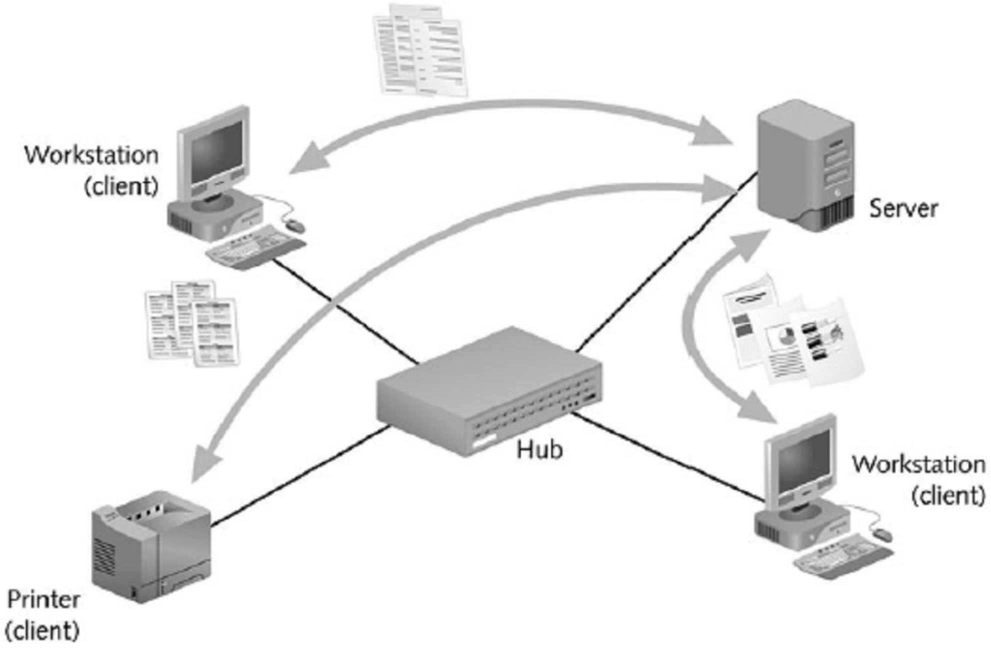

Figure 11. Resource sharing on a client/server network

Because client/server networks are the most popular type of network, they are therefore classified according to size.

LANs, MANs, and WANs

Local Area Network (LAN) is a network of computers and other devices that is confined to a relatively small space.
Metropolitan Area Network (MAN) is used to connect network that is larger than a LAN.
Wide Area Network (WAN) is used to connect two or more geographically distinct LAN or MAN.

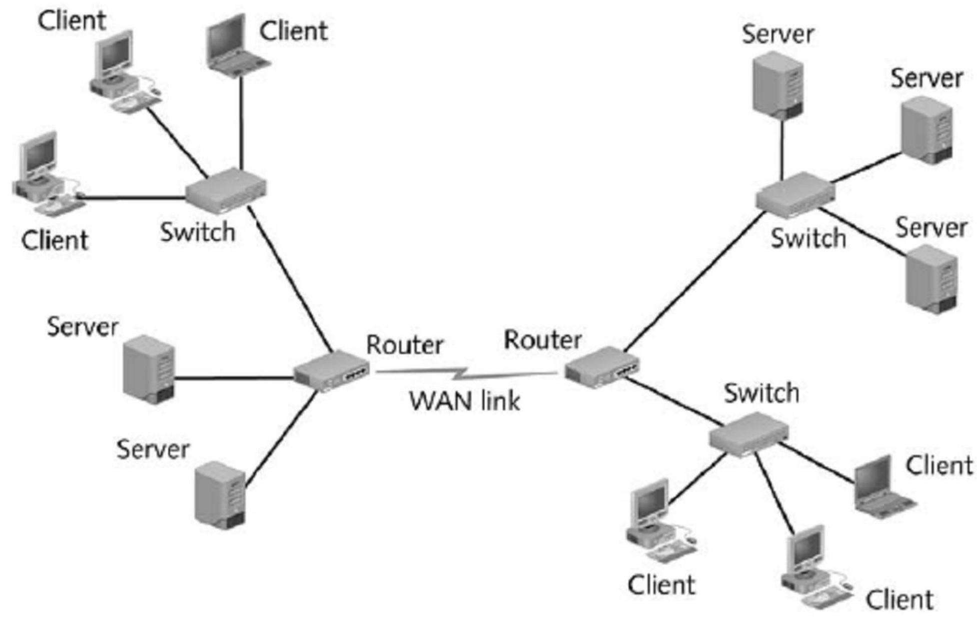

Figure 3. A simple WAN

ELEMENT COMMON TO CLIENT/SERVER NETWORK

Some of the element common to the client/server network includes:

1. Clients: This is a computer on the network that requests resources or services from another computer on the network.
2. Server: A computer on the network that manages shared resources.
3. Network Interface Card (NIC): This is the device inside a computer that connects a computer to the network media, thus allowing it to communicate with other computers.

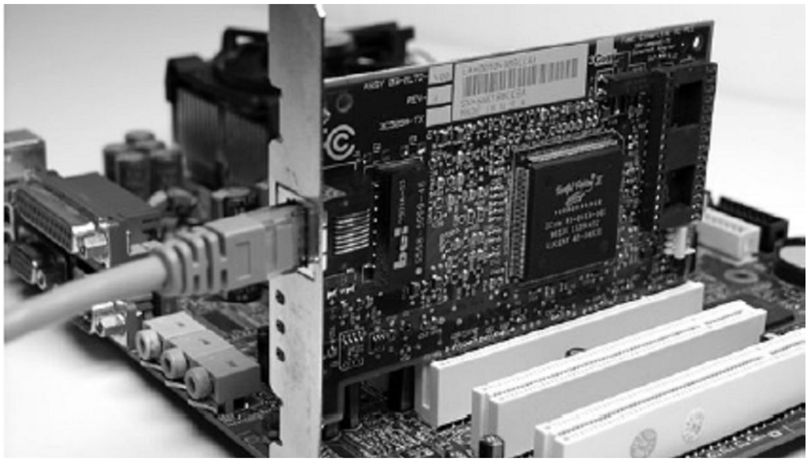

Figure 12. A network interface card (NIC)

4. Network Operating System (NOS): This is the software that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions.

5. Host: A computer that enables resource sharing by other computers on the same network.
6. Node: A client, server, or other device that can communicate over a network and that is identified by a unique number (network address).
7. Connectivity Device: A specialized device that allows multiple networks or multiple parts of one network to connect and exchange data.
8. Segment: It is composed of a group of nodes that use the same communications channel for all their traffic.

TOPOLOGY

This is the physical layout of a computer network, it defines the way in which computers printers, and other devices are connected to a network, and the main types include:

1. **BUS:** In this type of topology, each computer connects to a common cable, only one computer can transmit data at a time or frames will collide and be destroyed.
2. **RING**: This topology connects hosts in a physical ring or circle. In ring topology, there are no collisions.
3. **STAR:** It has a central connection point; a hub, switch, or router, Hosts connect directly to the central point with a cable which makes it easy to troubleshoot.
4. **HIERARCHICAL/EXTENDED STAR TOPOLOGY:** This is a star network with an additional networking device connected to the main networking device to increase the size of the network. It is often used for larger networks.
5. **MESH TOPOLOGY:** It connects all devices to each other; failure of any cable will not affect the network, often used in WANs that interconnect LANs.

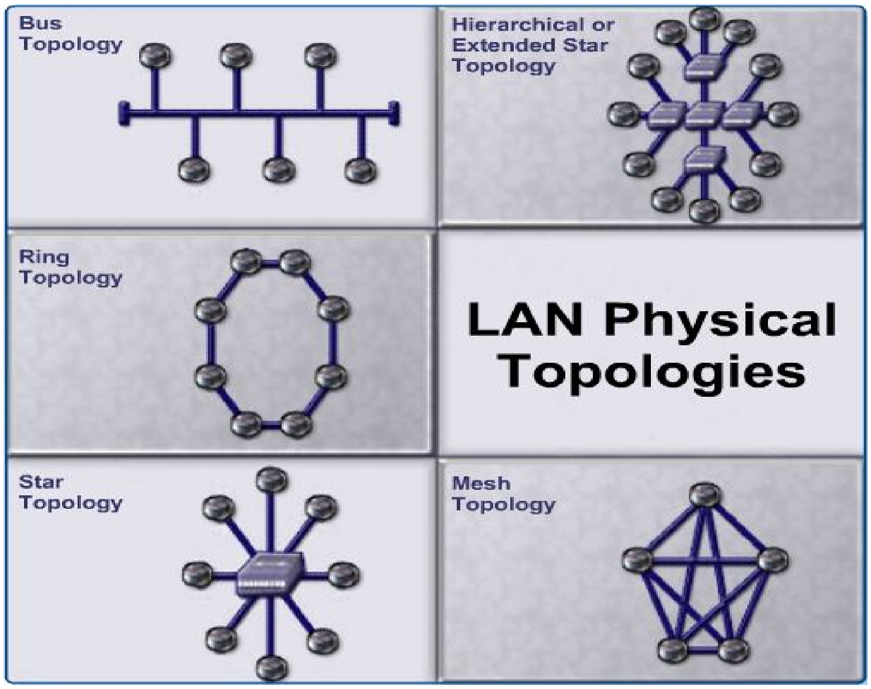

Figure 13.LAN physical topologies.

STUDY QUESTION

1. What is a network and what are its uses?
2. Explain the different types of network we have.
3. List and explain any 4 LAN topologies we have.

WEEK 8:

A further insight into computer networking; studying the standards of networking and discussing the Open System Interconnection (OSI) model.

Objective:

State the essence of having standards in networking.
Describe the OSI model and each of its layers.
Discuss the structure and purpose of data packets and frames.

LECTURE NOTE:

NETWORK STANDARDS

Standards are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed. Various organizations have been set up to maintain standards in networking, some of which are:

- ANSI (American National Standard Institute)
- EIA and TIA (Electronic Industries Alliance and Telecommunications Industry Association)
- IEEE (Institute of Electrical and Electronics Engineers)
- ISO (International Organization for Standardization) and so on.

The ISO organization developed the OSI model which divides network communication into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application which could be remembered using the mnemonic:

Please Do Not Throw Sausage Pizza Away

OSI MODEL

It is the theoretical representation of what happens between two nodes communicating on a network.

APPLICATION LAYER

It facilitate communication between software applications and lower-layer network services so that the network can interpret an application's request and, in turn, the application can interpret data sent from the network.

PRESENTATION LAYER

Protocols at the Presentation layer accept Application layer data and format it so that one type of application and host can understand data from another type of application and host. In other words, the Presentation layer serves as a translator.

SESSION LAYER

Protocols in the Session layer coordinate and maintain communications between two nodes on the network. The term session refers to a connection for on-going data exchange between two parties. It function includes establishing and keeping alive the communications link for the duration of the session, keeping the communication secure, synchronizing the dialog between the two nodes, determining whether communications have been cut off, and, if so, figuring out where to restart transmission, and terminating communications.

TRANSPORT LAYER

Protocols in the Transport layer accept data from the Session layer and manage end-to-end delivery of data. That means they can ensure that the data is transferred from point A to point B reliably, in the correct sequence, and without errors. Without Transport layer services, data could not be verified or interpreted by its recipient. Transport layer protocols also handle flow control, which is the process of gauging the appropriate rate of transmission based on how fast the recipient can accept data.

NETWORK LAYER

The primary function of protocols at the Network layer is to translate network addresses into their physical counterparts and decide how to route data from the sender to the receiver. Addressing is a system for assigning unique identification numbers to devices on a network.

DATA LINK LAYER

The protocols in the Data Link layer divides data they receive from the Network layer into distinct frames that can then be transmitted by the Physical layer. A frame is a structured package for moving data that includes not only the raw data, or "payload," but also the senders and receiver's network addresses, and error checking and control information. The addresses tell the network where to deliver the frame, whereas the error checking and control information ensure that the frame arrives without any problems.

The upper sub layer of the Data Link layer, called the LLC (Logical Link Control) sub layer, provides an interface to the Network layer protocols, manages flow control, and issues requests for transmission for data that has suffered errors. The MAC (Media Access Control) sub layer, the lower sub layer of the Data Link layer, manages access to the physical medium. It appends the physical address of the destination computer onto the data frame. The physical address is a fixed number associated with a device's NIC; it is initially assigned at the factory and stored in the NIC's on-board memory.

PHYSICAL LAYER

Protocols at the Physical layer accept frames from the Data Link layer and generate voltage so as to transmit signals. (Signals are made of electrical impulses that, when issued in a certain pattern, represent information). Physical layer protocols also set the data transmission rate and monitor data error rates. However, even if they recognize an error, they cannot perform error correction.

TCP/IP MODEL

The TCP/IP model (also called the DARPA or the DOD model) consists of only four layers, as opposed to the OSI Reference Model's seven. The TCP/IP suite of protocol communicates across any set of interconnected networks, its well suited for communication across both LANs and WANs.

NETWORK ACCESS LAYER

Consist of the physical and data link OSI model layers.

INTERNET LAYER

Provides routing of data from source to a destination and defines addressing schemes.

TRANSPORT LAYER

The core of the TCP/IP suite, providing communication services directly to the application layer.

APPLICATION LAYER

Provides specification of applications such as e-mail, file transfer, and network management.

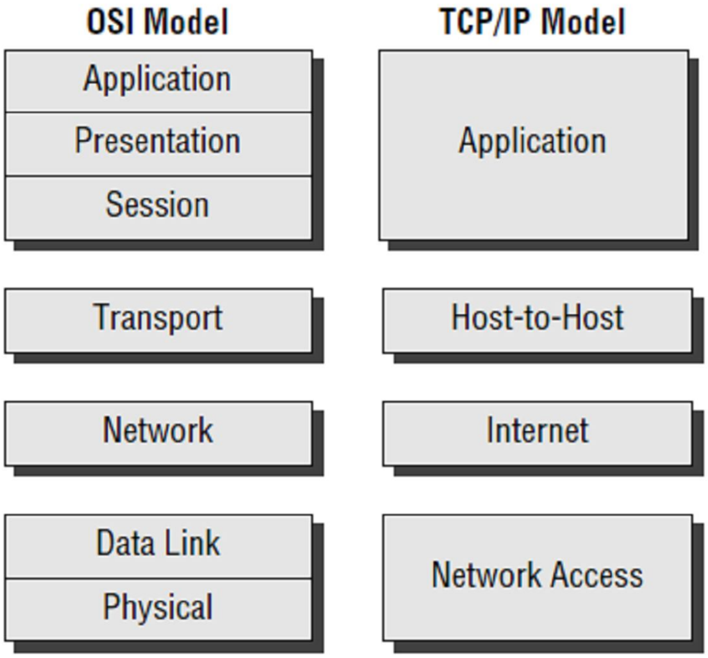

Figure 6.Comparing the OSI model with the TCP/IP model

STUDY QUESTION

1. Describe each layer of the OSI model and layers of the TCP/IP model.
2. State the reasons for having standards in network and the benefits.
3. Mention 3 organizations that are meant for maintaining standards in networking.

WEEK 9:

A basic understanding of computer networks is requisite in order to understand the principle of network security.

OBJECTIVE:

Identify security risks in LANs and WANs and design security policies that minimize risks.
Discuss hardware- and design-based security techniques.
Understand methods of encryption, such as SSL and IPsec, which can secure data in storage and in transit.

LECTURE NOTE:

NETWORK SECURITY

A networked system is exposed to threat (internal and external), hence the need for security in a network to guide against these threats. A security breach, however, can harm a network just as easily and quickly. To understand how to manage network security, you should first recognize the types of threats that your network may suffer. Not all security breaches result from a manipulation of network technology.

Risks Associated with People

By some estimates, human errors, ignorance, and omissions cause more than half of all security breaches sustained by networks. One of the most common methods by which an intruder gains access to a network is to simply ask a user for his password. For example, the intruder might pose as a technical support analyst who needs to know the password to troubleshoot a problem. This strategy is commonly called *social engineering,* because it involves manipulating social relationships to gain access.

Risks Associated with Transmission and Hardware

This is a security risk inherent in the Physical, Data Link, and Network layers of the OSI Model. The transmission media, NICs, hubs, network access methods, bridges, switches, and routers reside at these layers. At these levels, security breaches require more technical sophistication than those that take advantage of human errors. For instance, to eavesdrop on transmissions passing through a switch, an intruder must use a device such as a sniffer, connected to one of the switch’s ports. In the middle layers of the OSI Model, it is somewhat difficult to distinguish between hardware and software techniques. For example, because a router acts to connect one type of network to another, an intruder might take advantage of the router’s security flaws by sending a flood of TCP/IP transmissions to the router, thereby disabling it from carrying legitimate traffic.

Risks Associated with Protocols and Software

Like hardware, networked software is only as secure as you configure it to be. These are risks inherent in the higher layers of the OSI Model, such as the Transport, Session, Presentation, and Application layers. Network operating systems and application software present different risks. In many cases, their security is compromised by a poor understanding of file access rights or simple negligence in configuring the software.

Risks Associated with Internet Access

Although the Internet has brought computer crime, such as hacking, to the public’s attention, network security is more often compromised “from the inside” than from external sources. Nevertheless, the threat of outside intruders is very real, and it will only grow as more people gain access to the Internet.

SECURITY POLICY

A security policy identifies your security goals, risks, levels of authority.

Security Policy Goals.

Typical goals for security policies are as follows:

Ensure that authorized users have appropriate access to the resources they need.
Prevent unauthorized users from gaining access to the network, systems, programs, or data.
Protect sensitive data from unauthorized access, both from within and from outside the organization.
Prevent accidental damage to hardware or software.
Prevent intentional damage to hardware or software.

Types and Sources of Network Threats

There are several threats that are against networked computers; some of these threats are listed below:

Denial - of - Service

DoS (Denial-of-service) attacks are difficult to address because of their nature, they are very easy to launch, and difficult sometimes to track. in this type of attack, more request are sent to the machine than it can handle in other to make it collapse and hence giving way to attacks.

Unauthorized Access

It is a very high-level term that can refer to a number of different sorts of attacks, the goal is to access some resources that the machine should not provide the attacker. It comes in different form such as; Executing Command Illicitly, Confidentiality Breaches, Destructive Behavior (Data Diddling, and Data Destruction).

WAYS OF PREVENT SECURITY DISASTER

- Having backup for data.
- Avoid putting data where it doesn’t need to be.
- Avoid system with so much redundancy.

SECURITY IN NETWORK DESIGN

The best protection is to restrict access at every point where your LAN connects to the rest of the world. This principle forms the basis of hardware- and design based security.

FIREWALLS

A firewall is a specialized device, or a computer installed with specialized software, that selectively filters or blocks traffic between networks. A firewall typically involves a combination of hardware and software and may reside between two interconnected private networks or, more typically, between a private network and a public network (such as the Internet).

Figure 14. A firewall

Proxy Servers

One approach to enhancing the security of the Network and Transport layers provided by firewalls is to combine a packet-filtering firewall with a proxy service. A proxy service is a software application on a network host that acts as an intermediary between the external and internal networks, screening all incoming and outgoing traffic.

Remote Control

Remote control systems solve the remote access security risk, it enables a user to connect to a host system on a network from a distance and use that system's resources as if the user were sitting in front of it.

Dial-Up Networking

Another method for remote access, dial-up networking, requires users to dial into a remote access server attached to the network. Dial-up networking differs from remote control in that it effectively turns a remote workstation into a node on the network, through a remote access server.

Logon Restrictions

In addition to restricting users' access to files and directories on the server, a network administrator can constrain the ways in which users can access the server and its resources such as; Time of day, total time logged on, Source address, Unsuccessful logon attempt.

Passwords

Choosing a secure password is one of the easiest and least expensive ways to guard against unauthorized access.

Encryption

Encryption is the use of an algorithm to scramble data into a format that can be read only by reversing the algorithm—that is, by decrypting the data. The purpose of encryption is to keep information private. Many forms of encryption exist, with some being more secure than others.

SSL (Secure Sockets Layer)

SSL (Secure Sockets Layer) is a method of encrypting TCP/IP transmissions—including Web pages and data entered into Web forms—en route between the client and server using public key encryption technology.

STUDY QUESTION

1. Why do we need security in a network?
2. List 4 security policies.
3. Explain firewall, encryption, and password as used in networking security.
4. Explain the possible threat networked system could be exposed to.

WEEK 10:

After learning about how to secure a network, there is need to also study how to manage a network for effective usage.

OBJECTIVE:

Understand network management and the importance of base lining to assess a network's health.

Describe the steps involved in upgrading network software and hardware.

LECTURE NOTE:

IMPLEMENTING AND MANAGING NETWORKS

Network management refers to the assessment, monitoring, and maintenance of all aspects of a network. On some large networks, administrators run network management applications that continually check devices and connections to make certain they respond within an expected performance threshold. If a device doesn't respond quickly enough or at all, the application automatically issues an alert that pages the network administrator responsible for that device.

Baseline Measurement

It is the report of the network's current state of operation, which includes the utilization rate for your network backbone, number of users logged on per day or per hour, number of protocols that run on your network, statistics about errors (such as runts, collisions, jabbers, or giants), frequency with which networked applications are used, or information regarding which users take up the most bandwidth. Baseline measurements allow you to compare future performance increases or decreases caused by network changes with past network performance.

A baseline assessment should address the following:

Physical topology—which types of LAN and WAN topologies does your network use: bus, star, ring, hybrid, mesh, or a combination of these? Which type of backbone does your network use—collapsed, distributed, parallel, serial, or a combination of these? Which type and grade of cabling does your network use?

Access method—Does your network use Ethernet, Token Ring, wireless, or a mix of transmission methods? What transmission speed does it provide? Is it switched?

Protocols—which protocols are used by servers, nodes, and connectivity devices?

Devices—How many of the following devices are connected to your network—switches, routers, hubs, gateways, firewalls, access points, servers, UPSs, printers, backup devices, and clients? Where they are physically located, and what are their model numbers and vendors?

Operating systems—which network and desktop operating systems appear on the network? Which versions of these operating systems are used by each device? Which type and version of operating systems are used by connectivity devices such as routers?

Applications—which applications are used by clients and servers? Where do you store the applications? From where do they run?

STUDY QUESTION

1. What is network management?
2. What are the things involved in network management?
3. What is baselining?

WEEK 11:

Revisions and Examinations

OBJECTIVE:

The objective of the week lecture is for the student to be able to revise all they have been taught so far.

Description:

All the objectives for the course should be seriously overviewed