

# [Computer networks (cs610)](https://assignbuster.com/computer-networks-cs610/)

COMPUTER NETWORKS (CS610) VU COMPUTER NETWORKS (CS610) HANDOUTS LECTURERS # 01 — 45 PREPARED BY: HAMMAD KHALID KHAN 1 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Table of contents Lecture No. 1 ......................................................................................................... 4 INTRODUCTION ........................................................................................................... 4 Lecture No. 2 ......................................................................................................... 9 Motivation and Tools...................................................................................................... 9 Lecture No. 3 ....................................................................................................... 13 Overview of Data Communication ............................................................................... 13 Lecture No. 4 ....................................................................................................... 14 PACKETS, FRAMES AND ERROR DETECTION....................................................... 14 PACKETS AND TDM: ........................................................................................... 15 Figure 4. 2 illustration of TDM....................................................................................... 16 Lecture No. 5 ....................................................................................................... 17 BYTE STUFFING ........................................................................................................ 17 Lecture No. 6 ....................................................................................................... 22 SHIFT OPERATION .................................................................................................... 22 Lecture No. 7 ....................................................................................................... 24 GROWTH OF LAN TECHNOLOGY ............................................................................ 24 Lecture No. 8 ....................................................................................................... 28 CARRIER SENSE MULTIPLE ACCESS (CSMA) ....................................................... 28 Lecture No. 9 ....................................................................................................... 33 HARDWARE ADDRESSING ....................................................................................... 33 Lecture No. 10 ..................................................................................................... 35 FRAME TYPE IDENTIFICATION ................................................................................ 35 Lecture No. 11 ..................................................................................................... 39 INTERFACE HARDWARE .......................................................................................... 39 Lecture No. 12 ..................................................................................................... 43 LAN WIRING AND PHYSICAL TOPOLOGY ............................................................... 43 Lecture No. 13 ..................................................................................................... 48 FIBER MODEMS AND REPEATOERS ....................................................................... 48 Lecture No. 14 ..................................................................................................... 51 BRIDGES..................................................................................................................... 51 Lecture No. 15 ..................................................................................................... 54 SWITCHES AND WAN TECHNOLOGIES .................................................................. 54 Lecture No. 16 ..................................................................................................... 58 ROUTING .................................................................................................................... 58 Lecture No. 17 ..................................................................................................... 62 ROUTING ALGORITHMS ........................................................................................... 62 Lecture No. 18 ..................................................................................................... 66 CONNECTION-ORIENTED NETWORKING AND ATM .............................................. 66 Lecture No. 19 ..................................................................................................... 68 ATM: VIRTUAL CIRCUITS .......................................................................................... 68 Lecture No. 20 ..................................................................................................... 72 ATM AND NETWORK OWNERSHIP .......................................................................... 72 Lecture No. 21 ..................................................................................................... 75 NETWORK SERVICE PARADIGM ............................................................................. 75 Lecture No. 22 ..................................................................................................... 79 NETWORK PERFORMANCE ..................................................................................... 79 2 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 23 ..................................................................................................... 81 INTERNETWORKING: CONCEPTS, ARCHITECTURE AND PROTOCOLS............ 81 Lecture No. 24 ..................................................................................................... 85 IP: INTERNET PROTOCOL ADDRESSES ................................................................. 85 Lecture No. 25 ..................................................................................................... 87 INTERNET PROTOCOL ADDRESS NOTATIONS ..................................................... 87 Lecture No. 26 ..................................................................................................... 90 IP SUBNETING ........................................................................................................... 90 Lecture No. 27 ..................................................................................................... 93 ADDRESS REOLUTION PROTOCOL (ARP).............................................................. 93 Lecture No. 28 ..................................................................................................... 97 ARP MESSAGE FORMAT .......................................................................................... 97 Lecture No. 29 ................................................................................................... 101 IP DATAGRAMS AND DATAGRAM FORWARDING................................................ 101 Lecture No. 30 ................................................................................................... 105 IP ENCAPSULATION, FRAGMENTATION AND REASSEMBLY ............................. 105 Lecture No. 31 ................................................................................................... 110 THE FUTURE IP (IPV6) ............................................................................................ 110 Lecture No. 32 ................................................................................................... 113 IPv6 AND AN ERROR REPORTING MECHANISM.................................................. 113 Lecture No. 33 ................................................................................................... 117 AN ERROR REPORTING MECHANISM (ICMP) ...................................................... 117 Lecture No. 34 ................................................................................................... 119 UDP: DATAGRAM TRANSPORT SERVICE ............................................................. 119 Lecture No. 35 ................................................................................................... 122 DATAGRAM FORMAT AND TCP: RELIABLE TRANSPORT SERVICE .................. 122 Lecture No. 36 ................................................................................................... 125 TCP: RELIABLE TRANSPORT SERVICE (Cont.)..................................................... 125 Lecture No. 37 ................................................................................................... 128 NETWORK ADDRESS TRANSLATION (NAT) ......................................................... 128 Lecture No. 38 ................................................................................................... 131 NETWORK ADDRESS TRANSLATION .................................................................... 131 Lecture No. 39 ................................................................................................... 133 IP ROUTING (Part-1)................................................................................................. 133 Lecture No. 40 ................................................................................................... 135 IP ROUTING (Part-2)................................................................................................. 135 Lecture No. 41 ................................................................................................... 137 IP ROUTING (Part-3)................................................................................................. 137 Lecture No. 42 ................................................................................................... 139 IP ROUTING (Part-4)................................................................................................. 139 Lecture No. 43 ................................................................................................... 142 IP ROUTING (Part-5)................................................................................................. 142 Lecture No. 44 ................................................................................................... 144 IP ROUTING (Part-6)................................................................................................. 144 Lecture No. 45 ................................................................................................... 147 COURSE REVISION ................................................................................................. 147 3 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 1 INTRODUCTION NETWORK: A network is defined as a system for connecting computers using a single transmission technology. The computers can communicate with each other in a network. They can send and receive data from each other when they are in a network. INTERNET: The Internet is defined as the set of networks connected by routers that are configured to pass traffic among any computers attached to any network in the set. By internet many computers which are at longer distances from each other can communicate with each other. CLASSIFICATION OF NETWORKS Computer networks are classified by four factors which are as follow: 1) 2) 3) 4) BY SIZE: BY CONNECTIVITY: BY MEDIUM: BY MOBILITY: 1) BY SIZE: According to their size there are two classifications of networks. 1. Local Area Network. ( LAN) 2. Wide Area Network (WAN) In LAN network occupies the smaller area like a room a floor or a building. In WAN, network occupies larger areas like cities & countries. Internet is a Wide Area Network. LAN & WAN are compared by the speed of transmission, bandwidth and latency, management, security, reliability, billing and their standards. 4 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU 2) BY CONNECTIVITY: Networks are also classified by connectivity in which two topologies are discussed. a) Point-to-Point b) Broadcast a) POINT-TO-POINT: In Point-to-Point topology there are two topologies. 1) STAR topology 2) TREE topology In star topology each computer is connected to a central hub. The communication takes place through the hub. It is shown in the figure below. Error! Star Tree Figure 1. 1: star and tree topologies In Tree topology all computers are connected to each other in such a way that they make a tree as shown in the figure above. b) BROADCAST: In broadcast topology there are further two categories 1) SATELLITERADIO 2) RING TOPOLOGY In a satellite or radio topology all computers are connected to each other via satellite or radio wave as shown in the figure. 5 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Ring Satellite/Radio Figure: 1. 2 Satellite and Ring topologies: In a ring topology each computer is connected to other thorough a ring as shown in the figure above. 3) BY MEDIUM: The classification of networks is also based on the Medium of transmission. Following are the mediums of transmission: - - - - Copper wire Co-axial cable Optical fiber Radio waves All these mediums differ from each other with respect different parameters. These parameters are speed of transmission, range of the receiver and transmitter computer, sharing of information, topology, installation & maintenance costs and reliability. For example the range of radio waves will be much more than an optical fiber. Similarly other mediums differ from each other and appropriate medium is selected for the sake of transmission. 4) BY MOBILITY: The networks are also classified according to their mobility. In this respect there are two types of networks. - Fixed networks - Mobile networks In these days mobile networks are the hot case. Mobile networks have been emerged in the last decade. In this regard there are some issues which are attached with the mobility of networks which are as follows: - Location and tracking - - Semi persistent connections Complex administration and billing as devices and users move around the network. 6 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU NETWORKS IN DAILY LIFE: The major use of networks is in business side. Networks are used for advertising, production, shipping, planning, billing and accounting purposes. In fact now there is an entire industry that develops networking equipment. In addition to this networks are being used in homes as well for example, to switch and control different devices from one place. Networks are very much useful at government level as federal government, local government and military organization use networks for communication purposes. In education we have online libraries which we can visit at our home PC. This is all just due to the networks. COMPLEXITY OF NETWORK SYSTEMS: A computer network is a complex subject due to the following reasons: - MANY DIFFERENT TECHNOLOGIES EXIST: The first reason for the complexity of networks is that there are many different technologies exist for networking and each technology features is different from the other. This is because many companies have developed networking standards, which are not compatible with each other. In this way multiple technologies exist that are used to connect different networks. - NO SINGLE UNDERLYING THEORY OR MODEL: The second reason for the complexity of networks is that there is no single underlying theory or model, which specifies or defines different aspects of networking. Rather, various organizations and research groups have developed conceptual models that can be used to explain differences and similarities between network hardware and software. - MODELS ARE EITHER SO SIMPLISTIC OR SO COMPLEX: Another reason for the complexity of networks is that the conceptual models made by organization are either so simplistic that they do not distinguish between details, or they are so complex that they do not simplify the subject. - NO SIMPLE OR UNIFORM TERMINOLOGY: One reason for the complexity of networks is that there is no simple or uniform terminology that can be used for the same feature. Different technologies use different terminologies. In this way terms are confused with product names. 7 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU MASTERING THE COMPLEXITY To master the complexity one must follow the following points. - CONCENTRATE IN UNDERSTANDING THE CONCEPTS: Instead of details of wires used to connect computers to a specific network, it is important to understand a few basic categories of wiring schemes their advantages and disadvantages. For example: Instead of how a specific protocol handles congestion, we should concentrate on what congestion is and why it must be handled. - LEARNING THE NETWORKING TERMINOLOGY: The second tool for mastering the complexity is to learn the networking terminology. In addition to this one must concentrate the concepts and not details, concentrate on breath and not the depth of technologies, also one should understand the analogies and illustrations Network terminology is introduced with new concepts so it is much helpful to learn the terminology to overcome the complexity of networks. 8 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 2 Motivation and Tools One of the reasons of motivation towards networking was resource sharing which is discussed as follows. Resource sharing: Resource sharing means to share the resources available among many users. In an office as it is very expensive to give a separate printer to each worker. So if the printer is shared among the workers then a single printer will be accessible to each worker. This leads to the motivation of resource sharing. Goal of resource sharing: The goal of resource sharing is to make all programs, equipment and date available to anyone in the network without regard to physical location of the resource and the user. For example: the sharing of a printer among the workers in an office and also the sharing of information is a goal of resource sharing. Main reason for early resource sharing: The main reason for early resource sharing was not to share the peripheral devices rather to share the large-scale computational power because computer were extremely expensive in those days and the government budgets were not sufficient to provide computers for all scientist and engineers. By resource sharing a researcher could use whichever computer was best suited to perform a given task. Efforts of advanced research project AGENCY (ARPA): The efforts of ARPA was to enable all its research groups have access to latest computers. For this purpose ARPA started investing in ways to do data networking ARPA use a new approach consisting of packet switching and internetworking to fulfill the purpose of resource sharing. As a result of ARPA research the first network was established which was named ARPANET. In this way the internet was emerged in 1970’s and it has grown drastically since then as shown in the figure below. 9 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Figure. 2. 1 Growth of the Internet As shown in another figure below. In log scale the position on y-axis is proportional to the log of the number being represented. So the values along y-axis represent the power of 10. Fig. 2. 2 Growth of the internet on Log Scale 10 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU We see that on log scale the growth appears almost linear it means that internet experienced an exponential growth. We also observed that internet has been doubled every nine to twelve months. PROBING THE INTERNET: Let us see how are the figures in above graphs obtained? In the early days when there were some dozen computers on the network, it was done manually but now as we have seen that there are millions of computers on the internet so how can we calculate the number of computers connected to the internet. This is done through probing the Internet. Now an automated tool is required that tests to see whether the given computer is online or not. For this purpose the first tool is the `PING program` which is shown in the figure below. Figure 2. 3 THE PING Command We see that 5 packets of 64 bytes are sent to sears. com and 5 packets are received. We see that ping has also given some additional information such the IP addresses of sears. com, the sequence of packets and the times of transmission known as the round-trip time, as there is no packet loss so it means that sears. com is connected to the internet. PROBLEM WITH ‘ PING’: Ping, as a tool seems to be simplistic. Now let’s see what are the problems attached with ping. If ping does not review any responses from host computer it can not tell the reason of problem. Because one of the following reasons occurs, but ping will not specify the reason. - - - Remote computer might have a problem. Local computer might have a problem. Ping sometimes fails because of congestion. Some networks or computers reject the ping packets. They do this to avoid denial of service of flooding attack. Inspite of these problems ping is still heavily used as a diagnostic tool. Network administrators use ping as soon as they learn about the failure. Tracing a Route: There is another probing tool i-e Trace Route. To get more detail it is used. 11 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Figure 2. 4 As shown in the figure about the route to DANDELION-PATCH. MIT. EDU was traced out and the program showed all eight computers that were in the way. The additional information is also shown in the figure. Thus we see that tracing a route is more interesting tool than Ping as it tells about each computer that falls in the way of source and destination computers. 12 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 3 Overview of Data Communication NOTE: Chapter 4, 5, 6 deals with the course of DATA COMMUNICATION, which has been studied as a separate, course earlier. So these chapters are just overviewed and can be seen in the third lecture video. It should also be noted that these chapters will contain no assignment, or quizzes and these chapters will also be out of the examination. 13 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 4 PACKETS, FRAMES AND ERROR DETECTION INTRODUCTION: The previous chapters of data communication described how bits are transmitted across a physical network using a transmission medium. This chapter introduces the concept of packets of data rather than bits for communication. CONCEPT OF ‘ PACKET’: Network systems divide data in small blocks or junks called packets, which they send individually. Why we need packets rather than bits? The answer to this question is because a sender and receiver need to coordinate to detect transmission errors. Also the individual connection between each pair of computers is not possible. That’s why to solve these problems shard network connections are made among many workstations. PROBLEMS WITH SHARING: The demand of sharing is very high because many computers need to use the shared networks. In addition to this some applications have large data transfer. In this way they hold the network for long time. But on the other hand some applications cannot wait so long. So we need a mechanism for fairness. SOLUTION FOR FAIRNESS: To the fairness, the solution is to divide the data into small block or chunks called ‘ PACKETS’. Computers take turns to send one packet at a time over the shared connection. Because each packet is small so no computer experiences a long delay. 14 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Example: In the figure one reason for using the packets is illustrated. We see that in a shared resource when one pair of computer communicates, the other must wait. To understand the use of packet here, let’s suppose a transmission with packets in the figure. WITHOUT PACKETS: A 5MB file transferred across network with 56Kpbs capacity will require 12 minutes. This means that all that computers will be forced to wait for 12 minutes before initiating other transfers. 5x106 bytes \* 8 bits / byte = 11. 9 minutes 60 secs / minute \* 56x103 bits / second WITH PACKETS: Now if the file is broken into packets, other computers must only wait until packet (not entire file) has been sent. Suppose file is broken into 1000 byte packets. Now each packet takes less than 0. 2 seconds to transmit. Here other computers must only 1000 bytes \* 8 bits / byte =. 143 seconds 56x103 bits / second wait for 0. 14 sec before beginning to transmit. Note: - if both files are 5MB long, each now takes 24 minutes to transmit. But if the second file is 10MB long it sill be transmitted in only 2. 8 seconds while 5MB file still takes roughly 12 minutes. PACKETS AND TDM: Dividing data into small packets allow time division multiplexing. In TDM each packet leaves the source and is switched on the shared communication channel through a multiplexer. At the destination the packet is switched through a demultiplexer to the destination. In the figure this process is illustrated with a multiplexing circuit shown. 15 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Figure 4. 2 illustration of TDM PACKETS AND FRAMES: PACKETS: Packet is a generic term that refers to small block of data. Packet have different format. Each hardware uses different packet format. FRAME: A frame or hardware frame denotes a packet of a specific format on a specific hardware technology. FRAME FORMAT: We need to define a standard format for data to indicate the beginning and end of the frame. Header and tail are used to frame the data as shown in the figure below. Figure 4. 3 illustration of a Frame We see that in the figure soh and eot are used to denote the start of header and end of tail. FRAMING IN PRACTICE: In practice there is a disadvantage of overhead. To avoid the no delay between two frames each frame sends an extra character between block of data. The framing in practice also has some transmission problems just like: - Missing eot indicates sending computer crashed. - Missing soh indicates receiving computer missed beginning of message. - Bad frame is discarded. 16 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 5 BYTE STUFFING Sometimes the special character (i-e soh and eot) may appear in data and as a part of data they will be misinterpreted as framing data. The solution to this problem is Byte stuffing. In general to distinguish between data being sent and control information such as frame delimiters network systems arrange for the sending side to change the data slightly before it is sent because systems usually insert data or bytes to change data for transmission, the technique is known as Data Stuffing. There are two types of data stuffing: - Byte Stuffing - Bit Stuffing Byte stuffing refers stuffing with character oriented hardware and bit stuffing refers to bit oriented hardware. Byte stuffing translates each reserved byte into two unreserved bytes. For example: it can use esc as prefix followed by x for soh, y for eot and z for eco. The receiver then replaces each occurrence of esc x, esc y and esc z by the corresponding single character. This is shown in figure below: Figure 5. 1 Byte stuffing is illustrated in another figure below we can see the replacement of characters. 17 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU TRANSMISSION ERRORS: Transmission errors may occur due to different causes for example interference or power surges may destroy data during transmission. In result of which the bits are lost or the bit value may be changed. ERROR DETECTION AND CORRECTION: To detect and correct errors, frames include additional information, which is inserted by the sender and checked by the receiver. In this way incorrect data can be rejected. Also the incorrect data can be corrected and accepted. PARITY CHECKING: To detect the error there are different schemes in which parity checking is also commonly used. In parity checking, parity refers to the number of bits set to 1 in the data item. There are two types: - - Even Parity Odd Parity EVEN PARITY: In an even parity the no. of 1’s in data should be an even number. ODD PARITY: In an Odd parity the no. of bits should be an odd number. PARITY BIT: A parity bit is an extra bit transmitted with data item chose to give the resulting bit even or odd parity. 18 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU For example an even parity data 10010001 has parity bit 1 as it has odd number of 1’s. An odd parity data 10010111 has parity bit 0 as it has odd number of 1’s. Let us consider another example, if noise or other interference introduces an error one of the bits in the data will be changed from a 1 to a 0 or from a 0 to a 1. Thus the parity of resulting bits will be large. Suppose original data and parity is 10010001+1 (even parity). After interference the incorrect data is 10110001+1 and it has become an odd parity. LIMITATIONS OF PARITY CHECKING: Parity can only detect errors that change in odd number of bits for example the original data and parity is 10010001+1 (even parity) and the incorrect data is 10110011+1 (even parity). We see that even no. of bits have been changed due to noise so parity checking can not detect this error. Parity usually is used to detect on bit error. ALTERNATIVE ERROR DETECTION SCHEMES: In addition to parity checking alternative error detection mechanisms have been introduced. These mechanisms differ from each other by the following respects. - - - The size of the additional information (transmission overhead) Computational complexity of the algorithm (computational overhead) The number of bits errors that can be detected (how well errors are detected ) CHECKSUM The second procedure used to detect errors is checksum. In this procedure data is treated as a sequence of integers and their arithmetic sum is computed and the carry bits are added to the final sum. Then checksum is calculated by transmission then it is sent along the data and the receiver and the same calculation is performed and then compared with the original checksum transmitted. In this way errors are detected if the received checksum is different from the sent. The figure illustrates the example. Figure 5. 3 The integers can be 8, 16 or 32 bits. Checksum is easy to do. It uses only addition but it has also limitations and can not detect all errors. As shown below. 19 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Figure 5. 4 CYCLIC REDUNDANCY CHECK (CRC): To enable a network system to detect move error without increasing the amount of information in each packet another most successful approach is made which is called CRC. To understand the concepts of CRC consider data in a message as co-efficient of a polynomial. Their co-efficient set is divided by a known polynomial. The remainder of this division is then transmitted as CRC and checked at the receiver to detect errors. CRC has good error detection properties. It is easy to implement in hardware. HARDWARE COMPONENTS USED IN CRC: - - CRC uses just two hardware components: Shift register Exclusive OR ( XOR unit ) The XOR unit is shown in the figure below. Figure 5. 5 Shift register is also shown in figure. It performs two operations. - Initialize: sets all bits to zero - Shift: moves all bits to the left position. 20 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Figure 5. 6 21 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 6 SHIFT OPERATION This operation shifts all bits to the left one position. For example in the figure below a 16-bit CRC hardware is shown, which uses three shift registers and three Exclusive OR (XOR) units. Figure 6. 1 We see that this hardware can compute 16-bit CRC. Also in the figure, we see that the registers are initialized to zero and the bits of message are shifted through the input. When all 16 bits are shifted then the CRC is found in the registers. In another figure, we see that input data is all 1s and CRC shown after 15, 16, 17 bits are shifted and feedback introduces 0s in CRC. TYPES OF ERRORS: CRC can check the following errors better than check sums. a) Vertical errors b) Burst errors a) VERTICAL ERRORS: This type of error occurs due to a hardware failure. e. g. the second bit of every character will damage. b) BURST ERRORS: When a small set of bits changes near a specific location due to lighting or electric motor starting nearby etc. then these types of errors are called Burst errors. FRAME FORMAT AND ERROR DETECTION: The modified frame format also includes CRC. If there is an error occurred in frame, then it typically causes receiver to discard frame. The frame including CRC is shown in the figure. Figure 6. 2 22 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU LAN TECHNOLOGY AND NETWORK TOPOLOGY Most networks are local and are designed to share resources among multiple computers. Hardware technologies used for local networks allow multiple devices to connect with a shared network. In this shared medium the computers must take turns using the shared medium. DIRECT POINT-TO-POINT COMMUNICATION: Early networks used direct point-to-point communication. In such a mode of communication each communication channel connects exactly two computers. In this way it forms a mesh or point-to-point network, which is shown in the figure below. Figure 6. 3 ADVANTAGES: Direct point-to-point communication has the following advantages: - - The connection type of individual connections can be different. Individual connections can choose a different frame format and error detection mechanism etc. - It is easy to enforce security and privacy. DISADVANTAGES: Direct point-to-point communication has the following disadvantages: - - - - - The no. of connections grow more rapidly than the no. of computers For ‘ n’ computers connections = (n^2 — n)/2. Most computers use the same physical path. Direct point-to-point communication is expensive due to a no. of connections. Another disadvantage is that adding a new computer to the network requires N-1 new connections as shown in the above figure. 23 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 7 GROWTH OF LAN TECHNOLOGY The development of shared communication channels (LANs) started in 1960s and early 1970. The key idea behind was to reduce the number of connections by sharing connection among many computers Each LAN consists of a single shared medium. The computers take turns using the medium. First one computer uses the medium to send its data over the channel then second and son on. But sharing a single medium over long distances is efficient, due to the long delays. LAN technologies reduce cost by reducing no. of connections. But attached computers compete for use of shared connections. The local communication consists of LAN exclusively. But the long distance communication is point-to-point exclusively. SIGNIFICATION OF LANs AND LOCALITY OF REFERENCE: LANs are most popular form of computer networks. One of its bright features is that this technology is inexpensive. The demand of LANs is related to a principle known as “ Locality of Reference Principle". “ LOCALITY OF REFERENCE" PRINCIPLE: Principle of “ Locality of Reference" helps predict computer communication patterns. There are two patterns given as follows: A) SPATIAL LOCALITY OF REFERENCE B) TEMPORAL LOCALITY OF REFERENCE a) SPATIAL LOCALITY OF REFERENCE: In this pattern computers are likely to communicate with other computers that are located nearby. b) TEMPORAL LOCALITY OF REFERENCE: In this pattern computers are likely to communicate with the same computers repeatedly. Thus LANs are effective because of spatial locality of reference. Temporal locality of reference may give insight into which computers should be on a LAN. 24 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU LAN TOPOLOGIES: Network can be classified by shape. According to which there are three most popular topologies, which are given as follows; - - - Star Ring Bus STAR TOPOLOGY: In this topology, all computers are attached to a central point, which is sometimes called the “ Hub" as shown in the figure below. FIGURE 7. 1 AN IDEALIZED STAR NETWORK It is important to note that these networks are not physically like stars but they are logically like stars. It means that their shape does not look like a star but their connections are just like a star. The above diagram is idealized. Here is shown a star network in practice in the figure below: FIGURE 7. 2 STAR NETWORK IN PRACTICE RING TOPOLOGY: In this topology of network the computers are connected to each other in closed loop. In this network first computer passes data to the second and then second passes data to third and so on, as shown in the figure. 25 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU FIGURE 7. 3 Like star topology the ring network are also logically ring and not physically. BUS TOPOLOGY: In a bus topology all computers are attached to a single long cable and any computer can send data to any other computer. For this purpose, coordination is required to decide which computer has to use the line at what time. The bus topology is shown below: FIGURE 7. 4 BUS TOPOLOGY REASON FOR MULTIPLE TOPOLOGIES: Each topology has advantages and disadvantages, which are discussed below: IN A RING: It is easy to coordinate access to other computers however entire network is disabled if a cable cut occurs. IN A STAR: On the other hand only once computer is affected when a cable cut occurs. IN A BUS: The network needs fewer wires than a star, however entire network is disabled when a cable cut occurs. 26 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU EXAMPLE BUS NETWORK; ETHERNET: Ethernet is a widely used LAN technology. It was invented at EXROX PARC (Palo Alto Research Center) in 1970s. Xerox, Intel and Digital defined it in a standard so it is also called DIX standard. The standard is now managed by IEEE in which 802. 3 standard of IEEE defines formats, voltages of cable length etc. The Ethernet uses bus topology. It uses a single coaxial cable. To which multiple computers connect. One Ethernet cable is sometimes called a segment. This segment is limited to 500 meters in length. The minimum separation between connections is 3 meters. ETHERNET SPEEDS: The Ethernet speed was originally 3Mbps, and the current standard is 10Mbps the fast Ethernet operates at 100Mbps. There are also gigabits Ethernet available now. ENCODING USED IN ETHERNET: The encoding used in Ethernet is Manchester encoding. It uses signal changes to encode data. e. g. A change from positive voltage to 0 encodes as shown in the figure below: FIGURE 7. 5 27 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 8 CARRIER SENSE MULTIPLE ACCESS (CSMA) There is no central control management when computers transmit on Ethernet. For this purpose the Ethernet employs CSMA to coordinate transmission among multiple attached computers. CSMA is a coordination scheme that defines how to take turns using a shared cable. A computer listen to the codes i. e. it senses the carrier. If the cable is idle it starts transmitting and if the cable is in use then it waits. If simultaneous transmission occurs, the frames interfere with each other and this phenomenon is called collision. COLLISION DETECTION: As explained above, the signals from two computers will interfere with each other and the overlapping of frames is called a collision. It does not harm to the hardware but data from both frames is grabbled. ETHERNET CD: To detect the collision, Ethernet interfaces include hardware to detect transmission. It performs two operations: - - It monitors outgoing signals. Grabbled signal is interpreted as a collision. After collision is detected computers stop transmitting. So Ethernet uses CSMA/CD to coordinate transmission. RECOVERY FROM COLLISION: Computer that detects a collision sends special signal to force all other interfaces to detect collision. Computer then waits for other to be idle before transmission. But if both computers wait for same length of time, frames will collide again. So the standard specifies maximum delay and both computers choose random delay, which is lesser. After waiting, computers use carrier sense to avoid subsequence collision. The computer with shorter delay will go first and other computer may transmit later. 28 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU EXPONENTIAL BACK OFF: Even with random delays, collision may occur especially likely with busy segments. Computers double delay with each subsequent collision. It reduces likely hood of sequence of collision. 802. 11 WIRELESS LANs AND CSMA/CA: IEEE 802. 11 is standard wireless LAN that uses radio signals at 2. 4GHz. Its data rate is 11Mbps. The older devices use radio signals at 900MHz and data rate of 2Mbps. Bluetooth specifies a wireless LAN for short distances. It uses shared medium and radio waves instead of coaxial cable. LIMITED CONNECTIVITY WITH WIRELESS: In contrast with wired LANs, not all participants may be able to reach each other. Because: - - - It has low signal strength. In wireless LANs the propagation is blocked by walls etc. It can’t depend on CD to avoid interference because not all participants may hear. This is shown in the figure below: FIGURE 8. 1 CSMA/CA: Wireless uses collision avoid ness rather than collision detection. Transmitting computer sends very short message to receiver. Receiver responds with short message reserving slot for transmitter. The response from receiver is broadcast, so all potential transmitters receive reservation. COLLISION: The receiver may receive simultaneous requests, which results in collision at receivers and both requests lost and in this way no transmitter receives reservations and both use back off and retry. The receiver may receive closely spaced requests. It selects 29 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU one of them and then the selected transmitter sends message and the transmitter not selected uses back off and retries. LOCAL TALK: Apple invented the LAN technology that uses bus topology. Its interface is included with all Macintosh computers. It has relatively low speed i. e. 230. 4Kbps. Also it is of low cost and we can get a free with a Macintosh, which is easy to install and connect. It uses CSMA/CA. TOKEN RING: Many LAN technologies that are ring topology use token passing for synchronized access to the ring. The ring itself is treated as a single shared communication medium. Both pass from transmitter passed by other computers and are copied by destination. Hardware must be designed to pass token ever if attached computer powered down. This is shown in figure below. FIGURE 8. 2 USING THE TOKEN: When a computer waits to transmit it waits a token. After transmission computer transmits token on ring. Next computer is then ready to transmit, receive and then transmits. TOKEN AND SYNCHRONIZATION: Because there is only one token, only one computer will transmit at a time. Token is a short reserved frame that can not appear in data. Hardware must regenerate token if lost. Token gives computer permission to send one frame. If all computers are ready to transmit it enforces Round-Robin access. But if now computer is ready to transmit, token circulates around ring. 30 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU IBM TOKEN RING: It is very widely used. It was originally 4Mbps and now it is upto 16Mbps. It uses special connection cable between the computer and the Ring interface. FDDI: Fiber distributed data interconnect (FDDI) is another ring technology. Its most important features are: It uses fiber optics between stations and transmits data at 100Mbps. It uses pair of fibers to form two concentric rings. FDDI AND RELIABILITY: FDDI uses counter rotating rings in which data flows in opposite directions. In case of fiber a station failure, remaining stations loop back and reroute data through spare ring. In this way all stations automatically configure loop back by monitoring data ring. It is shown in figure below FIGURE 8. 3 FDDI AND RELIABILITY: ATM ----STAR NETWORK: The ATM (Asynchronous Transferred Mode) technology consists of electronic packet switches to which the computers can connect. ATM switches form a hub into which computers can connect in a star topology. Computer gets point-to-point connections. Data from transmitters is routed directly through hub switches to destination. An ATM star network is shown in the figure below: FIGURE 8. 4 ATM SWITCH 31 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU ATM DETAILS: - - - - It transmits data at over 100Mbps. It uses fiber optics to connect computer to switch. Each connection includes two fibers. It is also shown in figure. FIGURE 8. 5 32 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 9 HARDWARE ADDRESSING We need to devise technique for delivering message through LAN medium to single, specific destination computer. Sending computer uses a hardware address to identify the intended destination of a frame. The sending computer also identifies type of data carried in the frame. SPECIFYING A DESTINATION: The data sent across a shared network reaches all attached stations - for all LAN topologies. Interface hardware detects delivery of frame and extracts frame from medium. But most applications want data to be delivered to one specific application on another computer but not all computers. HARDWARE ADDRESSING: Most network technologies have a hardware-addressing scheme that identifies stations on the network. Each station is assigned a numeric hardware address or physical address. . Sender also includes hardware address in each transmitted frame. In this way only station identified in frame receives copy of frame. Most LAN technologies include sender's hardware address in frame too. LAN HARDWARE AND PACKET FILTERING: The figure below illustrates the LAN hardware: Figure 9. 1 LAN INTERFACE: LAN interface handles all details of frame transmission and reception which are given as follows: 33 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU - - - - - - - It adds hardware addresses, error detection codes, etc. to outgoing frames. It may use DMA to copy frame data directly from main memory. It obeys access rules (e. g., CSMA/CD) when transmitting. It checks error detection codes on incoming frames. It may use DMA to copy data directly into main memory. It checks destination address on incoming frames. The frames not addressed to the local computer are ignored and don't affect the local computer in any way. FORMAT OF HARDWARE ADDRESS: It consists of a numeric value and its size is selected for specific network technology. The length of the format is one to six bytes. ASSINGING HARDWARE ADDRESS: The hardware address must be unique on a LAN. How can those addresses be assigned and who is responsible for uniqueness? The answer to these questions depends on the particular LAN technology being used. There are three categories of address forms: - - - Static Configurable Dynamic STATIC: In this category the hardware manufacturer assigns permanent physical address to each network interface and manufacturer must ensure that every interface has a unique address. CONFIGURABLE: In this category, the address can be set by the end user either manually e. g. switches or jumpers on the interface or electronically (e. g. through software). The system administrators must coordinate to avoid the conflict. DYNAMIC: In this category the interface automatically assigns physical address each time it is powered up. This automatic scheme must be reliable to prevent conflicts. BROADCASTING: Some applications want to broadcast messages to all stations on the LAN. For this purpose shared communication channel can make broadcast efficient in such a way that message is delivered to all stations. A special broadcast address is used to identify broadcast message, which are captured by all stations. 34 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 10 FRAME TYPE IDENTIFICATION There are some problems with the broadcast. For every broadcast frame on the network each computer uses computational resources and places the contents into memory, which interrupt the CPU. It allows system software to make the decision whether to discard or use the frames. Another problem is that if a pair of computer use broadcasting instead of sending them directly all other computers waste CPU time while discarding the frames. MULTICASTING: The solution to above problem is multicasting. It is the restricted form of broadcasting. It works like broadcasting however it does not forward frames automatically to the CPU. The interface hardware is programmed in advance to accept certain frames that have multicast address as the destination address. If an application program wishes to receive certain frames then it program the interface hardware to accept an additional set of addresses. The interface hardware frame then begins accepting three types of frames: - Multicast frames - Broadcast frames - The frames that are distend to the station itself. MULTICAST ADDRESSING: We take an example of computers running an audio application. We see that they can receive audio frames if the interface are programmed to received them and the other computers that are not running that audio application will not waste resources . IDENTIFYING PACKET CONTENTS: The destination must get some clue about how to interpret frame data. For this purpose it can use two types which are given as follows. EXPLICIT FRAME TYPE: In this type the identifying value is included with frame describes types of included data. 35 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU IMPLICIT FRAME TYPE: In implicit frame the receiver must infer from frame data. HEADERS AND FRAME FORMAT: LAN technology standards define frame format for each technology. All contemporary standards use the following general format. a) Frame header b) payload Frame header has address and other identifying information. Information typically in fields has fixed size and location. The data area may vary in size. The Ethernet frame format is shown in the figure. Figure 10. 1 the Ethernet frame format The different friends of ether frame format and their purposes is explained below: FIELD Preamble Destination Address Source Address Frame Type Data CRC PURPOSE Receiver synchronization Identifies intended receiver Hardware address of sender Type of data carried in frame Frame payload 32-bit CRC code ETHERNET FIELDS: In Ethernet fields the preamble and CRC is often not shown in frame. The destination address of all is the broadcast address. There is special value reserved for frame type field. FRAME WITHOUT TYPE FIELDS: Some LAN technologies do not include a type field. Sender and receiver can agree on interpretation, which is as follows: They agree on single data format and use only that format this limits to one type of data. In this way all computers on LAN must use one format. Also they agree to encode the data format into first few bytes of the data field. 36 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU ENCODING THE DATA TYPE: The figure illustrates a frame in which the data type is specified by using the data area. Figure 10. 2. Encoding the data type To ensure interoperability format of encoding area must be universally agreed upon it typically set by standards only. IEEE 802. 2 LLC: IEEE 802. 2 standard includes logical link control (LLC) sub network attachment point (SNAP) header. SNAP/LLC format is widely used for example by Ethernet. This is shown in figure below: Figure 10. 3. SNAP/LLC format In the figure LLC portion indicates SNAP field to follow OUI (organizationally unique identifier) identifies Ethernet specification organization. Also the type field is interpreted as in Ethernet (in this case, IP ) as shown in figure above. UNKNOWN TYPES: For either encoding format some computer may not be prepared to accept frames of some types, which are unknown e. g. protocol type is not installed and the newly defined type. The receiving computer examines the field and discards any frame with unknown type. NETWORK ANALYZERS: A network analyzer also called network monitor or a network sniffer is used to examine the performance of or debug a network. It can report statistics such as capacity utilization, distribution of frame size, collision rate or token circulation time. 37 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU OPERATION OF NETWORK ANALYZERS: The basic idea behind the operation of network analyzer is a computer with a network interface that receives all frames, which is called promiscuous mode. Many desktop computers have interface that can be configured for promiscuous mode. When combined with software computer can examine any frame on LAN. In this way the communication across LAN is guaranteed to be private. This computer receives and displays (but does not respond to) frames on the LAN. Network analyzer can be configured to filter and process frames. It can count frames of specific type of size. It displays only frames from or to specific computers. In general it can be configured to match any value of any field and capture only these frames meeting the filter specifications. ` 38 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 11 INTERFACE HARDWARE LAN data transmission speeds are typically fast relative to CPU speeds. LANs speeds are defined independent of any specific processor speeds, which allows for mix of any attached systems. In this way new computers can be attached without affecting LAN speeds. NETWORK INTERFACE HARDWARE: CPU can’t process data at network speeds. So in order to connect to the network computer systems use special purpose hardware for network connections which consists of typically a separate card in the back plane which is called Network Adapter Card or Network Interface Card (NIC). The connector on NIC at the back of computer then accepts cable to physical network. The CPU structure is shown in the figure. Figure 11. 1 The Network Connector is also shown in the figure below. 39 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Figure 11. 2 NICs AND NETWORK HARDWARE: NIC is built for one kind of physical network. For example Ethernet interface can not be used with token ring and similarly ATM interface cannot be used with FDDI. Some NICs can be used with different but similar hardware for example thick, thin and 10 Base-T Ethernet, 10Mbps and 100Mbps Ethernet. NIC AND CPU PRCESSING: NIC contains sufficient hardware to process data independent of system CPU. In which some NICs contain separate microprocessor. In addition to this it also include analog circuitry interface to system bus, buffering and processing. NIC looks like any other I/O device to system CPU. The system CPU forms message request and sends instructions to NIC to transmit data. NIC also receives interrupt on incoming data. CONNECTION BETWEEN NIC AND PHYSICAL NETWORK: TWO ALTERNATIVES: NIC contains all circuitry and connects directly to network medium. A cable from NIC connects to additional circuitry that then attaches to the network medium. THIN ETHERNET VERSUS 10BASE-T: Thin Ethernet and 10Base-T are both Ethernet. The network technology is not limited to one style of connection. 40 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU THICK ETHERNET WIRING: It uses thick coax cable. AUI cable (or transceiver or drop cable) connects from NIC to transceiver. AUI cable carries digital signal from NIC to transceiver. The transceiver generates analog signal on coax cable. The wires in AUI carry digital signals power and other control signals. Thick Ethernet also requires terminators to avoid signal reflectance. This is shown in the figure below: Figure 11. 3 CONNECTION MULTIPLEXING: In some circumstances transceiver may be in convenient e. g. workstations in a LAN. Connection multiplexer connects multiple computers to a single transceiver. Each computer’s AUI cable connects to connection multiplexer. One AUI from multiplexer to Ethernet coax. Connection multiplexing is shown in the figure below. Figure 11. 4 41 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU THIN ETHERNET WIRING: Thin Ethernet uses thin coax cable that is cheaper and easier to install than thick Ethernet coax. In this case transceiver electronics are built into NIC and NIC connects directly to network medium. Coax cable use BNC connector on NIC. Coax runs directly to back of each connected computer by T-connector. The T-connector directly attaches to NIC. This is shown in the figure below. Figure 11. 5 Thin Ethernet is useful when many computers are located close to each other. It may be unreliable because any disconnection disrupts entire net. 42 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 12 LAN WIRING AND PHYSICAL TOPOLOGY 10BASE-T: This is another standard of wiring scheme. It is commonly called 10Base-T, Twisted Pair or TP Ethernet. It replaces AUI cable with twisted pair cable and thick coax with hub. This makes it cheaper and that ‘ s why it is most useful technology of today. It is shown in the figure below: Figure12. 1 HUBS: They are used for extension of connection with multiplexing concept. They are sometimes called Ethernet-in-a-box. It is effectively a very short Ethernet with very long AUI cables. It can be connected into larger Ethernet. PROTOCOL SOFTWARE AND ETHERNET WIRING: All wiring technologies use identical Ethernet specifications. e. g. they use same frame format. They use same CSMA/CD algorithms. They can mix different technologies in an Ethernet. NICs can provide all three-connection technologies. The protocol software can’t differentiate among wiring technologies. The NIC is shown in the figure below with three connectors. 43 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Figure 12. 2 COMPARISON OF WIRING SCHEME: The wiring schemes are compared as follows: Separate transceiver allows computers to be powered off or disconnected from network without disrupting other communication. Transceiver may be located in an inconvenient place, so finely malfunction transceiver can be hard. In other case, thin coax cable takes minimum of cable. Disconnecting one computer (on one loose connection) can disrupt entire network. Hub wiring centralizes electronics and connections. It makes management easier. Bottom line 10Base-T is most popular because of lowest cost. TOPOLOGIES AND NETWORK TECHNOLOGIES: 10Base-T network topology is a bus but wiring topology is a star. The token ring network topology is a ring but wiring topology is a star. We should remember to distinguish between logical and physical topologies. A topology is logically a star or it is physically a star. FILTERING INCOMING FRAMES: An analyzer can be configured to filter and process frames. It can count frames of a specific type or size. It can also display only frames from or to specific computers. 44 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU In general, it can be configured to match value of any field and capture only those frames making the filter specification. ADVANTAGE AND DISADVANTAGE OF WIRING SCHEMES: Each of three wiring schemes has advantages and disadvantages, which are explained as follows: RELIABILITY ISSUES: Wiring that uses a transceiver for each connection does not affect the entire network if a transceiver cable is disconnected. A cable cut occurring in hub wiring only affects one computer. COST ISSUES: Twisted pair Ethernet is the cheapest wiring that makes it so popular. Thicknet is the most costly wiring, which is no longer used. Figure 12. 3 As shown in the figure eight offices are wired with a) Thick Ethernet b) Thin Ethernet c) Twisted pair Ethernet We can see that the length of wired varies in three schemes so cost varies in three schemes. 45 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU THE TOPOLOGY PARADOX: The main feature of twisted pair Ethernet is that it forms a classic star topology however functions like a bus. 10Base-T Ethernet is often called a star shaped bus. Two different types OF TOPOLOGIES: LOGICAL TOPOLOGY: It is defined by the specific network technology. PHYSICL TOPOLOGY: It depends on the wiring scheme. NETWORK INTERFACE CARD AND WIRING SCHEMES: Figure 12. 4 To allow changing the wiring without changing the interface hardware, NICs support multiple wiring schemes. it is shown in the figure below. 10/100 NETWORK INTERFACES AND AUTONEGATIATION: 10Base-T version of twisted pair Ethernet operated at 10Mbps. 10Base-T Twisted pair Ethernet operates at 100Mbps. 46 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU 100Base-T technology is backward compatible and allows the participants to negotiate a speed when connection is established. This process is known as auto negotiation. CATEGORIES OF WIRES: Cable used for wiring should match the following: - The intended data rate - The distance between devices - The amount of em-noise - Anticipated future needs - Cost Some categories and their typical uses are shown in the figure below. Figure 12. 5 WIRING SCHEMES AND OTHER NETWORK TECHNOLOGIES: Multiple wiring schemes are not limited to Ethernet technology. Almost alltogether network technologies use different wiring schemes. e. g., local talk uses hubs (physical star) to simulate a bus topology. IBM’s token ring also uses hubs (physically a star topology) to simulate a logical ring network. 47 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU Lecture No. 13 FIBER MODEMS AND REPEATOERS LAN technologies are designed to operate within the same building. However most companies or institutions have offices located far apart from each other. DISTANCE LIMITATION AND LAN DESIGN: The maximum cable length of a LAN is fixed because the electrical signal level gets weaker as it travels. The delays must be short to allow access mechanisms (CSMA/CD, token passing) work properly. However in most cases a LAN needs to be extended layer distances than the maximum Cable length limit. For example: extending a company LAN to another building. LAN EXTENSIONS: Several techniques extend diameter of LAN medium. In this purpose most techniques use additional hardware. LAN signals relayed between LAN segments. Resulting mixed technology stays within original engineering constraints while spanning greater distance. FIBER OPTIC EXTENSION: The LAN extension using fiber optic is shown in the figure below: Figure 13. 1 The fiber-modem coverts digital data into pulses of light then transmits over the optical fiber. It also receives light and converts into digital data. This mechanism will successfully extend the optical fiber across several kilometers because delays on optical fiber are very low and bandwidth is very high. 48 © Copyright Virtual University of Pakistan COMPUTER NETWORKS (CS610) VU REPEATERS: Repeaters are used when copper wire communication is carries out. According to the fact that electrical signal gets weaker while traveling over copper wires. A repeater is used to increase the signal strength. It amplifies the weakening signal received from one segment and then retransmits onto another segment. It is shown in the figure below: Figure13. 2 One repeater doubles, two repeaters triple the maximum cable length limitation. Computers attached to different segments commu