Data link layer assignment

 Part 1: General review of data link layer Explain the working principles of the data link layer. The data link layer sits between the physical layer and the network layer.

It is responsible for sending and receiving messages to and from other computers. It is responsible for moving a message from one computer to next computer where the message needs to go. The data link layer performs the main functions and is divided into two sub layers. The first sublayer called logical link control (LLC) sublayer and the second sublayer called media access control (MAC) sublayer. The LLC sublayer software at the sending computer is responsible for transmitting the network layer Protocol Data Unit (PDU) with the data link layer.

At the receiving computer the MAC sublayer software takes the data link layer PDU from the LLC sublayer and coverts into a stream of bits and also controls when the physical layer actually transmits the bits over the circuit. The data link layer controls the way messages are sent on the physical media. The data link layer performs various functions depending upon the hardware protocol used in the network and both sender and receiver have to agree on the rules and protocols that govern how they will communicate with each other.

The data link layer is concerned with physical addressing, network topology, physical link management, error notification, ordered delivery of frames and flow control (Fitzgerald & Dennis 2009). Is controlled access better than contention for media access control? Discuss. There are two fundamental approaches to media access control that are control access and contention. In control access the polling process is used in which the mainframe computer (i. e. server) controls the circuit and determines which clients (i. e. computer or terminal) can access media at what time.

Polling is like a classroom situation where the instructor (i. e. server) calls students who have raised their hands to gain access to the media. Contention is altogether opposite to controlled access. In this case the computers wait until a circuit is free which means they have to check whether any computers are transmitting and then only they are allowed to transmit whenever they have data to send. But to determine which is better can be considered based on the largest amount of user data to be transmitted through the network.

The contention approach has worked better than controlled access approach for small network where there is low usage, but can be problematic in heavy usage networks. In heavy usage networks where many computers want to transmit at the same time the controlled access approach is better because it prevents collisions and delivers better throughput in such networks. But today's contention approach is better than controlled access because they have been improved to the point where they are able to deliver significantly better throughput than controlled access and are also competitive because of the hardware cost (Fitzgerald & Dennis 2009).

Why is error detection important in this layer? What is being measured? The responsibility of the data link layer is sending and receiving messages to and from different computers without errors. The data link layer also accepts streams of bits from the physical layer and organizes them into coherent messages that it passes to the network layer (Fitzgerald & Dennis 2009). Error detection is important in this layer because it protects the network from errors. There are human errors and network errors. The network errors are those that occur during transmission of messages from one computer to another computer.

During transmission of messages there are two possibilities of network errors that is corrupt data (data that have been changed) and lost data. The data link layer is responsible for the transmission of messages without errors from one computer over one circuit to the next computer where the message needs to go. Even if we know what types of errors can occur, we can recognize the error only if we have a copy of the intended transmission for comparison. But if we don't have the copy of transmission then detecting

errors for machine would be slow, costly and of questionable value (Forouzan 2002).

The error detection uses the concept of redundancy which means short group of bits appended to or inserted to each unit of data. The extra bits are redundant to the information (message); they are then discarded as soon as the accuracy of the transmission is determined for detecting errors at the destination computer. Identify three significant noises that can cause errors in data communication digital circuits. Briefly explain. Line noise and distortion can cause data communication errors. Errors can occur during data transmission.

Data transmitted both analogue and digital is susceptible to many types of noise and errors. The three significant noises that can cause error in data communication digital circuits are: White noise: white noise also called thermal noise or Gaussian noise. This noise is a relatively continuous type of noise and much like the static you hear on radio between two stations. It will always be present in some degree of transmission media and electronic device and is also dependent on the temperature of the medium. The level of noise increases due to the increased movement of electrons in the medium.

The white noise can be removed from the digital signal by passing the signal through a signal regenerator before the noise completely overwhelms the original signal (White 2007). Impulse noise: Impulse noise or also called noise spike is a noncontinuous noise and the most difficult errors to detect since it occurs randomly. Difficulty comes in separating the noise from the signal.

Some of the sources of impulse noise are voltage change, lightning flashes during thunderstorms, fluorescent lights and poor connection in circuits.

If the impulse noise interferes with the digital signal, often the original digital signal can be recognized and recovered. The way to prevent impulse noise is by shielding or moving cables (White 2007). Cross-talk: Crosstalk is like an unwanted coupling between two different signal paths. The unwanted coupling could be electrical, can also occur between two sets of twisted pair (in phone line) or it can be electromagnetic. Crosstalk during telephone calls can be experience when you hear other conversations in the background. Wet or damp weather can also increase crosstalk.

Even though crosstalk is relatively continuous it can be reduced by proper precautions and hardware; that is by increasing the guradbands or move or shielding the wires (White 2007) Part 2: General review of error correction Why is cyclical redundancy check (CRC) most popular error checking scheme? Three common error detection methods are parity checking, longitudinal redundancy checking and polynomial checking (that is particularly checksum and cyclic redundancy checking). Parity checking is one of the oldest and simplest error detection methods.

Any single error (switch of one bit 1 or 0) will be detected by parity, but it cannot determine in which bit was in the error. If two bits are switched the parity check will not detect any error. Therefore the probability of detecting an error is only 50 percent. Many networks these days do not use parity checking because of low error detection rate. The most popular polynomial error checking scheme is cyclical redundancy check (CRC) method which

adds 8 to 32 check bits to potentially large data packets and yields error detection capability approaching of 100 percent.

In CRC a message is treated as one long binary number, CRC performs quite well and the most commonly used CRC codes are CRC-16 (16-bit version), CRC-CCIT (another 16-bit version) and CRC-32(32-bit version). CRC -16 will detect about 99. 99 percent of all burst errors longer than 16 bits and CRC-32 will detect about 99. 99 percent of all burst errors longer than 32 bits (Fitzgerald & Dennis 2009; White 2007) How is Hamming distance used in error correction? Explain. The number of bits positions in which two codewords differ is called Hamming distance.

The significance of Hamming distance is that if two codewords are Hamming distance d apart then it will require d single bit errors to convert one into the other. The error correcting properties of code depends on tis Hamming distance (Forouzan 2007). To detect d errors we will need a distance d+1 code because with such a code there is no way that d single bit error can change a valid codeword into another valid codeword. So when the receiver sees an invalid codeword it can tell that a transmission error has occurred. Similarly when to correct d errors we will need a distance 2d +1 ode because by doing this the legal codewords are so far apart that even with d changes, the original codeword is still closer than any other codeword so that it can be uniquely determined. Normally a frame consist of m data (that is message) bits and r redundant or check bits. Let the total length be n (i. e. n= m+r). So the n-bit unit will contain data and check bits which are often referred to as an n-bit codeword. Given two possible code word say 10001001 and

10110001 then is it possible to determine how many corresponding bits differ. In this example 3 bits differ.

Thus to determine how many bits differ just exclusive OR the two codewords and count the number of 1 bits in the result (Tanenbaum 2003). Briefly explain how parity is used to find the location of single-bit errors in the forward error correction method? Parity bits are used on asynchronous data streams to determine whether the received data has error or not. The transmitter adds the parity bit to the data stream and then the receiver compares this to the status of the received parity bits. If the two states are the same then the receiver assumes that the received data is error free.

If in case the two states are different then the receiver assumes that the data was errored. How parity is used to find single- bit errors in forward error correction method can be explained with the Hamming code example. Consider three parity bits P1, P2, and P4 are added to data bits D3, D5, D6, and D7. The parity bits (P1, P2, and P4) are 101 and data bits (D3, D5, D6, and D7) are 1010. In this example Hamming code associates even parity bits with unique combinations of data bits. The parity bit P1 applies to data bits D3, D5 and D7.

The parity bit P2 applies to data bits D3, D6 and D7. And parity bit P4 applies to data bits D5, D6 and D7. For this example data bits (D3, D5, D6, D7) are 1010 so P1 must be 1 because there is only a single 1 among D3, D5 and D7 and parity must be even. Similarly P2 must be 0 and P4 must be 1 for even party. Now assume that during transmission data bit D7 is changed from 0 to

1 by line noise. Since data bit D7 is being checked by parity bits P1, P2 and P4, all three parity bits now show odd parity instead of correct even parity.

The data bit D7 is the only data bit which is monitored by all three parity bits; therefore when D7 is in error all three parity bits show an incorrect parity. In this way the receiver can determine which bit was in error and reverse its state, thus correcting the error without retransmission (Fitzgerald & Dennis 2009; Smillie 1999). Part 3: Demonstration of data link protocols Explain the necessity of data link protocols? The data link protocols are a set of specifications which are used to implement the data link layer. They contain rules that are used for framing, addressing, and error and flow control.

Data link layer protocols are divided into two subgroups: asynchronous protocols and synchronous protocols. The asynchronous protocols treat each character in a bit stream independently and synchronous protocols take the whole bit stream and chop it into characters of equal size. Nowadays asynchronous protocols are mostly outdated due to its inherent slowness and so asynchronous transmission is being replaced by higher speed synchronous mechanisms. Protocols governing synchronous transmission can be divided into two classes: character-oriented protocols and bit-oriented protocols.

In character- oriented protocols the control information is in the form of code words taken from existing character set of ASCII or EBCDIC. These multibit characters carry whole information about line discipline, flow control and error control. But the bit-oriented protocols can pack more information into

shorter frames. Initially the synchronous data link control (SDLC) was the basis for all bit oriented protocols but then in 1979, ISO designed high-level data link control (HDLC) which was based on SDLC and is the basis for all bit oriented protocols in use today.

HDLC is designed to support both half-duplex and full-duplex communication over point-to-point and multi point links (Forouzan 2002). Asynchronous communication is sometimes called start-stop transmission. Discuss with necessary diagram? In asynchronous transmission each character is transmitted independently of all other characters. For separation of characters and synchronization, as start bit and a stop bit are put in front and back of each individual character. When no character is being transmitted, the line between transmitter and receiver is in an idle state. pic] Figure 1: Asynchronous transmission Source: Fitzgerald & Dennis 2009 As shown in figure 1 the start bit is 0 and stop bit is 1. The recognition of start and stop of each message (called as synchronization) takes place for each individual character since the start bit is the signal which tells the receiver to start sampling all the incoming bits of the character so that data bits can be interpreted into proper character structure. The stop bit task is to inform the receiver that the character has been received and so it can reset the recognition for next start bit.

When the sender has no data to send and has finish transmitting a letter and waiting for more data to send, in this case it sends continuous series of stop bits (Fitzgerald & Dennis 2009; Stallings 2004). Explain the Ethernet protocols categories? Ethernet is very popular LAN protocol and was developed jointly by Digital, Intel and Xerox in the 1970s. Since then

Ethernet has been further refined and developed into a formal standard called IEEE 802. 3ac. There are several versions of Ethernet and Ethernet uses a contention media access protocol. [pic] Figure 2: Ethernet IEEE802. frame Source: Buchanan 2000 The figure 2 shows Ethernet IEEE802. 3 frame. The frame starts with 7-byte preamble which is repeating pattern of ones and zeros. Then is start delimiter which marks start of frame. The destination address specifies the sender while the source address specifies sender. The DSAP and SSAP are used to pass control information between the sender and receiver; these are used to indicate the type of network layer protocol the packet contains. Ethernet II is another commonly used version of Ethernet. The Ethernet II is similar to the IEEE802. frame it uses preamble and flag to mark the start and end of the frame. It has the same source and destination address format as Ethernet IEEE802. 3 (Buchanan 2000; Fitzgerald & Dennis 2009) References Buchanan, W 2000, Computer Busses: Design And Application, Elsevier, New Jersey. Forouzan, BA 2002, Business Data Communications, McGraw-Hill, New York. Forouzan, BA 2007, Data Communications And Networking, 4th edn, McGraw Hill, New York. Fitzgerald, J & Dennis, A 2009, Business Data Communications and Networking, 10th edn, John Wiley & Sons, New Jersey.

Smillie, G 1999, Analogue and Digital Communication Techniques, Butterworth-Heinemann, New Jersey. Stallings, W 2004, Data And Computer Communications, 7th edn, Pearson Prentice Hall, New Jersey. Tanenbaum, AS 2003, Computer Networks, 4th edn, Pearson Education, New Jersey. White, CM 2007, Data Communications and computer networks: A business user’s approach, 4th edn, Thomson Course Technology, Canada. ————————–

CENTRAL QUEENLAND UNIVERSITY 10 Review of Data Link Layer Assignment 1- COIS20027 Hemant Pol Student No: S0204260 Due Date: 20/08/2010 Lecture: Edilson Arenas Tutor: David Ling Total Word Count: 2, 828