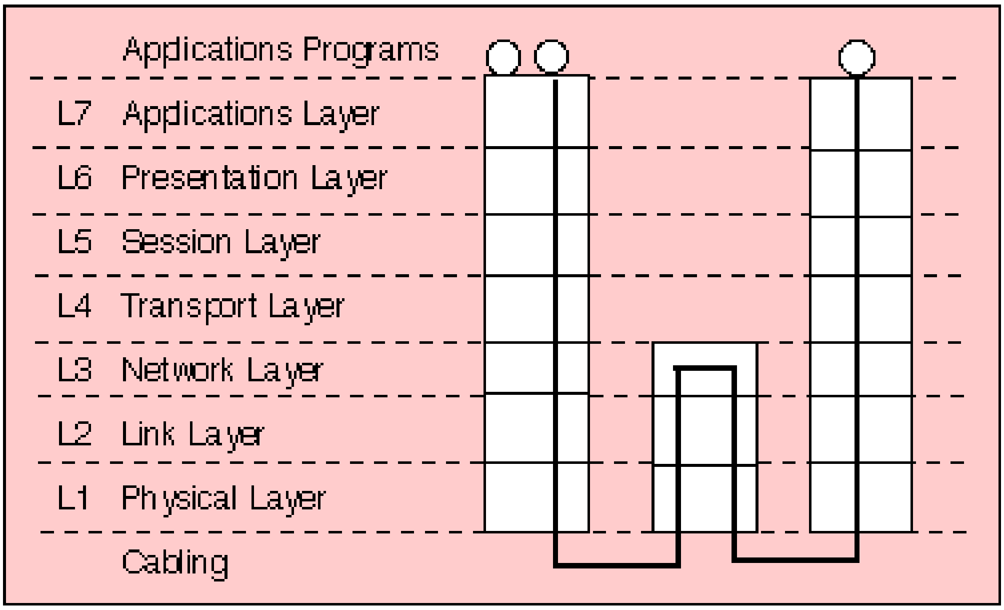
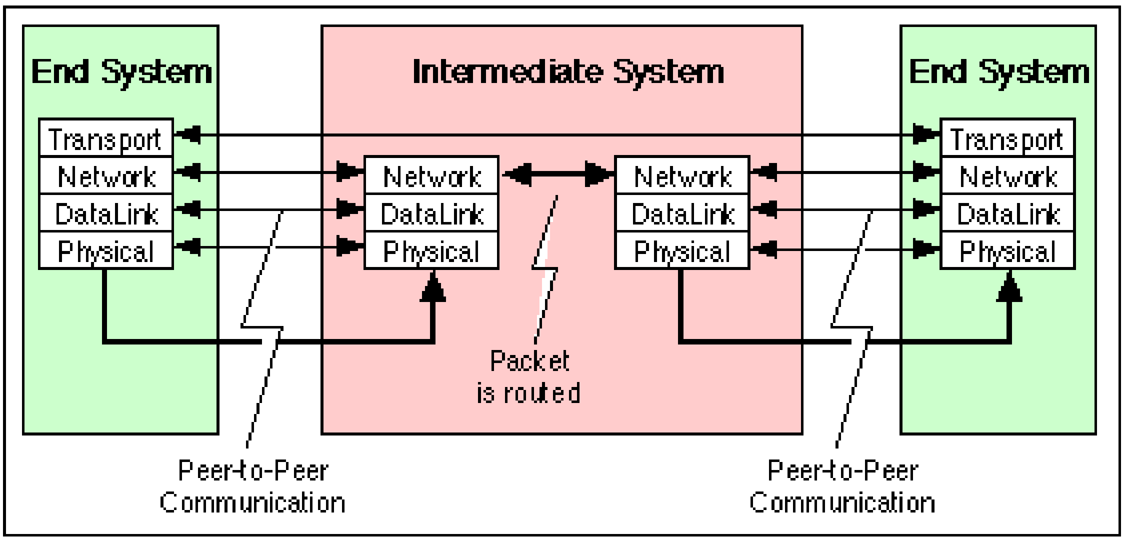
1. (a) The Open Systems Interconnection (OSI) reference model describes some proto cols as End-to-End and some as Link-by-Link (also known as Hop-by-Hop). Explai these two terms, and provide an appropriate diagram to illustrate End-to-End and Link-by Link communication. [8 marks]



The communications engineer is concerned mainly with the protocols operating at the bottom four layers (physical, data link, network, and transport) in the OSI reference model. These layers provide the basic communications service. The layers above are primarily the concern of computer scientists who wish to build distributed applications programs using the services provided by the network.

The two lowest layers operate between adjacent systems connected via the physical link and are said to work "hop by hop". The protocol control information is removed after eac "hop" across a link (i.e. by each System) and a suitable new header added each time the information is sent o a subsequent hop. The network layer (layer 3) operates network-wide and is present in all systems and re sponsible for overall co-ordination of all systems along the communications path. The layers above layer operate end-to-end and are only used in the End Systems (ES) which are communicating. The Layer 4 - protocol control information is therefore unchanged by the IS in the network and is delivered to the corre sponding ES in its original form. Layers 4-7 (if present) in Intermediate Systems (IS) play no part in th end-to-end communication.



8

Peer-to-Peer communication between OSI protocol layers

Mark

(b) A Universal Datagram Protocol (UDP) packet is sent via an Ethernet network. Draw a diagram to show the frame of data as it would appear on the Ethernet network. Your diagram should include all the protocol headers. [4 marks]

+1
+1
+1
+1

It is the responsibility of the network layer (IP) protocol to ensure that the UDP message is sent to the correct destination. This is achieved by setting the destination address of the IP packet. The source address is set to the address of the computer generating the UDP request and the IP protocol type is set to "UDP" to indicate that the packet is to be handled by the remote end system's UDP server program.

Encapsulation over an Ethernet LAN using an IP network layer header, and a MAC link layer header and trailer containing the 32-bit checksum consists of adding the following headers:

Ethernet Preamble (8 B) + Ethernet MAC Header (14 B) + IP Header (20 B) +
UDP Message (UDP Header + DATA) + CRC-32 (4 B)

=4

(c) What is the purpose of a pre-amble and why is it sometimes needed for synchronous communications? [2 marks]

The purpose of the idle time before transmission starts is to allow a small time interval for the receiver electronics in each of the nodes to settle after completion of the previous frame. A node starts transmission by sending an 8 byte (64 bit) preamble sequence. This consists of 62 alternating 1's and 0's followed by the pattern 11. When encoded using Manchester encoding, the 62 alternating bits produce a 10 MHz square wave. The purpose of the preamble is to allow time for the receiver in each node to achieve lock of the receiver Digital Phase Lock Loop which is used to synchronise the receive data clock to the transmit data clock. At the point when the first bit of the preamble is received, each receiver may be in an arbitary state (i.e. have an arbitary phase for its local clock). During the course of the preamble it learns the correct phase, but in so doing it may miss (or gain) a number of bits. A special pattern (11), known as the start of frame delimiter, is therefore used to mark the last two bits of the preamble. When this is received, the Ethernet receive interface starts collecting the bits into bytes for processing by the MAC layer.

2

(d) A client program sends one UDP packet with 100 B of data each second to a server and receives a corresponding reply also with 60 B of data. The client and server are connected by an Ethernet LAN. Calculate the total number of bits sent via the Ethernet network by this program in each second. From the number of bits per second calculate the Utilisation, given that Ethernet typically operates at 10 Mbps.
[6 marks]

1 UDP message sent per second, with 1 reply received per second.

Each message contains:

MAC-Preamble (8 bytes) + MAC Header (14 bytes) + IP Header (20 bytes) + UDP(48bytes) + UDP Payload (60 bytes) + CRC-32 (4 bytes)

+4

Total per second= (8+14+20+8+60+4) * 8 * 2= 912 * 2 bps = 1824 bps

Total per second= 1824 bits /sec

Assume 10 Mbps Ethernet operation.

Utilisation = 2464 / clock rate * 100 = 1824 x 10-7 x 100 = **0.018 %**

+2
=6

Utilisation = **0.018 %**

2. (a) Explain the properties of the Open Systems Interconnection (OSI) Physica Layer [4 marks]

The Physical layer provides electrical, functional, and procedural characteristics to activate, maintain, and de activate physical links that transparently send the bit stream; it is also concerned with the timing required t identify the centre of each transmitted bit.

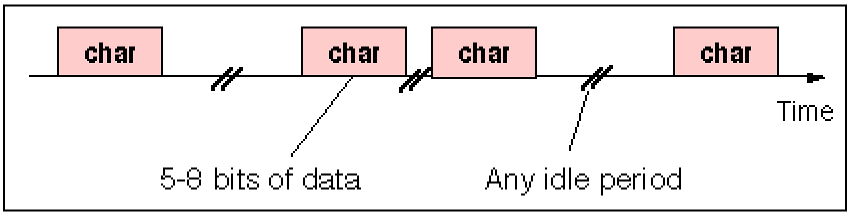
It only recognises individual bits, not characters or multicharacter frames.

4

(b) Provide a description of the following terms:

(i) Asynchronous Transmission

The asynchronous communication technique is a physical layer transmission technique which is most widel used for personal computers providing connectivity to printers, modems, fax machines, etc. The most signifi cant aspect of asynchronous communications is that the transmitter and receiver clock are independent and ar not synchronised. In fact, there need be no timing relationship between successive characters (or bytes c data). Individual characters may be separated by any arbitrary idle period.



Asynchronous transmission of a series of characters

An asynchronous link communicates data as a series of characters of fixed size and format. Each character i preceded by a start bit and followed by 1-2 stop bits. Parity is often added to provide some limited protectio against errors occurring on the link. The use of independent transmit and receive clocks constrains tranmis sion to relatively short characters (<8 bits) and moderate data rates (< 64 kbps, but typically lower). Th asynchronous transmitter delimits each character by a start sequence and a stop sequence. The start bit (0) data (usually 8 bits plus parity) and stop bit(s) (1) are transmitted using a shift register clocked at the nomina data rate.

+2

(ii) Synchonous Transmission

In the synchronous transmisison, the receiver uses a clock which is synchronised to the transmitter clock. Th clock may be transferred by either:

A separate interface circuit (as in X.21 or RS-449) or
Encoded in the data (e.g. Manchester Encoding, AMI encoding, HDB3 encoding)

An encoded clock is used in systems such as G.703, and Ethernet. Synchronous transmission has the advan tage that the timing information is accurately aligned to the received data, allowing operation at much highe data rates. It also has the advantage that the receiver tracks any clock drift which may arise (for instance due t temperature variation). The penalty is however a more complex interface design, and potentially a more diffi cult interface to configure (since there are many more interface options).

+2

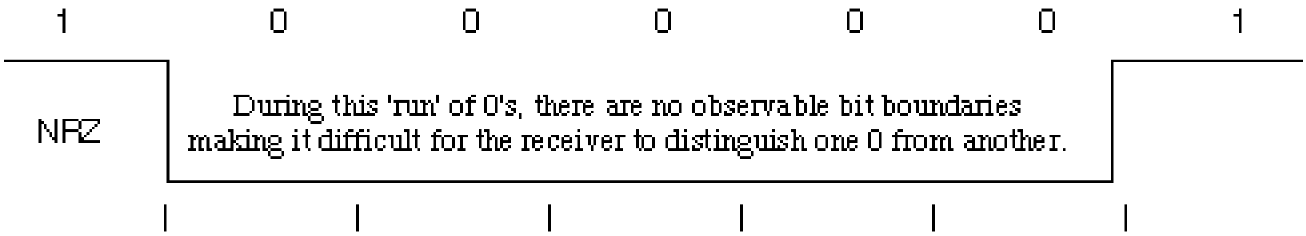
(iii) Non Return to Zero (NRZ)

Non-return to zero encoding is commonly used in slow speed communications interfaces for both synchro

Mark

nous and asynchronous transmission. Using NRZ, a logic 1 bit is sent as a high value and a logic 0 bit is sen as a low value (the line driver chip used to connect the cable may subsequently invert these signals).

In NRZ transmission, each data bit is represented by a level. A high level may represent a logic 1, where as low level may represent a logic 0. The term is derived from the earlier transmision technique of sending puls es to represent bits (called Return to Zero, RZ) in which a logic 1 is represented by a pulse and a logic 0 b the absence of a pulse. (AMI and HDB3 are technqiues derived from RZ). Manchester encoding uses a sti different scheme where a logic 1 is represnted by a transition in a particular direction (usually a rsising edge in the centre of each bit. A transitition in the opposite direction (downward in this case) is used to represent logic 0.



+2

(iv) Encoded Clock

Systems such as Manchester Encoding, AMI, HDB3 do not need a seperate clock circuit to synhronise th transmit and receive clocks. Instead the data is encoded prior to transmission. The encoding is desigend to in troduce sufficient edges in the bit stream to ensure that a DPLL may successfully recover the phase and fre quency of teh clock - even when the data contains long runs of 0's and 1's which may otherwise give rise t very few clock edges. An encoded clock saves one communications circuit.

+2

=8

[8 marks]

(c) Compare the properties of Alternate Mark Inversion (AMI) and Manchester encoding. [4 marks]

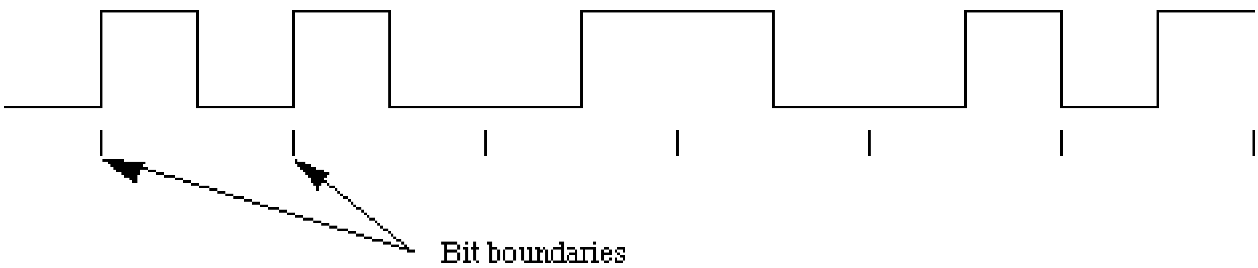
AMI (Alternate Mark Inversion) is a synchronous clock encoding technique which uses bipolar pulses to rep resent logical 1 values. It is therefore a three level system. A logical 0 is represented by no symbol, and a log ical 1 by pulses of alternating polarity. The alternating coding prevents the build-up of a d.c. voltage leve down the cable. This is considered an advantage since the cable may be used to carry a small d.c. current t power intermediate equipment such as line repeaters.

AMI coding was used extensively in first generation PCM networks, but suffers the drawback that a long ru of 0's produces no transitions in the data stream (and therefore does not contain sufficient transitions to guar antee lock of a DPLL). Successful transmission theerfore relies on the user not wishing to send long runs o 0's and this type of encoding is not therefore transparent to the sequence of bits being sent.

E.G. The pattern of bits " 1 0 0 0 0 1 1 0 " encodes to " + 0 0 0 0 - + "

In the Manchester encoding shown, a logic 1 is indicated by a 0 to 1 transition at the centre of the bit and logic 0 is indicated by a 1 to 0 transition at the centre of the bit. Note that signal transitions do not always oc cur at the 'bit boundaries' (the division between one bit and another), but that there is always a transition a the centre of each bit. (N.B. since most line driver electronics actually invertts the bits prior to tranmission you may observe the opposite coding on an oscilloscope connected to a cable).
A Manchester encoded signal contains frequent level transitions which allow the receiver to extract the cloc signal using a Digital Phase Locked Loop (DPLL) and correctly decode the value and timing of each bit. T allow reliable operation using a DPLL, the transmitted bit stream must contain a high density of bit trans

Mark tions. Manchester encoding ensures this, allowing the receiving DPLL to correctly extract the clock signal. Manchester encoding is used as the physical layer of an Ethernet LAN.



4 The waveform for a Manchester encoded bit stream carrying the sequence of bits 0010115

(d) Plot the waveform which you would observe on an oscilloscope when a byte wit the hexadecimal value of 0x57 is transmitted along an Ethernet coaxial cable. [4 marks]

The following points are to remembered:

+1 1) Bit reversal - the lsb of each byte is sent first. (01010111 becomes 11101010)

+1 2) Each bit is encoded at 10 Mbps (i.e. one bit period is 0.1 microseconds)

+1 3) Each bit is encoded (1 -> 0,1 and 0 -> 1,0)

+1 4) The bits are inverted prior to transmission (1 -> 0 and 0 -> 1)

=4

Mark

3. (a) An HDLC link may provide either a best effort or a reliable transmission service. In this context define what is meant by Best Effort and Reliable. [6 marks]

Reliable delivery has been succinctly defined as "Data is accepted at one end of a link in the same order as wa transmitted at the other end, without loss and without duplicates." This implies four constraints:

(i) No loss (at least one copy of each frame is sent)
(ii) No duplication (no more than one copy is sent)
(iii) FIFO delivery (the frames are forwarded in the original order)
(iv) A frame must be delivered within a reasonable period

For a communications protocol to support reliability, requires that the protocol numbers the PDUs that ar transmitted, implements an error recovery procedure (e.g. checkpointing or go-back-N), and provides error free procedures for link management.

There is very little data which is so important that it must be sent no matter how late. Layered protocols usual ly also employ timers at each level, governing this interval. The service provided by a protocol layer may b unreliable for various reasons including:

(i) Corruption of bits within the physical medium or the interface to the physical media.
(ii) Faulty bit-timing resulting in erroneous decoding of the value of a received bit.
(iii) A software error within the software used to implement the communications protocol.
(iv) Insufficient buffer space within the communications equipment.

A "Best Effort" service is one which does not provide full reliability. It usually performs some error control (e.g. discarding all frames which may have been corrupted) and may also provided some (limited) retransmis sion (e.g. CSMA/CD). The delivered data is not however guarenteed. A best effort service, normally require reliability to be provided by a higher layer protocol. An example of best effort services is:
Conenction-less Data Link Layer - HDLC (UI frames).

6

(b) What type of link service is required to support a network which uses the Interne Protocol (IP)? [1 mark]

A connection-less, such as the UNIT DATA service provided by HDLC using "UI" frames. A standard us ing this service is defined by the IP suite and is known as the "Point-to-Point Protocol (PPP)
1 (IP is itself a best effort service).

(c) Provide a detailed description of Stop and Wait Recovery. Your answer should in clude a frame transition diagram showing two cases: normal operation, and recovery fol lowing a transmission error. [8 marks]

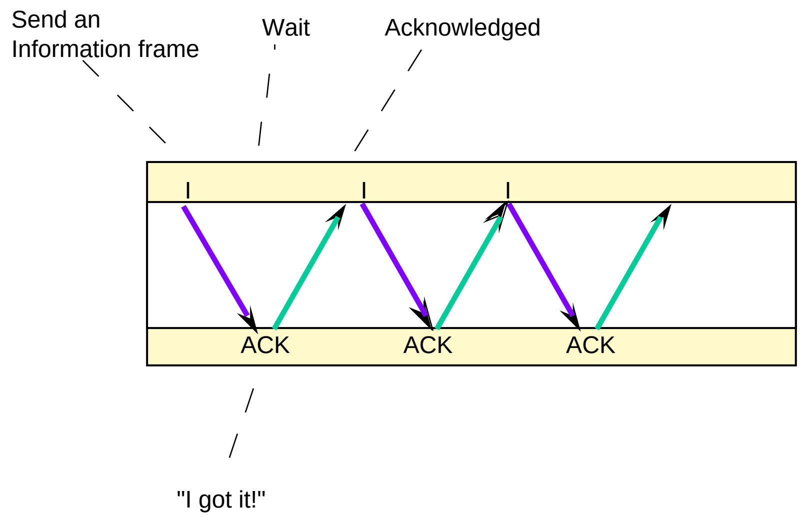
Stop and Wait transmission is the simplest reliability technique and is adequate for a very simple communi cations protocol. A stop and wait protocol transmits a PDU of information and then waits for a response. The receiver receives each PDU and sends an Acknowledgement (ACK) PDU if thedata was receievd correct ly, and a Negative Acknowledgement (NACK) PDU if the data was not received. In practice, the receive may not be able to reliably identify whether a PDU has been received, and the transmitter will usually als need to implement a tiemr to recover from the condition where the receiver does not respond.

Under normal transmisison the sender will receive an ACK for the data and tehn commence transmission o the next data block. For a long delay link, the sender may haveto wait an appreciable time for this response While it is waiting the sender is said to be in the "idle" state and is unable to send further data.

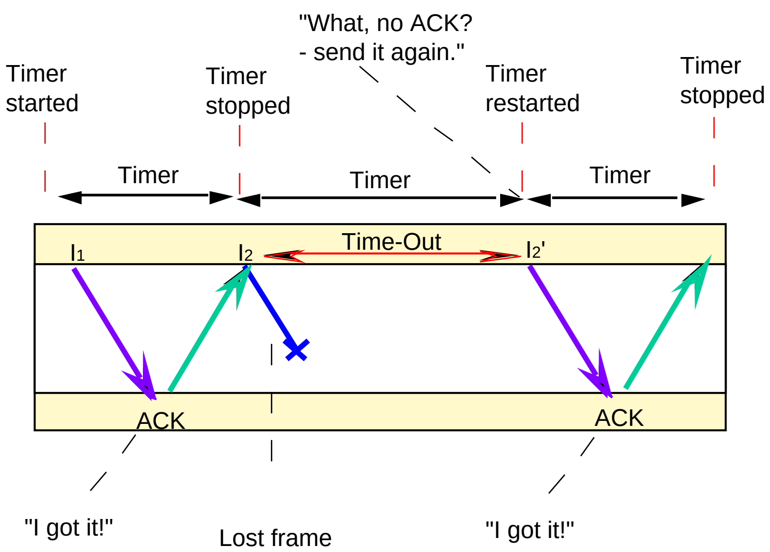
When PDUs are lost, the receiver will not normally be able to identify the loss (it does not receive anything) The transmitter must then rely upon a timer to detect the lack of a response. In the case where a receiver i able to accurately identify that corrupted data has been received, it may generate a NACK to indicate this to th sender (this pre-empts the timer expiry and triggers immediate retransmission.

Question Number	3	Solution	Page of 12

Mark



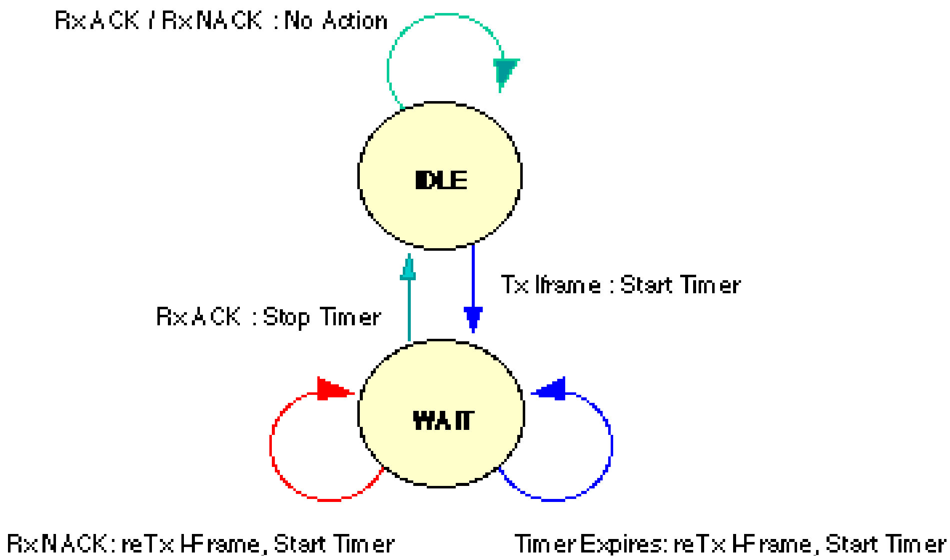
The blue arrows show the sequenc of data PDUs being sent across th link from the sender (top to the re ceiver (bottom). A Stop and Wa protocol relies on two way transmis sion (full duplex or half duplex) to al low the receiver at the remote node t return PDUs acknowledging the suc cessful transmission. The acknowl edgements are shown in green in th diagram, and flow back to the orig nal sender. A small processing dela may be introduced between receptio of the last byte of a Data PDU an generation of the correspondin ACK.



In the diagram, the second PDU c Data is corrupted during transmis sion. The receiver discards the co rupted data (by noting that it is fol lowed by an invalid data checksum) The sender is unaware of this loss but starts a timer after sending eac PDU. Normally an ACK PDU is re ceived before this the timer expires In this case no ACK is received, an the timer counts down to zero an triggers retransmission of the sam PDU by the sender. The sender al ways starts a timer following trans mission, but in the second transmis sion receives an ACK PDU befor the timer expires, finally indicatin that the data has now been receive by the remote node.

The state diagram (als showing the operation c NACK) is shown :

Green for ACK, Blu for Data, Red for NACI



8

Question Number	3	Solution	Page of 12

Mark

(d) How does HDLC overcome a fundamental limitation of stop and wait error recover when used over a link with a higher delay bandwidth product? [5 marks]

Sequence Numbers &Windows

Two sequence numbers are employed by HDLC when providing a reliable data link service. One sequenc number, the send sequence number (N(S)) records the number of each PDU sent. Another sequence numbe returns an acknowledgment confirming correct delivery of data to the receiver. This is the receive sequenc number (N(R)).

The send sequence number

The send sequence number is the number (in the specified modulus) of the current I-frame being sent by th local node. Each transmitted I-frame is numbered in succession with a sequence number. This is implemente by copying the send state variable, V(S), into the send sequence number, N(S), in the frame. After a frame i transmitted the send state variable is incremented. The N(S) in retransmitted frames are not changed (i.e. th original N(S) value is sent in the retransmitted frame).

The receive sequence number

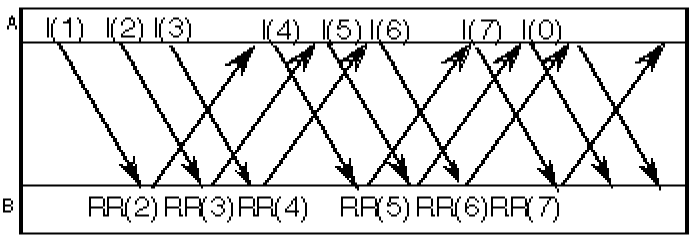
The receive sequence number is the number (in the same modulus) of the next I-frame expected by the node a the remote end of the link. For a link with no errors, the N(R) of the next frame sent by the remote nod should be one more than the N(S) of the last frame received by the node. The N(R) value is equal to the re mote node's receive sequence variable, V(R). Since the reception of a valid in-sequence I-frame causes the V (R) value to be assigned one plus the last N(S) value, the received N(S) value is one greater than the sent N (R) value. This process is known as "acknowledgement" and indicates to the local node that the remote nod has correctly received all I-frames sent with a N(S) sequence number less than the received N(R) value.

Windows

Many protocols need to number the PDUs which are sent by the protocol in order to provide a reliable ser vice. Usually this numbering is performed by including sequence numbers in the Protocol Control Informa tion (PCI) (i.e. the PDU header). The sequence numbers are normally stored using modulo-n arithmetic al lowing the same set of numbers to be used time after time. A technique known as a "window" is used t ensure that the same sequence number is never used by two frames at any one time.

Example of the use of a Window in HDLC

An HDLC link (operating in the ABM mode) connecting two equipments A and B is operated with a windov (k) of 3 frames. Part of the transmission is shown in the frame transition diagram below. This diagram will b used to explain the terms modulus and window size.



The window specifies the maximum number c frames which may be transmitted without receiv ing an acknowledgment. The current window i defined as the number of frames which may b sent at the current time, this is always less than o equal to the link window size. the diagram abov shows a window size of 3 frames. This results i a pause in transmission after sending the thir frame, until the first frame has been acknowledge by the remote node (B). The window size also de fines the amount of buffering required at the senc ing node (A) to hold one copy of each fram which is unacknowledged.

5

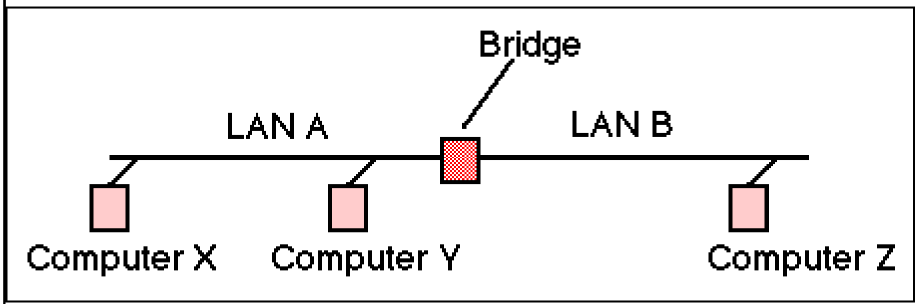
Question Number	4	Solution	Page of 12

Mark

4. (a) Explain in detail the operation of an Ethernet bridge when used to connect tw Ethernet LAN segments. [6 marks]

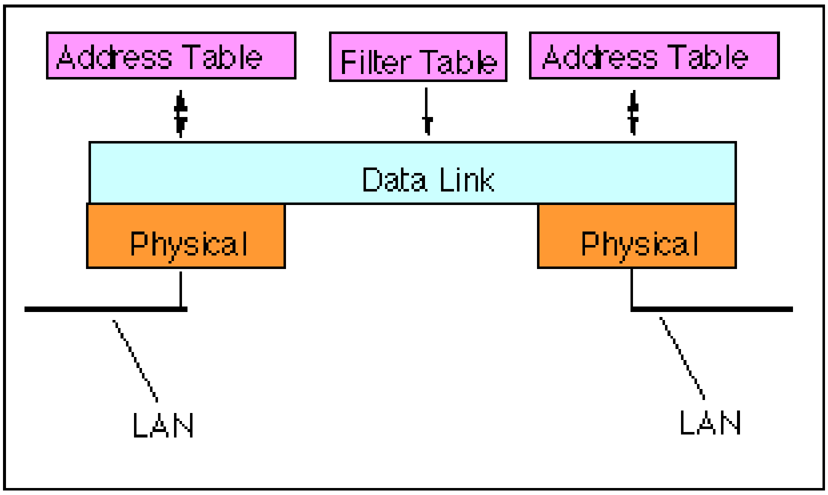
A bridge is a LAN interconnection device which operates ta the data link layer (layer 2) of the OSI referenc model. It may be used to join two LAN segments (A,B), constructing a larger LAN. A bridge is able to filte traffic passing between the two LANs and may enforce a security policy separating different work groups lo cated on each of the LANs.
The format of PDUs at this layer in a LAN is defined by the Ethernet frame format (also known as MAC Medium Access Control). It consists of two 6 byte addresses and a one byte protocol ID / length field. Th address field allows a frame to be sent to single and groups of stations. The MAC protocol is responsible fo access to the medium and for the diagnosis of failure in either the

A bridge connecting two LAN segments (A and B).



The bridge learns (by observing th feaders of Ethernet frames) whic MAC addresses belong to the com puters on each conected subnetwor by observing the source address va ues which originate on each side o the bridge. This is called "learning' In the figure in the question, th source addresses X,Y are observe to be on network A, while the ad dress of computer Z will be observe to be on network B.

A bridge stores the hardware addresses observed from frames received by each interface and uses this infor mation to learn which frames need to be forwarded by the bridge. Packets with a source of X and destinatio of Y are received and discarded, since the computer Y is directly connected to the LAN A, whereas packet from X with a destiantion of Z are forwarded to network B by the bridge



The learned addresses are stored in the corresponding interface address table. Once this table has been setup the bridge examines the destination address of all frames, and forwards them only if the address does not co respond to the source address of a computer on the local subnetwork.

A system administrator may overide the normal forwarding by inserting entries in a filter table to inihibit fo warding between different workgroups (for example to provide security). The filter table contains a list o source or destination addresses. Frames which match entries in the filter table will not be forwarded unde any circumstances.

6

Question Number	4	Solution	Page of 12

Mark

(b) Provide a description of the key differences between a 10BaseT hub, an Etherne Bridge, and an IP Router. Your answer should include appropriate diagrams and may in clude a table comparing the features provided by each equipment. [8 marks]

LAN Repeaters or Hubs – Join LAN segments (OSI Layer 1)

Very cheap
Regenerate the signal and timing information
Allow multiple types of media to be connected
Work below the MAC Layer (Support all protocols)
+3 Build one single LAN

Bridges – Separate work group traffic(form collision domains) (OSI Layer 2)

Cheap
Allow multiple types of media to be connected (also known as a “hub” or “switch”)
Work at the MAC Layer (Support all protocols)
May provide filtering to implement simple security policies
+3 Build one single IP network

Routers – Connect IP networks (OSI Layer 3)

More Expensive
Work at Network Layer (e.g. IP) and support one or more protocols
Connect separate networks into an internet
May protect networks from unauthorised access

+2 A router is most suited for the connection of a LAN to a MAN. The router allows two separately adminis tered networks to communicate without forming one homogenous network. The two networks may have dif ferent media, and belong to different IP networks (in the case of IP). The router also provides routing c packets to destinations reachable via the MAN and can control access to/from the MAN.

=8

(c) Ethernet supports Broadcast, Unicast and Multicast transmission modes, explain i detail what is meant by each term. Illustrate your answer by providing an example Medi um Access Control (MAC) address of each type. [6 marks]

Broadcast
Ethernet Defined Broadcast Destination Address = 01 00 00 00 00 (always)
1 to ALL
+2 All nodes receive the same PDU

Unicast
Sample Ethernet Unicast Destination Address = 08 00 20 01 62 f0 (i.e. unique address)
1 to 1 (point-to-point)
+2 One or more niodes may receive the same PDU at Layer 2, but only node with a unique (local) address matching the received destination forwards the received PDU to layer 3.

Multicast
Sample Ethernet Multicast Destination Address = 01 00 00 00 00 55 (Group 55)
1 to many (or many-to-many)
All nodes receive the PDU at Layer 2, but only nodes which "join" teh specified multicast group forward the PDU to Layer 3. A node may "register" or "join" none or more multicast groups
+2 and receive all PDUs which match any group.

=6

Question Number	5	Solution	Page of 12

Mark

5. (a) The following terms are used when describing the Internet Protocol. Define th following terms: [8 marks]

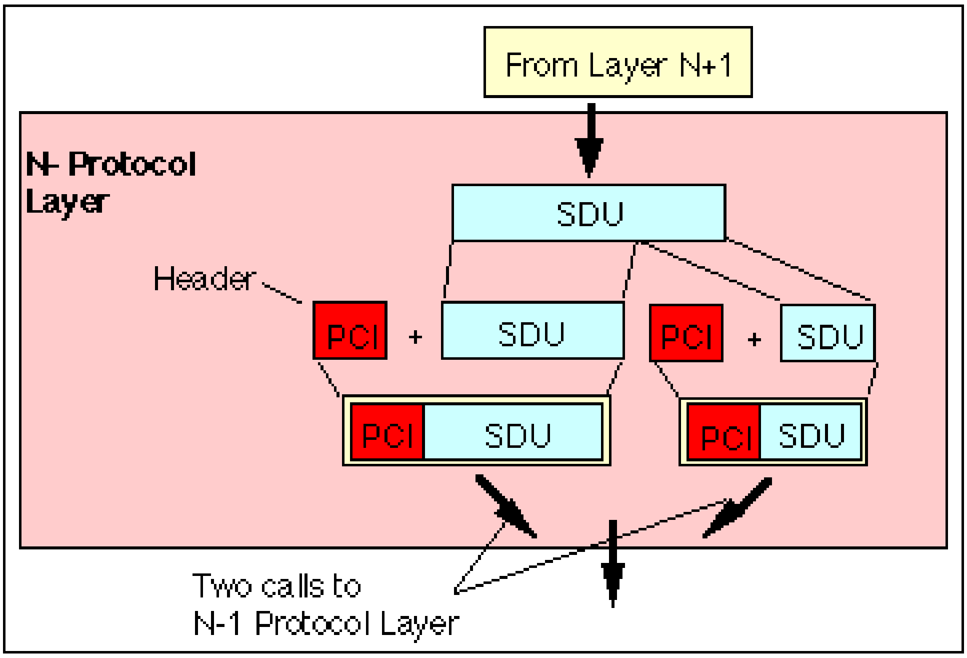
(i) Internet Protocol (IP) Address

An address is a data structure understood by a network which uniquely identifies the recipient within the net work. An IP address is a 32 bit value consisting of two parts, the network part (identifying the network t which the computer is attached) and the host part (which identifies the host within the local network). The I network address is identified as the bit-wise logical AND of the netmask and the 32-bit IP address.

+2

(ii)Fragmentation (or Segmentation)

Most communications protocols are specified using a layered architecture (e.g. using the OSI reference mod el). Each layer uses the service provided by the layer below. However, a layer is not always aware of th



maximum size of the packet payload (Service Dat aUnit (SDU)) which may be supported.

Encapsulation of a SDU by adding a PCI to form a PDU

In most cases packet networks limit the size of the maximum SDU at the network layer, but the actual maxi mum size will depend upon the network architecture which is being used. (LANs and MANs often allov comparatively large packets, whereas WANs often employ a much smaller maximum packet size). Man layers (e.g. the IP network protocol) therefore support a segmentation (also known as fragmentation) service which breaks large SDUs into a number of smaller SDUs. The corresponding peer protocol is responsible fc reassembling the complete SDU before forwarding to the layer above. The corresponding process of joinin together the received segments is known as "reassembly" and is performed by the receiver at the same protc col layer (i.e. peer-to-peer).

+2

(iii) Maximum Transmission Unit (MTU)

The maximum transfer unit is the largest size of IP datagram which may be transferred using a specific dat link connection The MTU value is a design parameter of a LAN and a mutually agreed value for most WAI links. The size of MTU may vary greatly between different links (from 128 B up to 10 kB) and is the reaso why fragmentation/segmentation is sometimes required by IP routers.

+2

Question Number	5	Solution	Page of 12

Mark

(iv) IP Router

A router is an Intermediate System (IS) which operates at the network layer of the OSI reference model. Rout ers may be used to connect two or more IP networks, or an IP network to an internet.

A router consists of a computer with at least two network interface cards supporting the IP protocol. The rout er receives packets from each interface and forwards the received packets to an appropriate output interface The router uses the IP address, along with routing information held within the router and stored in a routin table, to determine the destination for each packet. A filter table may also be used to ensure that unwante packets are discarded. The filter may be used to deny access to particular protocols or to prevent unauthorise access from remote computers.

Routers are often used to connect together networks which use different types of links (for instance an HDL(link connecting a WAN to a local Ethernet LAN). The optimum (and maximum) packet lengths (i.e. the Maxi mum Transfer Unit (MTU)) is different for different types of network. A router may therefore uses IP to pro
+2 vide segmentation of packets into a suitable size for transmission on a network.
=8

(b) The Address Resolution Protocol (ARP).is used when a local computer (with Mediur Access Control (MAC) address x) wishes to communicate with a remote computer (wit mac address y). Redraw the diagram above and provide notes to give a detailed explana tion of the operation of ARP. Ensure you decsribe the MAC addresses used in eac frame. [6 marks]

The address resolution protocol is a protocol used by the Internet Protocol (IP) network layer protocol to ma IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below th network layer as a part of the OSI link layer, and is used when IP is used over Ethernet.

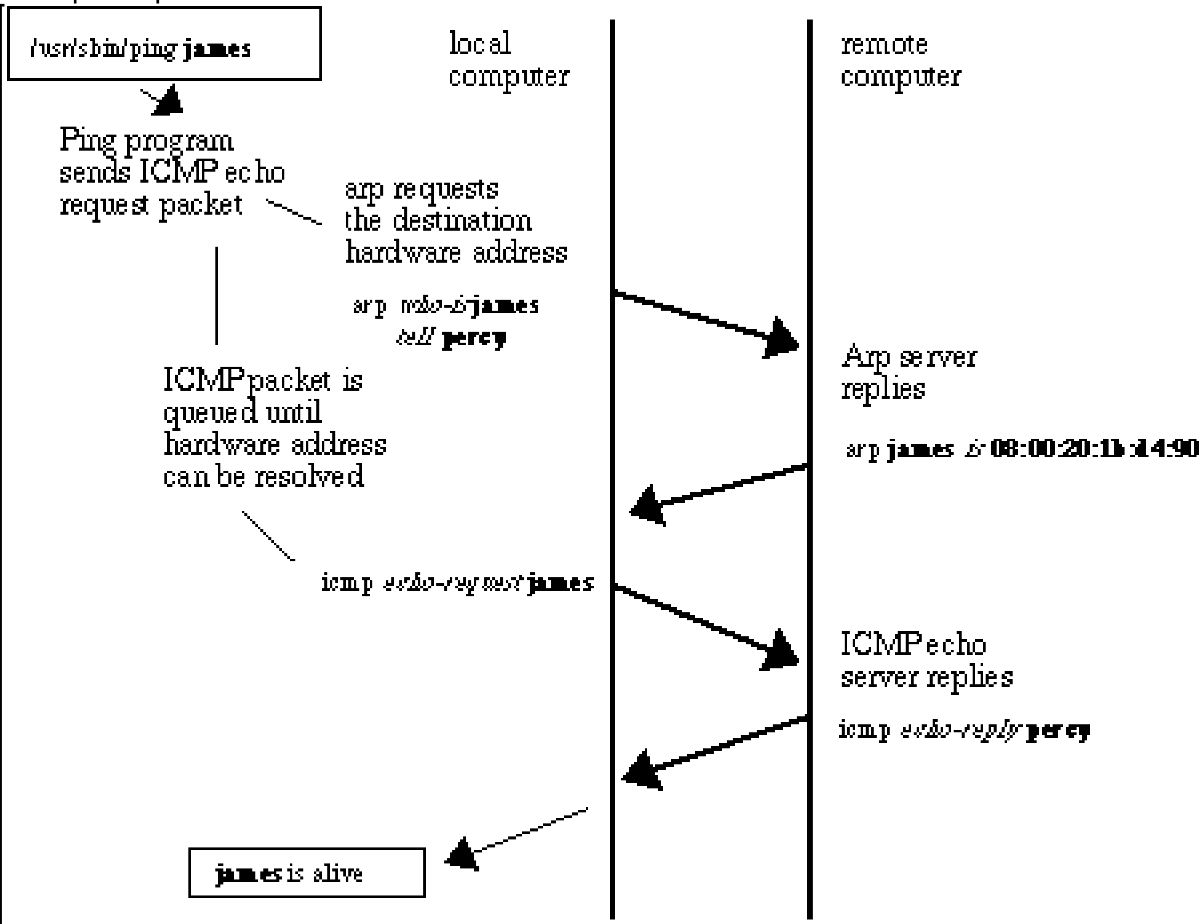
The term address resolution refers to the process of finding an address of a computer in a network. The ac dress is "resolved" using a protocol in which a piece of information is sent by a client process executing o the local computer to a server process executing on a remote computer. The information received by the serve allows the server to uniquely identify the network system for which the address was required and therefore t provide the required address. The address resolution procedure is completed when the client receives a re sponse from the server containing the required address.

An Ethernet network uses two hardware addresses which identify the source and destination of each fram sent by the Ethernet. The destination address (all 1's) may also identify a broadcast packet (to be sent to a connected computers) or a multicast packet (msb=1) (to be sent only to a selected group of computers). Th hardware address is also known as the Medium Access Control (MAC) address, in reference to the standard which define Ethernet. Each computer network interface card is allocated a globally unique 6 byte addres when the factory manufactures the card (stored in a PROM). This is the normal source address used by an ir terface. A computer sends all packets which it creates with its own hardware source address, and receives a packets which match its hardware address or the broadcast address. When configured to use multicast, a se lection of multicast hardware addresses may also be received.

The Ethernet address is a link layer address and is dependent on the interface card which is used. IP operate at the network layer and is not concerned with the network addresses of individual nodes which are to b used. A protocol known as address resolution protocol (arp) is therefore used to translate between the tw types of address. The arp client and server processes operate on all computers using IP over Ethernet. Th processes are normally implemented as part of the software driver which drives the network interface card.

Question Number	5	Solution	Page of 12

Mark



6

Frames:

MAC+ ARP request + CRC-32
src: percy-enet (x)
dst: Broadcast

MAC + ARP reply + CRC-32
src: james-enet (y)
dst: percy-enet (x)

MAC + IP + ICMP ECHO request + DATA + CRC-32
src: percy-enet (x)
dst: james-enet (y)

MAC + IP + ICMP ECHO reply + DATA + CRC-32
src: james-enet (y)
dst: percy-enet (x)

(c) Outline the protocol headers which are present in each of the four Ethernet frames and calculate the total size of each frame assuming the ICMP payload is 100 B. [6 marks]

MAC+ ARP request + CRC-32 = 14 + 28 + PAD + 4 = 64 B
MAC + ARP reply + CRC-32 = 14 + 28 + PAD + 4 = 64 B
Note minimum Ethernet PDU is 60 B (including MAC header, excluding CRC-32)
MAC + IP + ICMP ECHO request + DATA + CRC-32 = 14 + 20 + 8+ 100+ 4 = 146 B
MAC + IP + ICMP ECHO reply + DATA + CRC-32= 14 + 20 + 8+ 100+ 4 = 146 B
8 Byte preamble may be added in each case (no loss of marks for adding this).

6