# Session 2002-2003 Exam 1

# EG/ES 3567 Worked Solutions.

Please note that both exams have identical solutions, however the level of detail expected in ES is less, and the questions are phrased to provide more guidance on how to provide the solution.


Dr Gorry Fairhurst

G.Fairhurst@eng.abdn.ac.uk

Mark

**1. (a) Describe the operation of Message Switching and Packet Switching. [8 marks]**

In message switching, there is no need for a circuit to be established all the way from the source to the destination. This mode is used when a telex or email message is sent. The message first passes over a local connec). It is then passed at some later time to the next message switch, and from there to the destination (or another message switch on the way to the destination). At each message switch, the received message is stored, and a connection is subsequently made to deliver the message to the neighboring message switch. Message switching is also known as store-and-forward switching since the messages are stored at intermediate nodes en route to their destinations.

Since the message may be competing with other messages for access to facilities, a queuing delay may be incurred while waiting for the link to become available. The message is stored at B until the next link becomes available, with another queuing delay before it can be forwarded. It repeats this process until it reaches its destination. A delay for putting the message on the communications link (message length in bits divided by link speed in bps) is also incurred at each node en route. Message transmission time are slightly longer than they are in circuit switching, after establishment of the circuit, since header information must be included with each message; the header includes information identifying the destination as well as other types of information.

Although message switching is still used for electronic mail and telex transmission, it has largely been replaced by packet switching (in fact, most electronic mail is carried using message switching with the links between message switches provided by packet or circuit-switched networks).

Packet switching is similar to message switching using short messages. Any message exceeding a network-defined maximum length is broken up into shorter units, known as packets, for transmission; the packets, each with an associated header, are then transmitted individually through the network. The fundamental difference in packet communication is that the data is formed into packets with a pre-defined header format (i.e. PCI), and well-known "idle" patterns which are used to occupy the link when there is no data to be communicated.

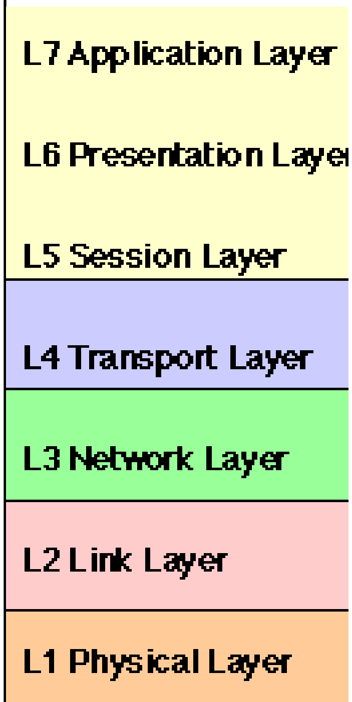
A packet network equipment discards the "idle" patterns between packets and processes the entire packet as one piece of data. The equipment examines the packet header information (PCI) and then either removes the header (in an end system) or forwards the packet to another system. If the out-going link is not available, then the packet is placed in a queue until the link becomes free. A packet network is formed by links which connect packet network equipment.

There are two important benefits from packet switching.

(i) The first and most important benefit is that since packets are short, the communication links between the nodes are only allocated to transferring a single message for a short period of time while transmitting each packet. Longer messages require a series of packets to be sent, but do not require the link to be dedicated between the transmission of each packet. The implication is that packets belonging to other messages may be sent between the packets of another message. This provides a much fairer sharing of the resources of each of the links.

(ii) Another benefit of packet switching is known as "pipelining". This simultaneous use of communications links represents a gain in efficiency, the total delay for transmission across a packet network may be considerably less than for message switching, despite the inclusion of a header in each packet rather than in each message.

8




**(b) Sketch a diagram showing each of the layers in the Open Systems Interconnection (OSI) Reference Model. Label each protocol layer in your diagram. [6 marks]**

*4 Marks for correct layering; 2 for detail in the diagram*

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 each "hop" across a link (i.e. by each System) and a suitable new header added each time the information is sent on a subsequent hop. The network layer (layer 3) operates network-wide and is present in all systems and responsible for overall co-ordination of all systems along the communications path.

The layers above layer 3 operate end-to-end and are only used in the End Systems (ES) which are communicating. The Layer 4 - 7 protocol control information is therefore unchanged by the IS in the network and is delivered to the corresponding ES in its original form. Layers 4-7 (if present) in Intermediate Systems (IS) play no part in the end-to-end communication.

6

**(c) What is the function of the Transport Layer in the OSI Reference Model [3 marks]**

The transport layer is the fourth layer of the OSI reference model. It provides transparent transfer of data between end systems using the services of the network layer (e.g. IP) below to move PDUs of data between the two communicating systems.

The transport service is said to perform "peer to peer" communication, with the remote (peer) transport entity. The data communicated by the transport layer is encapsulated in a transport layer PDU and sent in a network layer SDU. The network layer nodes (i.e. Intermediate Systems (IS)) transfer the transport PDU intact, without decoding or modifying the content of the PDU. In this way, only the peer transport entities actually communicate using the PDUs of the transport protocol.

This provides transparent transfer of data between systems, relieving upper layers from concern with providing reliable and cost effective data transfer; provides end-to-end control and information interchange with quality of service needed by the application program; first true end-to-end layer.

The transport layer relieves the upper layers from any concern with providing reliable and cost effective data transfer. It provides end-to-end control and information transfer with the quality of service needed by the application program. It is the first true end-to-end layer, implemented in all End Systems (ES).

3

**(d) A session uses the User Datagram Protocol (UDP). It sends a series of packets over an Ethernet LAN. The payload of each UDP packet has a size of 690 bytes. Determine the total size of the Ethernet frame using the information provided in the attached header chart. [3 marks]**

First determine theprotocol headers which contribute to the PDU size:

Preamble (8B) + MAC Header (14 B) + IP Header (20 B) + UDP (8 B) + UDP Payload (690 B) + CRC-32 (4 B)

8+14+20+8+690+4= <u>744 B (excluding the IFG)</u>

3

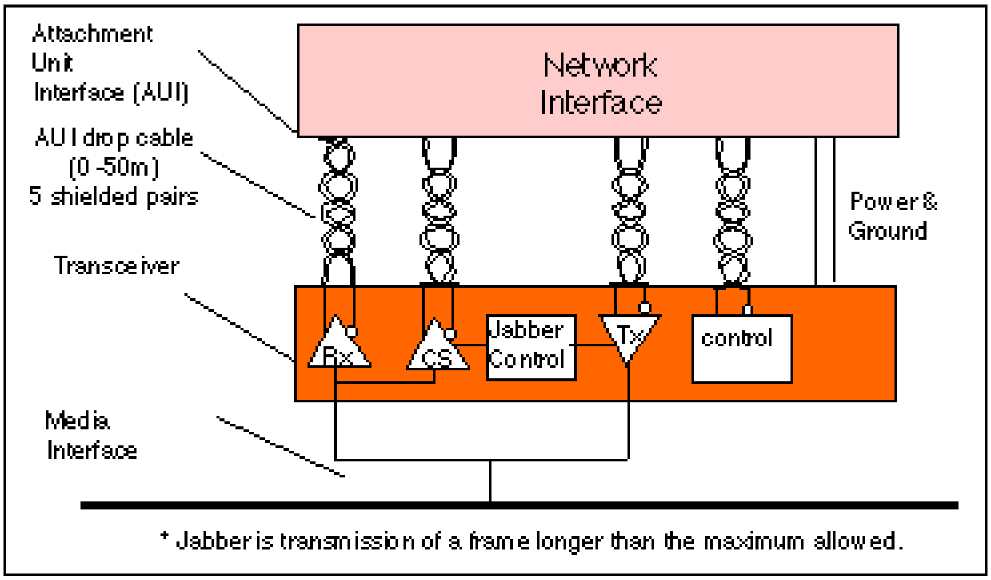
| Question Number | 1 | Solution | Page of 11 |
| --- | --- | --- | --- |

Mark

**2 (a) The Ethernet Local Area Network (LAN) uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to share the transmission medium. Define the following terms:**

**(i) Carrier Sense [4 marks]**

Ethernet uses a refinement of ALOHA, known as CSMA, which improves performance when there is a higher medium utilisation. When a node has data to transmit, the node first listens to the cable (using a transceiver) to see if a carrier (signal) is being transmitted by another node. This may be achieved by monitoring whether a current is flowing in the cable (each bit corresponds to 18-20 milliAmps (mA)). The Ethernet transceiver contains the electronics to perform this detection (labelled CS in the figure).



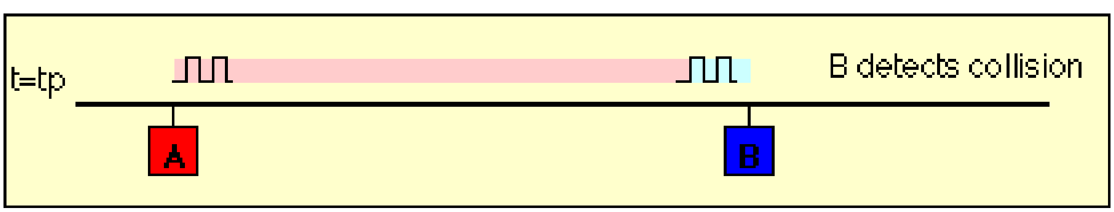

The individual bits are sent by encoding them with a 10 (or 100 MHz for fast Ethernet) clock using Manchester encoding. Data is only sent when no carrier is observed (i.e. no current present) and the physical medium is therefore idle.

However, this alone is unable to prevent two nodes transmitting at the same time. If two noes simultaneously try transmit, then both could see an idle physical medium (i.e. neither will see the other's carrier signal), and both will conclude that no other node is currently using the network. In this case, both will then decide to transmit and a collision will occur. The collision will result in the corruption of the data being sent, which will subsequently be discarded by the receiver since a corrupted Ethernet frame will not have a valid 32-bit MAC CRC at the end.

4

**(ii) Collision Detection [4 marks]**

A second element to the Ethernet access protocol is used to detect when a collision occurs. Each transmitting node monitors its own transmission, and if it observes a collision (i.e. excess current above what it is generating, i.e. > 24 mA) it stops transmission immediately and instead transmits a 32-bit jam sequence. The purpose of this sequence is to ensure that any other node which may currently be receiving this frame will receive the jam signal in place of the correct 32-bit MAC CRC, this causes the other receivers to discard the frame due to a CRC error.

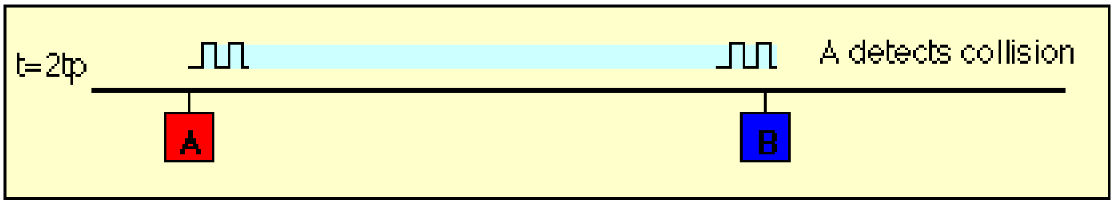



To ensure that no node may completely receive a frame before the transmitting node has finished sending it, Ethernet defines a minimum frame size (i.e. no frame may have less than 46 bytes of payload). The minimum frame size is related to the distance which the network spans, the type of media being used and the number of repeaters which the signal may have to pass through to reach the furthest part of the LAN. Together these de-

Mark

fine a value known as the Ethernet Slot Time.

When two or more transmitters each detect a corruption of their own data (i.e. a collision), each responds in the same way by transmitting the jam sequence. At time t=0, a frame is sent on the idle medium by computer A.




A short time later, computer B also transmits. (In this case, the medium, as observed by the computer at B happens to be idle too). After a period, equal to the propagation delay of the network, the computer B detects the other transmission from A, and is aware of a collision, but computer A has not yet observed that computer B was also transmitting. B continues to transmit, sending the Ethernet Jam sequence (32 bits).

After one complete round trip propagation time (twice the one way propagation delay), both computers are aware of the collision. B will shortly cease transmission of the Jam Sequence, however A will continue to
4 transmit a complete Jam Sequence. Finally the cable becomes idle.

**(iii) Collision Domain [4 marks]**

Traditional Ethernet uses a bus architecture in which all the computers connected to the cable share the capacity of the medium using CSMA/CD. In practice, most Ethernet networks employ hubs and repeaters, but these do not change thebasic rules of sharing. A network of repeaters and hubs is therefore called a "Shared Ethernet" or a "Collision Domain". The various systems sharing the Ethernet all compete for access using the CSMA/CD access protocol. This means that only one system is allowed to transmit within the Collision Domain at any one time. Each system has to share a proportion of the available network bandwidth.

4 Students should mention bridges/switches/routers separate collision domains. In contrast, the use of bridges, switches and routers separates each cable segment into an independent colission domain.

| Question Number | 1 | Solution | Page of 11 |
|---|---|---|---|

Mark

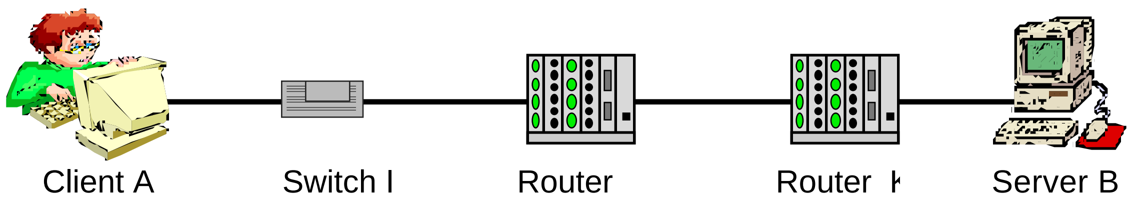



Figure 1: An Internet Path between two End Systems, A and B

**(b) The traceroute program may be used to determine an end-to-end Internet Path through a network. Explain (using appropriate diagrams) the set of packets that are exchanged when Client A uses traceroute to find the path to Server B. [8 marks]**

Traceroute uses ICMP echo messages. These are addressed to trhe target IP address. The sender manipulates the TTL (hop count) value at the IP layer to force each hop in turn to return an error message.

It starts with a TTL of 1, each router along the path decrements the TTL, and discards if zero, returning an ICMP message (which also indicated the router IP address of the router that discarded the message).

The switches pass each IP packet the un-modified.
The router J receives the packet with TTL=1 (it is on the path to B; It decrements the packet TTL.
This reduces to zero, the router generates an error message and returns this to the sender (A)

```
Client A ----ICMP echo src= W, dst=Z, TTL=1------> Router  J
                                                      |
ClientA <---ICMP error src= Y, dst=W, TTL=64----   Router J
```

The client receives the ICMP error message and notes that J is one hop away on the path to B.

It then probes by sending the same packet with a TTL of 2.
The router J receives the packet (it is on the path to B); It decrements the packet TTL
This is greater than zero, the router forwards this along the path to the destination.
The router K receives the packet (it is on the path to B); It decrements the packet TTL
This reduces to zero, the router generates an error message and returns this to the sender (A)

It then probes by sending the same packet with a TTL of 3.
The routers J and K receive the packet (on the path to B); The packet is then forwarded to B
This responds with an echo message and returns this to the sender (A)
Receipt of the response indicates that this has reached the final destination.

Summary:

ICMP Echo request message; TTL set to 1;

Router decrements TTL and discards; ICMP error message return (TTL exceeded);

sender repeats this uses larger TTL; Next hop returns ICMP message;

repeats; until final host accepts messgae and returns echo-response.

8 In this example TTL=3 is sucessful (i.e., only 2 routers)

| Question Number | 3 | Solution | Page of 11 |
|---|---|---|---|

Mark

**3. (a) In what cases may an IP Router not forward the packets it receives? [4 marks]**

The reasons an IP router may not forward packet may be divided into two types:

(i) Intended behaviour
- Routers may inetentionaly discard some types of packet.
Examples include:
  Packet with TTL=0
  Packet with IP header checksum error
  Packet with an illegal option or control field
  Packet for which there is no currently known destination (or to an illegal destination)
  Packets which match a filetr / firewall control list
  Packets sent to the router itself

(ii) Fault
- That is unintended discrad, following a fault or overload.
Examples include:
  Discard due to processing overload
  Discard due to corruption while being stored (queued) within a router
  Discard because there is no memory available to store the packet
  Software error
  Hardware or software reset.

0.5 mark for each valid answer, no marks for saying a link checksum error!

5

**(b) The Trivial File Transfer Protocol (TFTP) may be used to provide a reliable service. What guarantees must a reliable protocol must offer? [5 marks]**

Reliable delivery has been succinctly defined as "Data is accepted at one end of a link in the same order as was 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) No corruption of the content

A frame must also be delivered within a reasonable period.

5

**(d) An End System sends 5 packets per second using the User Datagram Protocol (UDP) over a full duplex 100 Mbps Ethernet LAN connection. Each packet consists 1500 bytes of Ethernet frame payload data. What is the throughput, when measured at the UDP layer? [8 marks]**

Frame Size = 1500B (Ether MAC headers are not included)

Packet has the following headers (see chart):
IP header (20B)
UDP header (8B)
Total header in each packet = 28 B

Total UDP payload data is therefore 1500-28 = 1472 B. (i.e. 1472 x 8 bits)

Throughput = Total bits sent per second = 1472 x 8 x 50 = 58880 bps

i.e. 58.8 kbps.

8

| Question Number | 4 | Solution | Page of 11 |
|---|---|---|---|

Mark

**(a) The End System C uses the Transmission Control Protocol (TCP) to send a packet to End System E with a payload of 100 bytes, sketch the Ethernet frame that is sent. Ensure your sketch shows the addresses at both the MAC and IP layers. [6 marks]**

Sketch a packet with the following headers

Preamble (8B)

Link: MAC Header (14 B)
  dst= E-mac address
  src = Router mac address <---2 Marks important detail
  type = 0x800 (IP)

  Network: IP Header (20 B)
    src = C IP address <--- IP header generatered by sender (C)
    dst = E IP address

    Transport: TCP Header (20 B)

    DATA (100 B)

Link CRC-32 (4B)

6

**(b) An Internet Protocol packet is broadcast by B. Which End Systems receive this? [2 marks]**

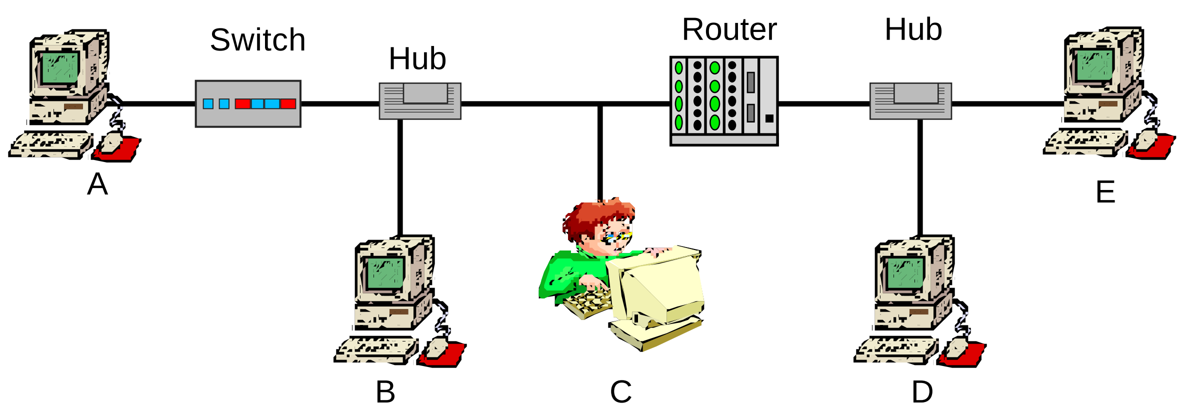
Hubs and switches are in the same broadcast domain

Routers separate broadcast domains

B is in the left broadcast domain
The frame is therefore received by A,B,C

The right broadcast domain does not receive the frame because the router does not forward it.
The frame is NOT received by D,E

2



| Question Number | | Solution | Page of 11 |
|---|---|---|---|

Mark

**(c) Outline the process of Path Maximum Transfer Unit (MTU) Discovery when End System A communicates with End System E in Figure 3. [4 marks]**

PMTU-D operates in the following way:

The sender transmits a packet with the largest possible header (1500B initial MTU) with the DF-bit set

Routers check the IP fragment size, if this exceeds the MTU of the next interface it discards the packet and sends an ICMP message (with size); Refragment (still DF set); Cache result for a sepcific route; Try again in 10 (or so) minutes (in case route changes)

A sends a maximum sized link frame (1500 B for Ethernet)
A sets theDon't Fragment boit in the IP header.

If Router has a lower MTU set, then router would be forced to fragment to the smaller MTU.
Instead router returns an ICMP error message indicating the smaller MTU value.

A receives the ICMP message, and caches this as the PATH MTU in a protocol table.

It starts a timer to reccheck-the PATH MTU of the route in the future.
While the timer is running it re-fragments this packet and all the following packets sent to the same IP address with the new size (from the protocol table).

4

**(d) Explain in detail the operation of Address Learning by an Ethernet Switch. Your answer should refer to the network shown in Figure 3. [8 marks]**

The switch is positioned between A and B,C.

Summary:
MAC Sources address observed for learning
Associated with a port in the address table
MAC Destination address observed for forwarding
Learned addreses -> forward only to specified port
Discard frames to own address (hence frames destined to A and sent by A are discarded)

Flood frames with unkonwn addresses to all ports
Aging is required and re-learning when computers change the port they are connected to

A bridge or switch (as it is now more commonly called) is a LAN interconnection device which may be used to join two LAN segments, constructing a larger LAN. A bridge is able to filter traffic passing between the two LANs and may enforce a security policy separating different work groups located on each of the LANs.

A bridge works within the data link layer (layer 2) of the OSI reference model. The format of PDUs at this layer in a LAN is defined by the Ethernet frame format (also known as MAC - Medium Access Control) consists of two 6 byte addresses and a one byte protocol ID / length field. The address field allows a frame to be sent to single and groups of stations. The MAC protocol is responsible for access to the medium and for the diagnosis of failure in either the hardware or the cabling.

The bridge learns which MAC addresses belong to the computers on each conected subnetwork by observing the source address values which originate on each side of the bridge. This is called "learning". 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 packet, and forwards them only if the address does not correspond 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 forwarding between different workgroups (for example to provide security).

8

| Question Number | 5 | Solution | Page of 11 |
|---|---|---|---|

Mark

*0800 2086 354B 00E0 F726 3FE9 0800 4500*
*0028 AAFE 0000 FC06 3A55* ***8A84 E902*** *8B85*
*D96E 0017 9005 9431 1028 7214 F131 5010*
*2238 1C64 0000 0000 0010 0000*

Figure 4: Hexadecimal dump of the Header of a Packet received on an Ethernet interface

**(a) Assuming the frame contains a Medium Access Control (MAC) header and an IP payload, use the supplied information about the packet header formats to determine the IP Source Address of the packet shown in Figure 4. [4 marks]**
**Decode of the Packet**

ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 9 arrived at 17:37:31.08
ETHER: Packet size = 60 bytes
ETHER: Destination = 8:0:20:86:35:4b, Sun
ETHER: Source = 0:e0:f7:26:3f:e9, CISCO Router
ETHER: Ethertype = 0800 (IP) <------------------- required in answer (b)
ETHER:
IP: ----- IP Header -----
IP:
IP: Version = 4
IP: Header length = 20 bytes
IP: Type of service = 0x00 (normal)
IP: Total length = 40 bytes
IP: Identification = 43774
IP: Flags = 0x0
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 252 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 3f56
IP: Source address = 138.132.233.2, server.abdn.ac.uk <------------------- required in answer (a)
IP: Destination address = 139.133.217.110, client
IP: No options

4 **(b) What is the value of the Ethernet Frame Type in the frame shown in Figure 4. Your answer must also describe the use of this value by the system that receives this frame. [4 marks]**

Ethertype = <u>0800 (IP)</u>

This is a service access point at thelink layer (SAP).
This is used by the receiver to <u>identify the type of payload being transported</u>, and hence thenetwork layert interface to which the received packet is to be passed. Some protocols which rely on this value are:

(i) IP - the network layer protocol of the Internet
(ii) arp - the address resolution protocol.

(IPv6 is another example, but not covered by the course)

4

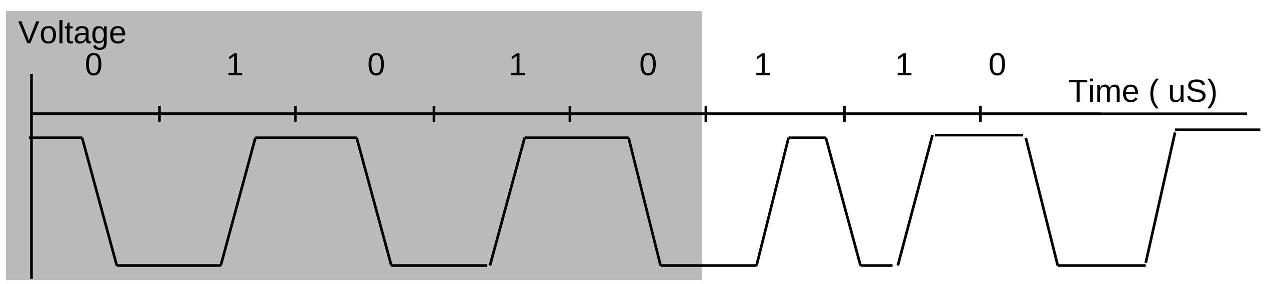
| Question Number | 5 | Solution | Page of 11 |
|---|---|---|---|

Mark

**(c) Explain what is meant by the term "Preamble" used by 10 Mbps Ethernet. [6 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.




6

**(d) Figure 5: Waveform recorded on a coaxial Ethernet cable**

**The waveform in Figure 5 shows the start of a Manchester encoded Ethernet frame. How many bits before the Start of Frame Delimiter (SFD) are shown in this Figure? [4 marks]**

Students must correctly decode the manchester encoded data, noting:

Manchester encoding follows the rules shown below:

| Original | Data | Value Sent |
|---|---|---|
| Logic 0 | 0 to 1 | (upward transition at bit centre) |
| Logic 1 | 1 to 0 | (downward transition at bit centre) |

Preamble consists of 101010 sequence followed by the SFD, with a pattern 11.

There are therefore 5 bits of preamble prior to the SFD.

4

**(e) Ethernet LANs traditionally used copper cable. Name two other media that may be used. [2 marks]**

Two examples which are common are:
(i) Fibre Optic Cables (802.3)
(ii) Radio Links at 2.4 GHz (802.11)

(802.11 also supports other media including Infra-Red (IR)).

2