THE BCS PROFESSIONAL EXAMINATIONS
Diploma

April 2006

EXAMINERS' REPORT

Computer Networks

General

The overall performance in this examination has significantly increased with the total pass rate a shade above 60%. Questions 2, 3, 4 and 6 were favourites and question 4 was attempted by over 87% of the students. There were good discussions and some answers were of high quality. However, it is highly recommended that students should read the questions well before answering them as answers to parts of questions 4 and 6 demonstrate that this was not done.

Question 1

1. By considering any data-link layer communications protocol based on HDLC that uses a sliding window error recovery mechanism, explain the function of the following:

i) The response window size (W)
ii) The send sequence number N(S) contained within each Information (I) PDU
iii) The Poll/Final bit (P/F)
iv) A Receive Ready (RR) PDU
v) A Receive Not Ready (RNR) PDU **(5 x 5 marks)**

Answer Pointers

i) the response window defines the maximum number of frames that can be transmitted without having received an acknowledgement. Once this limit is reached then no more frames may be transmitted until at least one of these frames is acknowledged or a re-transmission requested.

(3 marks for noting that it defines the maximum number of frames that can be transmitted without an acknowledgement; 2 marks for noting that once the limit is reached, no more frames can be sent).

ii) Each information I-PDU (I-PDU) must be uniquely identified to enable a receiver to request a specific packet to be re-transmitted or for a receiver to detect a loss of a packet. The send sequence number N(S) therefore provides this identification. It is an integer number that increments by one with each I-PDU sent. This number has a fixed number of bits and so wraps around to zero when the maximum limit is reached.

(2 marks for noting that N(S) uniquely identifies each I-PDU; 1 mark for noting that it wraps to 0; 2 marks for the reasons why each I-PDU needs to be uniquely numbered).

iii) The Poll/Final bit forces a receiver to generate a response. Any PDU received with the P/F bit set to 1 requires the received to issues a response which will also have the P/F bit set to 1. An example of when this is used is when a sender wishes to send fewer I-PDUs than the response window. The last I-PDU would have the P/F bit set to force the receiver to issue an acknowledgement.

(3 marks for knowing that if the P/F bit is set to 1 then the receiver must generate a response; 2 marks for an example of its use).

iv) A receive Ready PDU would be issued by a receiver to acknowledge receipt of I-PDUs from a sender. The RR PDU contains only a receive sequence number N(R) and P/F bit. The value of N(R) indicates the sequence number of the next I-PDU to be received, in other words all PDUs up to and including N(R) -1 have been received without error. The RR-PDU contains no user data. It also indicates to the sender that the receiver remains able to receive further I-PDUs.

(3 marks for noting how the RR PDU provides a positive acknowledgement to the sender;1 mark for noting that the RR contains no data; 1 mark for noting that the RR allows the sender to send more I-PDUs).

v) A receive not ready PDU would be issued by a receiver to acknowledge receipt of I-PDUs from a sender and at the same time to force the sender to stop transmitting I-PDUs. The RR PDU contains only a receive sequence number N(R) and P/F bit. The value of N(R) indicates the sequence number of the next I-PDU to be received; in other words all PDUs up to and including N(R)-1 have been received without error. The RR PDU contains no user data. On receiving an RNR PDU a sender must stop transmitting until an RR PDU is received.

(3 marks for noting how the RNR PDU provides a positive acknowledgement to the sender; 2 marks for noting that the RNR forces the sender to stop transmitting).

Examiner's Comments

Question 1 says: "By considering any data-link layer communications protocol based on HDLC that uses a sliding window error recovery mechanism, explain the function of the following...." None of the students actually did specify which protocol based on HDLC they were actually considering, but I did not take marks off for that.

i) the response window size - in general the students had understood the concept and function of a window

ii) the send sequence number N(S) contained within each Information (I) PDU - the answers were better on the whole if the students kept things short. The students who responded at greater length tended to show confusions between the use of sequence numbers in HDLC and TCP.

iii) The Poll/Final bit (P/F) - this was not accomplished very well. But the concepts are a little difficult, so that is not surprising.

iv) A Receive Ready (RR) PDU - this was more straightforward and the students scored well on this.

v) A Receive Not Ready (RNR) PDU – this was also straightforward and the students scored well on this.

Overall not many students attempted this question, but those that did scored reasonable marks, on the whole.

Question 2

2. *a)* With reference to IP addressing, what is the purpose of a subnet mask? **(5 marks)**

b) An organisation has been assigned a Class C IP address (200.253.67.0) for its local area network (LAN). If the network administrator has assigned a subnet mask of 255.255.255.240, how many sub-networks have been defined? **(8 marks)**

c) Two computers on this LAN wish to communicate with each other. If they know each other's IP address, explain how the Address Resolution Protocol (ARP) is used to allow them to obtain each other's MAC addresses. **(12 marks)**

Answer Pointers

a) the subnet mask provides a means by which the hosted part of an IP address can be further subdivided. A number of high order bits from this field can be assigned as a subnet identifier, the remaining bits continuing to identify individual hosts within each subnet. In order to determine how many of the hosted bits have been used for subnet addressing, the subnet mask has its bits set to one for the netid and subnet id parts of the IP address and zero for the hosted part. A logical AND of the subnet mask and IP address will reveal the subnet address.

(2 marks for the purpose of the subnet mask (subdividing the hosted field of an IP address); 2 marks for noting that the high order bits of the hosted field are used for subnet addressing; and 1 mark for knowing that a logical AND is performed between the IP address and subnet mask to reveal the subnet address).

b) Class C address assigns 24 bits to the netid and 8 bits to the hostid.
The subnet mask is:

255.255.255.192 = 11111111 11111111 11111111 11110000

Note that the three high order bits of the fourth octet are set to one. These bits are within the hosted field of the address and therefore these three bits are used for subnet addressing.

Four bits allow for 16 unique combinations and therefore 16 sub-networks can be supported on this system.

(4 marks for noting that three bits of the hosted field are used for subnet addressing; 4 marks for recognising that this allows for 16 sub-networks to be assigned).

c) Consider two computers – X and Y. We know that X and Y know each other's IP addresses but in order to send a LAN frame then they need to know each other's MAC address as well. The MAC address is needed for the LAN frame and the IP address for the IP datagram.

If X knows the Y's IP address then it can find its MAC address by using ARP in the following way:

X will issue an ARP request. This will be carried in a LAN frame with the destination address set to broadcast. The data field of this LAN frame will contain the ARP request PDU. This PDU contains the IP address of Y, the IP address of X, the MAC address of X and a blank field to indicate the MAC address of Y is required.

All devices on the LAN will receive this ARP request (MAC broadcast). They will each examine the ARP PDU and check the destination IP address. Only the device that has that address will respond. In this case it is Y and Y has now learned the MAC address of X.

Y will therefore now issue an ARP reply. This will be transported within a LAN fame that has a destination address equal to the MAC address of X and an ARP reply PDU in the data field. This PDU will contain all of the addresses that were in the original ARP request, however Y will add its own AC address into the blank address.

On receipt of the ARP reply, X has discovered the MAC address of Y.

(ARP request: 4 marks for noting that it is sent with the MAC destination set to broadcast; 4 marks for the fields within the ARP request PDU. ARP reply: 4 marks for the field within the ARP reply PDU).

Examiner's Comments

a) There are two possible ways of explaining the purpose of a subnet mask – either to stress the administrative reasons for sub-netting (simplification of administration, reduction of traffic etc.), or to give the technical role of the subnet mask (to divide the IP address into netid and hostid). Marks were given for either approach.

b) Some students had rather strange notions of how to calculate the number of sub-networks given the IP address and the subnet mask. But those who had the right general idea tended to do well. If the students did the binary arithmetic correctly (giving 1111000 as the binary form of 240), but did not understand the final calculation of the number of subnets, then 4 out of 8 marks were given. Either 14 or 16 were allowed as the number of subnets, since the loss of two subnets can be overcome by modern systems.

c) Again, some students did not understand how the Address Resolution Protocol worked, but those who did scored quite well on the question.

A lot of students did this question, and generally did well.

Question 3

3. *a)* A computer network operates using IP as its Network Layer protocol. Explain how the quality of service offered by IP is enhanced by the following Transport Layer protocols:

i) UDP
ii) TCP **(8 marks)**

b) If a server supports more than one application, explain how UDP/TCP port numbers can be used to multiplex these applications over IP. **(7 marks)**

c) Explain how TCP is able to ensure the reliable transfer of data between computers such that any errors that occur during transmission are corrected. **(10 marks)**

Answer Pointers

a) The quality of service offered by IP is a connectionless, unacknowledged, unreliable service.

UDP enhances this service by adding:

- Application multiplexing using port numbers only

TCP enhances this service by adding:

- A connection orientated service
- Reliable data transfer through error detection and correction
- Flow control
- Congestion control

- Application multiplexing using port numbers

(2 marks for summarising the quality of service offered by IP; 1 mark for noting that UDP only adds application multiplexing; 5 marks for identifying the features provided by TCP.

b) the server has only one IP address. Hence it is important to be able to differentiate which IP datagram is intended for which application.

UDP/TCP port numbers allow for multiplexing at the Transport layer. These port numbers are 16 bit numbers and each PDU contains both a source port and destination port number. In this way, port numbers are the equivalent of a source and destination address at the Transport layer.

Hence each application is assigned a unique port number within the server – call these P1 and P2. When a PDU is received the port number is checked. Those with a destination number P1 will be directed to application 1 and those with a destination port numbers of P2 will be directed to application 2 and so on.

(4 marks for the format of the port number and knowing that destination and source port number are carried in each UDP/TCP PDU; 5 marks for explaining how port number can be used to distinguish traffic flow to two applications).

c) The key field used to manage reliable data transfer within a TCP PDU header are: sequence number; acknowledgement number; ACK bit.

Each octet transmitted with a TCP data stream is uniquely numbered. The sequence number is a 32 bit integer that increments by 1 for each octet within the wrapping to zero when its maximum value is reached.

A positive acknowledgement is indicated by virtue of the fact that the ACK bit is set and then the acknowledgement number will indicate the number of the first non-acknowledgement octet. In other words all octets up to and including acknowledgement number -1 have been received.

TCP does not contain a message for negative acknowledgement or re-transmission request. If a TCP PDU is lost or received in error then the receiver ignores it and consequently does not issue an acknowledgement. The transmitter maintains a timer and if an octet has not been **a**cknowledged within a given time then it is simply re-transmitted. It is up to the receiver to ignore any duplicates which result from the process.

(2 marks for identifying the relevant fields within the TCP header; 2 marks for the octet numbering scheme; 2 marks for the octet numbering scheme; 3 marks for positive acknowledgement; 3 marks for detecting errors).

Examiner's Comments

a) A lot of students answered this question well. Some did not understand that UDP was unreliable and connectionless, but still scored half-marks for giving the right answer for TCP.

b) The students were fairly good on this part, but generally omitted to explain that the port numbers are carried in the segments. If they explained that the number system allowed the receiving system to de-multiplex the communications and send them to the right applications, they got most of the marks.

c) Generally the students got some of the relevant points about how TCP ensures the reliable transfer of data and corrects errors. Not many of the answers were very full and complete.

Overall a lot of students attempted this question and scored quite well.

Question 4

4. *a)* Modern networks including the Internet use the packet switching technique to transport message packets from the sender to the receiver. Briefly explain the concept of packet switching. List and explain the types of delays such message packets encounter along the path from sender to the receiver. **(11 marks)**

b) The Internet uses both TCP and UDP protocols to deliver services to the users. Identifying a service delivered by each protocol, discuss the characteristics of each protocol. **(14 marks)**

Answer Pointers

a) Packet switching concepts: Messages are divided into packets with source and destination addresses (headers) as well as data load. Source node sends packets via packet switches which use store-and-forward transmission. Packets are routed through links with least delays and are assembled at the destination node. 2 marks

Types of delays:

- Processing delay
- Queueing delay
- Transmission delay
- Propagation delay 1 mark
- Processing delay: The time required to examine the packet's header and also includes checking bit-level errors. Of the order of microseconds.

Queueing delay: Waiting time of a packet for transmission onto a link. Of the order of micro to milliseconds.

Transmission delay: Called store-and-forward delay as packets are transmitted on a FIFO basis. Of the order of micro- to milliseconds.

Propagation delay: The time required to propagate from a link to a router.
Can be of the order of milliseconds.

2 marks each. Total 8 marks

b) Examples of services:

TCP: Electronic mail
UDP: Streaming multimedia 1 mark

Discussion:
TCP characteristics:

Data transfer: connection establishment, buffering and forwarding (connection-oriented service)
Virtual circuit set up and connection state.
Reliability: Packet delivery with acknowledgement has time outs, error detection and recovery and ordering using sequence numbering facilities
Flow control, returning a window with ACK. which indicates number of bytes sender can transmit
Multiple simultaneous connections, each with sequence numbers, window size etc..

8 marks

UDP characteristics

Data transfer with no connection (connectionless service) (datagram)
No sequence number and does not support windowing
Expects application layer to provide reliability
No connection state.

Small packet header overhead

5 marks

Examiner's Comments

a) Though this question was answered by a large percentage of students, most of them seemed to have not read the question properly, and instead of briefly explaining the packet-switching concepts, pages of des transmissioncription and explanation were produced. Processing, queueing, transmission and propagation are the delays expected to be listed and explained. Most got at least the majority of these delays right.

b) Most students focused on the TCP and UDP protocols and missed identifying an example of a service that each protocol delivers. Mention of Electronic mail for TCP and streaming multimedia for UDP would have been sufficient. However, there were good discussions of protocol characteristics.

Question 5

5. *a)* Define the terms *bandwidth* and *capacity* as applied to data communication systems and briefly explain their significance.

In a data communication system, if the signal power is 10mW, the noise power is 1000 nW and the bandwidth of the system is 100kHz, calculate the maximum capacity of the system. **(12 marks)**

b) Explain the following technologies with reference to the local subscriber loop:

i) Integrated Services Digital Network (ISDN)
ii) Asymmetric Digital Subscriber Line (ADSL) **(13 marks)**

Answer Pointers

a) Bandwidth: The range of frequencies contained in a signal.
Capacity: Directly proportional to the bandwidth of the signals that the system carries.

Bandwidth indicates the amount of information that can be sent through the system. An important parameter to determine the capacity of the system 3 marks

Capacity = B Log_2 [1 +S/N] where B= bandwidth, S= signal power, N= Noise Power

2 marks

S/N = 10mW/1000nW = 10^4

Capacity = 100* 10^3 Log_2 [1+ 10^4]

$$= 10^5 * \text{Log}_{10}[10^4] \text{ ---------- bits/sec} = 13.3 * 10^3 \text{ bits/sec}$$
$$\text{Log}_{10}[2]$$

7 marks

b) ISDN bandwidth of the order of modest 64 Kbps was an effort to provide large scale digitised voice and data services to subscribers over the twisted pair copper wiring.

Offers three separate digital channels, designated B, B and D. The two B channels operating at 64Kbps carry digitised, voice and compressed video. The D channel operating at 16Kbpsis a control channel to request services for the B channels and terminate a session. The two B channels can be combined to give a single channel with a data rate of 128Kbs. 5 marks

ADSL provides the ability to send and receive digital information at high speed. The name asymmetric indicates that the bit rate in the downstream (from server to client) is much higher than the bit rate in the opposite direction. Typical downstream bit rate can be of the order of 6 megabits/s. The technology operates over the normal twisted pair wiring.

ADSL modems connect the users to the telephone central office and determine the missing word? and are highly adaptive. They use Discrete Multitone Modulation Technique (DMT), dividing the bandwidth into 286 separate frequencies, using 255 of them for downstream data. The remaining 32 are used for upstream data and 2 are used for control. This allows the ADSL to probe for available frequencies for data transmission. 8 marks

Examiner's Comments

a) The definitions of bandwidth as the range of frequencies contained in a signal, and the capacity as directly proportional to the bandwidth of the signals that a given system carries were well presented in most answers. However, the calculation of the maximum capacity of the system was not handled well because the formula of missing word? relating to the capacity to the signal to noise ratio was incorrect.

b) This part of the question was well discussed highlighting relevant issues. ISDN was comprehensively treated with explanation of the three channels and their bandwidths etc.. ADSL was equally well treated with very good explanation of the asymmetric downstream and upstream bit rates with typical values.

Question 6

6. *a)* Explain why bit errors are more common in wireless networks than in wired networks. Describe a method of detecting these errors. **(10 marks)**

b) Enterprise network systems are increasingly subjected to attacks by intruders. Describe THREE common types of these attacks. **(6 marks)**

c) List and explain the FOUR key properties of a secure data communication network. **(9 marks)**

Answer Pointers

a) Important difference between wired and wireless networks. In a wireless situation:

i) The electromagnetic radiation attenuates even in free space resulting in decreased signal strength as the distance between the sender and the receiver increases

ii) Interference from other sources when transmitted in the same frequency band.

iii) Multipath propagation occurs when portions of electromagnetic waves reflect off objects and the ground, taking paths of different lengths, resulting in the weakening of received signal.

All the above contribute to bit errors. 2 marks each. Total 6 marks.

The method to solve this problem is to use CRC error detection code. The CRC detection algorithm is described here. 4 marks

b) Three intrusion attacks:

i) IP spoofing attack: An unauthorised IP address is used, that is a legitimate IP address is stolen for a session when it is not in use.
IP datagrams are susceptible to these spoofing attacks.

ii) Packet sniffing: The intruder listens to TCP/IP packets through a packet sniffing hardware (a PC) and steals the information contained in the packet. This information is usually user name and password for misuse.

iii) Denial of Service attacks: A server is deluged with TCP SYN packets following an IP spoofing attack called SYN flooding which overwhelms the server.

Other attacks such as password attacks, session hijacking attacks etc.. could be discussed in the place of any of the above. 2 marks each. Total 6 marks.

c) The four properties for discussion:

i) Confidentiality: only the sender and intended receiver should be able to access and understand the message. For this reason, the messages are usually encrypted using one or more keys.

ii) Message Integrity: The content of the message should remain unaltered either maliciously or by accident in transmission. Again cryptographic techniques are used to encrypt the message as also use of error detecting codes.

iii) Availability: The networks services should be available to legitimate users unhindered by the attackers.

iv) Non-repudiation: A transferred message has been sent and received by the parties claiming to have sent and received the message. Nonrepudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. 9 marks

Examiner's Comments

a) The key factors that increase bit errors such as attenuation interference, multipath propagation were well dealt with by a majority of students. Networks important difference between wired and wireless networks, in some cases producing good examples. However, the desired method of using CRC error detection technique was described only in a minority of answers.

b) This part attracted some good answers and in some cases good discussion. While discussing the types of intrusion attacks, it is essential to indicate the purpose of each of these attacks, i.e. where are they directed at? For example, IP spoofing for steeling IP address, packet sniffing for stealing user name and password and denial of service attack is to flood the server with messages to make it inoperable etc..

c) This part was much misunderstood and a variety of answers ranging from cryptography to PKI were produced. Actually, the answer expected is much simpler as the four key properties of a secure service are confidentiality, integrity, availability and non-repudiation and this needed brief discussion. Reading the question and understanding what is expected is the best approach to getting the answers right.