THE BCS PROFESSIONAL EXAMINATION
Diploma

April 2004

EXAMINERS' REPORT

Computer Networks

General

The pass rate was a shade higher than 50%. Those who were successful did demonstrate a good understanding of the topic areas covered in the paper. The majority of those who were not successful demonstrated good understanding only in parts which can be attributed to the weak preparation for the examination.

It would help if in future the candidates prepare for the examination well in advance and use the past examination papers to test their understanding in topic areas and to familiarise with protocols and standards.

The success rate suggests a definite improvement over the last year, and the answers indicate tangible improvement in the quality of preparation for the examination. There were very good answers for questions 1 and 5.

Question 1

a) Explain *circuit switching* and *packet switching* techniques. What are the advantages and disadvantages that the packet-switching technique has over the circuit-switching technique.

(15 marks)

b) What is frame relay and why it is preferred to X.25 packet-switching service in wide area networks?

(10 marks)

Answer Pointers

a) In circuit switching, a physical path is established all the way from the source DTE to the destination DTE, prior to data transmission. In packet switching, no physical path between the source DTE and destination DTE is established. The data to be transmitted is assembled into units called packets with source and destination addresses at the source DTE, and are then bit serially passed through packet switching exchanges (PSE) to the destination DTE. The packets are buffered in routers as they are forwarded through links by the PSEs, and are assembled to form the original data at the destination DTE.

Circuit switching advantages include, simplicity and transparency of the Technique, and the cost of transmission depending purely on distance and time and not on traffic. Disadvantages include path monopoly, wastages of unused bandwidth in a static bandwidth reservation situation. Packet switching advantages include no path monopoly, throughput increase as packets can be routed through different links and error correction facility.
Disadvantages include lack of transparency as the carrier determines the basic parameters and limits on block size and buffers.

Marking scheme: 2 marks for circuit switching and 5 marks for packet switching explanations, 4 marks each for advantages and disadvantages of each technique.

b) Frame relay service is based on the basic connection-oriented way to transfer data as frames or packets using a virtual circuit between two points. The X.25 is also a connection-oriented service and supports virtual circuits The difference between the two is that the X.25 has a lower maximum speed - 64 Kbps for transmission, is a layered protocol and the X.25 network provides a number of features such as packet acknowledgement, packet recovery etc.. where as the frame relay operates at a higher speed- 1.5Mbps, providing a minimal service features and lets the connected user computers handle the rest of the features thus reducing the work done by the network itself. The preference is clear.

Marking scheme: 4 marks for explaining frame relay, 6 marks for explaining the difference as the basis for preference.

Examiner's Guidance Notes

Most of the candidates got the frame relay and X.25 basics right. The weaker candidates were unable to explain why the frame relay features are minimal by arguing the technology shift which has moved the features-related work from the networks to the user computers thus providing higher speed for the movement of packets.

Question 2

a) Explain the term data transparency and how it may be achieved using
i) character stuffing
ii) zero bit insertion. **(8 marks)**

b) What are the two main approaches used to control errors in transmitted data streams? **(6 marks)**

c) A 7-bit ASCII character encoded using Hamming code and is transmitted. The bit pattern received is represented
as follows: 00110010001.

i) Show how the above bit pattern is checked by applying the Hamming coding at the receiving end, indicate any error and correct it
ii) Extract the original 7-bit ASCII character
iii) Determine the code efficiency of the encoder
iv) Explain the limitation of using Hamming code as an error correcting technique, and outline the simple technique which can be used to overcome the limitation. **(11 marks)**

Answer Pointers

a) An 8-bit byte of data transmitted between a sender and a receiver achieves data transparency when it is ensured that the data contents are not interpreted as a flag. Normally achieved by pacing the byte between opening and closing flags.

i) The transmitter inspects each byte in a data frame to determine whether it resembles a DLE character, if it is it, stuffs a second DLE character next to it, and this procedure is continued for the entire frame whenever the DLE bit pattern is encountered. At the receiver end, the stuffed DLEs are removed.

ii) Bit stuffing is similar to the character stuffing in that whenever a consecutive five 1bits are encountered a 0 bit is inserted immediately after this sequence to ensure that the bit pattern is not interpreted as the flag bit 01111110.

Marking scheme: 2 marks for explaining data transparency, 3 marks each for explaining character and bit stuffing.

b) Two main approaches:

i) Error Detection: uses only enough redundant information with each data block transmitted so that at the receiving end it is possible to detect error/s occurred in the data block during the data transmission.

ii) Error Correction: uses enough redundant information associated with each data block transmitted so that at the receiving end it is possible to correct any error/s occurred in the data block during transmission and recover the original data block.

Marking scheme: 3 marks each for explaining the respective approaches.

c)
The check bits are at 1, 2, 4, 8,16, ….in the bit pattern received:
0 0 1 1 0 0 1 0 0 0 1

The Modulo-3 sum of all 1 bits in the bit pattern = 0101 suggesting that the bit 5 is affected . inverting this bit, the bit pattern now:
0 0 1 1 0 001 0 0 0 1

The ASCII bit pattern(excluding the check bits): 0010000

Code efficiency = 7/11 = 63.6%

Limitations of the technique:

- useful only in correcting single bit errors
- burst error correction needs modification of the technique.

Marking scheme: 7 marks for hamming code application, 1 mark for ASCII bit pattern extraction, 1 mark for code efficiency and 2 marks for limitation.

Examiner's Guidance Notes
Many were confused about the error control approaches. The hamming code application was done correctly by most of the students. However only a few could extract the ASCII bit pattern.Many got the code efficiency and limitations right.

Question 3

a) Explain the difference between *passive* and active *security* threats in the context of a typical LAN within the internet environment. **(8 marks)**

b) What are the five basic ingredients of a conventional encryption scheme? Taking the encryption algorithm DES as example, explain how the vulnerability of a conventional encryption scheme be improved?**(11 marks)**

c))Define the terms public key and private key as applied to a public key encryption scheme. What are the main steps involved in the operation of such a scheme? **(6 marks)**

Answer Pointers
a) Discussion should include:

Passive threat definition like not requiring action on the network from the attacker giving examples such as packet snooping with brief explanation. Active threat definition like requiring action on the network from the attacker giving examples such as injecting a worm with brief explanation.

Marking scheme: 4 marks each for giving definitions and examples in a LAN environment.

b) Five ingredients: the message text, encryption key, decryption key, cipher. Text and the algorithm.
Brief explanation of DES:
encryption in blocks pf 64 bits

- 56 bit key and 19 distinct stages with 16 encrypt
- iterations in the middle, and 32 bit swap after the
- last iteration.

DES vulnerability: its weaknesses

Weaknesses: - no of iterations-16 iteration insufficient
- key length- only 56 bits

Discussion should cover preferably with a block diagram:
Improvement: obviously increasing iterations and key length.
Use triple DES: Three stages of encrypt, decrypt and encrypt operations,
with three keys, tripling iterations and key lengths

Marking scheme: 2 marks for listing the five ingredients, 4 marks for brief DES features and explaining the weaknesses, 5 marks for improvement using the triple DES.

c) Public key: visible to the world and used for encrypting the messages to be sent to a receiver.
Private key: invisible to the world and known only to the receiver and is used to decrypt the encrypted text.

Steps using public and private key encryptions:

1. Two parties- sender and receiver
2. Sender gets the public key (which receiver also uses) from a trusted third party
3. Sender encrypts the message text with the public key
4. The cipher text is sent to the receiver
5. The receiver uses his/her private key to decrypt the text.

Marking scheme: 2 marks for definitions of public and private keys and 4 marks for the steps.

Examiner's Guidance Notes
Many students attempted this question and a few were successful in presenting good discussions. Many were familiar with the terms public and private key. Most did not get the weaknesses of DES.

Question 4

a) Explain by means of a diagram the frame format used by an IEEE 802.3 CSMA/CD LAN. Clearly show the size and function of each of the fields within the frame. You may ignore the Preamble and Start of Frame Delimiter.

(12 marks)

b) Why does CSMA/CD set a maximum limit to the frame size? **(6 marks)**

c) By considering a maximum size frame (1518 bytes) and a minimum size frame (64 bytes) determine the percentage of the frame that is used to carry protocol data. Hence, suggest why a maximum size frame will result in a higher effective data rate than a minimum size frame**.** **(7 marks)**

Answer Pointers

a)

Destination Address (6 bytes)	Source Address (6 bytes)	Length (2 bytes)	Data (46 to 1500 bytes)	PAD	CRC (4 bytes)

Fields:

Destination Address = MAC address of the device to which this frame is being sent. It comprises 6 bytes (48 bits). One bit is reserved for group/individual and one bit is reserved for global/local. Hence, 46 bits are used as a unique identifier.

Source Address = MAC address of the device that sent this frame. Format is the same as the destination address.

Length = the number of bytes within the data field that contain protocol data.
Data = field that carries protocol data. It has a minimum size of 46 bytes and a maximum size of 1500 bytes.

PAD = field that is used to ensure that the total data field equals a minimum of 46 bytes. When the frame contains 46 bytes or more of protocol data then the PAD field will be eliminated.

CRC = cyclic redundancy check field which allows bit errors occurring within the entire frame to be detected. Frames with a CRC error will be discarded.

Marking scheme: 2 marks for the diagram, 2 marks for the address format, 1 mark for the purpose of the destination address, 1 mark for the purpose of the source address, 1 mark for purpose of the length field, 1 mark for purpose of the data field, 2 marks for the purpose of the PAD field and 2 marks for the purpose of the CRC field.

b) When a computer attempts to gain access to a CSMA/CD LAN it must first check that no-one else if transmitting. Even if the network is free, there is always a chance that a collision could up to a time governed by the round trip delay of the network. However, after this time, if no collision has occurred then the computer is said to have acquired the network. At this point no other computer can gain access to the network. Any computer wishing to transmit would sense the network as busy and back-off. If the frame size was not limited by a maximum value then, once a computer has acquired the

network, it could , in theory transmit for ever and lock everyone else out. Hence, in the interests of fairness and to ensure that the medium is truly shared, a maximum frame size is defined to force a computer to stop transmitting after a given time. This pause in transmission then allows others to gain access to the network.

Marking scheme: 4 marks for realising that once a computer has acquired the network, no one else can transmit. 2 marks for specifying that the maximum limit is to allow sharing of the medium.

c) By considering any frame size, it is noted that they all require a destination address (6 bytes), a source address (6 bytes), a length field (2 bytes), and a CRC field (4 bytes). This means that every frame – whatever its size, contains 18 bytes of overhead – non data bytes.

For a maximum size frame the percentage of the frame used to carry protocol data is given by (1500/1518) * 100% = 98.8%.

For a minimum size frame the percentage of the frame used to carry protocol data is given by (46/64) * 100% = 71.8%.

Hence, a maximum size frame has a higher efficiency.

In simple terms this means that maximum size frames will use a higher percentage of the network's bandwidth and hence, result in a higher effective bandwidth, 9.88Mbps versus 71.8Mbps for a 10Mbps LAN.

Marking scheme: 2 marks for noting that all frames have an 18 byte overhead. 2 marks for the maximum frame percentage, 2 marks for the minimum frame percentage and 1 mark for concluding why the maximum frame results in a higher effective bandwidth.

Examiner's Guidance Notes:
In answering this question there was a strong tendency for the students to answer different questions from what was actually asked. In particular, in part b, there was a tendency for the students to try and explain why there is a minimum frame size on an Ethernet network, whereas they were asked why there is a maximum frame size. Also the students wanted to talk about
collisions, because they recollected there were collisions on an Ethernet, but this was not asked in any of the parts.

Question 5

a) With reference to the ISO Reference Model, explain what functions are performed by the Network and Transport layers. **(7 marks)**

b) Two computers are communicating via a wide are network. What quality of service is offered to their respective transport layer protocols if the Network layer is provided by:
i) IP
ii) X.25 **(10 marks)**

a) If two computers use IP as their Network layer protocol, what quality of service is offered to their respective higher layer protocols if the Transport layer is provided by:
i) TCP
ii) UDP **(8 marks)**

Answer Pointers

a) Network Layer
- responsible for inter-networking
- includes provision of a network wide addressing scheme
- routing traffic through an inter-network
- providing a connectionless or connection-orientated service to the Transport layer.

Transport Layer
- responsible for end to end communications and present only in the end-stations, not the network
- responsible for accepting the quality of service from the network layer and translating this into the quality of service required by the application
- provides application level multiplexing functions

4 marks for the Network layer and 3 marks for the Transport layer.

b) IP
- connectionless
- datagram service
- no error correction – detection and discard only
- no flow control
- best-effort service

X.25
- connection-orientated
- a hierarchy of protocol data units is defined
- full error detection and correction by packet re-transmission
- flow control provided with both local and end to end significance
- guaranteed delivery

Marking scheme: 5 marks for identifying the features of IP and 5 marks for identifying the features of X.25

c)TCP
- connection orientated
- error detection and correction through positive acknowledgement and byte re-transmission

- flow control provided
- congestion control provided
- limited provision for marking data priority

UDP
Connectionless
Datagram protocol
No error detection and correction or flow control

Marking scheme: 5 marks for TCP, 3 marks for UDP

Examiner's Guidance Notes:
In general, the first part was answered quite well – the students could distinguish the functions of the network and transport levels.
Part b was sometimes answered well. Some of the students, however, did not seem to appreciate very well the characteristics of an X.25 network, and, in that case, the comparison with IP was obviously less effective.
Part c was generally answered well – most students who attempted this seemed to know that TCP offers a connection-oriented service and UDP a connectionless service and were able to explain the difference in a reasonably effective way.

Question 6

a) Two computers A and B and a server S are connected to a CSMA/CD LAN. These computers and the server support the TCP/IP protocols. Why does each computer and server need both a MAC and IP address? **(6 marks)**

b) If computer A knows the IP address of the server, explain how it can use the Address Resolution Protocol (ARP) to determine the MAC address of the server. **(10 marks)**

c) If a server supports more than one application explain how TCP port numbers can be used to allow computer B to access these two applications at the same time. **(9 marks)**

Answer Pointers
a) Each computer and server attach to the LAN using an adapter. This adapter operates at the Data-Link layer and will contain a unique MAC address. The MAC address is needed to transfer frames from point to point on a LAN. Hence, the MAC frame is used by the LAN to effect basic data transport from one device to another.

Each computer also needs a layer 3, Network Layer, IP address to permit inter-working. In other words, in order to communicate with devices on another LAN, the IP address will provide the inter-network routing information.

Given the above functionality, each device will require both a layer 2, MAC and layer 3, Network layer address.

Marking scheme: 3 marks for identifying purpose of the MAC address and 3 marks for identifying the purpose of the IP address.

b) In order for A to communicate with the server it needs to know the servers MAC and IP addresses. The MAC address is needed for the LAN frame and the IP address for the IP datagram.

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

A 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 the server, the IP address of A, the MAC address of A and a blank field to indicate
that the MAC address of the server 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 the server.

The server will therefore issue an ARP reply. This will be transported within a LAN frame that has a destination address equal to the MAC address of A 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, the server will add its own MAC address into the blank field.

On receipt of the ARP reply, A has discovered the MAC address of the server.

Marking scheme :ARP request: 2 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 fields within the ARP reply PDU .

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

TCP port numbers allow for multiplexing at the Transport layer. TCP port numbers are 16 bit numbers and each TCP 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 ach application is assigned a unique port number within the server – call these TP1 and TP2. Now when B wishes to access application 1, it will issue a TCP PDU with a destination port of TP1 and when it wishes to access application 2 it will issue a TCP PDU with a destination port of TP2. Both of these will be carried over the same IP datagram flow but when they arrive at the server, the server's TCP protocol will separate the PDUs based on thei destination port numbers with TP1 being directed to application 1 and TP2 being directed to application 2.

Marking scheme: 5 marks for the format of the port number and knowing that destination and source port numbers are carried in each TCP PDU. 4 marks for explaining how port numbers can be used to distinguish traffic flow to two applications.

Examiner's Guidance Notes
For part a, the students generally appreciated that there are indeed two levels of addressing, but they often found it difficult to answer the question and explain *why* there are two levels of addressing. In general the question 'why?' is rather difficult for students in the early stages, although it looks fairly simple to answer.Part b asked the students to explain how the ARP protocol actually works to resolve IP addresses to

MAC addresses, and they did this better. Quite a lot of them had quite a good idea of how the address resolution takes place.Some of the explanations of how TCP port numbers can be used to allow a client computer to access two applications on a server at the same time were a little circuitous – essentially arguing that port numbers are good because they allow a client to access two applications at the same time! How well they did, therefore, tended to depend on the degree to which they could find some terminology to explain what was going on in this case, which did not simply use the terms in which the question was posed.