THE BCS PROFESSIONAL EXAMINATION
Diploma

April 2003

EXAMINERS' REPORT

Computer Networks

General
This was a popular paper, 51% of those attempting this examination passed and the average mark for the module was 44% which was lower than in previous years.
It may be that the current network protocols available around the world differ. Apart from this anomaly the performance of the candidates was similar to that of former years.

Again this year, a large number of candidates were poorly prepared for this examination and produced answers that ranged from weak to totally irrelevant. A generic weakness was an inability to actually read the question. Strangely, those candidates who attempted the more discursive questions were those whose poor grasp of English meant that the answers they produced were incomprehensible. However, all questions were answered well by several candidates, indicating a lack of breadth in the preparation undertaken by the majority.

Lots of candidates were unable to attempt all parts of their chosen questions.

Question 1

a) Outline the protocols used for addressing and routing the OSI datagram and virtual circuit services offered by the network layer. (14 marks)

b) Discuss the relative merits and limitations of the two services. (11 marks)

A majority of candidates chose to ignore the question and write about TCP and UDP which (a) didn't relate to OSI and (b) didn't relate to the network layer.

Answer Pointers

Datagram and Virtual Circuit services are provided by the OSI Network Layer to facilitate routing of messages between two stations on the network.

Datagram

Analogous to the service provided by the Post Office

- Simplest of the two approaches
- Each message treated as a separate entity
- Have to provide a destination address for each message
- Assumes only minimal functionality from the network
- Does not enhance the reliability of the underlying service

Most early networks were based on the use of datagrams (e.g. Arpanet & Xerox Internet)

Protocol

- Full source and destination addresses are inserted into each message
- Intermediate nodes use the destination address to choose the route on a per-message basis
- Choice of route is dependent upon the current situation, so:
  - messages to the same destination do not necessarily follow the same route
  - routing mechanism can easily adapt to component failure
  - adaptive routing my result in some messages in a sequence being delayed
  - can result in lost/duplicated/out of sequence messages
- Much simpler to implement than a VC protocol
- Flow & congestion control is difficult, as no information is maintained to relate messages within a sequence.

Virtual Circuit

Analogous to the telephone network

- A virtual circuit is a logical point-to-point connection between 2 end stations
  - may traverse a number of intermediate nodes
  - provides a reliable message stream service
- Connection is established before data transfer & released afterwards
- Once the initial connection is made, we can use VC numbers as abbreviated addresses.
- Ensures in-sequence delivery of messages and no loss of messages without notification

Protocol

- VC has a 3 phase protocol:
  - Establishment
  - Data
  - Termination
- A virtual circuit is set up by a *connect message* which contains the full source and destination addresses.
- The VC is assigned a *VC number*
- The network maintains tables to map the VC number onto the source and destination addresses
- Once the VC has been established, the VC number is used to route a message rather than the source and destination address

- Once a VC has been terminated, the VC number may be reused

- As the VC number takes up less room than full addresses, the control information overhead in data packets is much reduced.

Question 2

a) Describe clearly, including advantages and disadvantages, 1-persistent, non-persistent and p-persistent CSMA. (12 marks)

b) Describe the function of repeaters, bridges and routers. Your description should include details of the purpose of each and details of the levels of the OSI 7-Layer Reference Model at which they operate. (8 marks)

c) Identify THREE types of cabling technology which may be used in a 10-Mbps Ethernet network. What are the advantages and disadvantages of each? (5 marks)

Part a) answers demonstrated that most people had never heard of the different types of CSMA.
Part b) was answered correctly in most cases, although a greater level of detail would have been preferred.
Part c) was either very well answered or very poorly with a number of candidates discussing topologies rather than media types.

Answer Pointers

(a) Discussion to include:

1-persistent

If a station detects a collision, it continues to sense the transmission medium until it is idle, then immediately transmits

+ reduces idle time, as station can transmit as soon as channel is idle
- if >1 station wishes to transmit, collisions are unavoidable

non-persistent

If a station detects a collision, it transmits a jamming signal and then waits for a random period of time before sensing channel again.

+ stations are liable to “back off” for differing periods, thus the chances of collision are reduced
- likely to be wasted idle time at the end of a transmission

p-persistent

If a collision is detected, then the station continues to sense the medium until the channel is idle, the transmits with probability p. If the station does not transmit, it backs off for a period of time before sensing the channel again.

compromise - attempts to minimise both idle times & collisions
- cannot completely prevent collisions

(b) Discussion to include:

Routers connect dissimilar networks at the network layer, and are used to link networks that operate different network protocols.
Bridges are used to link networks that use either different physical media, or different media access control (MAC) protocols. (Datalink layer of OSI model)

Repeaters link networks that use the same MAC protocols over identical, or very similar, physical media. (Physical layer of OSI model)

(c) The three cabling technologies readily available for CSMA/CD networks are:

10 Base 2
10 Base 5
10 Base T

which correspond to Thick Ethernet, Thin Ethernet and Twisted Pair Ethernet

Both Thick Ethernet and Twisted pair require the use of expensive hardware (AUI transceivers in the case of Thick Ethernet, and hubs in the case of Twisted Pair). Thin Ethernet, on the other hand relies on inexpensive BNC hardware and coaxial cable.

Both Thick and Thin Ethernet support longer cable runs than Twisted Pair, as the coaxial cabling used is not as susceptible to EMI as the cheaper twisted pair (particularly when unshielded)

Question 3

a) What is the role of the LLC and MAC layers in the IEEE architecture? How do these layers compare with those in the ISO OSI 7 Layer Reference Model? (8 marks)

b) Explain why direct connection to an FDDI network is not usually recommended. (2 marks)

c) Show how the FDDI "wrap" mechanism may be used to maintain network viability in the case of:

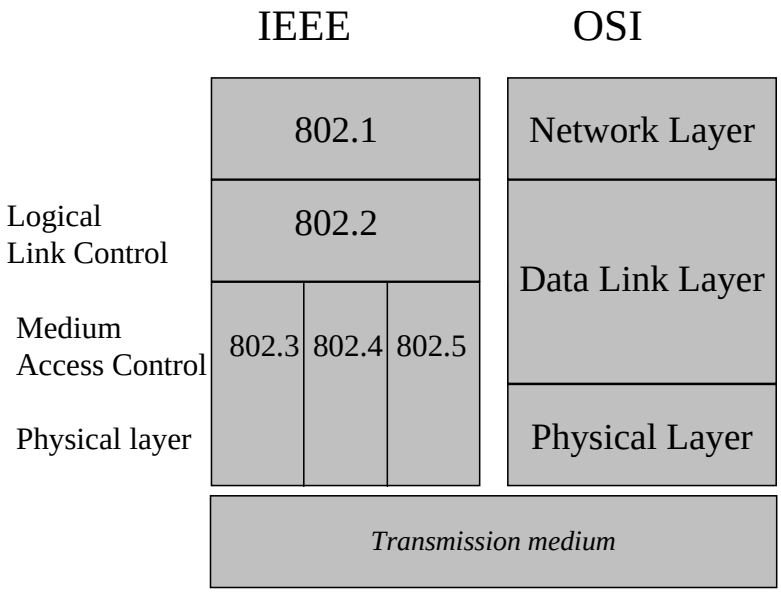
i. Link failure
ii. Node failure (10 marks)

d) Using diagrams where appropriate, show how a translation bridge may be used to link an Ethernet LAN to an FDDI backbone. (5 marks)

Generally, answers were reasonable with candidates showing an appreciation of both FDDI and the IEEE stack. However, very few candidates were able to explain how a translation bridge actually worked.

Answer Pointers

(a) Discussion to include:



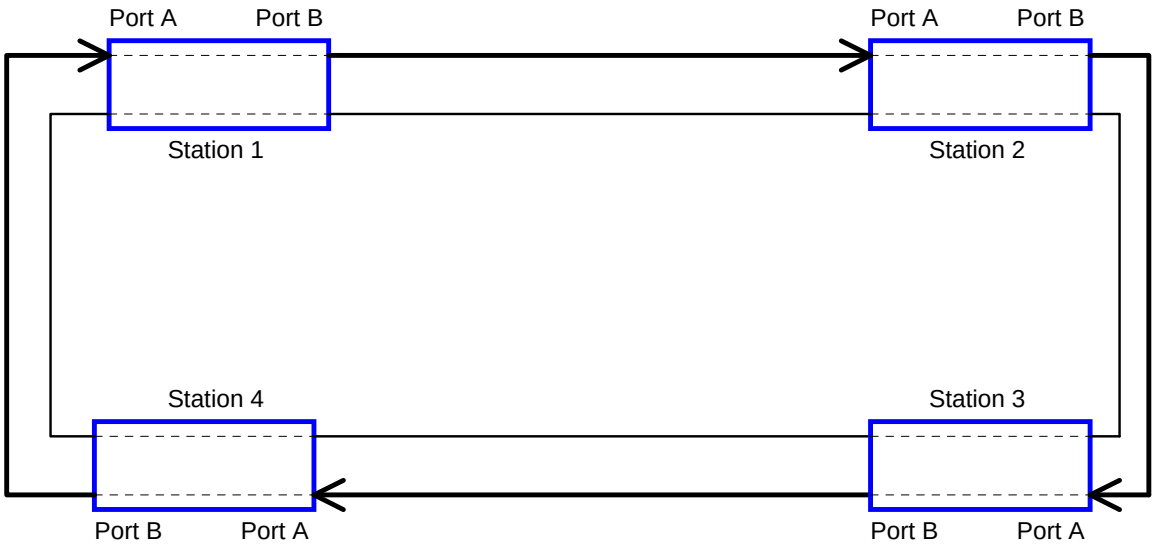
Physical layer: provides a broadcast channel
LLC: provides a logical link to higher layer software, independent of the underlying technology
MAC: provides a standard set of primitives to LLC

(b) Direct connection is expensive (£1000's)

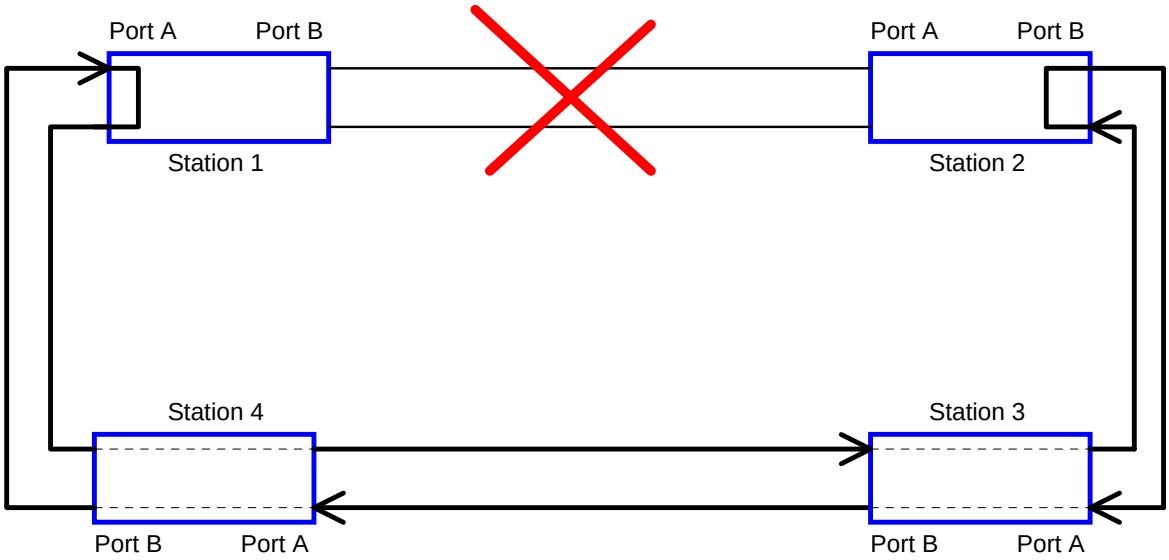
- H/W to perform optical/electrical conversion is expensive
- Connection to fibre optic cabling is expensive - v. difficult to use taps

(c)

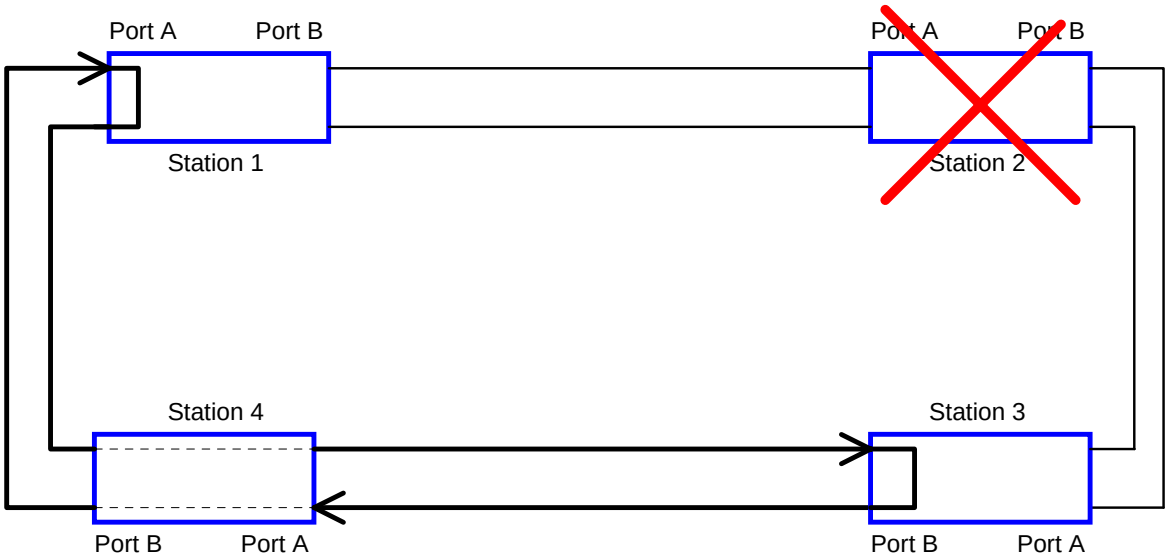
Under normal circumstances, FDDI employs dual fibre rings, only one of which is used for data transmission:



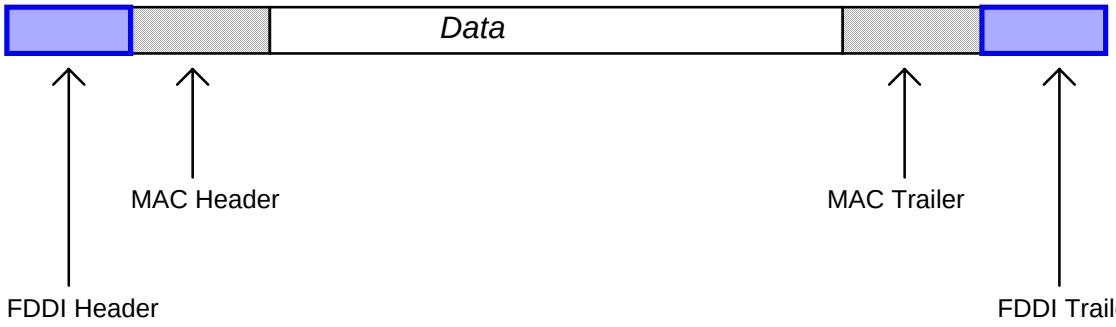
In the case of link failure, the “wrap” mechanism uses the secondary ring for data transmission, thus preserving the integrity of the network:



In the case of node failure, neighbouring stations detect the problem and again utilise the wrap mechanism to transmit data, avoiding the faulty station:



(d) Bridges used are “translation bridges” - they take the whole of a frame from a sub-LAN, consider it to be pure data (including Ethernet/Token Ring MAC header & trailer) and append a FDDI header/trailer for transmission across the FDDI backbone.



(

When this is received by another bridge for onward transmission to a sub-LAN, the reverse occurs and the FDDI header/trailer is simply stripped off.

Question 4

a) Define the term latency when used in the context of a data network. (2 marks)

b) Describe a common approach for measuring latency within a data network. (2 marks)

c) Describe four contributors to latency within a data network, and the way in which they contribute to the latency. (16 marks)

d) Given a network with an unacceptable latency, what should be done to analyse the cause and to overcome problems. (5 marks)

Part a) answers were variable, with a significant minority of candidates unable to express the concept.
Part b) was poorly answered with no real idea of how to measure delays using common tools.
Part c) and d) were poorly answered, demonstrating an inability to look at the bigger picture.

Answer Pointers

(a) Latency is a synonym for delay.

Latency is an expression of how much time it takes for a packet of data to get from point to another

(b) Latency can be measured by sending a packet that is returned to the sender e.g. a 'ping'
The round trip time of a packet is considered to be the latency.

(c) Propagation. The time it takes for a packet to travel between one place and another.

- Transmission. The medium itself (e.g. optical, wireless) introduces some delay.

- The size of the packet introduces delay in a round trip, as a larger packet will take longer to receive and return than a short one.
- Router and other processing. Each node takes time to examine and

- possibly change the header in a packet
- An example of a change e.g. hop count or time-to-live field
- Other computer and storage delays. A packet may subject to storage and hard disk access delays.

These delays could occur at switches or routers.

(d) Discussion to include

Measure the latency using an appropriate tools within ICMP (Internet Control Message Protocol) e.g. 'ping'
Measuring the round-trip-time
By varying the network load and measuring the corresponding throughput and latency
reduce network latency by employing a higher performance network hardware e.g. Fast Ethernet
reduce communication software overhead by implementing more efficient communication libraries

Question 5

a) Explain the term QoS and how it can be achieved in data networks. (1 mark)

b) Describe in detail the terms Availability, Reliability, Resilience and Serviceability when used in the context of data networks. (8 marks)

c) Describe in detail four examples of threats to network security. (8 marks)

d) Describe in detail four countermeasures that can be employed to remove or reduce the threats of network security. (8 marks)

Parts (a) and (b) were very poorly answered with few candidates able to give a convincing explanation of the concepts.
Parts (c) and (d) were better answered perhaps due to their discursive nature, but many candidates were let down by an incredibly weak grasp of the English language.

Answer Pointers

(a) QoS enables the provision of better service to certain flows. Can be done by either raising the priority of a flow or limiting the priority of another flow.
A congestion management tool will raise the priority of a flow by queuing and servicing queues in different ways. Queue management tools are used for congestion avoidance, and raise priority by dropping lower priority flows before higher-priority flows. Link efficiency tools limit large flows to show a preference for small flows.

(b) Availability. In a data network this is the availability of input and output ports.
Reliability. That the components, and therefore the network as a whole, conforms to specification. The absence of bugs or technical errors; a high MTBF indicates high reliability.
Resilience. The ability to recover from failure, techniques include alternate routing; backup lines; redundant components

Serviceability. The continuation of service without going off-line. Engineering work, maintenance, upgrades, extensions and analysis can be done without and interruption to service.

(c) Unauthorised access to the network e.g. using another persons password
Hacking and IP spoofing. To gain access to information via the network or to use the network for unauthorized purposes.
The introduction of viruses.
Theft of network components, and/or deliberate damage

Other valid examples

(d) A firm and well policed security policy, which forces the regular change of passwords. The limited availability of system/administrator passwords.
Firewall technology
Anti-virus software. Regularly updated.
The installation of network components in secure areas. Asset management.
Cabling in secure runs.
Other valid examples

Question 6

a) Mobile computing has a number of requirements and places a number of demands on computer networks. What are these requirements and demands? (14 marks)

b) Describe the performance considerations that must be addressed when implementing mobile computing. (6 marks)

c) Describe Client Server computing. How does network use differ between *thin client* and *client server*? (5 marks)

Again, a poorly answered question because candidates did not read the question and proceeded to tell the examiner about what a wonderful thing mobile computing was rather than focussing on the network impact. Very few candidates had heard of thin-client technology.

Answer Pointers

a) Range of traffic types e.g. video, voice and data
The need for co-existence and interoperability of different systems of connection e.g. Bluetooth and IEEE 802; different MAC protocols
Conflicting standards e.g. wireless and cellular networks
The need for data synchronisation across the network.
Security considerations
The control of growth of network users.

b) Determining the variable user population
Bursty traffic types e.g. video and large data transfers
Interference on wireless and cellular networks
Differing wireless technologies, giving rise to delay in packet handling
User mobility

c) This architecture is based around two programs making requests over the network. It is very common and is the central idea of 'Network Computing'. The nature of the design is that one program makes a

request to another, which can give rise to large bursts of data being sent along the network in response.
The network design and capacity must be able to provide a service for this type of activity. Software updates are also sent over the network.

d) This architecture uses terminal server software. Regular software updates to the user are not required. Data is processed at the server end, not the user end, with results being sent to the user. This usually requires less bandwidth than client server. An industry example of thin client is citrix. Thin client is particularly useful for mobile computing, as it can run on small capacity devices e.g. PDAs.