BCS THE CHARTERED INSTITUTE FOR IT

BCS HIGHER EDUCATION QUALIFICATIONS
BCS Level 6 Professional Graduate Diploma in IT

NETWORK INFORMATION SYSTEMS

Monday 20th March 2017
Answer **any** THREE questions out of FIVE. All questions carry equal marks.
Time: THREE hours.

Answer any Section A questions you attempt in Answer Book A
Answer any Section B questions you attempt in Answer Book B

For all questions illustrate your answers with diagrams where appropriate

EXAMINERS' REPORT

General comments on candidates' performance

The standard of answers was reasonably consistent across questions this year, although question A3 was less popular than the other questions. Despite this, those candidates who attempted question A3 generally showed a competent understanding of the subject, which was reflected in the answers.

There were some excellent answers for all questions and the spread of marks was as expected for those who chose to answer each question.

The evidence suggests that the majority of candidates paid attention to the marks being awarded and used them as an indication of the complexity of the questions being asked. However, there were a few who spent too much time writing long answers for sections which only required short answers; consequently, getting lower marks for later sections.

There were some cases in the questions below where certain misunderstandings were widespread, although by no means universal. These have been addressed in specific comments below. It would be advised that future candidates would benefit from paying attention to the question as a whole and to note that questions are usually designed to be progressive.

SECTION A

A1.

a) Outline the main differences between unicast, broadcast and multicast internet protocol usage.

(6 marks)

b) An Internet Service Provider wishes to provide services for domestic customers. These services are: access to the Internet; a customer facing web service; security through a firewall router; a Domain Name System (DNS) server; multicast IP television services. Customers will connect to the ISP by various technologies but you may consider these as point to point links for this purpose.

Describe, with the aid of a diagram, an appropriate network topology for this network. Ensure that you clearly label all major network elements.

(10 marks)

c) Taking the network topology in b), describe the way in which multicast provides the television services by ensuring data flow to users of the services without impacting on non-users.

(5 marks)

d) Explain why the company would probably not choose to use multicast for a video on demand service.

(4 marks)

Answer Pointers:

a) **Unicast:** Unicast traffic is traffic that is meant for a single host. All other hosts will ignore unicast traffic not meant for them. In a switched environment, unicast traffic is generally not "heard" by any hosts other than the host for which the traffic is intended.
Broadcast: Broadcast traffic is traffic that is sent with the intent of being "heard" by all hosts on a particular network segment. Examples of broadcast traffic would be an ARP request or a DHCP request.
Multicast: Multicast traffic is traffic that is sent with the intent of being "heard" by a particular group of hosts on a network segment. Some multicast traffic can be considered broadcast traffic, such as traffic to the multicast address 224.0.0.1, which is multicast traffic meant for all hosts on the same network segment, but it is still ignored by any connected nodes not running TCP/IP. Another example of multicast traffic would be traffic sent to the multicast address 224.0.0.9 used by routers to send routing information to other RIP enabled routers on the same network segment. Candidates were not expected to be able to enumerate specific IPv4 (or IPv6) multicast ranges to get full marks – it was an understanding of the concept that was required here. Illustrating with a diagram was often helpful.

b) The diagram should have included all the key elements in the scenario: Firewall, routers for the point to point connection, DNS servers, multicast streaming server, web server. Candidates may also have included switches and other such network components, although these were not strictly required. A DHCP service, or some other means to provide network information to the customer, would be implied and consideration of network configuration in the diagram was thus awarded 2 marks. Because point to point links were used, there should also have been some consideration of

network numbering, and the best answers would envisage use of a /31 IP range (in IPv4), or the use of Network Address Translation, or the use of an IPv6 /64 at the end of the point to point link. Although open ended, again it is consideration of the issue that would gain full marks. Nevertheless, see the examiners' comments.

c) This part of the answer expands on part a) and allowed the candidate to demonstrate knowledge of multicast routing in relation to the network diagram. In the diagram it could be demonstrated that the end user registers for a multicast address and that the router (and/or switches) keep tables as to which segments/links to transmit the multicast transmissions onto. In this way, there would be a single multicast stream to multiple customers on the network backbone but only those customers who register for the stream would receive the data on their point to point links.

d) The benefits of the multicast stream are that, even on the backbone, there is only one stream and then this can be registered by multiple customers but not by all. Only those registering for the stream are sent the data. However, video on demand requires that the stream be started at user request. As different customers start the service at different times, it is not usually possible to aggregate the same stream for multiple customers. If customer 1 starts the stream and ten minutes later customer 2 requests video, a new stream must be started for customer 2. This is better served by unicast transmission, because sending it via multicast merely adds load to the network components that must switch traffic based on a table of registered users.

Examiners' Comments:

There were many good answers to part a) of this question. The evidence suggests that a minority of candidates did not notice the specific mention of internet protocol usage and instead wrote about broadcast transmissions of, for example, television; however, this was rare. A more common issue was a failure to correctly distinguish broadcast (sent to all nodes) from multicast (sent to nodes that have elected to become a part of the multicast group).

In part b) the evidence suggests that candidates did not have the required knowledge of the term "topology. A number of candidates describing a general topology rather than that specific to this question. For example, where these answers stated that a star topology was required but offered no support for that view, the answers were insufficient; however, where a reasoned argument was made for a generic topology with relation to the demands of this scenario, the full range of marks was available. Nevertheless, full marks could only be obtained by following the instruction to label the major network elements.

Parts c) and d) relied upon an understanding of multicast. However, the evidence suggests that even when that understanding was lacking, many candidates were able to gain some credit for part d) when they showed they understood the nature of video on demand as not being appropriate to a broadcast or multicast solution but, rather, that it was reliant on unicast. One or two candidates even showed a deep level of knowledge here in discussing how the UDP protocol would be appropriate, and why, although that level of detail was not required to gain full marks on this question part.

A2.

a) ISO 27001 (and formerly BS7799) creates a key concept of an information security triad of Confidentiality, Integrity and Availability (CIA).

Describe what is meant by each of these.

(6 marks)

b) A company wishes to share data through a website with a portal that trusted users can log into using a username and password combination.

Describe the extent to which the CIA triad is met by the following implementations:

i) An HTTP based web page accessed through a password and with IP address access control.

(3 marks)

ii) An HTTP based web page that can only be accessed by first connecting via VPN into the company's secure intranet.

(3 marks)

iii) An SSL/TLS based web page with password based access.

(3 marks)

iv) A web page that may only be accessed by coming into the company's office.

(3 marks)

c) Make a recommendation as to the most appropriate solution above, describing briefly how you would implement this.

(7 marks)

Answer Pointers:

Confidentiality, integrity and availability (CIA), is a conceptual model designed to guide policies for information security within an organisation. In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of timely and reliable access to the information by authorised users.

For each sub part, there should be at least three points made:

- Confidentiality is poor. Such pages have no encryption preventing interception of data, although the password provides a measure of access security. Integrity is also poor in that there is no defence from man in the middle attacks and change of the data. Availability is good, as long as the password is known.

- Confidentiality is much better, although has a weakness in that the last hop to the website across the corporate network is unencrypted, so there remains a vector for attack. Integrity is also better for the same reason, and a man in the middle attack would have to occur in the company or involve a breach. Availability is reduced in that now a special tunnel must be created before the information can be accessed and this is an additional point of failure.

- Confidentiality is very good, with SSL providing a good and secure means of encryption. Integrity is also excellent for the same reason (use of public key cryptography to share session keys provides authentication and integrity). However, there is a weakness if a certificate is signed by a compromised key that the client trusts, allowing a man in the middle attack (e.g. as in the Diginotar attack). Availability is good, as SSL/TLS is built into the web server and client and does not require additional steps.

- Confidentiality is good but no better, in fact, than the VPN solution as, again, the information is probably unencrypted on the corporate network and vulnerable to a breach within the company. Integrity is good but again suffers from the susceptibility to breach and man in the middle attacks that could allow for data to be modified in transmission. Availability is now very poor, requiring a visit in person to access the data.

Having completed part b), the best solution is likely to be SSL/TLS from those listed above. Candidates may also have proposed a hybrid VPN and SSL solution for added security (but slightly reduced availability). SSL/TLS can also be improved by editing the list of trusted Certificate Authority certificates to include only those that are genuinely trusted by the organisation.

SSL/TLS requires configuration of the web server to support this but also, for best security, the purchase of a certificate from a CA which will ensure authentication of the host. The CA will need to verify the identity of the organisation purchasing the certificate. If VPN is recommended, then the candidate needed to describe the required VPN server and, again, the need to purchase a certificate for authentication purposes.

Examiners' Comments

Almost all answers showed a good understanding of the Security Triad. However, not understanding the need for encryption on wired or wireless networks to ensure confidentiality was a reasonably common failing. In part b) (iv) the entirely private solution, as well as the earlier VPN solution, have a weakness on this score, as it is important to remember that not all threats to data lie outside of a corporate network (see the answer points above). Even though this was missed by many, most candidates scored well on part b).

On part c), many candidates suggested solutions other than those in the answer points above. Although these answers were not optimal, they could still attract many of the marks available where the case was made appropriately and described a suitable implementation. Nevertheless, few candidates understood the necessity for purchasing certificates as per the answer points.

A3.

A social media company is developing an application for sharing targeted educational videos to subscribers based on user preferences and profiling data. The videos are specially produced with language subtitles to assist language learners.

The application distributes data across multiple regional data centres to avoid network bottlenecks for viewers of the videos. The company maintains a single server for central data processing, and videos are uploaded to the central server and distributed from there to the regional data centres.

For EACH of the THREE data transfer scenarios listed below, discuss the strengths and weaknesses of the use of SOAP web services for the data transfer mechanism over the use of an in house protocol designed around the use of Secure File Transfer Protocol (SFTP).

In your answer, consider network performance issues and the need to accommodate firewalls and network security. Make a recommendation as to which mechanism to use in each case.

a) The profile data of subscribers needs to be transmitted from regional data centres and processed daily. In the first instance there are estimated to be 50,000 subscribers but the business plan hopes to see that number increase to 500,000 within two years.

(8 marks)

b) Video creators need to be able to upload new content from a number of different locations. Owing to the specialised nature of the content, it is thought that there will be no more than 100 videos uploaded per day.

(9 marks)

c) Video creators need to be able to retrieve usage summaries of their uploaded content, which will also be used to calculate advertising revenue. The reports will be downloaded from a number of different locations. There will be no more than 1000 report requests per day.

(8 marks)

Answer Pointers:

a) Web services have the advantage of using standard protocols which pass easily through firewalls. Nevertheless transferring 50,000 SOAP messages will have performance issues, and 500,000 will create a very significant load.

Candidates may have suggested that messages could be batched and compressed and sent as attachments to improve performance, and could also suggest compression schemes. Any scheme must be appropriate, without losing the benefits of using SOAP. The data transmitted here is sensitive and the candidate must realise the need to use SOAP encryption or to encrypt data prior to transmission. (4 marks)

Using an SFTP server is good for the high data volumes, particularly if the file is compressed. The SFTP protocols are easy to get through firewalls and they can be secured, as there are only a small number of machines involved. SSH

encryption ensures security. The application described is bespoke, based on SFTP, and the use of the known protocol can make development easy whilst relying on SFTP benefits. This data interchange is between the company's own servers with client and server under their control, which ensures the bespoke protocol can be fully accommodated. This solution should be preferred in this case. (4 marks)

b) Web services have the advantage of using standard protocols and are good for being accessed from a number of locations and easily pass through firewalls. SOAP encryption can be used. Due to the low volumes, there are no large inefficiencies. SOAP messages are self-contained, so a partial message will not occur; however, candidates must demonstrate an understanding of the need to use SOAP attachments for large binary data files such as videos. (5 marks)

Using SFTP requires that the video be uploaded to a server. The processing will need to poll the server periodically to see if new videos must be distributed to the regional sites, and partial videos may not easily be recognised unless some metadata is uploaded too. Files will need to be uploaded with a different name and renamed or moved to prevent distributing a partially uploaded file. SSH encryption ensures security. (4 marks)

c) Web services have the advantage of using standard protocols and are good for being accessed from a number of locations and easily pass through firewalls. SOAP encryption can be used. Due to the low volumes, this is quite efficient. SOAP messages are self-contained, so a partial message will not occur. Providing this functionality as a Web service means that the reports can be customised by parameters. The same web servers can also provide online web based summaries. This is the preferred solution. (4 marks)

Using SFTP requires that the information be processed regularly and uploaded to a server. The processing generates reports on a frequent basis, even if they are not required. SSH encryption ensures security. Although the bespoke protocol is implemented and in use elsewhere, it need not be distributed to client applications if the standards based SOAP protocol is used in conjunction with vanilla HTTP, so there is no advantage in using this solution here. (4 marks)

Examiners' Comments

This question proved less popular than the others, although if this was because candidates considered it harder, this was not reflected in the marks, with many good answers to the question; and where answers were weaker, this did not appear to be more so than in other questions. It may be that candidates were put off by the requirement to think into the scenario but, where they did so, they were capable of producing good answers.

The evidence suggests that candidates would benefit from reading the question thoroughly to inform their answer. Some candidates missed the scalability issue in part a) and how that mitigated against use of SOAP in that scenario. Also, many missed the need for encryption of sensitive data. This was true in all question parts. The question specifically compared SOAP with Secure File Transfer Protocol, SFTP. The encryption is something that SFTP provides. Although not absent from SOAP, SOAP encryption must be an explicit choice and implemented as such.

Nevertheless most answers identified the correct mechanism in each case and candidates were usually able to explain why the chosen mechanism was correct.

SECTION B

B4.

a) Name the computer network architecture shown in Figure 1 and explain how it works.

(3 marks)

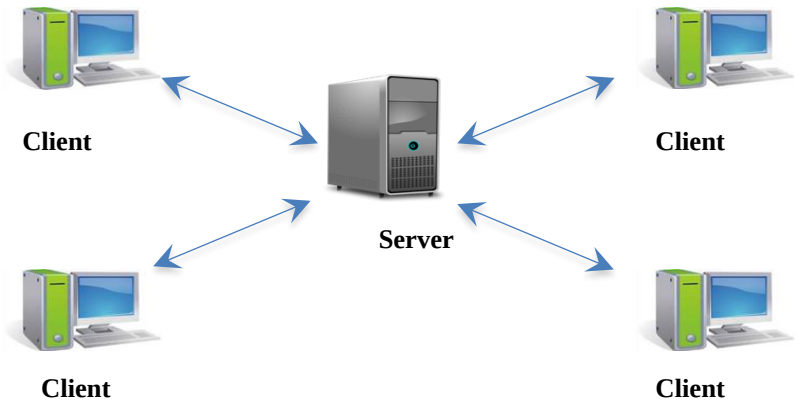


Figure 1

b) Describe the most important characteristics of the building blocks of the architecture shown in Figure 1 above.

(4 marks)

c) Explain the advantages and disadvantages of this architecture.

(6 marks)

d) Explain the differences between the following types of client-server architecture and give a brief description of how each type works. Include a drawing of EACH architecture in your answer.

i) 1-tier architecture
ii) 2-tier architecture
iii) 3-tier architecture

(12 marks)

Answer Pointers:

a) The computer network architecture shown is an example of client server technology.

Client sends a request/query to server and server responds accordingly. The client does not share any of its resources. They are subordinates to servers, and their access rights are defined by servers only. They have localised databases.

b) **Characteristics:**

- **Client.** A client is a single-user workstation that provides presentation services, database services and connectivity along with an interface for user interaction.

- **Server.** A server is one or more multi-user processor with a high capacity of shared memory which provides connectivity and the database services along with interfaces relevant to the business procedures.

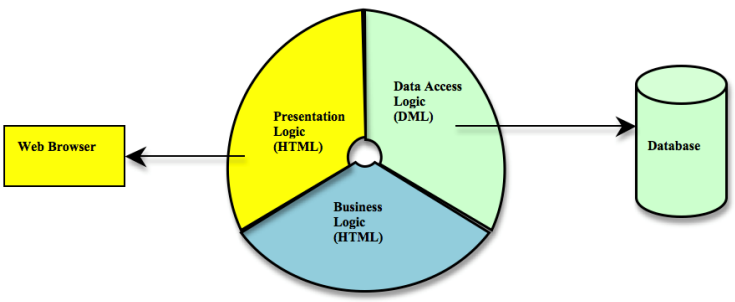
c) **Advantages (if compared with P2P):**

- Centralisation. Unlike P2P, where there is no central administration, in this architecture there is a centralised control. Servers help in administering the whole set-up. Access rights and resource allocation is done by servers.
- Management. All the files are stored at the same place. In this way, management of files is straightforward and it becomes easier to find files.
- Back-up and Recovery. As all the data is stored on the server, it is easy to make a back-up. In the event of breakdowns, data can be recovered easily and efficiently, whilst in P2P backups are required for each workstation.
- Maintenance and Scalability. Changes can be made easily by just upgrading the server. New resources and systems can be added at the server.
- Accessibility. The server can be accessed remotely.
- As new information is uploaded to the database, each workstation need not have its own storage capacities increased (as may be the case in P2P). All the changes are made only in the central computer on which the server database exists.
- Security. Rules defining security and access rights can be defined easily.
- Servers can perform different roles for different clients.

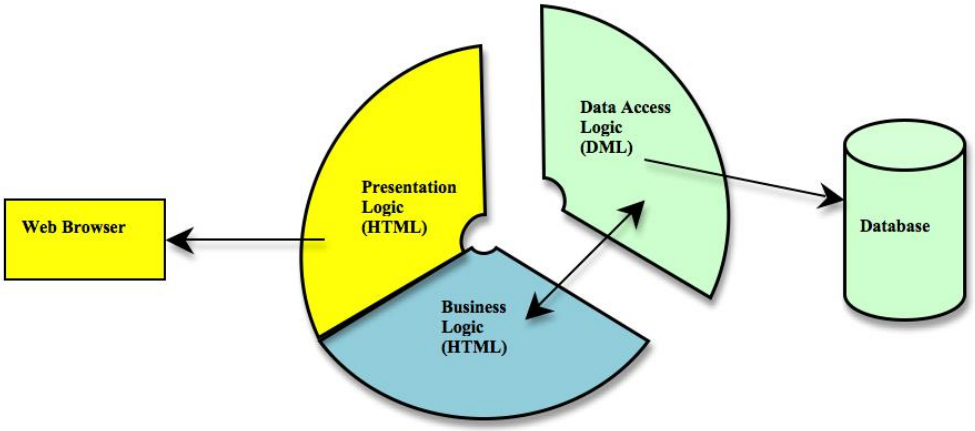
Disadvantages (if compared with P2P):

- Congestion in Network. Too many requests from the clients may lead to congestion, which rarely takes place in a P2P network. Overload can lead to breakdown of servers. In P2P, the total bandwidth of the network increases as the number of peers increases.
- Client-Server architecture is not as robust as a P2P; if the server fails, the whole network fails. Also, if you are downloading a file from a server and it aborts, the download stops altogether.
- Cost: It is very expensive to install and manage this type of computing.
- Professional IT people are needed to maintain the servers and other technical details of network.

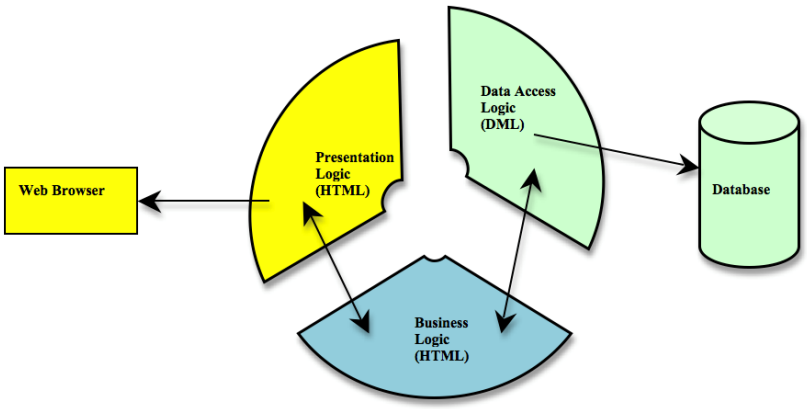
d) (i) **1-Tier architecture.** This is where the Presentation logic, Business logic and Data Access logic are all contained within a single component.



d) (ii) **2-Tier architecture.** This has more than one layer, where all database access is handled by a completely separate component provided by a vendor.



d) (iii) **3-Tier architecture.** For this there should be a separate component in the Presentation layer for each user transaction; a separate component in the Business layer for each business entity (database table); and a separate component in the Data Access layer for each supported DBMS.



Examiners' comments:

With regard to Section B, questions B4 and B5 were similarly answered, with most answers having some parts that were answered correctly and other parts where the candidates had difficulty. For B4 there were few mistakes and most candidates correctly identified the client-server architecture represented in the paper. Most candidates also correctly explained the workings of such architecture, part b), and also provided an adequate account of its advantages and disadvantages, part c).

However, part d) of the question differentiated the candidates, with only a few candidates able to provide an adequate explanation of the architectures.

B5.

a) Define a wide area network.

(4 marks)

b) Give a short description of the characteristics of each of the following WAN technologies:

i) Circuit Switching

(4 marks)

ii) Message Switching

(4 marks)

iii) Packet Switching

(4 marks)

c) Define Switched Multimegabit Data Service (SMDS) and explain its main advantages and disadvantages.

(4 marks)

d) Explain which WAN technology is shown in Figure 2 and list its advantages and disadvantages, especially with respect to SMDS.

(5 marks)

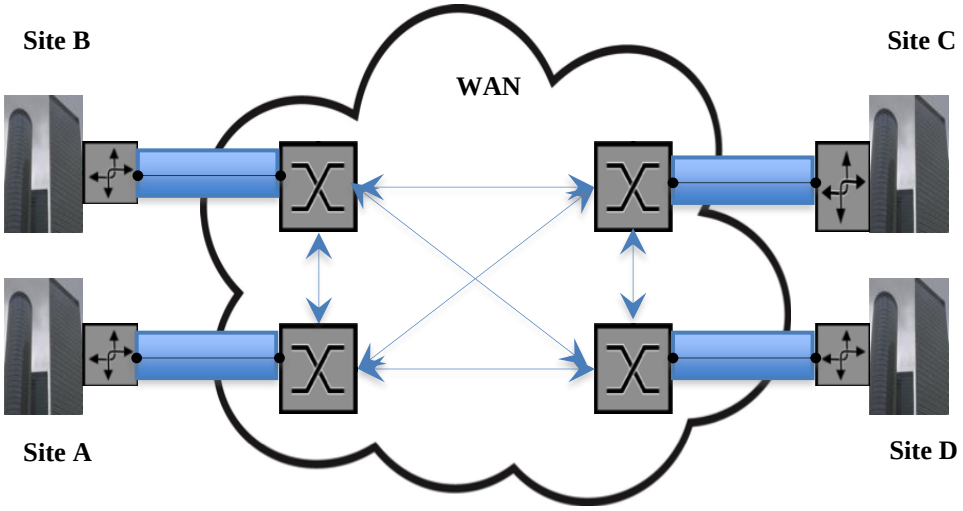


Figure 2

Answer Pointers:

a) A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LAN) and metro area networks (MAN). This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.

b) **WAN characteristics:**

- **b) (i) Circuit switching.** This involves creating a direct physical connection between sender and receiver, a connection that lasts as long as the two parties need to communicate. Although both sender and receiver must abide by the same data transfer speed, circuit switching does allow for a fixed (and rapid) rate of transmission. The primary drawback to circuit switching is the fact that any unused bandwidth remains exactly that: unused. Because the connection is reserved only for the two communicating parties, that unused bandwidth cannot be "borrowed" for any other transmission. The most common form of circuit switching happens in that most familiar of networks, the telephone system, but circuit switching is also used in some networks. Currently available ISDN lines, also known as narrowband ISDN, and the form of T1 known as switched T1, are both examples of circuit-switched communications technologies.

- **b) (ii) Message switching.** Unlike circuit switching, message switching does not involve a direct physical connection between sender and receiver. When a network relies on message switching, the sender can fire off a transmission, after addressing it appropriately, whenever it wants. That message is then routed through intermediate stations or, possibly, to a central network computer. Along the way, each intermediary accepts the entire message, scrutinizes the address and then forwards the message to the next party, which can be another intermediary or the destination node. What is especially notable about message-switching networks and, indeed, happens to be one of their defining features, is that the intermediaries are not required to forward messages immediately.

- **b) (iii) Packet switching.** In packet switching, all transmissions are broken into units called packets, each of which contains addressing information that identifies both the source and destination nodes. These packets are then routed through various intermediaries, known as Packet Switching Exchanges (PSEs), until they reach their destination. At each stop along the way, the intermediary inspects the packet's destination address, consults a routing table and forwards the packet at the highest possible speed to the next link in the chain leading to the recipient. As they travel from link to link, packets are often carried on what are known as virtual circuits - temporary allocations of bandwidth over which the sending and receiving stations communicate after agreeing on certain "ground rules," including packet size, flow control, and error control. Thus, unlike circuit switching, packet switching typically does not tie up a line indefinitely for the benefit of sender and receiver.

c) SMDS is a broadband public networking service offered by communications carriers as a means for businesses to connect LANs in separate locations. It is a connectionless, packet-switched technology designed to provide business with a less expensive means of linking networks than through the use of dedicated leased lines. Besides reducing cost, SMDS is notable for being well-suited to the type of "bursty" traffic characteristic of LAN (or LAN-to-LAN) communications.

Because SMDS is connectionless, it is available when needed, rather than being "on" at all times. It is also a fast technology, transmitting at speeds of 1 Mbps to (in the United States) 45 Mbps. The basis of an SMDS connection is a network address designed as a telephone number that includes country code and area code, as well as the local number. This address is assigned by the carrier and is used to connect LAN with LAN. A group address can also be used to broadcast information to a number of different LANs at the same time.

d) The technology is ATM (Asynchronous Transfer Mode). ATM is a transport method capable of delivering not only data, but also simultaneous voice and video over the same communications lines. ATM is a connection-oriented networking technology and is suitable for high-speed LAN and WAN networking over a range of media types, including traditional coaxial cable, twisted pair, and fibre optical cabling.

A disadvantage is that ATM networks must be made up of ATM-compatible devices which are both expensive and not yet widely available. In addition, there is a "chicken-or-egg" dilemma facing serious ATM deployment: businesses are unlikely to incur the expense of investing in ATM-capable equipment if ATM services are not readily available through communications carriers over a wide area. As a result, carriers may be reluctant to invest in ATM networking solutions if there is insufficient demand for the service.

Examiners' comments

The answers to B5 followed a similar pattern to B4 in that parts a) and b) were relatively easier than c) and d). Candidates therefore obtained the bulk of their marks answering a) and b), with only the more able candidates gaining high marks in c) and d).