BCS THE CHARTERED INSTITUTE FOR IT

BCS Higher Education Qualifications
BCS Level 5 Diploma in IT

September 2018 Sitting

EXAMINERS' REPORT

Computer Networks

General comments on candidates' performance

The September 2018 exam continued the trend of focusing on evaluating the candidate's understanding and knowledge of basic computer networks concepts. April results improved so there is reason to believe that September 2018 results should also show an improvement from previous years.

Question 1 was the most popular question with almost 97% of the candidates responding to the question and almost 81% of those attempts obtaining a favourable mark. The least popular question was question 6 with only 11% of candidates attempting it and a pass rate of 22%.

Candidates seemed to prefer questions from Section A and most of the efforts were directed to questions 1, 2 and 3.

There is evidence that candidates would benefit from:

- preparing for all topics indicated in the syllabus;
- using the examiners' report and past papers to focus on a deeper understanding of concepts;
- prepare to answer questions relating to specific scenarios and develop critical thinking skills.

Candidates should continue to practice their examination skills to include reading the questions carefully and to focus only on what has been asked. They should also structure their answers appropriately and consider the marks allocated per question. As it can be indicated in the report below, most of the questions could have been answered with short statements rather than extensive paragraphs.

It is also recommended to the candidates to read the recommended reading list as most of the questions are based on it.

Question A1

A1. This question focuses on TCP/IP and the OSI model.

a) Indicate the 7 layers of the OSI model in the correct order and briefly describe the function of each layer. **(7 marks)**

b) Explain the difference between TCP and UDP protocols. Provide an example of an application that uses TCP and an application that uses UDP. **(6 marks)**

c) Explain the purpose of the 3-way handshake in TCP/IP connections and briefly describe the steps involved in it. **(8 marks)**

d) Explain the use of port numbers for both TCP and UDP. Define the term 'well-known' ports. **(4 marks)**

Answer Pointers:

Part (a)

The 7 layers of the OSI model are:

Application	Network process to application
Presentation	Data representation and encryption
Session	Inter-host communication
Transport	End-to-end connections and reliability
Network	Path determination and IP addressing
Data Link	Physical addressing (MAC)
Physical	Data encoding, physical medium attachment.

Part (b)

TCP is connection-oriented protocol – once a connection is established, data can be sent bidirectional and delivery is guaranteed.

UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

Examples of applications that use TCP are: FTP, SMTP
Examples of applications that use UDP are: VoIP, DNS, Streaming media

Part (c)

Three-way handshake is a method used in a TCP/IP network to create a connection between a local host/client and server. It is a three-step method that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins.

Three steps: the client sends a SYN message indicating it wants to establish a connection; the server sends a message that combines an ACK for the client's SYN and contains the server's SYN; and then the client sends an ACK for the server's SYN.

Part (d)

When a program on a computer sends or receives data over the Internet it sends that data to an IP address and a specific port on the remote computer and receives the data on a usually random port on its own computer.

If it uses the TCP protocol to send and receive the data, then it will connect and bind itself to a TCP port. If it uses the UDP protocol to send and receive data, it will use a UDP port. Once an application binds itself to a particular port, that port cannot be used by any other application. It is first come, first served.

The port numbers in the range from 0 to 1023 are the well-known ports or system ports. They are used by system processes that provide widely used types of network services.

Examiner's Comments

This was the most popular question of Section A, with 97% of candidates attempting it. It was also the one with the highest passing percentage as almost 81% of the candidates that attempted the question passed it. The average mark for this question was 14.

There is evidence that candidates were well prepared for this question. They had good knowledge of the OSI model and were able to describe its layers. Candidates seemed to understand the differences between TCP and UDP protocols. They could provide correct examples of applications that use these protocols and identify common ports that are used by these protocols.

Question A2

A2. This question focuses on Local Area Networks (LAN) and Ethernet technologies.

a) Provide a definition for the networking devices known as router and switch and explain the operational difference between them. **(6 marks)**

b) Discuss three differences between distance-vector and link-state routing protocols. **(9 marks)**

c) Briefly discuss two reasons why Quality of Service is necessary in IP networks. **(4 marks)**

d) Describe three Quality of Service parameters that are used to characterise the behaviour of a network connection. **(6 marks)**

Answer Pointers:

Part (a)

A router is a device that is capable of sending and receiving data packets between computer networks, also creating an overlay network. Router operates at the network layer. Routers store IP address in routing table and can use routing protocols to calculate the best path to remote networks.

A switch is a networking device that performs the same job as the hub; it connects network segments or devices making them act as a single network. Switch operates at the data link layer. Switch stores MAC addresses of locally connected devices.

Part (b)

Distance Vector routing protocols base their decisions on the best path to a given destination based on the distance. Distance is usually measured in hops, though the distance metric could be delay, packets lost, or something similar. If the distance metric is hop, then each time a packet goes through a router, a hop is considered to have traversed. The route with the least number of hops to a given network is concluded to be the best route towards that network.

Link state protocols are also called shortest-path-first protocols. Link state routing protocols have a complete picture of the network topology. Hence, they know more about the whole network than any distance vector protocol.

Three separate tables are created on each link state routing enabled router. One table is used to hold details about directly connected neighbours, one is used to

hold the topology of the entire internetwork and the last one is used to hold the actual routing table.

Part (c)

QoS helps manage packet loss, delay and jitter on a network infrastructure and some applications are sensitive to those parameters.

A network administrator can identify the applications that have priority and assign an appropriate QoS to treat the traffic.

Part (d)

Loss—A relative measure of the number of packets that were not received compared to the total number of packets transmitted. Loss is typically a function of availability.

Delay—The finite amount of time it takes a packet to reach the receiving endpoint after being transmitted from the sending endpoint.

Delay variation (Jitter)—The difference in the end-to-end delay between packets.

Examiner's Comments

Second most popular question of section A with almost 92% of the candidates attempting it. However, only 42% of the those attempts obtained a passing mark. The average mark for this question was 9 with a high of 23 and a low of 0 marks.

This question was attempted by the majority of candidates and there is evidence that they seemed familiar with network routers and switches. However, their familiarity was mostly about home use devices rather than network appliances that are used in business and large corporate networks. Candidates demonstrated difficulty in explaining Distance Vector and Link-State routing protocols as well as QoS.

Question A3

A3. This question focuses on error control in communications systems.

a) Briefly discuss the operational functionality of Cyclic Redundancy Check. **(8 marks)**

b) Explain the difference between single-bit and burst errors and indicate an error technique that can be used to detect each of them. **(6 marks)**

c) Explain the term residual error rate as an error detection control technique. **(5 marks)**

d) Explain transverse parity check and longitudinal parity check. Describe how the combination of these can provide error correction capability. **(6 marks)**

Answer Pointers:

Part (a)

Cyclic redundancy checking is a method of checking for errors in data that has been transmitted on a communications link. A sending device applies a 16- or 32-bit polynomial to a block of data that is to be transmitted and appends the resulting

cyclic redundancy code (CRC) to the block. The receiving end applies the same polynomial to the data and compares its result with the result appended by the sender. If they agree, the data has been received successfully. If not, the sender can be notified to resend the block of data.

Part (b)

Single bit error: The term single bit error means that only one bit of a given data unit (such as byte character/data unit or packet) is changed from 1 to 0 or from 0 to 1.

Burst error: Means that 2 or more bits in the data unit have changed from 1 to 0 from 0 to 1.

Hamming code can be used to detect single-bit errors whilst CRC can be used for burst errors.

Part (c)

In digital transmission schemes, including cellular telephony systems, a certain percentage of received data will be detected as containing errors, and will be discarded. The likelihood that a particular bit will be detected as erroneous is the bit error rate.

Residual error rate characterises the likelihood that a given bit will be erroneous but will not be detected as such. Bit errors that are not detectable by coding techniques at the receiver side occur with a residual error probability. The better the coding technique is, the lower is its residual error probability for different bit error rates.

Part (d)

If we regard a block of, say, 1024 bits as being divided into a number of equal length frames, say 128 8-bit frames, then we can use one bit of each frame as a parity bit for that frame. This is known as a transverse parity check.

We can also use the last of the 128 frames as a parity frame, with bit 1 of the frame acting as a parity bit for the string of bit 1s, bit 2 as a parity bit for the string of bit 2s and so on. This is known as a longitudinal parity check.

If there is a single-bit error in the block, then the transverse parity check will reveal which frame contains the error and the longitudinal parity check will reveal which bit within the frame has been corrupted, and hence allow it to be corrected. The combination of transverse and longitudinal parity checks thus allows a single-bit error to be detected and corrected.

Examiner's Comments

This was the least popular question of section A with 57% of the candidates attempting it and 47% of those attempts obtaining a passing mark. The average mark for this question was almost 9 with a high of 20 and a low of 0 marks.

Despite this being the least popular question of section A, there is evidence that candidates who attempted this question demonstrated familiarity with error control in digital communications; they also seemed to understand the function of CRC. There is evidence that few candidates were able to correctly explain the term residual error rate.

Question B4

B4. This question is about Wide Area Networks (WANs).

a) Describe the key differences between circuit switching and packet switching networks. For each type, provide examples of two typical technologies. **(10 marks)**

b) Explain the problems that a large international organisation might have when operating a large leased line full mesh network. Detail how a managed service such as Frame Relay might alleviate those problems.

(7 marks)

c) Explain how a cost-conscious business with multiple sites might benefit from using the Internet as a public network to provide WAN connectivity between its sites. Detail the technical considerations, technologies and security operation necessary to utilise this option. **(8 marks)**

Answer Pointers:

Part (a)

For a packet-switched network, data is transferred by dividing the data into individual packets and passing it through the circuits to the other host. In packet-switched networks, the route is not exclusively determined when the packets hit the wire. Using routing algorithms, each packet may actually take a different route through the network to arrive at the destination host. Unlike a circuit-switched network where a static route is setup and pre-established prior to initializing connections to the host.

For packet switched, could include Frame Relay, ATM, MPLS.

For circuit switched, could include POTS/Dialup, ISDN.

Part (b)

Problems with leased line full mesh network include:

- Number of links grows exponentially with the number of sites (n(n-1)/2)
- Fixed bandwidth and cost whether it's used or not
- Can get very complex to manage and maintain (routing tables for example)
- To make use of all links careful design of routing protocols is needed

Frame Relay managed service might offer:

- Organisation only pays for local loop between sites and local exchange
- Full mesh can be achieved by use of virtual circuits so reduces line rental cost
- Organisation has choices over bandwidth options like CIR, access rate, etc.

Part (c)

Essentially anywhere which has a connection to the Internet could use the public Internet to provide connections between sites, connection to a central office or teleworker/SOHO offices access to a central office as businesses will only pay cost of a local loop.

Considerations when utilising this option might include:

- Virtual Private Networks (VPN's)need to be used
- Need to consider end points carefully where encryption ends
- VPN's don't provide anonymity because of endpoints
- Connectivity consideration – need tunnelling between sites (encapsulation)

- Security Considerations – Encryption because of public traffic/sniffing
- Use of IPSec or SSL/TLS based VPN's or even TOR

Examiner's Comments

This question was attempted by 53% of the candidates and had a very low passing mark of 12%. The maximum mark for this question was 15 whilst the minimum was 0 and the average 4 marks.

There is evidence that candidates listed facts rather than structured, thought out responses.

There is evidence that basic application of network knowledge to simple case study examples missing.

The evidence also indicates that candidates would benefit from taking their time to read the question to understand what is being asked for and to demonstrate an understanding of terminology e.g. the question asks for recommending a type of network media and candidates answers recommend UDP or TCP or packet switching or circuit switching picked up from previous questions. Sometimes when asked about network media, candidates discuss MPLS/UDP/Streaming in one part of the question and then revert to recommending wireless in another.

There is evidence that terminology is used which is not standard vocabulary, for example "guided networks". There is also evidence that candidates are unable to distinguish the difference between media, protocol, topology or technology and are not familiar with basic circuit switching, packet switching or WAN protocols which could be under each type.

Question B5

B5. This question focuses on Local Area Networks (LAN) and Ethernet technologies.

a) Explain the types of networking media would be most appropriate for the following scenarios and justify the reasons for selecting it. **(15 marks)**

   i. Two hundred end users in a large office block working for a financial trading company with fast changing financial data.

   ii. An IT research lab researching big data search and storage solutions with data centre research facilities located across a large geographic area.

   iii. A festival venue based at a farm with a fixed broadband connection, where several thousand festival goers attend a festival several times a year and for the remaining time the fields are used for sheep grazing.

b) Discuss why fibre optic cables are more suitable than copper wired or wireless media for high voltage AC environments. **(5 marks)**

c) Explain the key protocol and operational differences between Ethernet (IEE 802.3) and Wireless LAN's (IEEE80.11) **(5 marks)**

Answer Pointers:

Part (a)

(i) Media: Structured cabling using UTP
Justifications:
- users will usually be in fixed positions and a modern building will be designed with modern cabling in mind;
- individual bandwidth to end users with high bandwidth computing requirements;
- also wired networks and easier to physically secure for sensitive data.

(ii) Media: Fibre Optic Cabling
Justifications:
- Data centres with big data will require large bandwidth capacities (dark fibre can support up to Tbps)
- As fibre optic uses light waves in a glass vacuum, the signal can go for several hundred km, but the signal needs to be boosted
- Service providers often have a national infrastructure of fibre-based networks to major cities.

(iii) Media: Wireless connectivity (Wifi or WiMax)
Justifications:
- Temporary networking requirements across a large area with a fixed wired networking point suited to wireless.
- No wasted fixed infrastructure needs to be in place to cater for limited usage.
- Compatible with users' mobile devices and no dedicated specialist devices or hardware needed
- Good for user mobility.

Part (b)

(1) Copper networks are affected by electromagnetic interference
(2) Wireless networks are impacted by interference at certain frequencies
(3) Fibre optic being light is not affected by either
(4) Fibre optic cables can share ducts or pylons with electrical cables.
(5) Fibre optic doesn't conduct electricity

Part (c)

(1) Ethernet uses collision detection (CSMA/CS) and Wifi uses collision avoidance (CSMA/CA)
(2) Ethernet can be restricted to known physical cabled points so limited access opportunities
(3) Wireless traffic is in the air, so anyone can see and read the traffic if it's not encrypted
(4) In large multi access environments, wireless devices can't communicate directly and need to go through an access point to connect with non-wireless devices as well
(5) Frame format for WiFi and Ethernet are different.

Examiner's Comments

This question was attempted by 85% of the candidates making it the most popular one of section B, however it was the question with the lowest passing ratio of almost 9.8%. The maximum mark for this question was 17 and the average mark was 5.

There is evidence that few candidates knew the disadvantages with mesh networks or what constitutes a mesh network and little understanding was demonstrated on the differences between 802.11 and 802.3.

Question B6

B6. This question IP Inter-networking and WAN's.

a) Briefly discuss the meaning of each of the following terms and explain their relationship to WAN connectivity. **(16 marks)**

b) Explain and justify which IP routing protocol is best for WAN connectivity in a scenario where an organisation wants to utilise all its WAN links between all of its sites even though the links have different bandwidths. **(4 marks)**

c) Explain and justify which IP routing protocol is best for WAN connectivity in a scenario where two large businesses have merged together and have different vendor's routers and they want to minimise the impact of routing changes between the organisations **(5 marks)**

Answer Pointers:

Part (a)

(i) DCE (Data Communications Equipment) In computer data transmission, DCE (Data Communication Equipment) is the interface that a modem or other serial device uses in exchanging data with the computer. It terminates the analogue or digital local loop and provides the clocking to synchronise the signal over the WAN.

(ii) DTE (Data Termination Equipment) DTE is typically the serial port on a computer/workstation/router/switch which connects to the DCE.

(iii) CSU/DSU/NTU (Channel Service Unit/Data Service Unit/Network Terminating Unit) A CSU/DSU terminates a digital local loop and converts digital signals from a router to a leased line. It synchronizes the signal to a given clock rate.

(iv) CPE (Customer Premises Equipment) Customer premises equipment (CPE) is telephone or other service provider equipment that is located on the customer's premises (physical location) rather than on the provider's premises or in between. Telephone handsets, cable TV set-top boxes, and Digital Subscriber Line routers are examples.

(v) Demarcation point - Also called point of demarcation (POD), demarc extension, or demarc, it is the physical point at which the public network of a telecommunications company (i.e., a phone or cable company) ends and the private network of a customer begins - this is usually where the cable physically enters a building.

(vi) Local loop. The local loop is the physical link or circuit that connects from the demarcation point of the customer premises to the edge of the common carrier or telecommunications service provider's network.

Part (b)

Typically, an answer should be looking to suggest OSPF or EIGRP but essentially the feature which is needed is unequal cost load balancing which is a feature of EIGRP where WAN links can have different bandwidths and still be used to carry data over them.

Part (c)

Typically, an answer should be looking to suggest internal routing protocols such as IS-IS, OSPF or EIGRP which can scale. However, it is OSPF which provides the area functionality to minimise the impact of routing changes, provides the interoperability between different router vendors.

Examiner's Comments

Least popular of the questions with only 11% of attempts. However, from those attempts almost 22% of them were successful. This also was the question with the lowest maximum mark, which was 13 marks and an average of 5.

There is evidence that few candidates demonstrated understanding of the basic components of WAN's, DCE, DTE etc which are the basic building blocks of WAN connectivity. In addition, the evidence shows that some lacked knowledge of the basic routing protocols, the difference between internal/external routing protocols and the properties of each routing protocol (like link state/distance vector and the concepts of equal cost or unequal cost routing).