BCS THE CHARTERED INSTITUTE FOR IT

BCS Higher Education Qualifications
BCS Level 5 Diploma in IT

March 2016 Sitting

EXAMINERS' REPORT

Computer Networks

General comments on candidates' performance

The top 25% of candidates performed very well and every question had a few candidates gaining close to full marks.

It was still the case that some 25% of candidates gained a mark of less than 25%. While some of these candidates appear to have such poor skills in written English that they cannot express the knowledge, the majority seem to be inadequately prepared. Future candidates are reminded to use the previous exam papers and the answer pointers provided in the examiners' reports and available on the BCS website.

Question A1

This question is about broadband Internet access.

a) A common method for providing broadband Internet access over existing telephone lines is Asymmetric Digital Subscriber Line (ADSL).

i. Why is it called asymmetric? **(4 marks)**

ii. Briefly describe how ADSL is able to transmit both data and telephone calls over the same twisted pair cable connecting a house to a local exchange without the two signals interfering with each other. **(8 marks)**

This part of the question is about local area networks and the technology usually known as WiFi (IEEE802.11)

b) Briefly explain the difference between the terms infrastructure and ad-hoc when used to describe the operational modes of a WiFi. **(8 marks)**

c) In what circumstances is it appropriate to use ad-hoc mode, and why? **(5 marks)**

Answer Pointers

Part (a)

(i) ADSL is optimised for accessing the web where there is a requirement for greater download than upload rates. This is what makes ADSL, asymmetric where there is a greater data carrying capacity from the exchange to a home than from the home back to the exchange.

(Marking scheme: 2 marks for noting that ADSL was optimised for accessing the web; 2 marks for there being a greater download than upload speed.)

(ii) ADSL delivers data and telephony over the same twisted pair by using higher frequencies for the data services. Telephony occupies the first 3kHz of a line's bandwidth and ADSL uses frequencies in the range 26kHz to 1.1MHz for data. This bandwidth is then divided into 256 channels, each of 4.3kHz and within these 256 channels, adaptive coding is used (QPSK, QAM) to encode up to 64 kbps per channel. Within a home it is important to keep data and telephony separate, which requires the installation of micro-filters.

(Marking scheme: 2 marks for telephony being within 3kHz band; 2 marks for ADSL using higher frequencies for data; 2 marks for dividing the data frequencies into upstream and downstream; 1 mark for appreciating that adaptive coding is used and 1 mark for the need to local micro-filters)

Part (b)

In infrastructure mode, there are network access points, typically wireless routers, through which all devices communicate. In other words, if device A wishes to communicate with device B, it sends packets to a network access point, which then forwards the packets to device B or to another router. (4 marks)

In ad-hoc (peer-to-peer) mode, there are no access points or dedicated routers. The devices communicate directly with each other, which means that each must maintain routing tables and a network map. (4 marks)

Part (c)

Ad-hoc node is appropriate only when no wireless router is available, the number of devices to be connected is small and the connection is temporary. (3 marks)

This is because ad-hoc networks do not scale well and many devices do not support ad-hoc mode connections because they lack the software or hardware necessary to function as a router. (2 marks)

Examiner's Comments

One of the most popular questions but very poorly answered, with only 37% of the candidates achieving a pass mark. The evidence shows that many candidates failed to demonstrate overall knowledge of this area rather than a lack in any specific area.

Question A2

This question is about virtual circuits and the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

a) Define the concept of virtual circuit? **(4 marks)**

b) Explain the three-way handshake process used by TCP to establish a virtual circuit. **(9 marks)**

c) Explain how the TCP protocol would be able to detect errors and data loss, and how it would ensure that the lost data is re-transmitted, whilst transmitting data over a TCP virtual circuit. **(8 marks)**

d) In contrast to TCP, UDP is described as a connectionless protocol. Briefly explain how data is transmitted between two computers using the UDP protocol. **(4 marks)**

Answer Pointers

Part (a)

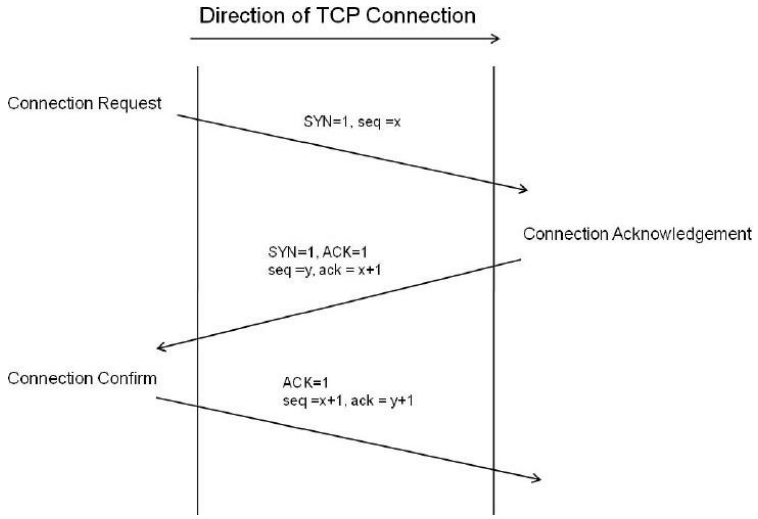
A virtual circuit is a means of establishing a connection between two points on a packet switched network. It is virtual in the sense that it appears as though there is a dedicated link between these two points.

(Marking scheme: 2 marks for the definition of a circuit; 2 marks for the definition of virtual)

Part (b)

A TCP connection is uni-directional which means that for two-way communications, a connection must be established from each side. Each process does however, follow the same three-way handshake procedure.

The end-station requesting the connection will issue a TCP segment with the SYN flag set and the sequence number equal to some initial value – say x. The receiving end-station – if it wants to accept the connection request – will return a TCP segment with both the SYN and ACK flags set. It will also choose a sequence number starting value – say y. The acknowledgement field of this segment will be set to x+1 to acknowledge receipt of the connection request segment. When the requesting end-station receives this response it will issue one further TCP segment with the ACK field set. The acknowledgement in this segment will be y+1 and the sequence number will be x+1.



(Marking scheme: 3 marks for the description of each part of the three-way handshake procedure)

Part (c)

- Every octet transmitted through TCP is uniquely identified by a 32 bit sequence number which increases by one for each new octet.

- Data is transmitted and acknowledged by the receiving end station. Acknowledgements are identified by means of the ACK bit and acknowledgement number within the TCP header.

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

- If errors occur in transmission and data is lost, this will be detected by virtue of the fact that an acknowledgement has not been received within a given time – determined by a timer – then the transmitter simply sends the data again. It is the responsibility of the receiver to ignore any duplicates it receives. Hence, the transmitter will continue re-sending data until a positive acknowledgement is received.

(Marking scheme: 2 marks per bullet point)

Part (d)

With UDP there is no need to establish a connection before sending data. Data is simply packaged into a UDP datagram and transmitted to the destination. There are no sequence numbers or acknowledgements. Hence, there is no way for the transmitter to know whether or not data has been correctly received by the receiver.

(Marking scheme: 2 marks for the connectionless description in terms of sequence numbers; 2 marks for recognising the non-existence of acknowledgements)

Examiner's Comments

This was the most popular question on the paper with 89% of candidates attempting it. It was also reasonably well answered with 54% of candidates achieving a pass mark.

The evidence shows the main weakness in the answers was that candidates' explanations were confused. Thus, for example, while they seemed to have understand how the three-way handshake process is used to establish a virtual circuit, they failed to specify what went on at each step.

Question A3

This question is about providing global network services.

a) Telecommunication companies (Telcos) that provide global network services, define the services they offer to customers within a Service Level Agreement (SLA). Explain the purpose of a SLA and give examples of what it might contain. **(7 Marks)**

b) Companies that have offices in several countries around the globe need to create a private corporate network that is able to connect these sites together and transport traffic of different types between them. An increasingly popular way of providing such a network is to use Multiprotocol Label Switching (MPLS) data services. Briefly explain how MPLS works and how it is able to support different traffic types. **(12 Marks)**

c) An alternative to MPLS might be to consider using the Internet. What are the main disadvantages of the Internet that mean it would offer a worse solution than MPLS? **(6 Marks)**

Answer Pointers

Part (a)

The SLA is an agreement between a customer and a Telco and defines what service is being provided to the customer and what the customer is allowed to do with that service.

The SLA would define:

- The data rate being delivered
- QoS parameters such as expected error rates, lost packets, time delays
- availability of the service (including any downtime for maintenance)
- how the service is being charged to the customer
- what the customer is allowed to connect to and use the service (acceptable use
- policy)
- how the customer can complain if they are unhappy with the service being
- provided

(Marking scheme: 2 marks agreement between Telco and customer; 1 mark for defining service being offered; 1 mark for a relevant example of what is contained within the SLA up to a maximum of 4 marks)

Part (b)

MPLS operates as follows:

- A label switching protocol; a 'label' which is typically a 32 bit number
- Labels are added to data packets by an ingress router based on a classification of the incoming traffic
- Virtual circuits are established through the network for different classes of service. This ensures that each virtual circuit is able to support the QoS demands of a particular traffic class or type.
- Information about which label identifiers have been assigned to which data flow is exchanged between routers using a Label Distribution Protocol. The label that is added by the ingress router identifies the QoS virtual circuit to use and all routers within the MPLS network route according to this label field.
- All intermediate routers are termed label switching routers and route this data based on its label only.
- On reaching the far end of the connection, the final or egress router, removes the label.

(Marking scheme: 2 marks for label switching protocol; 2 marks that virtual circuits are established through the network for different classes of traffic; 1 mark for the mentioning that labels assigned to these circuits are distributed by a label distribution protocol; 2 marks for incoming traffic being classified and assigned to

a specific virtual circuit; 1 mark for labels added and intermediate routers route using only the labels; 1 mark for label being removed by egress router)

Part (c)

Internet QoS:

- The Internet is a connectionless network with data being routed towards the destination.
- The Internet is a best effort service which means that there is no guarantee that data will be delivered and if it is delivered, there is no way of predicting how long it will take.
- No prioritisation – all traffic types handled equally which means that you cannot differentiate time critical applications from non-time critical ones.
- The volume of traffic on the Internet cannot be predicted which means that the bandwidth being delivered for a service cannot be predicted either.

MPLS QoS:

- MPLS network establish virtual circuits between points.
- MPLS networks seek to differentiate traffic types.
- Each different traffic type is assigned to its own QoS defined by the class of service.
- MPLS is able to guarantee the applied QoS.

(Marking scheme: 2 for Internet being connectionless compared to MPLS which is virtual circuit based; 2 marks for Internet being best effort whereas MPLS applies QoS to each traffic flow; 2 marks for Internet treating all data the same and MPLS classifying traffic by their class of service, 2 marks for the fact that the delivered bandwidth via the Internet is not known and 1 mark for the fact that within MPLS this is guaranteed.)

Examiner's Comments

A reasonably popular question attempted by 70% of the candidates, 61% of whom attained a pass mark.

As with question 2, there is evidence that the main weakness in the answers was they were vague and imprecise. Most candidates clearly had knowledge about the topics but were able to demonstrate only superficial knowledge.

Question B4

This question is about routing tables and the way routers maintain them.

a) Describe three different sources a router can use to put/maintain the information contained in the routing table. **(6 marks)**

b) Indicate three main differences between link-state and distance-vector routing protocols. **(6 marks)**

c) Indicate the type of routing protocol (distance-vector or link-state) and the metric used by each of the following protocols: **(6 marks)**

- RIPv1
- EIGRP
- OSPF

d) Briefly describe the link-state protocol known as OSPF and explain how it copes with routing inside a large and complex autonomous system. **(7 marks)**

Answer Pointers

Part (a)

Routers learn/maintain routing information from three different sources:

i. Directly connected networks, these are the networks the router has directly connected through is interfaces and that eventually will distribute to the rest of the routers
ii. Static routes, manually configured by the administrator.
iii. Dynamic routes, learned by means of a routing protocol.

(Marking scheme: 2 marks for identifying each of the sources)

Part (b)

The main differences are:

- Distance vector protocols are used in small networks whereas link state protocol can be used in larger networks
- Distance vector protocol has a high convergence time, but in link state, convergence time is low.
- Distance vector protocol periodically advertise updates, but link state advertises only new changes in a network.
- Distance vector protocol advertises only the directly connected routers and full routing tables, but link state protocols only advertise the updates, and flood the advertisement.
- In distance vector protocol, loop is a problem, and it uses split horizon, route poisoning and hold down as loop preventing techniques, but link state has no loop problems.

(Marking scheme: 2 marks for each of the difference correctly identified with a maximum of 6 marks for this part of the question).

Part (c)

RIPv1 is a distance-vector routing protocol that uses hop count as metric.
EIGRP is a link-state routing protocol that uses a composite metric of bandwidth, delay, reliability, load and MTU.
OSPF is a link-state routing protocol that uses bandwidth as metric.

(Marking scheme: 2 marks for each correctly identified protocol and their metric)

Part (d)

OSPF splits the network in which it is being used into subsets it calls areas one of which is called the backbone area or area zero. The routers are considered to be of different types. A router with all links inside a single area is called an interior router and only gains detailed knowledge of the topology of its own area. A router with some interfaces in the backbone area is referred to as a backbone router. A router with interfaces in more than one area is called an Area Border Router and gains detailed topological information about all those areas which it keeps in separate link-state databases and it inserts summaries of one area into another. A router with an interface to another external network is known as an Autonomous System Boundary Router.

(Marking scheme: 1 mark for identifying areas; 1 mark for indicating the backbone area; 3 point for identifying at least three different roles for the routers; 2 marks for describing how these helps with large and complex autonomous systems)

Examiner's Comments

This was one of the least popular questions, with only 45% of the candidates attempting it. Of those attempting it, 45% achieved a pass mark.

The evidence shows that a common error amongst candidates was to confuse layer-2 and layer-3 functionality, thus referencing the contents of the MAC address table of a switch instead of the routing table of a router. Candidates also failed to explain the difference between link state and distance-vector protocols and failed to recognise examples of such technologies. Finally, candidates did not demonstrate understanding the concept of metric, which is the main parameter used by a routing protocol to calculate the best path.

Question B5

This question concerns the provision of Quality of Service (QoS) within networks that use the Internet Protocol (IP).

a) The Internet is often described as being a "best effort network". Briefly explain what is meant by the term "best effort network". **(4 marks)**

b) Identify, and briefly describe, three QoS parameters that are often measured to characterise the behaviour of a network or network connection. **(6 marks)**

c) Discuss the quality of service requirements of a Voice-over-IP (VoIP) application and how they differ from those of a video-based application. **(8 marks)**

d) Briefly describe the RSVP approach to the provision of QoS. **(7 marks)**

Answer Pointers

Part (a)

A best effort network is one in which no traffic is given preference over any other and where a guarantee of in-order delivery is not promised. Indeed, the network may not guarantee delivery at all. The standard Internet we have today has exactly these characteristics and is thus correctly termed a best efforts network.

(Marking scheme: 2 marks for defining a best effort network in terms of no guarantee of in-order delivery and 2 marks for indicating no preference on traffic type)

Part (b)

The possible answers are:

- usable bit rate , which is the rate with which data can be transferred through the network
- the error rate, which would include both corrupted data and data lost
- transmission delay or latency, that is, the time it takes from when a single bit (or perhaps packet) enters the network to when it emerges at its detonation
- jitter, which is a measure of the variation in delay

(Marking scheme: 1 mark for each parameter and 1 mark for its description with a maximum of 6 marks)

Part (c)

Voice –over-IP is a relatively low data rate application. However, as it is an interactive inter-human application we require a relatively low delay. We need an

"evenness" of delivery and so also want jitter to be low. However, we can cope with a relatively low error rate as a conversation would be difficult to understand if the audio fails. On the other hand, video can have the same restrictions as voice but the error rate can be higher just as long as the voice is audible.

(Marking scheme: 5 marks for describing each parameter requirement and 3 marks for the video requirements)

Part (d)

The Resource ReServation Protocol (RSVP) is defined in RFC 2205 for performing resource reservation in an internet environment. RSVP has the following characteristics:

- RSVP makes reservations for both unicast and multicast transmissions reserving resources based on the individual requirements of multicast members.
- RSVP makes reservations for unidirectional data flow.
- The receiver of a data flow initiates and maintains the resource reservation for that flow.
- RSVP maintains a soft state at intermediate routers and leaves the responsibility for maintain these reservations states to end users.
- These allow RSVP users to specify how reservations for the same multicast group should be aggregated at the intermediate switches.
- Transparent operation through non-RSVP routers.

(1 mark per characteristic and 1 mark for the definition of RSVP.)

Examiner's Comments

Question 5 was attempted by 72% of candidates but with only 37% achieving a pass mark.

The evidence shows most of the candidates did not demonstrate knowledge of the concepts of Quality of Service (QoS); in particular, they failed to identify and describe the main parameters used to measure QoS. Many candidates were unable to describe basic concepts such as "Best effort" in IP networks and provided a confused answer that only repeated the same words of the question without actually providing an answer.

Many candidates confused bandwidth and security as a QoS parameter and were not able to relate QoS parameters with video and/or voice. Most of the candidates failed to explain the RSVP protocol.

Question B6

This question is about error detection and correction.

a) Explain the difference between single-bit errors and burst errors in data transmission. (4 marks)

b) What is meant by a parity bit and a parity check? What sort of errors can a parity check detect? (4 marks)

c) Explain the terms transverse parity check and longitudinal parity check. How can they be combined to provide an error correction capability? (6 marks)

d) In coding theory, what is meant by:
   i. the Hamming distance between two bit strings of equal length? (3 marks)
   ii. the minimum Hamming distance of a code? (3 marks)

e) How does the minimum Hamming distance of a code relate to its error detection and correction capability? (5 marks)

Answer Pointers

Part (a)

Single-bit errors are errors that result in an isolated bit being transmitted wrongly. Burst errors occur when a number of adjacent or nearly adjacent bits are transmitted wrongly. They are typically the result of a burst of electromagnetic noise.

Part (b)

A parity bit is a bit added to the end of a string of binary digits to indicate whether the number of bits in the string with the value 1 is even (even parity) or odd (odd parity). When the string is received, the number of 1s is computed and a check is made to see that this is consistent with the parity bit. This parity check can only detect single bit errors.

Part (c)

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.

Part (d)

(i) The number of bits in which the two strings differ. Thus the Hamming distance between 11010110 and 01111010 is 4

(ii) The minimum of the Hamming distance between all pairs of different valid codewords in the code.

Part (e)

A code with minimum Hamming distance d between its code words can detect at most d-1 errors and can correct (d-1)/2 (rounded down) errors. This question is about error detection and correction including Hamming codes and cyclic redundancy checks.

Examiner's Comments

This was the least popular question on the paper but had the highest pass rate.

Candidates showed a good understanding of the type of errors in data transmission as well as the different methods available to perform error detection. However, there is evidence that they showed less understanding of Hamming distance and its relationship to error detection and error correction.