BCS THE CHARTERED INSTITUTE FOR IT

BCS HIGHER EDUCATION QUALIFICATIONS
BCS Level 5 Diploma in IT

SEPTEMBER 2019

COMPUTER NETWORKS

Answer **any** FOUR questions out of SIX. All questions carry equal marks
Time: TWO hours

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

The marks given in brackets are **indicative** of the weight given to each part of the question.

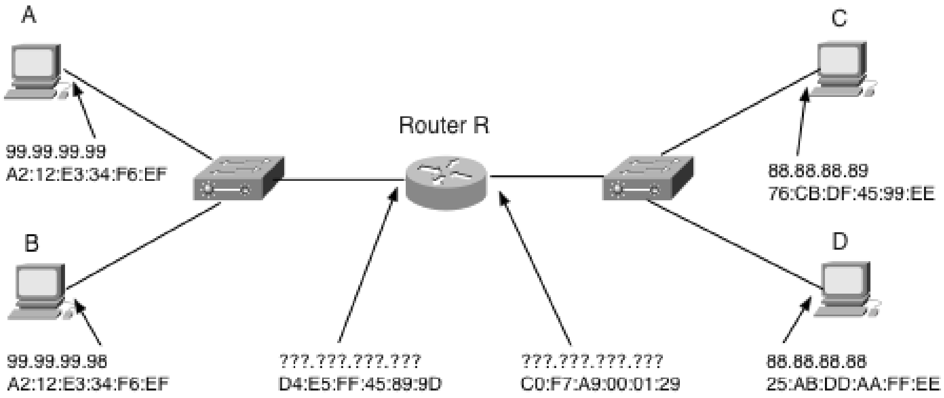
EXAMINERS' REPORT

General comments on candidates' performance

The results for this sitting improved in comparison to the March sitting but the passing rate is still low. There is an improvement in the results of Section B, which might be an indication that candidates are reviewing previous exams. However, it is important that candidates demonstrate an in-depth knowledge as expected in Level 5 and do not focus only on general knowledge. Candidates would benefit from reading the questions and providing thought out answers. Examiners recommend that the candidates provide concise answers. Candidates are reminded that listing the questions answered in the correct order is required.

Section A
Answer Section A questions in Answer Book A

A1. This question is about the operation of IPv4 networks. Considering the information provided in the image below, respond each of the following questions.



a) Given that the subnet mask used in the scenario is /24:

i. Explain which IP addresses cannot be assigned to each interface of R and indicate why. **(6 marks)**

ii. Assign IP addresses to the left and right interfaces interface of the router R. **(2 marks)**

b) Suppose computer A wants to send an IP datagram to computer B and knows B's IP address. Does computer A need to know computer B's MAC address to send the datagram to computer B? If yes, explain the operation used by A to obtain B's MAC address. If not, explain why not and what information would be used for the datagram to arrive to computer B. **(6 marks)**

c) Suppose computer A wants to send an IP datagram to computer C and knows C's IP address. Does computer A also need to know C's MAC address to send the datagram to computer C? If yes, explain the operation used by A to obtain C's MAC address. If not, explain why not and what information would be used for the datagram to arrive to computer C. **(6 marks)**

d) Suppose that R has a datagram (that was originally sent by A) to send to C. Indicate:

i. The MAC addresses on the frame that is sent from R to C. **(3 marks)**

ii. The IP addresses in the IP datagram encapsulated within this frame. **(2 marks)**

ANSWER POINTERS

a)
i. Left-hand interface:
Except for .98 and .99 and these are already allocated (1 mark)
99.99.99.0 is reserved for the network address (1 mark)
99.99.99.255 is reserved for the broadcast address (1 mark)

Right-hand interface:
Except for .88 and .89 and these are already allocated (1 mark)
88.88.88.0 is reserved for the network address (1 mark)
88.88.88.255 I reserved for the broadcast address (1 mark)

ii. Left hand interface any address starting with 99.99.99.* is fine (except for the ones indicated above) (1 mark)
Right hand interface any address starting with 88.88.88.* is fine (except for the ones indicated above) (1 mark)

b)

A must user an ARP request to obtain B's MAC address (1 mark)

ARP = Address Resolution Protocol. (1 mark)

When workstation A wishes to send a packet to workstation B, it first asks the ARP program to look in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine B. (2 marks)

If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine (B) knows that it has that IP address associated with it. (1 mark)

Machine B that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied. (1 mark)

c)

A does not need to obtain C's MAC address (1 mark)

A will forward the frame to the router (1 mark) and the router will then de-capsulate the datagram (1 mark) and then re-encapsulate 1 mark) the datagram in a frame to be sent over the right subnet (1 mark). R will need to run ARP in this case to get C's MAC address, but A will not). (1 mark)

d)

i. MAC Addresses (2 marks + 1 mark for identifying the right interface on Router R)
Right hand side of Router R: C0:F7:A9:00:01:29
Computer C: 76:CB:DF:45:99:EE

ii. IP Addresses (2 marks)
Computer A – 99.99.99.99
Computer C – 88.88.88.89

Examiner's Comments:

This question was attempted by just over half of the candidates. Overall, the responses demonstrated a limited understanding of IPv4 and how it operates. Candidates seemed to have difficulty understanding how routing and subnets work.

A2. This question is about TCP/IP and network protocols.

a) With the aid of a diagram indicate, in the correct order, the layers of the TCP/IP protocol stack that are implemented on the following network components:

i. End system (host). **(1 mark)**
ii. Router. **(1 mark)**
iii. Switch. **(1 mark)**

b) State the primary differences between the link state and distance vector routing algorithms. **(6 marks)**

c) Briefly explain, with the use of an appropriate diagram:

i. The implementation of the Domain Name Service (DNS). **(2 marks)**

ii. How DNS queries are resolved in the DNS system with recursive and iterative queries. **(8 marks)**

d) Indicate in which layer of the TCP/IP Reference model would Internet Control Message Protocol (ICMP) be found. Explain what ICMP is used for, indicating its key areas of functionality with suitable examples. **(6 marks)**

ANSWER POINTS

a)

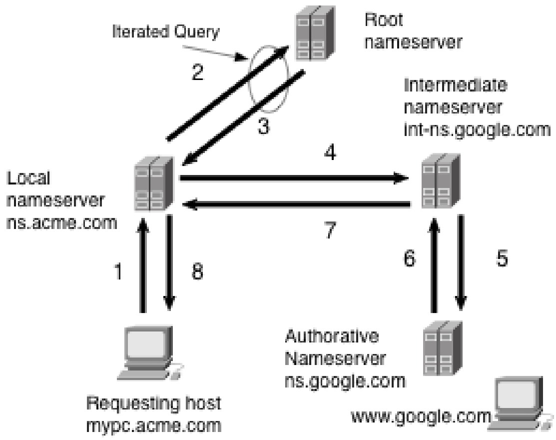
i. Application->Transport-> Network/Internet->Data Link - > Physical (1 mark)
ii. Data Link - > Physical (1 mark)
iii. Network/Internet->Data Link - > Physical (1 mark)

b) Link state: whole knowledge of network topology, Djikstra's algorithm, triggered updates, cost/bandwidth related metrics (3 marks)
Distance Vector: knowledge about directly connected nodes, Bellman Ford algorithm, share info with directly connected devices only, routing by rumour (3 marks)

c)

i. The Domain Name System maps names to IP addresses. It is a distributed database implemented in hierarchy of many name servers. has an application layer protocol for host, routers, name servers to communicate to resolve names. There are 13 root servers; it is broken into zones containing primary and secondary name servers. A diagram such as the following may be used. (2 marks)

ii. Recursive Query: Burden of name resolution on contacted name server, heavy load potential (2 marks) Iterative Query: Contacted server replies with details of server to contact, I don't know this server but please contact x. (2 marks)
A diagram similar to the one below must be provided (4 marks)



d)

ICMP = Internet Control Management Protocol (1 mark)

ICMP is part of the Network/Internet layer (1 mark)

Made up of error reporting and query messages. (1 mark)
Examples include echo, timestamp, address mask, quench, time exceeded destination unreachable... (3 marks)

Examiner's Comments:

This question was attempted by the majority of candidates. Most of the candidates demonstrated a basic level of understanding of TCP/IP but demonstrated a lack of understanding of routing algorithms. They also demonstrated difficulty when explaining the operation of the DNS system, and ICMP.

A3. This question deals with IPv4 and IPv6 interworking.

a) Describe and illustrate the different types of datagram fragmentation in IPv4 when communicating over the internet. Discuss why fragmentation is not a problem in IPv6. **(8 marks)**

b) With the gradual transition from IPv4 to IPv6, discuss the techniques ISP's could use to make this transition easier and achieve interworking between the two. Recommend one solution and justify your choice. **(8 marks)**

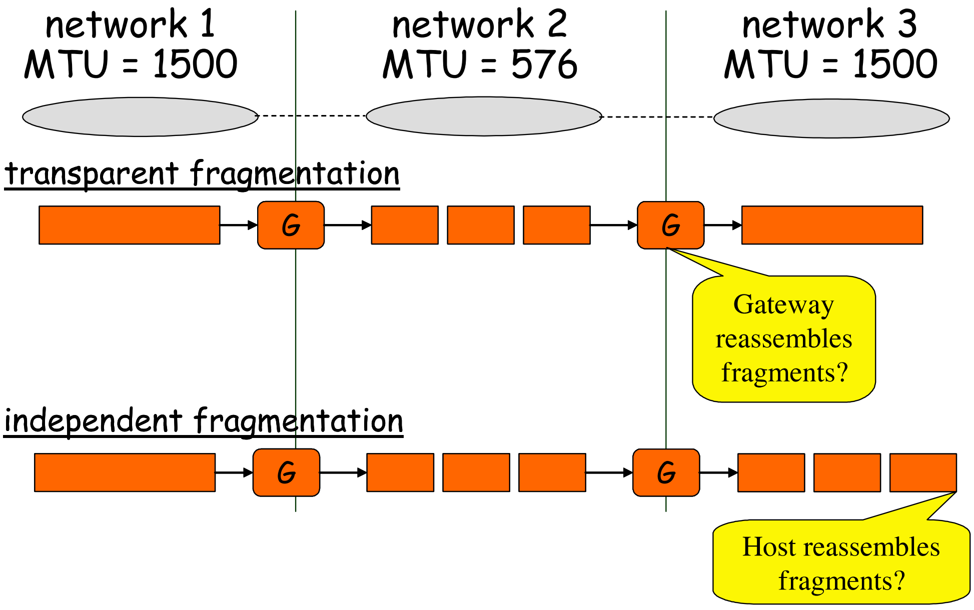
c) Describe how Port Address Translation (PAT – a form of Network Address Translation) works for connecting RFC1918 based private networks to the public Internet. Indicate the data structure required to maintain mapping between the internal private addresses and the public address, illustrating with diagrams where necessary. **(9 marks)**

ANSWER POINTERS

a)

In IPv4 Independent fragmentation is used in the internet except for special cases such as interworking with ATM where transparent fragmentation is required due to cell size in ATM.

IPv6 does not allow fragmentation at routers, the transmitter creates datagrams of the maximum transmission unit. ICMP v6 tells the source what the max transport unit (mtu) of the path is.

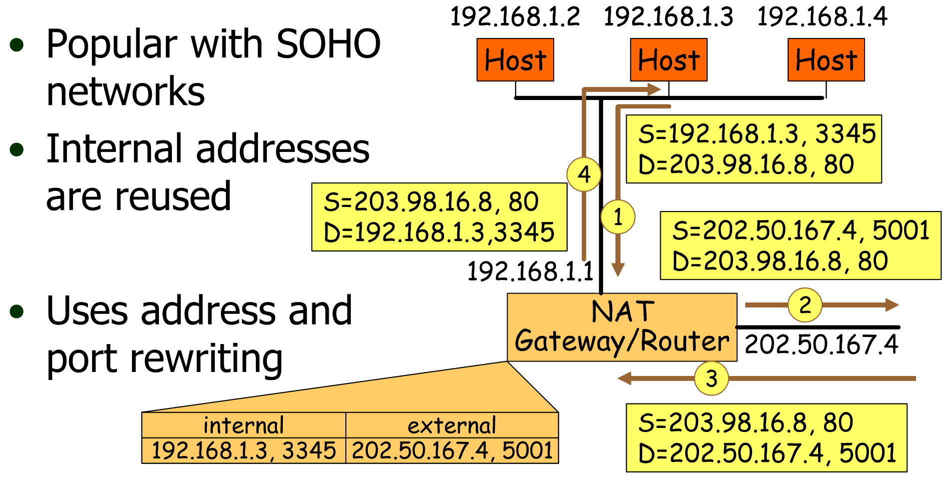


b) Choices include (in order of preference) (1 mark for each)

Dual Stack, Manual tunnelling
Automatic 6-4 Tunnelling
ISAKMP Tunnelling
Teredo Tunnelling
NAT Protocol Translation

Should be dual stack, simultaneous connectivity (2 marks) c)

Single or small number of external public IP addresses mapping (can support up to65535 concurrent connections per public IP addresses) (2 marks)
Use of random ports for the mapping exercise (1 mark)



2 marks for the use of the port mapping table
2 marks for detailing the IP address and ports changing
1 mark for use of external gateway IP public address
1 mark for use of RFC1918 addresses internally

Examiners' Comments:

This was by far the least popular question. There is evidence that candidates were unprepared for questions on IPv6.

Section B
Answer Section B questions in Answer Book B

B4. This question is about types of networks.

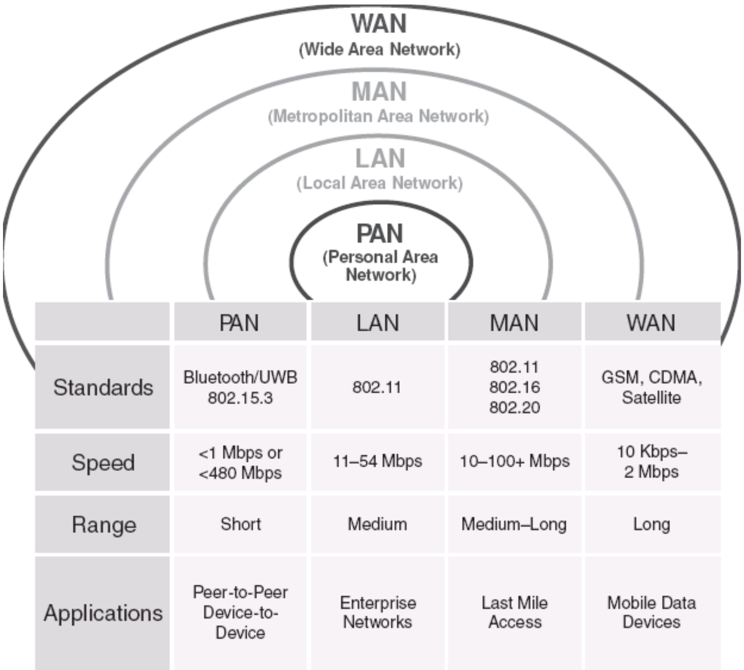
a. For each of the wireless network classifications: WAN, MAN, LAN and PAN, indicate:

   i. Meaning of the acronym. **(4 marks)**
   ii. Typical operational distances. **(4 marks)**
   iii. Typical speed. **(4 marks)**
   iv. Example of a standard. **(4 marks)**

b. Compare and contrast the features of simplex, half-duplex and full duplex modes of network communication in terms of mode/direction of communication performance and examples of each. **(9 marks)**

ANSWER POINTERS

a)
Answer given in the image below (1 mark per correct answer)



	PAN	LAN	MAN	WAN
Standards	Bluetooth/UWB 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	<1 Mbps or <480 Mbps	11–54 Mbps	10–100+ Mbps	10 Kbps– 2 Mbps
Range	Short	Medium	Medium–Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

b)
Answers provided in the table below (1 mark for each correct one)

Basis for Comparison	**Simplex**	**Half Duplex**	**Full Duplex**
Direction of Communication	Communication is unidirectional.	Communication is two-directional but, one at a time.	Communication is two directional and done simultaneously.

Basis for Comparison	Simplex	Half Duplex	Full Duplex
Send/Receive	A sender can send data but, cannot receive.	A sender can send as well as receive the data but one at a time.	A sender can send as well as receive the data simultaneously.
Performance	The half-duplex and full duplex yield better performance than the Simplex.	The full duplex mode yields higher performance than half duplex.	Full duplex has better performance as it doubles the utilization of bandwidth.
Example	Keyboard and monitor.	Walkie-Talkies. Standard Ethernet (Hub or repeater based)	Telephone. Switch based Ethernet

Examiners' Comments:

Most candidates could answer what is meant by LAN or WAN, some knew MAN, but fewer knew what was meant by PAN. Knowing the range and applicability of each type was variable and again there was evidence that knowledge was vague on where the use of MAN and PAN might be the case especially in terms of distance/speed. Giving examples of technologies used was also very variable. Many examples of out of date technologies which haven't been used for a long time (e.g. FDDI, X25 and Token Ring).

In part (b) most candidates who answered were able to differentiate between the different types of communication and given reasonable examples of typical use.

B5. This question deals with Error Detection.

a. Define the two types of errors that occur in data communication. **(4 marks)**

b. In order to address errors in data communication it is first necessary to be able to detect them. Indicate the main error detection technique used in data communications and identify 4 different types of this technique with brief explanation of how they operate. **(14 marks)**

c. Once an error has been detected, explain how Hamming Codes can be used for error correction. **(7 marks)**

ANSWER POINTERS:

a)

Single bit error (1 mark): This 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. (1 mark)

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

b)

Redundancy is an error detecting mechanism, which means a shorter group of bits or extra bits may be appended at the destination of each unit. (2 marks)

There are 4 types of redundancy checks are used in data communication. (1 mark for identification and 2 marks for detail)

Vertical redundancy checks (VRC). The most common and least expensive mechanism for error detection is the vertical redundancy check (VRC) often called a parity check. A redundant bit called a parity bit, is appended to every data unit so, that the total number of 0's in the unit (including the parity bit) becomes even.

Longitudinal redundancy checks (LRC). In longitudinal redundancy check (LRC), a block of bits is divided into rows and a redundant row of bits is added to the whole block.

Cyclic redundancy checks (CRC). The most powerful of the redundancy checking techniques is the cyclic redundancy checks (CRC). CRC is based on binary division. Here a sequence of redundant bits, called the CRC remainder is appended to the end of data unit.

Checksum. The error detection method used by the higher layer protocol's is called checksum.

- The units are divided into k sections each of n bits.
- All sections are added together using 2's complement
- to get the sum.
- The sum is complemented and become the checksum.

The checksum is sent with the data.

c)

Hamming Codes, set of linear error-correcting codes used for forward error correction (FEC) (1 mark)

Hamming code can detect and correct single-bit errors by adding multiple parity bits to a data set. (1 mark)

As an example, one of the simplest Hamming codes is the 7,4 code, which uses each group of four bits to compute a three-bit value, which it appends to the original four bits prior to transmission. (2 marks)

If any of the seven bits is altered in transit, the receiving device can easily identify, isolate, and correct the errored bit. (1 mark)

The 7,4 code is generally considered impractical, as it involves a non-standard character length. (1 mark)

More complex Hamming codes based on standard character lengths (e.g., 11,7 for ASCII and 12,8 for EBCDIC) can also detect and distinguish two-bit and three-bit errors, but not correct them. (1 mark)

Examiner's Comments:

In part (a), a reasonable number of candidates were able to detail the two typical types of error but there was a significant number of answers detailing attenuation/jitter /delay as the types of error encountered.

In part (b) there is evidence that many candidates struggled with answers and being able to score marks (many listed types of error correction which was not a suitable answer).

The evidence shows that candidates were unable to identify redundancy as a concept.

CRC was identified correctly in many cases, some candidates identified parity checks (but not by its redundancy identifier) and checksums featured in many answers. Many candidates listed descriptions on Hamming codes, but this is error correction not detection and was needed for the next part.

In part (c), many candidates identified how Hamming Codes worked reasonably well.

B6. This question relates to TCP/IP Reference Model and Transport Layer.

a. Explain the differences between the two main Transport Layer protocols, TCP and UDP, of the TCP/IP Reference Model. **(6 marks)**

b. Compare the TCP and UDP headers by detailing the fields that are missing from the UDP header when compared to the TCP header. **(8 marks)**

c. Consider the TCP connection mechanism.

  i. What technique is used to set up a TCP connection? **(1 mark)**
  ii. Why is the technique needed? **(2 marks)**
  iii. Outline how this technique works. **(3 marks)**

d. Explain what is meant by flow control and how it is implemented in TCP. **(5 marks)**

ANSWER POINTERS

a)

Answers given in the table below (1 mark for each feature difference)

TCP	**UDP**
Connection Orientated	Connectionless
Traditional Client Server Apps	Real time applications
TCP has a larger header (more fields)	UDP has a much smaller header
Error Checking	No Error Checking
Packets are ordered	Packets are Non ordered
Reliable	Unreliable
Slower	Faster

b)

Identify any 8 fields not in the UDP header as seen in the image below (1 mark for each)

UDP Header

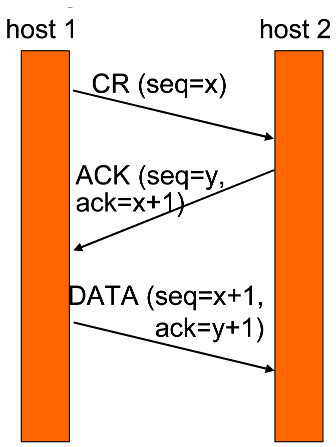
0	16	31
16-bit source port number	16-bit destination port number	8 bytes
16-bit UDP length	16-bit UDP checksum	
data (if any)		

TCP Header

0								16	31
16-bit source port number								16-bit destination port number	20 bytes
32-bit sequence number									
32-bit acknowledgment number									
4-bit header length	reserved (6 bits)	URG	ACK	PSH	RST	SYN	FIN	16-bit window size	
16-bit TCP checksum								16-bit urgent pointer	
options (if any)									
data (if any)									

c)

i. 3-way handshake (SYN, SYN+ACK, ACK) (1 mark), ii. overcomes issue of duplicate connection requests and spurious data packet delivery can be rejected (2 marks), iii. Diagram:



d)

Caused by overload in network nodes causing packets to be delayed (causing timeout) or dropped (lost). Identified by end system either through timeout or triple ACK (loss, fast recovery mechanism). (2 marks)

Max that can be transmitted is the receive window (rx buffer) or congestion window (MSS*number of MSS that can be transmitted) whichever is the smaller. (1 mark)

Uses slow start mechanism up to a threshold (half of congestion window) then start linear increase to probe for upper limit of the network capability. (1 mark)

On event (timeout or triple ACK) the limit is detected, and congestion window is set. The threshold is set to half congestion window at the event and the congestion window is set to 1 or the threshold (1 mark)

Examiners' Comments:

Candidates seemed to understand connection-less and connection orientated, reliable/unreliable but many other differences amounted to the same thing in part (a).

In section (b) there was evidence that candidates were not able to identify that the TCP flag option fields, sequence numbers and window size. Very few could document the TCP/UDP header diagrams.

In part (c), most candidates understood what was required in terms of the 3-way handshake, why it was necessary and how the SYN, SYN/ACK and ACK worked. A reasonable number could document the operation sufficiently.

In part (d) only a small number of candidates were to be able to articulate the concept of window sizes, sliding windows et al. There is evidence that knowledge of the concept of flow control was very limited.