BCS THE CHARTERED INSTITUTE FOR IT

BCS HIGHER EDUCATION QUALIFICATIONS
BCS Level 5 Diploma in IT

COMPUTER NETWORKS

MARCH 2019

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 were extremely low as well as the passing rate. The questions are covering the syllabus and are appropriate to the Level of the module, Level 5. Candidates need to be able to read the questions properly and format their response ensuring that text is given in a form of explanation of the answer, not lists of facts, and the question is answered in the correct order. Candidates would benefit from being prepared to answer in an organised way – for example clearly labelling which part of the question (a, b or c) next to the answer.

Section A
Answer Section A questions in Answer Book A

A1. This question focuses on IPv6 Addressing.

a) IPv6 Addresses have a distinct number of address types, i.e. global unicast, loopback, multicast, unique-local and link-local. Identify the address types for the following compressed IPv6 addresses:

i. 2001:FF00:1:ACAD::FE55:6789:B210
ii. ::1
iii. FF00::997:AB12:F999:67C
iv. FF02::9
v. FC00:22:A:2::CD4:2001:76FA
vi. 2033:DB8:1:1:22:FF01:259A:21FE
vii. FE80::3201:CC01:65B1
viii. FF00::

(8 marks)

b) Using the standard rules of Ipv6 address abbreviation, compress or decompress (as appropriate) the following IPv6 addresses:

i. 2005:0EC0:0200:000a:0000:000B:4400:0802
ii. FE80:0000:0000:000a:0000:6000:008E:9009
iii. FE80::1234:ABC7:FACE:00FF
iv. FF00::
v. 2001:033:0001:1000:0000:330E:10C2:32BF

(5 marks)

c) After executing the ifconfig command on a Linux workstation, the administrator observes the following output:

```
eth0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 3c:15:c2:e0:2d:24
    inet6 fe80::3e15:c2ff:fee0:2d24%en0 prefixlen 64 scopeid 0x4
    inet 10.249.98.1 netmask 0xffffe000 broadcast 10.249.127.255
    nd6 options=1<PERFORMNUD>
    media: autoselect
    status: active
```

i. From the output above, the Linux workstation has been assigned an IPv6 address with a randomly generated interface ID. Explain what this allocation might indicate about the type of network the workstation is connected to. As part of your answer indicate how the device might be obtaining the IPv6 address shown as well as the type of IPv6 address.

(6 marks)

ii. Apart from the type of IPv6 address allocation shown above, explain the other four methods that an IPv6 address can be allocated.

(6 marks)

ANSWER POINTERS

a) i. Global unicast address, ii. Loopback address, iii. Multicast address, iv. Multicast address, v. unique-local address, vi. Global unicast address, vii. Link-local address, viii. Multicast-address (one mark for each correct answer and a total of 8 marks)

b) i. 2005:EC0:200:A::B:4400:802, ii. FE80::A:0:6000:8E:9009, iii. FE80:0000:0000:0000:1234:ABC7:FACE:00FF, iv. FF00:0000:0000:0000:0000:0000:0000:0000, v. 2001:33:1:1000::330E:10C2:32BF (one mark for each correct answer and a total of 5 marks)

c) The output indicates that the device is connected to a local network where an IPv6 enabled gateway is not present and therefore there the IPv6 parameters (global address, local address, or subnet information) are not been provided by such device (4 marks). The workstation is allocating a link local address to itself by using its own internal MAC address as it has no network component to learn from (2 marks).

d) Manual Interface ID Assignment – manually assigned to device by administrator (1 mark). EUI-64 Interface ID Assignment – network portion is assigned by administrator and the rest is determined from the devices MAC address (1 mark). Stateless Auto-Configuration using router advertisements to determine network configuration automatically (2 marks). DHCPv6(Stateful) – similar to DHCPv4 but uses multicast. If no response from a DHCP server, defaults back to a link local address. (2 marks)

Examiners' Comments:

This question was attempted by just over half of the candidates. Overall, the responses demonstrated a limited understanding of IPv6 addressing, including lack of fundamental understanding of IPv6, e.g. address types.

A2. This question is on Local Area Networks.

a) Explain why the existence of active loops in Layer 2 Local Area Networks represents a problem.

(2 marks)

b) Describe three types of problems that can occur when active loops are present in a Layer 2 Local Area Network.

(6 marks)

c) What protocol-based standard is used by bridges and switches to prevent such loops from occurring in the first place and explain briefly how such solution works.

(8 marks)

d) Explain why introducing solutions to loop prevention in Layer 2 networks can also cause a negative impact on network stability and performance. Indicate at least three enhancements made to improve network stability and performance in these scenarios.

(9 marks)

ANSWER POINTERS

a) Loops often implemented for resilience. Layer 2 networks have no mechanism for network traffic to timeout (like TTL in IP) so traffic could potentially go around in a loop forever if there is no end destination (broadcasts and multicasts for example) (2 marks)

b) Switch MAC database instability may result from MAC addresses flip flopping between ports due to loops (2 marks) Broadcast storms which may result in complete network instability and eventually crashing network devices (2 marks) Multiple frame transmissions, the same frame may be transmitted around the network multiple times due to switch instability (2 marks)

c) The protocol used is Spanning Tree Protocol (IEEE 802.1D) (1 mark). Spanning Tree Protocol is implemented on switches to monitor the network topology. Every link between switches, and in particular redundant links, are catalogued. STP then disables redundant links by setting up one preferred and optimised link between switches in the LAN. This preferred link is used for all Ethernet frames unless it fails, in which case the non-preferred redundant link is enabled. When implemented in a network, STP designates one layer 2 switch as root bridge. On this root bridge the preferred and non-preferred links are calculated. The root bridge switch constantly communicates with the other switches in the LAN that implement STP, called non-root bridges, using Bridge Protocol Data Units (BPDUs). After link failure the spanning tree algorithm computes and spans new least-cost tree. (2 marks)

Provided there is more than one link between two switches, the STP root bridge calculates the cost of each path based on bandwidth. STP will select the path with the lowest cost, that is the highest bandwidth, as the preferred link. STP will enable this preferred link as the only path to be used for Ethernet frames between the two switches, and disable all other possible links by designating the switch ports that connect the preferred path as root port (2 marks)

After STP enabled switches in a LAN have elected the root bridge, all non-root bridges assign one of their ports as root port. This is either the port that connects the switch to the root bridge, or if there are several paths, the port with the preferred path as calculated by the root bridge. Because not all switches are directly connected to the root bridge, they communicate amongst each other using STP Bridge Protocol Data Units (BPDUs). Each switch adds the cost of its own path to the cost received from the neighbouring switches to determine the total cost of a given path to the root bridge. Once the cost of all possible paths to the root bridge have been added up, each switch assigns a port as root port which connects to the path with the lowest cost, or highest bandwidth, that will eventually lead to the root bridge. (3 marks)

d) Every time a new loop is added to the topology, the spanning tree algorithm has to be recomputed. Using default timer values this can take up to 45 seconds meaning all communications cease whilst switches are in learning mode etc and then timeouts occur. (3 marks) If links are flapping up and down, spanning tree may constantly be recalculated and hence a large measure of instability results (3 marks) Improvements to Spanning Tree could include (1 mark each, 3 marks maximum)
Rapid Spanning Tree (RSTP) – Standards based IEEE 802.1w
Per VLAN Spanning Tree (PVST/PVST+) (Cisco Proprietary)
Multiple Spanning Tree (MSTP) IEEE 802.1s
VLAN Spanning Tree (VSTP) (Juniper Proprietary)
Shortest Path Bridging (SRB) IEEE 802.1aq

Examiners' Comments:

There is evidence that candidates were unprepared for this question. Candidates either did not attempt the question or their response demonstrated a lack of understanding of local area networks. There was evidence that only a small proportion of candidates were familiar with the concept of active loops. Candidates demonstrated great difficulty in explaining the Spanning Tree Protocol. No candidates achieved a pass in this question.

A3. This question is on Network Fundamentals.

a) What typical network devices operate at the following layers of OSI 7 Layer Model?

i. Layer 1
ii. Up to and including Layer 2
iii. Up to and including Layer 3
iv. Up to and including Layer 7

(4 marks)

b) Indicate the Protocol Data Unit (PDU) used at each layer of the OSI Layer Model.

(7 marks)

c) Explain the key differences between the OSI Layer model and the TCP/IP Reference model.

(5 marks)

d) Describe how the processes of encapsulation/de-encapsulation work within the TCP/IP Reference Model. Expand your answer by using an example of a well-known protocol, such as HTTP, for an end to end conversation between a client and server (assume a direct connection between both devices).

(9 marks)

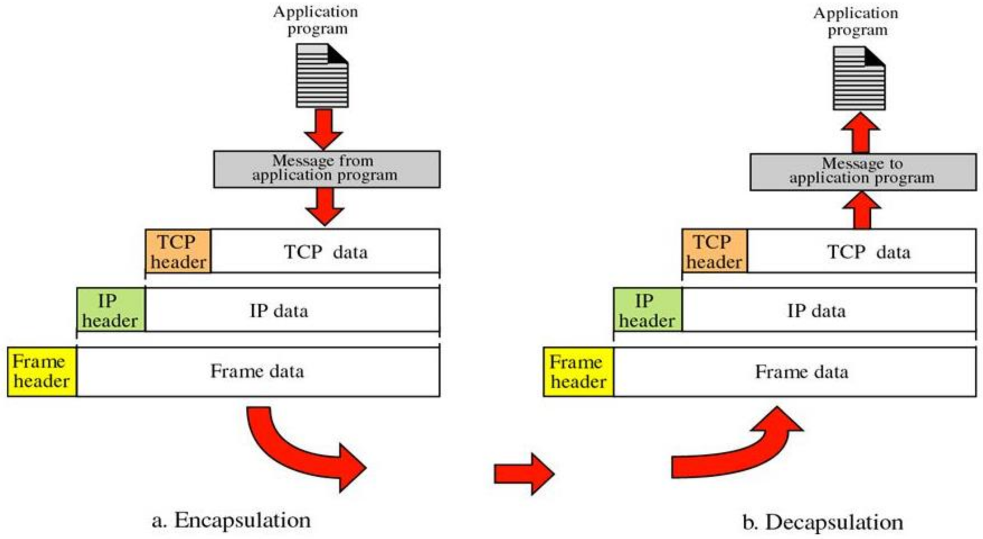
ANSWER POINTERS

a) i. hub or repeater, ii. Bridge or switch, iii. Router or layer 3 switch, iv. Application gateway, application proxy, or application firewall. (1 mark each and a total of 4 marks).

b) layers 5, 6, 7: data (3 marks), layer 4: segments (1 mark), layer 3: packets (1 mark), layer 2: frames (1 mark), layer 1: bits (1 mark) (7 marks in total)

c) Key differences include: Application layer in TCP/IP reference model is made up of Session, Presentation & Application layers in the OSI layer model. (3 marks) Network Access Layer in TCPIP Reference Model is made up of Data Link Layer and Physical Layers of the OSI 7 Layer Model (1 mark) Network Layer is often termed as the Internet Layer in the TCPIP Reference Model (1 mark)

d) An answer similar to the sample diagram shown below is expected. 3 marks for encapsulation at each level, 3 marks for decapsulation at each level, 2 mark’s for application level at each end, 1 mark for making application web browser and web server for HTTP.



a. Encapsulation

b. Decapsulation

Examiners' Comments:

This was by far the most popular question of section A and was attempted by most candidates. There is evidence that candidates were familiar with network fundamentals and the OSI 7-layer model. Almost all candidates demonstrated an understanding of the layers that networking devices operate as well as key differences between the OSI layer model and TCP/IP reference model. However, many candidates were not able to explain the process of encapsulation and decapsulation within TCP/IP and the majority of candidates failed to provide an acceptable diagram.

Section B
Answer Section B questions in Answer Book B

B4. This question is on Digital Communication.

a) Given the following scenarios, indicate the recommended type of network medium, Layer 2 technologies and maximum transmission rates.

i. A purpose-built office building with large open plan floors suitable for 500 fixed seating positions to accommodate both data and voice connections.

ii. A large research-based organisation involved into particle physics research with large data sets in needs to send between test sites in the same country but several hundred kilometres apart.

iii. A student house accommodating 6 students with their own laptops, desktops, tablets and phones which are used throughout the house. A conventional POTS connection is available at the property.

(15 marks)

b) Describe the techniques by which broadband technologies such as Cable & xDSL can utilise a conventional local loop to offer both voice and data services to consumers. Mention should be made of the technologies that need to be present in both the consumers premises and at service providers premises to allow this to happen.

(6 marks)

c) Explain and discuss the advantages and disadvantages of achieving confidentiality by using physical and wireless media for digital transmission.

(4 marks)

ANSWER POINTERS

a) i. copper-based cabling using unshielded twisted pair UTP). LAN technology utilising Ethernet in star configurations to switches. Maximum distances about 90m at speeds up to 1Gbps (5 marks), ii. A fibre optic-based network using dark fibre technology and possibly fibre repeaters between end nodes. Use technologies such as DWDM to carry SONET/SDH networks. Transmission speeds up to 10Gbps, can be much faster and potentially terabits with multiplexing technologies, can cover 100's km) (5 marks), iii. Broadband provision utilising DSL technology, usually ADSL which is a higher frequency than the voice traffic usually asymmetric 50 M download 1-2 Mbps upload speeds. SOHO style router might also offer WIFI, wireless LAN technology IEEE 802.11 a/b/g/n/i. At speeds potentially up to a shared 1GBps between all the house users (5 marks)

b) Both technologies use a form of multiplexing the data signal on top of the voice signal (in DSL) or the TV signal in Cable. (2 marks)

A frequency splitter is employed at the both the customer premises and the local exchange in the case of DSL to multiplex the frequencies at the customer premises from both the phone and DTE equipment and demultiplex the other end connecting the voice circuit to the telephone exchange and the data to the DSLAM unit. (2 marks)

Similar splitter technology is applied to Cable network except the signals are split between TV broadcast and data networks (2 marks)

c) In physical networks, some basic level of confidentiality is achieved by needing physical access to the network (like a physical data appoint for Ethernet or the equipment). Further protection can be offered by encrypting the data at higher layers using VPN style encryption technologies either between end points or across strategic links. (2 marks)

In wireless media, data transmission is visible to all regardless of what physical barriers maybe in the way. To ensure confidentiality of data, transmission encryption of the data of the ether must be undertaken. (2 marks)

Examiners' Comments:

This was the most consistently well answered question for Section B.

Many of the candidates answering the first part of this question did not seem to understand what was meant by a "network medium". The answers given were very varied but quite a large proportion of candidates answered with single terms such as LAN, WAN, MAN & PAN which are the fundamental types of computer networks which will use different network mediums to communicate between computers and devices over varying distances. This indicates a very poor understanding by many of the candidates of the most basic computer network fundamentals.

There is evidence that many did not understand what was meant by maximum transmission speed or distance, many gave a range of answers in MHz/GHz. They failed to give any credible answers for Layer 2 technologies in use over the physical medium.

For part (b), there is evidence that some candidates have been taught the frequency splitting for both cable and xDSL networks and some candidates were able to draw on examples from their home nations. However, a large candidate population were not able to evidence how broadband technologies work.

For part (c) many candidates only answered the question in terms of differences between physical copper media and wireless communication when the question was asking in terms of confidentiality indicating the question was not read correctly.

B5. This question is related to Wide Area Networks.

a) Describe how flow control is handled in the following WAN protocols for issues such as congestion.

i. Frame Relay
ii. ATM
iii. VPN

(14 marks)

b) Explain how techniques such as MPLS can be used on existing and future large-scale networks to improve packet delivery and routing efficiency. Use supporting diagrams to describe how MPLS can be overlaid on conventional networks to deliver the perceived benefits.

(11 marks)

ANSWER POINTERS

a) i. FECN bits are used by the destination devices for flow control and BECN is used by the originating device for the flow control. They are functional whether you use traffic shaping or not. (1 mark) The FECN bit is part of the Address field in the Frame Relay frame header. The FECN mechanism is initiated when a DTE device sends Frame Relay frames into the network. If the network is congested, DCE devices (switches) set the value of the frames' FECN bit to 1. When the frames reach the destination DTE device, the Address field (with the FECN bit set) indicates that the frame experienced congestion in the path from source to destination. The DTE device can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow control may be initiated, or the indication may be ignored. (2 marks) The BECN bit is part of the Address field in the Frame Relay frame header. DCE devices set the value of the BECN bit to 1 in frames traveling in the opposite direction of frames with their FECN bit set. This informs the receiving DTE device that a particular path through the network is congested. The DTE device then can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow-control may be initiated, or the indication may be ignored. (2 marks)

ii. ATM resources such as bandwidth and buffers are shared among users, they are allocated to the user only when they have something to transmit. So, the network uses statistical multiplexing to improve the effective throughput. (1 mark) Flow control for different applications is very complex. For example, voice is delay-sensitive but not loss-sensitive, data is loss- sensitive but not delay-sensitive, while some other applications may be both delay-sensitive and loss-sensitive. Different modes of ATM have different flow control needs for congestion, ABR is the most commonly used. (1 mark) To make it easier to manage, the traffic in ATM is divided into five service classes (1 mark). These service categories relate traffic characteristics and flow control requirements to network behaviour (1 mark). The flow controls requirement for each class is different. The traffic management policy for them are different, too. (2 marks)

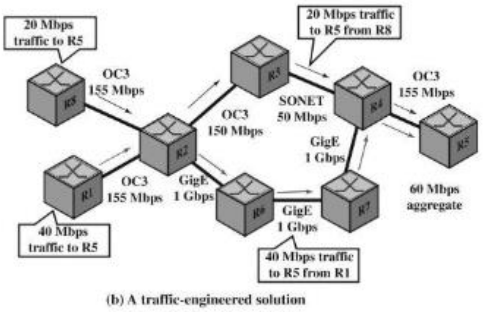
iii. Essentially because a VPN encapsulates and encrypts the original payload at the start of a tunnel, the packets are recreated with a new header and new flow control requirements (essentially like all IP packets traversing the Internet it is a best effort delivery as there is now flow control over the duration of the IP tunnel) (1 mark) When used in a private WAN, additional technologies such as MPLS can be used to achieve the flow control desired. (1 mark) Before and after the tunnel starts, existing flow control mechanisms utilised by the original packets (ICMP) and transport layer (TCP) would exist. (1 mark)

b) MPLS is a set or protocols designed to address a number of issues, including traffic engineering, QoS, virtual private network and IP integration, which are vital for future large-scale networks. (2 marks)

Traffic engineering seeks to allocate traffic to the network to maximise the use of the network capacity and seeks to ensure the most desirable route through the network for packet traffic, taking into account the QoS requirements of the various packet flow (2 marks)

Virtual Private Networks, MPLS allows we creation of both layer 2 and layer 3 VPNs. (2 marks)

The following diagrams depict how this can be implemented in current IP networks (5 marks).



(b) A traffic-engineered solution

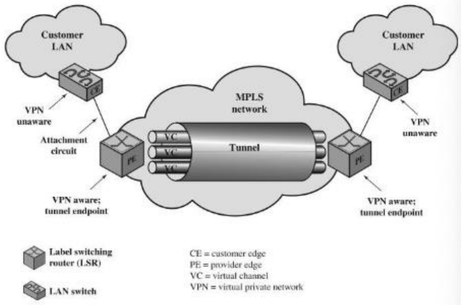


Figure 12 Layer 2 VPN Concepts

Both images were taken from (Stallings, 2016)

Examiners' Comments:

In part (a), when candidates were asked about flow control and congestion in this question, candidates answered describing the technologies which included Frame Relay, ATM and VPN's but this attracts no marks. Many candidates were unable to describe FECN/BECN or the use of different types of services within ATM to manage congestion.

In part (b), there was evidence that some candidates have a good grasp of what MPLS is and to an extent how it works.

B6. This question is related to Quality of Service.

a) Compare and the contrast the use of QoS techniques Intserv and Diffserv applied to IP networks. In your discussion include:

i. Advantages/disadvantages of Intserv **(5 marks)**
ii. Advantages/disadvantages of DiffServ **(5 marks)**
iii. Differences between Intserv and DiffServ in the following QoS Services:
   a. Isolation
   b. Guarantee
   c. Service Scope
   d. Scalability

(8 marks)

b) Explain how QoS techniques, such as Intserv and Diffserv, can be used to improve the network performance of real time and streaming protocols.

(7 marks)

ANSWER POINTERS

a) IntServ advantages (1 mark per valid point)

- Good solution for managing flows in small networks.
- Intserv enables hosts to request per-flow, quantifiable resources, along end-to-end data paths and to obtain feedback regarding admissibility of these requests.

IntServ disadvantages (1 mark per valid point)

- Poor scalability.
- High resource consumption on the network nodes.
  - Per flow processing (CPU): signalling & processing load.
  - Per flow state (memory): to keep track of every flow traversing the node.
  - Continuous signalling (RSVP is a soft state protocol).
- It's very difficult to implement.

DiffServ advantages (1 mark per valid point)

- Highly scalable QoS mechanism.
- Does not require any resource reservation mechanism on end hosts.
- Easy configuration, operation and maintenance.
- Support complex traffic classification and conditioning at the edge.
- Can aggregate multiple app flows into a limited number of TCs.
- Reduced overhead associated to the maintenance of policies on a per flow basis.
- Diffserv nodes can process traffic more easily than Intserv devices.
- Diffserv is a distributed QoS service model. Resource allocation is distributed among all the routers of a Diffserv domain, allowing for a greater flexibility and efficiency in the routing process.

DiffServ disadvantages (1 mark per valid point)

- Coordination between domains in the QoS end-to-end service.
- SPs QoS customization may affect the guaranteed QoS end-to-end service.

QoS Service	**IntServ**	**DiffServ**
Isolation	Per flow isolation	Per aggregation isolation
Guarantee	Per flow	Per aggregation (Traffic Class)
Service Scope	End-to-end	Per domain
Complexity	Per flow setup	Long term setup
Scalability	Not scalable (each router maintains per flow state)	Scalable (edge routers maintain per aggregate state; core routers per class state)
Suitable for Real Time traffic	Yes, resource reservation.	Yes, LLQ.
Admission Control	Deterministic based on flows.	Statistic based on Traffic Classes.
Applicability	Small networks and flow aggregation scenarios.	Networks of any size.
Resource Reservation	Per flow on each node in the source-destination path.	Per Traffic Class on every node in the domain.
Complexity	High	Medium

b) 1. QoS helps manage packet loss, delay and jitter with an infrastructure.

2. Identify what applications would benefit from managing those 3 characteristics and have priority over bandwidth on a network, the next step is to identify that traffic.

3. Identify or mark the traffic. Class of Service (CoS) and Differentiated Services Code Point (DSCP) are two examples. CoS will mark a data stream in the layer 2 frame header while DSCP will mark a data stream in the layer 3 packet header.

4. Allows the network equipment to be able to categorize data into different groups.

5. Place policy on those groups in order to provide preferential treatment or priority of some data streams over others (queuing). For example, if voice traffic is tagged and policy is created to give it access to the majority of network bandwidth on a link, the routing or switching device will move these packets/frames to the front of the queue and transmit them immediately.

6. if a standard TCP data transfer stream is marked with a lower priority, it will wait (be queued) until there is sufficient bandwidth to transmit.

7. If the queues fill up too much, these lower-priority packets/frames are the first to get dropped.

Examiners' Comments:

There is evidence that candidates lack knowledge of QoS mechanisms in TCP/IP or their respective differences. Even when prompted with attributes of the two techniques there is evidence that candidates failed to understand how the technologies worked.

There is evidence that candidates do not understand how these technologies are applied in even simple scenarios such as video streaming.