BCS Level 4 Certificate in Network and Digital Communications Theory
Answer Key and Rationale - QAN 603/0703/1

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**C**	The Data Link layer has two sub layers: Media Access Control and Logical Link Control.	2.2
2	**A**	802.3 is a standard specification for Ethernet (which is maintained by the Institute of Electrical and Electronics Engineers (IEEE)).	1.1
3	**B**	A bottleneck, in a communications context, is a point in the enterprise where the flow of data is impaired or stopped entirely. Causing data to be buffered or retransmitted. Adopting Traffic shaping will allow traffic to that node to be reduced.	4.2
4	**D**	Data Link layer protocols, such as PPP, format the IP datagram into a frame. They attach a header and a footer to 'frame' the datagram. The frame header includes a cyclical redundancy check (CRC) field that checks for errors as the frame travels over the network media. Then the Data Link layer will convert the data into binary digits such as 1 and 0 and then prepare them for the physical layer.	2.1
5	**B**	**Advantages of OSPF:** • Changes in an OSPF network are propagated quickly. • OSPF is hierarchical, using area 0 as the top of the hierarchy. • OSPF is a link state algorithm. • OSPF supports Variable Length Subnet Masks (VLSM). • OSPF uses multicasting within areas. • After initialization, OSPF only sends updates on routing table sections which have changed, it does not send the entire routing table. • Using areas, OSPF networks can be logically segmented to decrease the size of routing tables. Table size can be further reduced by using route summarization. • OSPF is an open standard, not related to any particular vendor. **Disadvantages of OSPF:** • OSPF is very processor intensive. • OSPF maintains multiple copies of routing information, increasing the amount of memory needed. • Using areas, OSPF can be logically segmented. • OSPF is not as easy to learn as some other protocols.	3.1

6	**A**	**Advantages of OSPF:** • Changes in an OSPF network are propagated quickly. • OSPF is hierarchical, using area 0 as the top of the hierarchy. • OSPF is a link state algorithm. • OSPF supports Variable Length Subnet Masks (VLSM). • OSPF uses multicasting within areas. • After initialization, OSPF only sends updates on routing table sections which have changed, it does not send the entire routing table. • Using areas, OSPF networks can be logically segmented to decrease the size of routing tables. Table size can be further reduced by using route summarization. • OSPF is an open standard, not related to any particular vendor. **Disadvantages of OSPF:** • OSPF is very processor intensive. • OSPF maintains multiple copies of routing information, increasing the amount of memory needed. • Using areas, OSPF can be logically segmented (this can be a good thing and a bad thing). • OSPF is not as easy to learn as some other protocols.	3.1
7	**A**	**Advantages:** • It can be used to establish / set-up connection between different types of computers. • It operates / works independently of the operating system. • It supports a number of routing-protocols. • It enables the internetworking between the organisations. • It has a scalable client-server architecture. **Disadvantages:** • IPX is faster than TCP / IP. • The shallow / overhead of TCP / IP is higher-than IPX.	2.1
8	**A**	Traffic shaping causes identified traffic to be buffered, no traffic is dropped and there is no effect on the amount of traffic transferred. It doesn't directly affect the speed of transmission.	4.2
9	**C**	Bandwidth throttling will control the overall speed of data transfer. Bandwidth cap controls the amount of data transferred over a set time period. Traffic Policing and Shaping control specific types of traffic.	4.1
10	**B**	Checksum will only show that data is valid it can't correct data or authenticate it. Encryption is unrelated.	1.4
11	**D**	Contention is when 'nodes' transmit at the same time, when contention occurs nodes need to 'back-off' and retransmit.	4.1
12	**B**	Routing to a stub network you would use a static route. For redundancy and large networks, dynamic routing would be used.	3.2

13	**C**	Static routing has lower overhead than dynamic routing. It is not scalable; it is not resilient, and it is not easy to update compared with dynamic routing.	3.2
14	**C**	Parity is single bit error detection; an even number of errors will cancel out and the error will be missed.	1.4
15	**D**	Physical layer defines the low-level network, the transmission medium but not protocols. The Data layer defines the link between 2 nodes, the protocols to establish the links.	2.2
16	**C**	SMTP = Simple Mail Transfer Protocol TCP / IP = Transmission Control Protocol / Internet Protocol (networking protocol) SNMP = Simple Network Management Protocol UDP = User Datagram Protocol	1.2
17	**D**	The Network / Data layer relates to the network connections.	1.3
18	**D**	UDP just sends the packets, which means that it has much lower bandwidth overhead and latency. User Datagram Protocol is: • Datagrams – Packets are sent individually and are checked for integrity only if they arrive. They include a checksum but there is no way to correct errors. • Unreliable – When a UDP message is sent, it cannot be known if it will reach its destination; it could get lost along the way. There is no concept of acknowledgment, retransmission, or timeout. • UDP itself does not provide flow control. • Packets are not retransmitted, this can be seen or heard in voice or media transmissions as stuttering.	1.2
19	**A**	802.1x is a standard for port-based access control on the LAN or WAN. DHCP does not prevent access but can be configured to not provide IP addresses, 802.1q is the network standard to support VLANs and NIDS (Network Intrusion Detection System) can detect but not prevent.	1.1
20	**A**	The creation of a loop by having both ends of a cable connected into a switch will cause the network to 'hang' by the re-broadcast of the same data in a loop. This is assuming it does not have a spanning tree protocol (STP) set. Fibre operates on light and should not be impacted by an electric motor. The operating range of network cables average from -55 ℃ to +60 ℃ so should not be impacted. Cat5e has a maximum range of 100 m using 100BASE-T.	1.3
21	**D**	To stop specific types of traffic a network policy needs to be applied that stops the transfer of selected types of traffic (e.g. peer to peer).	4.2
22	**A**	Dynamic routing refers to changes in the network to select the path to a network. All routing is done via routing tables.	3.2

23	**D**	Dynamic routing is less secure because routing changes are communicated over the network. Static routing is not scalable, nor does it adapt to changes in the network. Dynamic routing is easier to configure assuming knowledge of the protocols.	3.2
24	**C**	**Similarities between OSPFv2 and OSPFv3:** • Both are link-state Interior Gateway Protocol (IGP) routing protocols. • Both use a 2-level hierarchy with Area 0.0.0.0 at the core. • Both use Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs). • Both use the Shortest Path First (SPF) calculation within each area utilizing Edsger Dijkstra's SPF algorithm. • Both use metrics that are based on interface bandwidth (or manual configuration). • Both have 5 common protocol packet types: Hello, Database description (DBD), Link-state request (LSR), Link-state update (LSU), Link-state acknowledgment (LSA). • They use similar interface types: Broadcast, P2P, P2MP, NBMA, and Virtual-Links. • They have the same LSA flooding and aging timers. **Differences between OSPFv2 and OSPFv3:** • They use different address families (OSPFv2 is for IPv4-only, OSPFv3 can be used for IPv6-only or both protocols (more on this following) • OSPFv3 introduces new LSA types. • OSPFv3 has different packet format. • OSPFv3 uses different flooding scope bits (U / S2 / S1). • OSPFv3 adjacencies are formed over link-local IPv6 communications. • OSPFv3 runs per-link rather than per-subnet. • OSPFv3 supports multiple instances on a single link, Interfaces can have multiple IPv6 addresses. • OSPFv3 uses multicast addresses FF02::5 (all OSPF routers), FF02::6 (all OSPF DRs). • OSPFv3 Neighbour Authentication done with IPsec (AH). • OSPFv2 Router ID (RID) must be manually configured, still a 32-bit number.	3.1
25	**B**	In computer networks, bandwidth is used as a synonym for data transfer rate, the amount of data that can be carried from one point to another in a given time period (usually a second). Network bandwidth is usually expressed in bits per second (bps); modern networks typically have speeds measured in the millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps).	4.1
26	**A**	The data link layer provides node-to-node data transfer; a link between two directly connected nodes. It detects and possibly corrects errors that may occur in the Physical layer.	2.2

27	**D**	The Physical layer is the 'Physical' connections e.g. cables, specifications. The data link is the protocols etc. use over the Physical link.	2.2
28	**D**	Contention is when 'nodes' transmit at the same time, when contention occurs nodes need to 'back-off' and retransmit increasing latency (the delay before a transmission occurs). Contention will cause retransmission but the effect on performance is an increase in Latency.	4.1
29	**C**	Traffic control is concerned with the speed of connections which is governed by latency, see above for definition.	4.2
30	**B**	The Application layer in the TCP/IP model is equivalent to the Application, Presentation and Session layers in the OSI model. The Transport layer is a separate layer in both models. The Data Link layer in the OSI model is part of the Physical layer.	2.1
31	**D**	**Difference between RIPv1 and RIPv2:** RIPv1 is a classful routing protocol and it does not support VLSM (Variable Length Subnet Masking). RIPv2 is classless routing and it support VLSM (Variable Length Subnet Masking). RIPv2 has the option for network mask in the update to allow classless routing advertisements. RIPv2 the updates are sent as multicast In RIPv2, it is sent as broadcast. This feature reduces the network traffic. The multicast address RIPv2 is 224.0.0.9. RIPv2 supports authentication. Authentication helps in confirming that the updates are coming from authorized sources.	3.1
32	**C**	A system failure will most likely cause congestion as it could reduce the capability of the network. Legal action is an unlikely consequence of system failure. Misconfiguration is the incorrect input of a setting, once set it is very unlikely to change. Link failure is usually accounted for in the system build with a link failover system.	1.3
33	**B**	Forward error correction (FEC) is a digital signal processing technique used to enhance data reliability. FEC provides the receiver with the ability to correct errors without the requirement to request the retransmission of data. A checksum is a digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data. Error-correcting codes are used to reliably transmit digital data over unreliable communication channels subject to channel noise. Feedback error control allows the detection of data errors but require a retransmission of the data.	1.4
34	**A**	The ping command uses the services of the Internet Control Message Protocol (ICMP), the latter being encapsulated in the IP header. Therefore, the ping utility operates basically on layer 3 (the Network layer) of the 7 layer OSI model.	2.1

35	**C**	When the sending TCP wants to establish connections, it sends a segment called a SYN to the peer TCP protocol running on the receiving host. The receiving TCP returns a segment called an ACK to acknowledge the successful receipt of the segment. The sending TCP sends another ACK segment, then proceeds to send the data. This is known as the Three-way handshake. A datagram exchange is the transfer of data with a header across a packet-switched network. A DNS query provides information to allow a three-way handshake to occur. When initialising the communication between two hosts, the negotiation has to be performed to agree on some parameters of protocols.	1.2
36	**D**	HTTPS is the only protocol listed that uses security or encryption.	1.2
37	**B**	ARP is used to retrieve the MAC address of the destination host. At layer 3 it knows the destination IP but when it has to add the L2 header it does not know the mac address of the destination host. To get the mac address the router sends an ARP packet. After getting the response it will update its ARP tables for future lookups. It does not convert anything, only looks up from the ARP table therefore the remaining answers are incorrect.	1.1
38	**C**	In backward or feedback error control, along with each character, a little additional information is provided for the detection of errors; the receiver in this technique performs no error correction. If the received data is found to contain errors, the entire data is retransmitted.	1.4
39	**A**	If an interface is shut down on a cisco router, when queried it will display administratively down when using the “show interface” command. A DOS ARP attack requires the interface to remain open allowing the poisoned ARP cache to provide false information. The display cannot be seen if the device is powered off. If the routing table is being rebuilt the interface will not be down.	1.3
40	**A**	SLIP means Serial Line Internet Protocol. SLIP is the result of the integration of modem protocols prior to the suite of TCP/IP protocols and is associated with serial ports.	1.1