BCS THE CHARTERED INSTITUTE FOR IT

BCS HIGHER EDUCATION QUALIFICATIONS
BCS Level 6 Professional Graduate Diploma in IT

NETWORK INFORMATION SYSTEMS

Friday 1st April 2016 - Afternoon
Answer **any** THREE questions out of FIVE. All questions carry equal marks.
Time: THREE hours.

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

For all questions illustrate your answers with diagrams where appropriate

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

Calculators are **NOT** allowed in this examination.

Section A
Answer Section A questions in Answer Book A

General comments on candidates' performance:

The standard for this examination was high, with 84% of the candidates sitting obtaining a pass. Successful candidates heeded the advice given in previous reports and took account of the marks available for each question part. However, there were a few who wrote long answers for question parts with few marks and then appeared to run out of time for question parts with higher marks.

Future candidates should note that for some questions the parts are not arbitrary or can be considered to be standalone. For some, there is a clear link between each question part, often with some progression from one part to another; this can be used by candidates to structure their answers. For example, in this paper, Question 1 Part d) posed a problem, the solution for which was based on the understanding of capacity in Part c), which, in turn, requires an understanding of latency referenced in Parts a) and b).

Please note that the answer pointers contained in this report are examples only. Full marks were given for valid alternative answers.

SECTION A

A1.

a) Describe the sources of latency (delay) in a packet switched network.

(7 marks)

b) Explain which of these sources of latency are reduced or eliminated in circuit switched networks.

(4 marks)

c) Explain what is meant by network capacity and how this is related to a network's bandwidth.

(4 marks)

d) Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol that can be used to transfer data over Internet Protocol networks using User Datagram Protocol (UDP). TFTP files are transferred one packet at a time and each packet must be acknowledged by the receiver before the next packet of the transfer is sent.

Explain why use of TFTP would be sub-optimal for large file transfers, and over Wide Area Networks. In view of your answer, why would TFTP be used at all?

(10 marks)

Answer Points:

Part a): There are four sources of latency and 1-2 marks were given for each, with one mark for knowing the source of latency and the second for a short (correct) description. Maximum marks were 7.

- Nodal processing - The router must minimally check CRC, decrement TTL and select an outgoing network link. Some routers might add network address translation or other processing.
- Queuing delay - The packet must wait for the outgoing link to be clear to send.
- Transmission delay - This is the time to transfer the bits of the packet onto the network link.
- Propagation delay. This is the delay experienced by the packet to reach the next router once the packet is on the network link. **(7)**

Part b): In a circuit switched network, queuing delay is eliminated because the router has allocated bandwidth for the connection. Circuit-switching also reduces nodal processing since the outgoing link was selected when the circuit was established, and no processing need be spent on selection. **(4)**

Part c): Capacity is defined as bandwidth x latency. It is the total amount of data a network can (theoretically) hold at any one time. Bandwidth is the throughput but the capacity refers to how much data a network pipe can hold. See, for instance, TCP/IP Illustrated section 24.3 Long Fat Pipes by Richard Stevens. **(4)**

Part d): This part of the question builds on the former parts to present a problem that demonstrates the capacity issue. In a high latency network such as a WAN link, the TFTP protocol is very inefficient because of the lock step nature of the protocol – a packet is sent only when the previous packet is received. The data transfer will thus consume a tiny fraction of the link capacity. Consider a road network, where a single goods vehicle repeatedly drives to a location to pick up deliveries, takes them to a destination and returns (the TFTP case) against a fleet of vehicles constantly departing with deliveries as quickly as the receiver can handle them, and as long as there is room on the roads (FTP bulk data case). Candidates must demonstrate this understanding to earn the full 9 marks, perhaps by providing diagrams or by describing how more complicated protocols handle this. Candidates should also understand that TFTP may be used for its simplicity – UDP may be used so no TCP is required, allowing simple network stack implementations and a simple TFTP process that handles no special cases, and is thus suitable for fitting into tight firmware storage space for, e.g. bootstrap purposes. **(10)**

Examiners' Comments:

The standard of answers on this question varied, with evidence showing that some candidates clearly understood and detailed all sources of latency in packet switched networks, while many others focused just on processing latencies. Those who did not grasp the full range of sources of delay therefore often had trouble with Part b) and opted, instead, just to give a general overview of circuit switched networks. Where this understanding was relevant, some marks were awarded.

Part c) had almost no correct answers as per the marking scheme. Bandwidth is the throughput, but the capacity refers to how much data a network path can hold. See, for instance, TCP/IP Illustrated by Richard Stevens, section 24.3: Long Fat Pipes. This definition is of direct relevance to the sliding windows flow control scheme that has been the focus of questions in previous years. It is also known as the bandwidth delay product. However, the evidence shows that many candidates gave answers that could accord in varying degrees to the IETF definition of network capacity in RFC 5136, which defines capacity differently at various ISO layers and, for the network layer, states:

2.3.2. Definition: IP-type-P Link Capacity

We define the IP-layer link capacity, C(L,T,I), to be ***the maximum number of IP-layer bits that can be transmitted from the source S and correctly received by the destination D over the link L during the interval [T, T+I], divided by I****.*

As mentioned earlier, this definition is affected by many factors that may change over time. ***For example, a device's ability to process and forward IP packets for a particular link may have varying effect on capacity, depending on the amount or type of traffic being processed.***

2.3.3. Definition: IP-type-P Path Capacity

Using our definition for IP-layer link capacity, we can then extend this notion to an entire path, such that the IP-layer path capacity simply becomes that of the link with the smallest capacity along that path.

C(P,T,I) = min {1..n} {C(Ln,T,I)}

This definition is not at odds with the bandwidth delay product understanding of capacity but approaches the question slightly differently. Inasmuch as an answer accorded with this definition, marks were awarded. To gain full marks with this definition, it would be necessary to include the information that is marked in bold above (in a candidate's own words – there was no requirement to quote verbatim).

Part d) saw a few excellent answers that showed a full understanding of the issue, although many candidates missed the link between this part and the previous parts that were talking about delay and latency. Key to answering this was recognising that the lock-step nature of TFTP performs poorly on high latency networks because in those cases only a fraction of the network capacity is being used, as the application repeatedly pauses to await acknowledgements before sending the next packet.

A2.

A university is running TCP/IP over a network which consists of wired Ethernet segments and WiFi connected spaces. The university is also connected to the Internet. With reference to this context:

a) Describe the functionality of a bridge and identify at what layer of the ISO Open System Interconnection (OSI) network model it operates. In your answer you should explain how it handles broadcasts and what level of packet filtering may occur.

(8 marks)

b) Describe the functionality of a router, identifying at what layer of the OSI network model it operates, what filtering can be performed to make routing decisions and how it handles broadcasts.

(8 marks)

c) Explain the need for routing protocols and describe the main differences between RIP and OSPF in terms of protocol type, ease of configuration and convergence speed. Your answer should also explain what is meant by convergence.

(9 marks)

Answer Points:

a) A bridge connects two or more network segments at the data link layer of the OSI model. Traffic is forwarded through it from one network to another. It is capable of filtering using MAC (hardware) addresses. Where a bridge filters all traffic across segments so that only traffic for MAC addresses attached to a segment see the data, this is often referred to as a switch or layer 2 switch. Broadcasts are retransmitted on all connected segments. **(8).**

b) A router connects two or more network segments at the network layer (layer 3) of the OSI model. Traffic is forwarded through it from one network to another. It is capable of filtering using IP addresses. Broadcasts are not retransmitted on connected segments. **(8)**

A candidate may also mention firewall routers that can filter on other protocol information. The wording of the question has attempted to head this off by referring to the filtering for routing decisions, which would discuss IP address filtering only, and is uncalled for. Moreover, it would not strictly be correct to consider a firewall router wholly at layer 3 if it is making decisions based on, e.g., transport layer headers.

c) Routing protocols allow changes in network topology to be multicast to other routers to ensure that all routers have valid routes. If a network is connected or disconnected, the connecting router informs others in its multicast group. RIP is a popular distance-vector protocol which is easy to configure but relatively slow to converge. The concept of convergence should be described: for a set of routers to have converged, they must have collected all available topology information from each other via the implemented routing protocol, the information they gathered must not contradict any other router's topology information in the set, and it must reflect the real state of the network**.** OSPF is a link-state protocol which is quite complex to configure but converges quickly. **(9).**

Examiners' Comments:

Many candidates showed good understanding on all of these points. Some candidates mentioned that bridges were outdated, distinguishing between bridges and switches, which was quite correct, but those answers should at least mention switches that filter traffic to nodes by mac address, or make clear that a traditional bridge does not carry out such per-segment filtering. Many answers made that point, but not all.

On Part b), many candidates made reference to WiFi routers when describing how routers work. WiFi routers are not the best example of routers in this instance because WiFi routers are typically both routers and bridges at the same time and, in common parlance, a device that is a WiFi to Ethernet or WiFi to WiFi bridge only, and that does no network layer routing, may be referred to as a WiFi router, although "access point" is a better description of such devices.

The question contrasts bridges (link layer, layer 2) with routers at the network layer (layer 3). As such, marks were awarded for recognition of network layer routers using network layer addressing (IP addresses) to forward packets from one network to another. Marks would only be awarded for a description of "link layer routing" if a candidate explicitly contrasted that with network layer routing, thus showing the necessary understanding of network layer routing too.

Part c) showed some good understanding from many candidates of the difference between RIP and OSPF and was, in general, well answered.

A3.

Transport Layer Security (TLS), also known as Secure Sockets Layer (SSL), uses Public Key Encryption algorithms and Symmetric Encryption algorithms to achieve a secure layer of encryption over an insecure transport layer.

For each of the following and with reference to TLS/SSL, describe how the technique is used. In each case you should also identify any security weaknesses:

a) Public key (asymmetric) and symmetric encryption.

(6 marks)

b) Message digest.

(6 marks)

c) Digital signature.

(6 marks)

d) Digital server certificate.

(7 marks)

Answer Points:

Public key encryption requires two keys which are often (i.e. in Diffie/Helman in SSL/TLS) based on large prime numbers. The encryption and decryption is asymmetric. Data encrypted with the public key can only be decrypted with the secret key and vice versa. The algorithm relies on the computationally difficult task of factoring prime numbers to maintain the asymmetry. The secret key should be kept secret, whereas the public key must be widely known and trusted as genuine. In SSL/TLS, a server public key can be shared with a client in an x.509 certificate (see below) and this can be used to encrypt a session key, which can then only be decrypted by the server, even if the session key is intercepted, because only the secret key of the server will decrypt the session key. Decryption with a valid key remains much more computationally intensive than symmetric encryption. Symmetric key requires a shared key (the session key in SSL/TLS) to be used in conjunction with a cryptographic algorithm such as RSA to produce a cryptographic stream of ciphertext that is pseudorandom, and unpredictable unless the key is known. Symmetric encryption is fast but suffers from the weakness that over a prolonged period the re-use of the session key can lead to statistical attacks of an analysed stream to recover the symmetric key, particularly where parts of the stream are known or can be guessed. For this reason, session keys must be rotated often. **(6)**

A message digest is a one way hashing algorithm, such as SHA-2. The algorithm produces a fixed length hash from any data source. The hash is statistically unlikely to clash with any hash produced from any other data, so that a slight modification to the data produces a completely different hash. It is important that there is no reliable means to generate a predictable hash value from source data, to avoid “hash collisions” where two differing source messages can be reliably hashed to the same value. One well known hash function, MD5, has been proven to have collisions. SSL/TLS uses a digest in a digital signature by hashing the contents of the certificate (including server public key) and then encrypting the hash with a secret key (actually a CA key). The client has the public key for the CA so can decrypt the hash and then generate its own hash over the received certificate. If the hashes match, then this guarantees there was no corruption (deliberate or not) of the certificate in transit. Encrypting the hash ensures that less data is encrypted than the whole certificate, which is thus less computationally intensive. **(6)**

A Digital signature is a message digest which has been encrypted with the data originator's secret key. It requires the public key to decrypt the message digest and validate the data.

Usage ensures that the messages digest comes from the data originator and not some third party who has modified the data. This requires a genuine public key which has a secure secret key. In SSL/TLS the CAs provide this role, and their keys are usually pre-loaded in bowsers or operating systems. The risk is that a CA that a client trusts could be compromised and lose control of its secret key. SSL has key revocation but, in the event this breach is not discovered or not reported, then it is possible that a client could trust a certificate signed by a rogue secret key (as in the DigiNotar/Google Mail case that candidates may choose to refer to). **(6)**

A Digital server certificate is the public key of a server with some identification information which includes the server's FQDN. The whole certificate has a digital signature, created by a trusted third party certificate authority (CA), to validate it. Users of certificates have the public keys, themselves as part of certificates, of trusted CA's so the digital signature can be validated.

Usage has been described above (and candidates may point to earlier answers if they describe usage in those parts) to obtain and validate a genuine copy of a server's public key to establish SSL connection to a trusted server.

Certificate needs to be in date and signed by a trusted CA to be genuine. The CA validates the certificate for the owner of the server but there is no client communication directly with the CA in SSL/TLS. The CA's public keys must already exist on the client.

An x.509 digital certificate contains the following but candidates need not produce this exactly. Nevertheless, all important elements of the certificate below are in the discussion above and should be mentioned at some point to gain full marks.

Certificate: Version, Serial Number, Signature Algorithm,
Issuer: Certificate authority,

Validity dates,

Subject: Owner identity
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: md5WithRSAEncryption
Digital signature **(7)**

Examiners' Comments:

This question was answered well by a large number of candidates, who showed good understanding of issues in cryptography. In general, the evidence shows that the section that caused most difficulty or blank answers was the concept of a message digest. Also, descriptions were good for each section, but the understanding of weaknesses was often lacking.

Part a) showed good understanding of the key issues of public key cryptography. Descriptions of Asymmetric encryption need not specify actual algorithms to gain the majority of marks but should have, at least, been clear on how information encrypted with one key may only be decrypted by the other, and how a private key must be kept securely (thus pointing to the weakness of the system if it is revealed). Speed of the algorithms also needed to be mentioned, as failure to recognise that public key cryptography is slower than symmetric encryption does not explain why a scheme such as SSL/TLS uses both.

As noted above, there is evidence that many candidates seemed to skip or show little knowledge of message digests. As these are used in digital signatures, failure to appreciate what constitutes a message digest also was often reflected in a more basic understanding of the concept of a digital signature, and also in what constitutes a digital certificate. Nevertheless, there were some excellent answers on this, discussing the problem of hash collisions and the danger they pose for the use of digital signatures and certificates.

Most candidates demonstrated some understanding of certificates but, to gain the majority of the marks here, it was necessary to provide explanations beyond the general level of understanding that these may be used to provide authentication of a node (usually of the server, e.g. a web server, in SSL/TLS). The evidence shows that few candidates were able to demonstrate the weakness of the certificates around the issue of the client's trust of a range of certificate authorities. As per the answer points: "The CA's public keys must already exist on the client." Many operating systems and/or browsers come with large lists of trusted CAs and the end user usually has little knowledge of the chain of trust and may not notice when this chain fails (as in the Diginotar case).

SECTION B

B4.

a) Define the term “distributed system” and explain the most important aspects of the definition.

(5 marks)

b) List and explain distributed systems transparencies with regard to Access, Migration, Location, Relocation, Replication, Concurrency and Failure.

(14 marks)

c) In the figure below, each of the computers labelled a, b, c and d has a stored numerical value which it needs to relay to the computer marked Server to enable the Server to compute the sum of all values.

i) With the aid of a diagram, explain the message passing necessary to accomplish this task.

(3 marks)

ii) Show one mechanism where the same task can be accomplished with fewer messages.

(3 marks)

Answer Points:

Part a)

A distributed system is a collection of independent computers that appears to its users as a single coherent system. This or similar definition gained 2 marks. The remaining three marks were given as follows:

- Identifying that the computers are independent (autonomous) entities
- Identifying that these entities are connected through a network
- Identifying that the system behaves as a single coherent system

Part b) Two marks each, as follows:

- **Access Transparency** - hiding differences in data representation and the way that resources can be accessed by users.
- **Location Transparency** - users cannot tell where a resource is physically located in the system.
- **Migration Transparency** - Distributed systems in which resources can be moved without affecting how those resources can be accessed are said to provide migration transparency.
- **Relocation Transparency** - resources can be relocated while they are being accessed without the user or application noticing anything.
- **Replication Transparency** – the possibility of replicated resources to increase availability or to improve performance by placing a copy close to the place where it is accessed.
- **Concurrency Transparency** – sharing resources at the same time without noticing that the other users are making use of the same resources at the same time.
- **Failure Transparency -** user does not notice that a resource (he has possibly never heard of) fails to work properly, and that the system subsequently automatically recovers from that failure.

Part c) (i)

4 + 3 + 2 + 1 = 10 messages. An annotated diagram would be needed for full marks.

Part c) (ii)

d -> c sends V(d)
c -> b sends V(d+c)
b -> a sends V(d+c+b)
a -> Server sends V(d+c+b+a)

4 messages all together. Again, an annotated diagram would be needed for full marks.

Examiners' comments:

This question was popular, with most candidates correctly defining a distributed system.

However, the evidence shows that parts b) and c) were less well understood and some answers were inadequate. For Part b), some answers were based on information about WLAN and LAN networks and, although they contained true statements, candidates lost marks as the information contained was irrelevant.

For Part c), a number of candidates did not explain the message passing used or wrote about different network architectures from that illustrated in the question. However, in general this question was answered well.

B5.

a) Define the Simple Network Management Protocol (SNMP) and state two common devices that use it.

(4 marks)

b) Define a Network Management System (NMS) and explain four of its key functions.

(11 marks)

c) List and outline the most important performance indicators which an NMS should be able to measure and evaluate.

(5 marks)

d) Explain the significance of the term “round-trip time” and describe one method by which its value can be obtained.

(5 marks)

Answer Points:

Part a)

SNMP is based on Internet standards protocol and it is used to manage devices on IP networks (2 marks). Devices that support SNMP - routers, switches, servers, workstations, printers (2 marks for mentioning any 2 on the list).

Part b)

A network management system (NMS) is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework (3 marks).

Two marks each for the following:

- **Network device discovery** - identifying what devices are present on a network.
- **Network device monitoring** - monitoring at the device level to determine the health of network components.
- **Network performance analysis** - tracking performance indicators such as bandwidth utilization, packet loss, latency, availability and uptime of routers, switches and other Simple Network Management Protocol (SNMP) -enabled devices.
- **Intelligent notifications** - configurable alerts that will respond to specific network scenarios to alert the network administrator.

Part c)

Performance indicators (one/two marks each):

- **Delay** - time for a packet to be delivered across networks
- **Packet Loss** – packets not delivered to their destination (packet loss ratio)
- **Retransmission Rate** – linked to packet loss – the rate of retransmitted messages related to the overall number of messages
- **Throughput** - The amount of traffic a network can carry is measured as throughput, usually in terms such as kilobits per second

Part d)

Round-trip time: In reliable protocols where a receiver acknowledges delivery of each chunk of data, it is possible to measure the time elapsed between sending the packets and receiving acknowledgments for the successful delivery. This is known as round-trip time (3 marks).

Round-trip time value: According to the value of round-trip-time, reliable protocols such as TCP/IP can finely tune their timeouts before re-transmitting packets to achieve better transmission performance (2 marks).

Examiners' comments:

Candidates attempting the question generally answered Part a) well, although the most common error was not to refer to SNMP as a protocol.

Answers to Part b) and Part c) were often mixed and confused with the answers to Part c), with some candidates repeating the answers given in Part b).

Most answers to Part d) were correct.