THE BCS PROFESSIONAL EXAMINATION
Professional Graduate Diploma

April 2005

EXAMINERS' REPORT

Network Information Systems

The number of candidates selecting this module dropped for the sitting in April 2005 which, given the importance of network information systems in the current business world, seems strange. Those that have selected the module over the last few years have demonstrated good knowledge and this year there were some exceptionally good answers with the best script obtaining an impressive 88%. The overall pass rate this year is 90%.

Question 1

1. **Figure 1** below shows the protocol layers in the ISO Open System Interconnection (OSI) protocol.

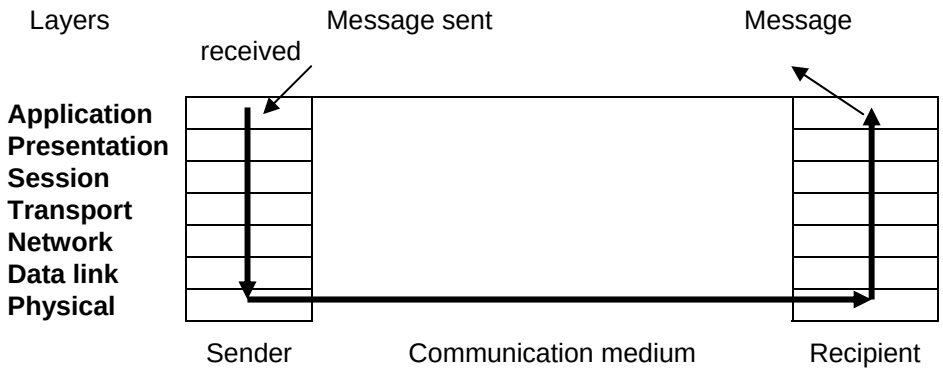

Figure 1: OSI Protocol Model

a) Explain the function of each layer and give examples of actual protocols used in practice. **(14 marks)**
b) Internetwork protocols are overlaid on underlying networks as shown in **Figure 2** below.

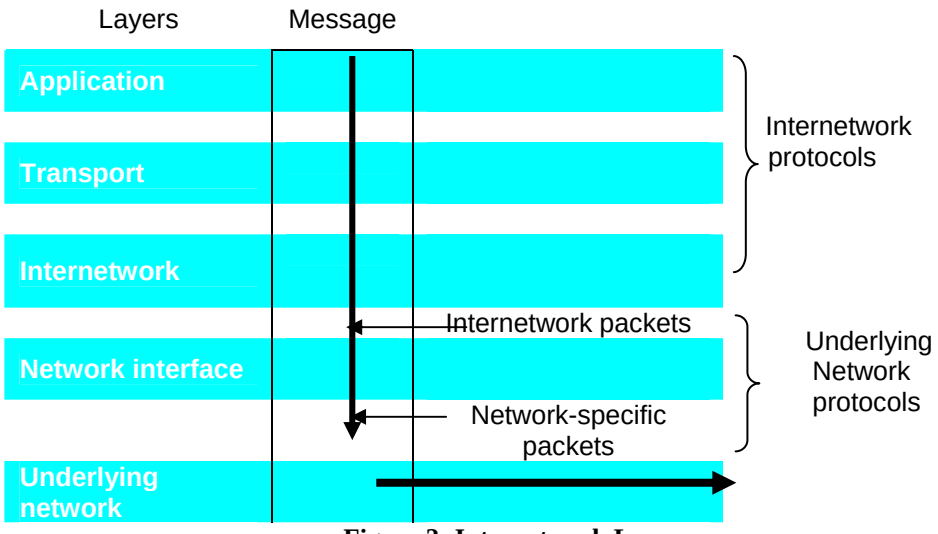

Figure 2: Internetwork Layers

The network interface layer accepts internetwork packets and converts them into packets suitable for transmission by the transport layer of a specific underlying network. The underlying network consists of the transport, network, data link and physical layers of all the real networks that constitute the internetwork. Discuss the following relevant issues:

i) Packet assembly **(3 marks)**
ii) Virtual circuit packet delivery **(4 marks)**
iii) Datagram packet delivery **(4 marks)**

Answer Pointers

a) Application: protocols that are designed to meet the communications req. of specific applications, e.g. FTP, Telnet, SMTP, X400 and X500
Presentation: protocols at this level transmit data in a network representation that is independent of individual computer representation; encryption is also done here, e.g. XDR, ANS.1
Session: for setting up communications between processes and error recovery, not needed for connectionless communications.
Transport: lowest message level, connection-oriented or connectionless, e.g. TCP, UDP
Network: transfers data packets between computers, e.g. X25, IP.
Data Link: responsible for error free transmission of packets for directly connected computers, in WANs between pairs of PSE & PSEs and hosts, e.g. HDLC, Ethernet: CSMA/CD
Physical: for circuits and hardware, e.g. X21, Ethernet: baseband & signalling.
(14 marks)

b)

i) Packet Assembly: In the internet suit of protocols, the IP protocol is a 'network layer' protocol; the MTU packet for IP packets is unusually large- 64 Kbytes including packet leader & the data field. This means UDP transport layer datagrams seldom need to be subdivided before being put in IP packets, although this may need to be sub-divided by the network interface layer, e.g. to fit into Ethernet packets.
(3 marks)

ii) Virtual circuit packet delivery: Each network layer packet contains a virtual circuit number; it needs to contain the destination address for identification. Packets are routed at each switch by reference to the circuit no. Packets are also checked & acknowledged at each step along the route. On arrival at destination, they are passed to the transport layer in a format that includes a channel identifier in a connection-oriented service and sender's address in a connectionless service.
(4 marks)

iii) Datagram packet delivery: Each network level packet contains the network addresses of the source and destination PCs. At the source, and at each switch along the route to the destination, the destination address is used to find the next step along the route, using pre-defined routing tables held in each switch. Tables are modified subject to network faults or loading. (4 marks)

Examiner's Comments

A popular question, attempted by 60% of candidates, with around 85% obtaining a pass. Answers varied considerably in content and in depth, reflecting the varied personal experience of candidates. For the candidates who scored high marks (one achieved full marks), some answers indicated practical knowledge based on direct experience with the subject matter, while others represented more theoretical knowledge derived from the recommended text books. For the candidates who scored

low marks, some had clear language difficulties in formulating the answers, while others lacked essential understanding of the issues related to the question.

Question 2

2. *a)* Briefly describe each of the following terms:
- *ii)* Public key encryption
- *iii)* Message digest
- *iii)* Digital signature
- *iv)* Digital certificate **(12 marks)**

b) Describe how a message digest can be used to validate the integrity of a data file. How is a digital signature an improvement over a message digest for validating the integrity of data files. **(6 marks)**

c) Describe how a digital certificate is used by a server to establish trusted communication between a *client* and a server. **(7 marks)**

Answer Pointers

i) Public key encryption requires two keys which are 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 secret key should be kept secret. The public key needs to be widely known and it is important that others trust the public key to be genuine. (3 marks)

ii) A message digest is a one way hashing algorithm, such as MD5. The algorithm produces a fixed length hash from any data source. The hash is statistically unique so that a slight modification to the data produces a completely different hash. (3 marks)

iii) 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. It ensures that the messages digest comes from the data originator and not some third party who has modified the data. (3 marks)

iv) A Digital certificate is the public key of an individual or server with some identification information. The whole certificate has a digital signature, created by a trusted third party certificate authority, to validate it. Users of certificates have the public keys, themselves as part of certificates, of trusted CAs so the digital signature can be validated. (3 marks)

b)
If a data file needs to be validated later, the originator can generate the hash, using md5sum, and publish the hash with the file. If someone retrieves the file they can run md5sum on the file and compare the resultant hash with the published hash. If they are the same then the file is OK. One problem with this is that if a third party replaces the data file with another they can provide the new hash. A digital signature is better because it can only be generated with the originator's secret key. If you have the originator's public key and you know that it is genuine, then if the digital signature matches the file then the data is genuine. (6 marks)

c)
The main purpose of a server's digital signature is to allow a client to obtain the server's public key with some confidence that it is genuine. On establishing communication, the server sends its certificate to the client. The client uses its CA certificates to validate the certificate using its CA digital signature. If the certificate validates then it can safely be used to send encrypted data, usually a session key, to

the server using the public key in the certificate to encrypt the data. Only the server can decrypt the data (session key) using its secret key. (7 marks)

Examiner's Comments

This was a popular question which was attempted by 85% of the candidates with a few excellent answers and one candidate being awarded full marks. Others gave a range of good and generally valid points such that 68% obtaining a pass.

a) Most candidates explained the principles of public key encryption well. Marks were lost for not stating that data encrypted with one key can only be decrypted with the ther. Most candidates correctly described a message digest as a hash created using a one way algorithm such as MD5. Some solutions incorrectly stated that encryption is involved.

   There was confusion as to what is encrypted in a digital signature. It is only the message digest hash which in encrypted and not the whole data. Some solutions incorrectly confused a digital signature with an electronic equivalent of a written signature. Most candidates described the structure of a digital certificate.

b) A correct solution should have stated that if data is modified, a new message digest can be created. A digital signature defends against this because the originator's private key is required to encrypt the message digest. Some solutions incorrectly talked about encrypting the entire message.

c) This section was not well answered. The purpose of the certificate is to allow the server to send a client its public key giving the client a level of confidence in its validity. Many solutions confused client certificates with server certificates. Some solutions incorrectly stated that the certificate authority was involved in the connection between client and server where in fact the CA generates a digital signature which can be used to validate the certificate.

Question 3

3. The *Network File System* (NFS), developed by a major market leader, has been widely adopted in industry and in academic environments since its introduction in the mid 1980s.

a) **Figure 3** below shows local and remote file systems accessible on an NFS client. Design goals of NFS with reference to transparency include: i) Access transparency, ii) Location transparency, iii) Failure transparency, iv) Performance transparency, and v) Migration transparency. Explain these design goals and comment on the extent to which they have been achieved. **(15 marks)**

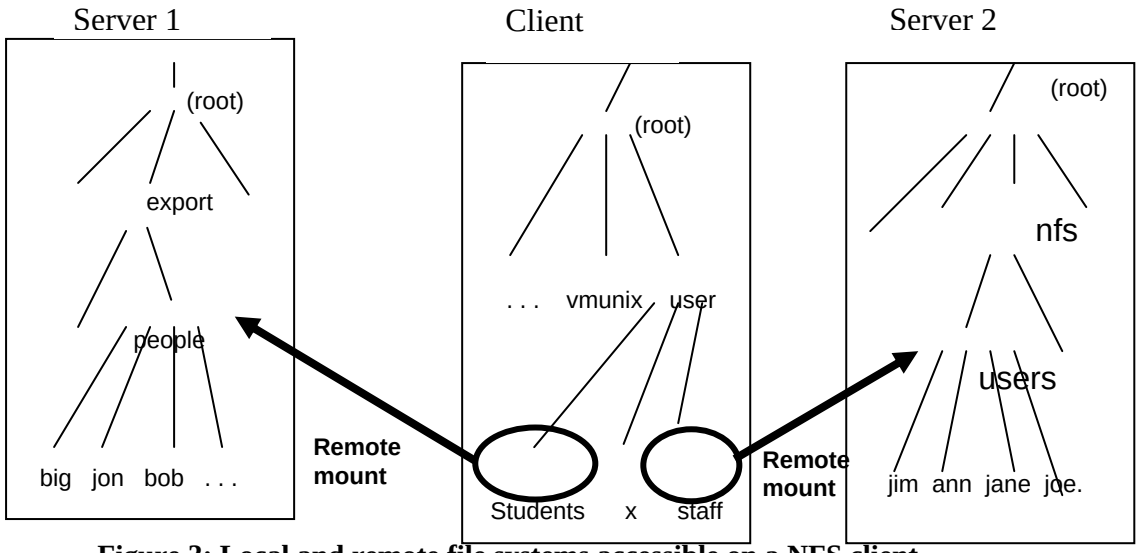

Figure 3: Local and remote file systems accessible on a NFS client

b) The software architecture of NFS clients and servers is shown in **Figure 4** on the next page. The components of NFS concerned with the mounting of remote file systems are not shown. Processes using NFS are referred to here as *user level client processes* in order to distinguish them from *NFS client* module which resides in the UNIX kernel on each client computer.

Describe the communication operations involved in this architecture. **(10 marks)**

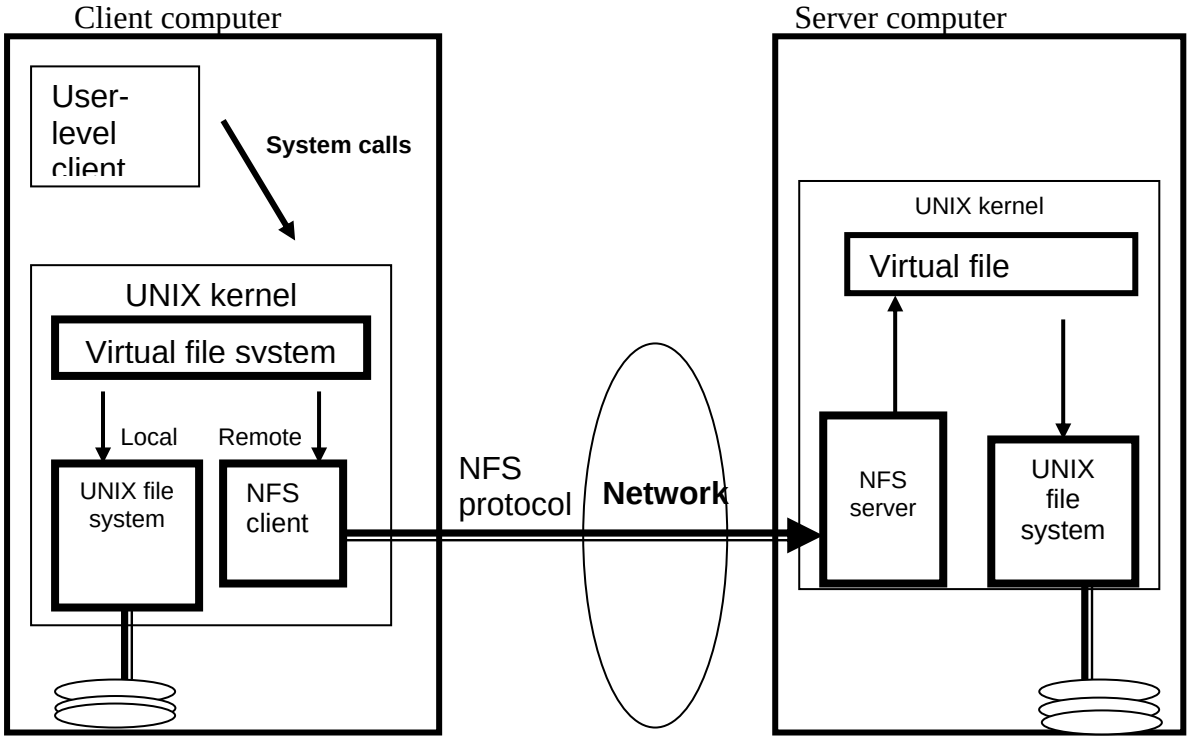

Figure 4: NFS Software Architecture

Answer Pointers

a)

i) Access transparency: The NFS client module provides an application programming interface to local processes that is identical to the local operating systems' interface.

ii) Location transparency: Each client establishes a file name space by adding remote file systems to its local name space. File systems have to be exported by the node that holds then and remote-mounted by a client before they can be accessed by processes running in the client.

iii) Failure transparency: The NFS service is stateless and most of the operations of the file access protocol are repeatable or idempotent. UNIX file operations are translated into NFS protocol operations by an NFS client module that resides in each client.

iv) Performance transparency: Both client & server employ caching to achieve performance. The caching in the server is straightforward, using the conventional UNIX disk block caching mechanism. The client module maintains a local cach of blocks from remote files, directories and file attribute data.

v) Migration transparency: In addition to the NFS file access service, there is a separate service, the mount service that supports the mounting of remote file systems in the client's local file name space. A mount service process runs in each node and provides an RPC interface to clients for mounting and un-mounting local file systems at the client node.

(5x3 =15 marks)

b)

The NFS server module resides in the kernel on each computer that acts as an NFS server. Requests referring to files in a remote file system are translated by the client module to NFS protocol operations and then passed to the NFS server module at the computer holding the relevant files. The NFS client & server modules communicate using remote procedure calling. A port mapper service is included to enable clients to bind to services in a given host by name, although in early releases of NFS, NFS clients accessed the server by quoting a well known port number. Any process can send requests to an NFS server and if the requests are valid and contain the correct authentication information, they will be acted upon. Client and server modules are operating systems independent.

(10 marks)

Examiner's Comments.

This question was not popular and only 13% of candidates selected this question, however those that did so gave some good answers and 82% reached the pass mark. A large portion who attempted the question showed good understanding of the associated syllabus material. As with other questions the candidates' answers reflected their practical experience or good understanding of the theory and application. The depth and length of answers varied enormously, some showing an outstanding grasp of the subject matter and related peripheral issues. Those who scored high marks clearly enjoyed the challenge of this question and responded well to all parts of the question.

Question 4

4. *a)* Describe the functionality of a repeater, a bridge and a router for use with IP traffic on LocalArea Networks, giving details of what information is transferred and what filtering can be performed. **(10 marks)**

b) For each of the following local area network (LAN) problems identify whether each of a repeater, a bridge or a router can solve the problem. In each case describe, using different scenarios where appropriate, how the device could solve the problem and identify which device is the best solution.

i) The LAN requirements exceed the maximum cable length for a single segment. **(3 marks)**

ii) The LAN interconnects several departments of the organization. The total traffic exceeds the maximum bandwidth for a single LAN. **(3 marks)**

iii) One department on the LAN generates a lot of internal network traffic and needs to be on a separate subnet. **(3 marks)**

iv) One department exchanges confidential information internally and does not want its data to be intercepted by a packet sniffer run from a machine in another department. **(3 marks)**

v) One or more departments use a different domain and IP address range to the others. **(3 marks)**

Answer Pointers

a) A repeater links LAN segments at the physical layer and allows LAN segments to be joined by copying all frames. A bridge links LAN segments at the data link layer and allows frames to be copied selectively, only if they need to be copied. A router links networks at the network layer and allows packets to be routed through dynamic network topologies. (10 marks).

b)

i) All will do the job. A repeater is the best unless congestion control is required (bridge) or there are different subnets on the LAN (router).

ii) A repeater is of no use. A bridge or a router can be used as they will selectively forward frames or packets. A bridge is best for a single subnet. A router is required for multiple subnets.

iii) A repeater is of no use. A bridge or a router can be used to create a separate segment or subnet.

iv) A repeater is of no use. A bridge or a router can be used to create a separate segment or subnet.

v) A router is the only option here as they can filter packets by IP address whereas the repeater and bridge cannot. Although different subnets can operate simultaneously on the same physical network.

(3 marks per section)

Examiner's Comments

The most popular question which was attempted by 94% of candidates with 95% obtaining a pass.

a) Most attempts at this section correctly defined the functionality of repeaters, bridges and routers. Marks were lost for not stating that they operate at different layers, physical, datalink and network.

b) Most attempts at this section correctly identified the best device for each of the problems. The question asked how EACH device could or couldn't be used for each problem. Most answers describe the best device and did not mention the other two.

Question 5

5. *a)* Describe how the POP3 protocol can be used to view and retrieve remote mail and identify the major advantages and disadvantages of using this protocol. **(7 marks)**

b) Describe how the IMAP4 protocol can be used to view and retrieve remote mail and identify the major advantages and disadvantages of using this protocol. **(7 marks)**

c) Describe how the ESMTP protocol is used to send electronic mail between two mail transport agents (MTA). Specify the checks which the MTA's should perform to prevent them from being used to deliver spam mail. **(11 marks)**

Answer Pointers

a) POP3 is a network service using TCP/IP on port 110 (or port 995 if using SSL). It allows POP3 enabled mail browsers to view the headers of their remote mail inbox and to download mail messages, optionally leaving the original on the server. POP3 requires a log in using the normal login user name and password. (4 marks)

POP3 allows remote access to mail boxes, so the user does not need to be connected all of the time to receive mail. Can only have one mailbox per user. Mail cannot be shared between remote machines. Passwords sent in clear text. (3 marks)

b) IMAP4 is a network service using TCP/IP on port 143 (or port 993 if using SSL). It allows IMAP enabled mail browsers to view the headers and content of their remote mail inbox and to have multiple remote mail folders. IMAP requires a log in using the normal login user name and password. (4 marks)

IMAP allows remote access to mail boxes, so the user does not need to be connected all of the time to receive mail. Can have multiple shared mailboxes which can be shared between remote machines. Mail can take up a lot of space on the server. Passwords sent in clear text (3 marks)

c) ESMTP is a network protocol using TCP/IP on port 25. It is used to transfer mail messages between the sender and recipients MTA. Each mail messages has content which consists of headers and a message body. Messages are sent by opening a connection on port 25 and sending; the from email address, the to email address and the message body. The sender and recipient email addresses used in the message and used in the transfer do not have to be the same. (6 marks)

An MTA should not allow mail messages to be transmitted unless either the sender or the recipient is local. If it allows mail to be sent where both are remote it is acting as an open relay and can be utilised for relaying spam. Using TLS and digital certificates, or POP before send, can be used to allow relaying for trusted remote senders. (5 marks)

Examiner's Comments

This question was attempted by about half of the candidates, many of whom demonstrated little knowledge of the syllabus area and around half obtained a pass.

a) Most solutions correctly described the functionality and some advantages and disadvantages of POP3. Most candidates failed to state that POP3 only allows a single mailbox which is the mail drop on the server.

b) There was a general lack of understanding about how IMAP works. Most candidates failed to mention the ability to have multiple mail boxes on the server. Few mentioned that a user name and password is required for login. Few mentioned IMAPS

c) This section was in general not well answered. The important points are that an email has an envelope and a body. ESMTP only uses the envelope to deliver the mail, so the to and from addresses in the header don't have to agree with the envelope which is part of the ESMTP protocol. Few answers addressed the issues of an open relay by a spammer. The important point, which was missed by all, is that the same message can be sent to many different recipients with the sender address spoofed so that it appears that the message came from elsewhere.