THE BCS PROFESSIONAL EXAMINATIONS
BCS Level 6 Professional Graduate Diploma in IT

April 2008

EXAMINERS' REPORT

Network Information Systems

General Comments

The number of candidates selecting this module dropped slightly from last year. The examiners were pleased to note almost all candidates were well prepared and marks around 75% or higher were obtained on each question. Overall more than 77% of candidates obtained a pass.
A very small number of candidates appeared to have very little to offer as an answer to any question which they attempted. Such candidates obtained between 4% and 15% for their complete paper. Without such candidates the pass rate this year would have been over 80%. Examiners again stress the need for candidates to study and understand the syllabus and in addition to test themselves on past papers using the answer pointers given in examiners reports to compare their answers with those expected by the examiners. Weak candidates identify a question on which they feel they may be able to obtain a few marks by offering very general points on the subject. On this paper question 2 is a good example. Many candidates felt they knew about some issues on security and provided all they appeared to remember without applying their scant knowledge to the question. Random points not addressed to the question as set, which asked candidates to "focus on technical issues", are unlikely to obtain marks.

Question 1

The scope for open, configurable distributed systems is enhanced if the file service is structured as three components (refer to figure 1 below): a flat file service, a directory service and a client module.

a) Explain the operation and the relationships between the various entities shown in the diagram.

(5 marks)

b) Define and discuss the division of responsibilities between the three components. You are expected to refer to unique file identifiers (UFID's) in your answer.

(10 marks)

c) Discuss the design issues involved in providing a range of services to address the requirements of clients with different goals with respect to these three components and the issue of fault tolerance.

(10 marks)

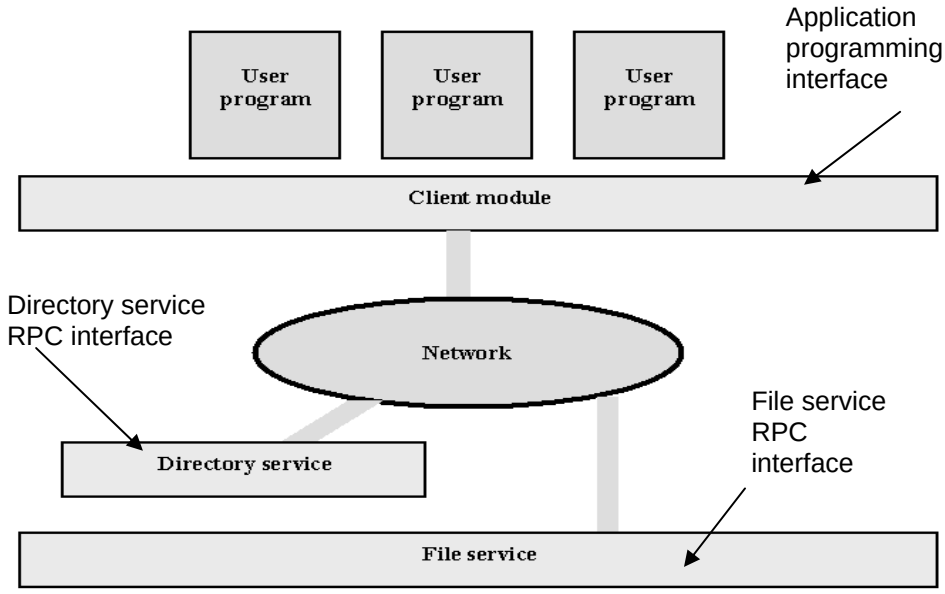


Figure 1: File service components

Answer Pointers

a)

Flat file service & directory service each export an interface for use by client programs and their RPC interfaces to provide a comprehensive set of ops for access to files. Client module (CM) integrates the flat file service and the directory service to provide a single programming interface with operations on files similar to those found in conventional file systems. The design is open as different directory services can be used with a single flat file service to support different naming rules and directory structures. Different client modules can be used to implement different programming interfaces to simulate the file operations of different op systems and optimize performance to diff workstation and server hardware configurations.

b)

Flat File service (FFS): concerned with implementing operations on files' contents. UFIDs are used to refer to files for flat file service operations. Responsibilities division between file service and directory service is based on use of UFIDs,- they are long integers unique to each file in a distributed system. Flat file service generates & return to the requester a new UFID when it receives a request to create a file.

(3 marks)

Directory service (DS): provides mapping between *text names* for files and their UFIDs. Upon file creation: client module must record the UFID and text name of each file, clients may then get a file's UFID by giving its text name to the directory service. Provides functions to generate & update directories & obtain UFIDs from directories,- it is a client of the flat file service, it's directory files are stored in files of the flat file service.. When a hierarchic file naming scheme is adopted (e.g. Unix) directories will hold references to other directories. (4 marks)

Client module (CM): Is an extension of the user package concept,- a single client module runs in each client computer to integrate and extend the operations of FFS & DS under one application programming interface available to user-level programs in client computers. CM also holds info re network locations of the FFS & DS processors. CM also implements a cache of recently used file blocks at the client to enhance performance.

c)
FFS: designed to offer a simple, general purpose set of operations. File contains data (as items accessible for read/write any portion) & attributes; as a single record to hold
i. file length,
ii. timestamp,
iii. type,
iv. owner
v. access control list,
FFS maintains i - iii, DS iv & v.. (2 marks)

Fault Tolerance: RPC interface is designed as *idempotent* operations ensuring duplicated requests do not result in invalid updates to files,- servers can be *stateless* to enable restart to restore service after failure without recovering previous state.
(2 marks)

DS: creates & modifies entries in simple one-D directories, looks-up text names in directories to return UFID after checking user's authorization. Separation of DS from FS enables different DS to be designed for use with a single file service, each supporting a diff name syntax and access control regime,- e.g. Unix, MS/DOS, VMS. Translation from file name to UFID is a *stateless* substitute for the *open file* op in non-distributed systems. DS also looks after access control where UFIDs take the role of *capabilities.* (4 marks)

CM: hides low level constructs such as UFIDs used in RPC interfaces of the FFS and DS from user level programs, i.e. emulating I/O functions of the host op sys in the client mode. CM locates files distributed in several nodes based on identity of the file group. (2 marks)

Examiner's comments

Around one third of candidates attempted this question, perhaps many were put off by the level of difficulty and depth of detail required in the answers. However, it is very pleasing to note that 72% of candidates who attempted this question passed. Some of the high scoring candidates clearly enjoyed the challenge posed by the question, which gave them the opportunity to draw on their experience and knowledge of the subject. Those who failed to pass did so through obtaining so few marks that it is difficult to provide helpful advice to such candidates. It is clear they had not covered the subject of the question in their preparation for the examination.

Question 2

A University Computer Science Department wishes to offer some of its courses through remote access. Registered students should be able to connect to server machines over the Internet and access course material and submit coursework for continuous assessment. Discuss the security requirements for implementing a remote access coursework system addressing each of the following areas. Your answer should focus on the technical issues.

a) Physical security.
b) Operating system security.
c) Network security.
d) Data access.
e) User authentication.

(5 x 5 marks)

Answer Pointers

a) Physical security: rooms containing vital equipment locked, restricted access to server room, all consoles located in server room or other secure room, UPS. Consider relevant environmental hazards.
b) Operating system security: restrict administrator rights, limit users to minimum, file permissions, run web server as restricted user. Monitor user accounts, delete unused, remove guest accounts.
c) Network security: firewall, web server as static route, web server as proxy, Web server in DMZ, don't allow unused network services
d) Data access: password protected database, encrypt files, HTTPS/SSL for upload, file permissions, version control
e) User authentication: password, certificate, session, session timeout, password aging

Examiner's comments

As expected almost all candidates attempted this question with around 65% obtaining a pass. Those that failed to obtain sufficient marks for a pass provided very general points on security without relevance to the question.
a) Physical security: Most correctly recommended a locked server room with monitoring and also protection from a variety of environmental hazards. Very few recommended the use of an UPS, which is surprising given the problems occurring with the main electricity supplies in some parts of the world. No candidate recommended securing the operations consoles attached to servers.
b) Operating system security: Many answers failed to attract marks in this section. Most answers were concerned with software updates and virus checking. Few candidates considered and therefore failed to recommend restricting administrator access and disabling guest and unused user accounts. Few recommended restricting user access rights to prevent users from reading each other's data.
c) Network security: Most correctly identified the need for a firewall. Few mentioned the need for putting servers in a DMX or the use of static routes. Few suggested removing unused network services.
d) Data security: This section was quite badly answered. Some correctly identified the need to limit database access and to use encryption. Few mentioned file permissions and the use of version control to keep track of submissions.
e) User security: most identified the need for usernames and passwords and

alternatively certificates. Few mentioned password quality and password aging, very few mentioned the use of sessions and session timeouts

Question 3

You have been tasked to provide a review of user requirements for a new distributed system being planned in your organisation. Discuss the issues you would consider under the following three headings and provide suitable explanations of the factors associated with each.

a) Functionality.
Among the factors you need to consider are operating systems. Discuss the following three options:
   i) Adapt the existing operating system.
   ii) Move to an entirely new operating system designed specifically for distributed systems.
   iii) Emulation

(9 marks)

b) Re-configurability.
Refer to the following two timescales in your discussion:
   i) Short term changes
   ii) Medium to long term evolution.

(8 marks)

c) Quality of Service.
Include the following three factors in your discussion:
   i) Performance.
   ii) Reliability and availability.
   iii) Security.

(8 marks)

Answer Pointers

Functionality: services for users & application writers, minimal requirements, improvements, sharing, new functionalities, costs of new SW, transition problems; operating systems: option-1 is limited in new functionalities, option-2, ideal for designers but not for current users, option-3 may not be practical e.g. emulation of Unix.

Re-configurability: scalability, heterogeneity; short term changes: coping with failed process or component of computer or network, shifting of workload, activities transfer to reduce network communications; medium to on term evolution: re-assigning new roles to machines, new/more machines/servers.

Quality of service: response time, consistency, communications optimization at all levels; coping with failure, convenience or absolute requirement, reliability & response time, critical applications e.g. financial & air traffic control, fault tolerance, resilience against HW failure; security: two main threats: against privacy & integrity of data passing thro the network, interference with sys SW, e.g. bogus file server.

Examiner's comments

This question proved to be a popular choice with three quarters of candidates making an attempt and of those around 80% obtaining sufficient marks to pass. The answers varied widely in detail, quality and length, with quite a number of candidates demonstrating a refreshing insight to the concepts based on first hand practical experience with computer systems. Those who had studied and understood the subject also obtained good marks. Those who failed the paper should review the question taking note of the answer pointers given above.

Question 4

A company has a DSL Internet connection with 5 fixed IP addresses in the range 217.40.76.1 through to 217.40.76.5. The DSL router has the IP address 217.40.76.6. The company needs to have two Web servers, an FTP server and a mail server which are accessible from the Internet. The IT department has twenty employees, each of whom require unrestricted Internet and Intranet access from their desktop PCs. There are twenty administrative staff who require restricted Internet Web browsing and full Intranet access. There are ten sales staff who require wireless connections when on site with full Internet and Intranet access.

a) Design a network topology for the company. Draw a diagram of the network layout and assign IP addresses to any subnets and computers. Clearly show any switching components and describe their function. Justify any decisions which you make.

(15 marks)

b) Identify the major software components which are required to implement the company's network. For each component recommend a product and give any configuration requirements.

(10 marks)

Answer Pointers

a)
Router 217.40.76.6, Web1 217.40.76.1, Web2 217.40.76.2, FTP & Mail 217.40.76.3 – (5 marks)
Nat router for developers 217.40.76.4 connecting subnet 10.0.0.0/24 and wireless NAT router connecting subnet 10.0.2.0/24 – (5 marks)
Proxy server for administrators 217.40.76.5 connecting subnet 10.0.1.0/24 – (5 marks)

b)
Apache Web servers –(2 marks)
Any suitable FTP server accepted -Washington University or Very Secure FTPD, consider using ssh and sftp
SMTP server, sendmail, qmail or exim –(2 marks)
Linux as a NAT router –(2 marks) Squid proxy server –(2 marks)

Examiner's comments

a) Most answers provided a good diagram of the proposed network topology. However many failed to allocate IP addresses to the subnets for the departments. Quite a few mistakenly allocated addresses from the 172.40.0.0 network for the local subnets when they should have used non-Internet routable IP address ranges such as 10.0.0.0/8.
Many missed the detail of requiring a NAT router to route from the local subnet to the Internet.
Very few candidates suggested the use of a proxy server with both an external and an internal IP address for giving restricted Web access.

b) A lot of answers were unable to attract marks due to candidates giving hardware components when the question clearly asked for "software components" such as Linux NAT, Apache, WU-FTP, Sendmail and Squid or their equivalents.

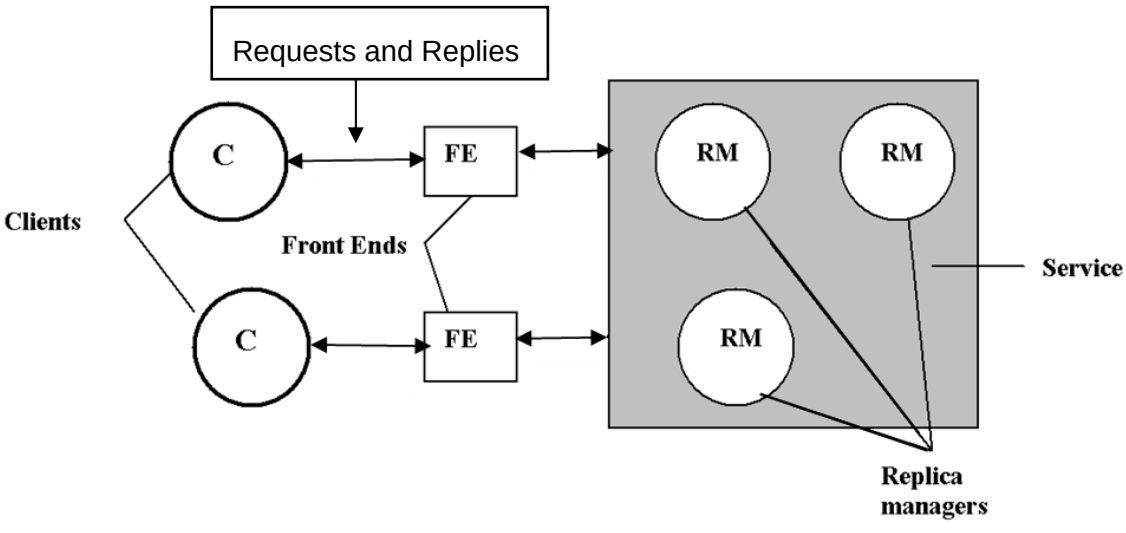
Question 5

Replication is the maintenance of on-line copies of data and other resources. For example, the USENET system maintains replicas of items posted to electronic bulletin boards across the Internet, the replicas being held within, or close to, the various organisations that provide access to it.

a) Discuss the motivation for replication in terms of:
- performance enhancement
- enhanced availability
- fault tolerance.

(6 marks)

b) The figure below shows a basic architectural model for the management of replicated data.



A basic model for the management of replicated data

i) Discuss the operation of this model.

(4 marks)

ii) If the clients and replica managers are separate processes, the model becomes what is commonly referred to as the 'gossip' model. Produce a modified version of the above diagram and use it to explain the ‘gossip’ model.

(7 marks)

iii) To enhance availability, the 'primary' copy model is often used. Produce a modified version of the above diagram and use it to explain the operation of the ‘primary’ model. Suggest an architecture for a shared editor, which might be used in a multi-user collaboration environment and often referred to as 'groupware'.

(8 marks)

Answer Pointers

a)
Performance enhancement: Data shared between a large client community is not held at a single server but distributed among many servers, each provides to a smaller community of users close to it.

Enhanced availability: client SW can access an alternative server when default server fails.
If n servers have probability p of failing then enhanced availability is $1 - p^n$. Much better than caching, which doesn't always hold files in their entirety,- Coda filing system is an exception.

Fault tolerance: if each server processes every client request in parallel it is possible to guarantee correct request processing should a server fails. It includes real time guarantees against arbitrary (Byzantine) failures, e.g. stock market, rocket engine calculations

b i)
Clients each make a series of requests first handled by FEs to communicate by message passing with one or more of the replica managers. FE can be a user package executed in each client or a user process,- trade-off: efficiency & sharing info.

b ii)
Diagram: 2 way communication between all Replica managers (RMs). RMs exchange gossip messages periodically to convey the updates (news) they receive. FE normally talks to one RM for each op; alternatively, it can talk to more than one RM. FEs propagate their vector timestamps whenever clients communicate directly.

b iii)
Diagram: all FEs talk with the same primary server (PS) when updating a particular data item; PS is accessed for all update requests,- PS propagates the updates to the other, Salve, servers (SS). FEs may read the item from a slave. If PS fails one of the SS is promoted to PS, e.g. in Sun Net Info Service, also known as Yellow Pages, passwords which change infrequently are updated at a master server & propagated to SS.

Shared editor, diagram: each editor talks to all others, each circle is a combined client, FE and RM, one per user. Each holds a replica of the overall document state; only one class of process & it performs roles of client & RM; a FE module is used to hide replication from other modules that access the shared document state.

Examiners comments

Around one third of candidates attempted this question, many were possibly discouraged by the level knowledge and depth of technical detail required to fully answer the question. However, it is welcoming to see two thirds of those who attempted the question obtained a pass. Candidates who failed and are considering retaking the examination should ensure they understand the syllabus and are advised to compare the answers pointers given above against their own attempts.