

NAPIER UNIVERSITY
SCHOOL OF COMPUTING

SECOND DIET EXAMINATION

SESSION 2001-2002

MODULE: CO32010

NETWORK OPERATING SYSTEMS

DATE:

DURATION: 2 HOURS

START TIME:

EXAMINER(S)

DR. W.BUCHANAN
MR. J.JACKSON

QUESTION PAPER DATA

Number of pages - 6
Number of questions - 5
Number of sections - ONE

INSTRUCTION TO CANDIDATES

Complete any three of the questions from five.

- 1 (a) Table Q1a Shows the result of running the command *rpcinfo* on Unix system *mars*.
- (i) By examining the list determine whether this system is a network file system *server*. (3)
- (b) Describe the role of the *rpcbind* service in the list above and state why it is important. (6)
- (c) Figure Q1c shows an outline directory structure for three networked Unix systems (*mercury*, *venus* and *mars*) each could be both NFS server and/or client. It is desired that any one of three users (*anne*, *bob* or *colin*) should be able to login to any of the three systems and see their own files using the same pathname. In other words the perceived location of each users' files is not dependent on the machine they are using. Detail the configuration actions required to achieve this. (11)
- (d) Describe the role of an NIS Slave in managing network information. (5)

Total Marks [25]

| Line no. | UNIX processes |
|----------|--|
| 1 | <code>mars:~ > rpcinfo -s</code> |
| 2 | <code>program version(s) netid(s) service owner</code> |
| 3 | <code>100000 2,3,4 udp,tcp,ticlts,ticotsord,ticots rpcbnd superuser</code> |
| 4 | <code>100029 3,2,1 ticots,ticotsord,ticlts keyserv superuser</code> |
| 5 | <code>100232 10 udp - superuser</code> |
| 6 | <code>100011 1 ticlts,udp rquotad superuser</code> |
| 7 | <code>100024 1 ticots,ticotsord,ticlts,tcp,udp status superuser</code> |
| 8 | <code>100001 4,3,2 ticlts,udp rstatd superuser</code> |
| 9 | <code>100235 1 tcp - superuser</code> |
| 10 | <code>100078 4 ticlts kerbd superuser</code> |
| 11 | <code>100068 5,4,3,2 udp - superuser</code> |
| 12 | <code>100021 4,3,2,1 tcp,udp nlockmgr superuser</code> |
| 13 | <code>100005 3,2,1 ticots,ticotsord,tcp,ticlts,udp mountd superuser</code> |
| 14 | <code>100003 3,2 tcp,udp nfs superuser</code> |
| 15 | <code>100227 3,2 tcp,udp - superuser</code> |
| 16 | <code>788585389 1 udp - superuser</code> |

Figure Q1a: UNIX processes

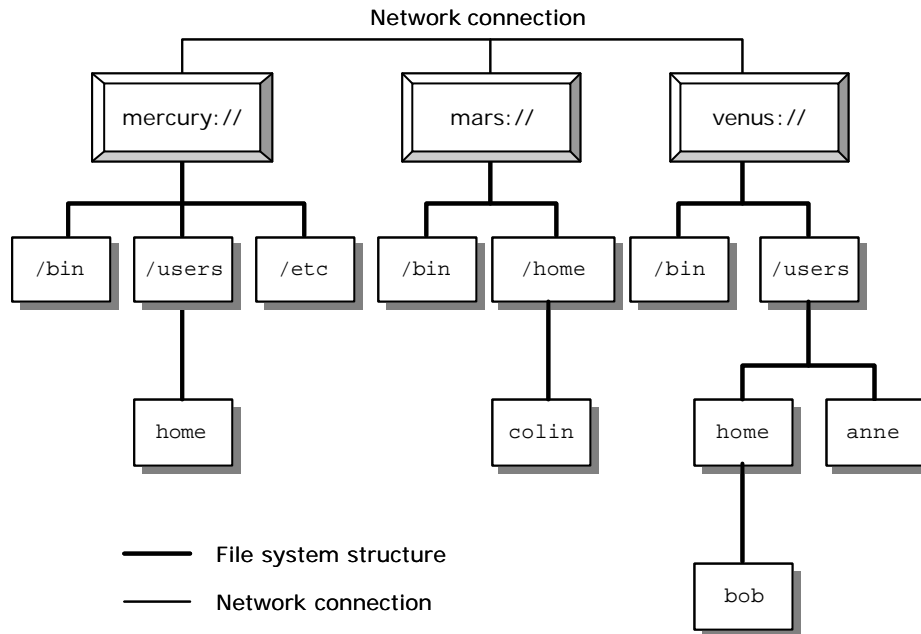


Figure Q1c: UNIX processes

| Part | Sample answer | Marking schedule |
|----------|--|------------------|
| a | This system can be assumed to be an NFS Server since rpcinfo lists all supported RPC services and the nfs service is included. | |
| b | rpcbind operates as the broker/manager for all the RPC services, it listens on port 111 for queries, it will reply to an RPC query by returning a port number corresponding to the service request. This function is also sometimes referred to as portmapping. | |
| c | <p>Firstly a common directory needs to be created on the machines, let's create a /users/home directory on mars.</p> <p>mars and venus will need to export file systems so they should be configured as servers. All three machines will also be clients. Mercury will be set to export it's /users/home directory whilst venus exports /users.</p> <p>mars will need to mount the following</p> <pre>venus://users/anne AS /users/home/anne venus://users/home/bob AS /users/home/bob</pre> <p>venus will need to mount the following</p> <pre>mars://home/colin AS /users/home/colin</pre> <p>mercury will need to mount the following</p> <pre>venus://users/home/bob AS /users/home/bob venus://users/anne AS /users/home/anne mars://home/colin AS /users/home/colin</pre> <p>Finally a unix soft link can be used to make /home/anne point to /users/home/anne</p> | |

| | | |
|----------|---|--|
| d | <p>An NIS Slave receives copies of the NIS maps from the NIS master, these maps contain the network critical data e.g. password files, groups, aliases. The NIS master will "push" new maps down to the slaves as they are updated, they will also be pushed at regular intervals in case earlier map transfers were missed due to network problems or a slave crash.</p> <p>The NIS slave will therefore always hold a local copy of the critical data required to authenticate user sand allow them to login.</p> | |
|----------|---|--|

- 2
- (a) Explain the benefit public-key encryption has over conventional encryption. (4)
 - (b) Describe the *man-in-the-middle* attack as applied to a public key encryption system. (6)
 - (c) Show which of the sets of values given in Figure Q2 for E , n and D could be used as valid RSA public/private key pairs (E, n) (D, n). Note a value for x has been included to help with the derivation. (8)
 - (d) Show how one of the valid key pairs from Q2 would be used to encrypt and decrypt a message. (7)

Total Marks [25]

| Encryption Exponent E | Product of primes $n=a \cdot b$ | Decryption Exponent D | $x=(a-1)(b-1)$ |
|-------------------------|---------------------------------|-------------------------|----------------|
| 5 | 247 | 216 | 164 |
| 7 | 589 | 463 | 540 |
| 7 | 400 | 258 | 361 |

Figure Q2: Encryption

| Part | Sample answer | Marking schedule |
|----------|--|------------------|
| a | <p>Public key encryption uses two keys, one of which is public and can safely be released over unprotected networks. This means that a sender can use it to send a message to the recipient in an encrypted form. Because the encrypted message can only be read by using the Private key it is safe from hackers.</p> <p>Conventional encryption relies on the use of a single key known by both sender and recipient, if the key is kept secret then any messages sent are secure, the problem lies in making sure that the single key gets to the sender without being intercepted by a hacker.</p> | [4] |
| b | <p>The "man in the middle attack" can be applied to the public key encryption system and it is based on the idea that a hacker could impersonate another individual and pass their public key to the message sender. When the sender encrypts a message they will be fooled into encrypting it with the wrong recipient's public key. The impostor could then decrypt the message and read it,</p> | [6] |

| | | |
|----------|---|-----|
| | <p>they could even encrypt it again with the recipient's real public key so that they receive the message which appears to be secure.</p> <p>The solution is to apply caution to the use of any unverified public keys.</p> | |
| c | <p>400 is obviously not the product of 2 prime numbers so can be discounted, the remaining key values can be check using the formula $E \cdot D \text{ mod } x = 1$.</p> <p>$5 \times 247 \text{ mod } 164 = 87$ $7 \times 463 \text{ mod } 540 = 1$</p> <p>therefore only the middle row represents a valid set of numbers for RSA keys.</p> | [8] |
| d | <p>The two keys are (7,589) and (463,589)</p> <p>therefore</p> <p>$\text{Plaintext}^7 \text{ MOD } 589 = \text{Ciphertext}$</p> <p>$\text{Ciphertext}^{463} \text{ MOD } 589 = \text{Plaintext}$</p> | [7] |

3 For the running configuration of a router given in Figure Q3:

- (a) Show the programming steps to set the login password for the console. (3)
- (b) Determine the number of subnets that can connect to the network which connects to the Serial0 connection, and also the number of hosts that can connect on each subnet. (8)
- (c) Explain the ACL restrictions placed on the Serial0 port. (5)
- (d) Design an ACL for the Ethernet0 port which blocks access for all the nodes with even IP addresses from access to a remote FTP server (155.10.10.11). All odd addresses are allowed to access it. All other traffic is allowable. (7)
- (e) What problem would an incorrect entry in the IP HOST table have on the router? (2)

Total Marks [25]

| Line no. | Router program |
|----------|---|
| 1 | hostname myRouter |
| 2 | ! |
| 3 | enable secret 5 AB\$1\$tA1\$9437T32ab9DT33GmAchl |
| 4 | ! |
| 5 | username mylogin password 7 11200B044813 |
| 6 | ! |
| 7 | interface Ethernet0 |
| 8 | ip address 160.10.2.1 255.255.255.0 |
| 9 | ! |
| 10 | interface Serial0 |
| 11 | ip address 192.168.10.65 255.255.255.252 |
| 12 | ip access-group 101 in |
| 13 | encapsulation ppp |
| 14 | no fair-queue |
| 15 | ppp authentication chap |
| 16 | ! |
| 17 | interface Serial1 |
| 18 | ip address 160.10.1.1 255.255.255.0 |
| 19 | ! |
| 20 | router igrp 10 |
| 21 | network 160.10.0.0 |
| 22 | ! |
| 23 | ip host Satellite_connection 160.10.1.2 |
| 24 | ip local-dns-server 160.10.2.10 |
| 26 | no ip classless |
| 27 | ip route 0.0.0.0 0.0.0.0 192.168.10.66 |
| 28 | access-list 101 deny tcp any 160.10.3.0 0.0.0.255 eq telnet |
| 29 | access-list 101 permit ip any any |
| 30 | ! |
| 31 | line aux 0 |
| 32 | line vty 0 4 |
| 33 | password cisco |
| 34 | login |
| 35 | ! |
| 36 | end |
| 37 | |
| 38 | |
| 39 | |

Figure Q3: Router program

| Part | Sample answer | Marking schedule |
|----------|---|---|
| a | <pre>config t line con 0 password cisco login exit</pre> | [3] – Programming commands. |
| b | <pre>Serial0 ip address 192.168.10.65 255.255.255.252</pre> <p>This gives 255.255.255.11111100b [2].</p> <p>Thus there are 6 bits for the network part [2]</p> <p>and 2 bits for the host part [2].</p> <p>Thus there can be 2^6-2 subnets [2], and 2^2-2 hosts [2]</p> | [8] – Calculations |
| c | <pre>access-list 101 deny tcp any 160.10.3.0 0.0.0.255 eq telnet access-list 101 permit ip any any</pre> <p>All traffic coming into the port [1] will be barred telnet access [1] to the 160.10.3.0 network [2].</p> <p>All other traffic will be allowed [1].</p> | [5] – Define ACL. |
| d | <pre>access-list 102 deny tcp 160.10.2.0 0.0.0.254 host 155.10.10.11 eq ftp access-list 102 permit ip any any</pre> <pre>interface Ethernet0 ip access-group 102 in</pre> | [5] – Design of ACL. [2] – Application of ACL. |
| e | It will not cause any problems with the operation [1], but the actual name defined will not be accessible [1]. | [2] – Explanation. |

- 4 (a) Contrast distance-vector routing protocols with link-state routing protocols. What methods may a distance-vector protocol use to determine the best route? (13)

| Part | Sample answer | Marking schedule |
|------|---|--|
| i | <p>Distance-vector . Distance-vector routing uses a distance-vector algorithm, which uses a direction (vector) and distance to any link in the internetwork to determine the best route. [1]</p> <p>Each router periodically sends information to each of its neighbours on the cost that it takes to get to a distance node. [1]</p> <p>The main problem with distance-vector is that updates to the network are step-by-step [1]</p> <p>Another problem is the high bandwidth requirements as each router sends its complete routing table to all of its neighbours at regular intervals. [1]</p> <p>Link-state. Link-state involves each router building up the complete topology of the entire internetwork (or at least of the partition on which the router is situated). [1]</p> <p>Thus each router contains the same information. [1]</p> <p>With this method, routers only send information to all of the other routers when there is a change in the topology of the network. [1]</p> <p>Each router builds a hierarchical topology of the internetwork, with itself at the top of the tree. [1]</p> <p>The main problem with linkstate is that routers require much more processing power to update the database [1]</p> <p>More memory is also required as routers require to build a database with details of all the routers on the network. [1]</p> | <p>[4] – Distance-vector.</p> <p>[6] - Three marks awarded for the student thinking of their own example. An important factor is for the student to select resources which cannot be shared.</p> |
| ii | <p>Methods a link-state method may use [3]:</p> <ul style="list-style-type: none"> • Bandwidth. The data capacity of a link, which is typically defined in bps. • Delay. The amount of time that is required to send a packet from the source to a destination. • Load. A measure of the amount of activity on a route. • Reliability. Relates to the error rate of the link. • Hop count Defined by the number of routers that it takes between the current router and the destination. • Cost. An arbitrary value which defines the cost of a link, such as financial. | <p>[3]– One half a mark for each type defined and described.</p> |

- (b) A router has three ports 141.10.193.1, 22.11.10.254 and 192.33.44.10, which have the subnets of 255.255.240.0, 255.128.0.0 and 255.255.255.248. Determine the router programming statements to setup RIP routing on the connected networks. (12)

| Part | Sample answer | Marking schedule |
|-----------|--|--|
| i | <p>141.10.193.1</p> <p>Subnet 255.255.240.0 = 255.255.11110000b.0 [1]</p> <p>141.10.193.1 is 141.10.1100 0001b.1 [1]</p> <p>Thus network address = 141.10.1100 0000.0 = 141.10.192.0 [1]</p> <p>22.11.10.254</p> <p>Subnet 255.128.0.0 = 255.1000 0000b.0.0 [1]</p> <p>22.11.10.254 is 22.11.1100 0001b.10.254 [1]</p> <p>Thus network address = 22.11.1000 0000.0 = 22.11.128.0 [1]</p> <p>192.33.44.10</p> <p>Subnet 255.255.255.248 = 255.255.255.1111 1000b [1]</p> <p>192.33.44.10 is 192.33.44.0000 1010b [1]</p> <p>Thus network address = 192.33.44.0 [1]</p> | [9] – Calculations for network addresses. |
| ii | <p>Commands are:</p> <pre> config t [1] router rip [1] network 141.10.192.0 [1] network 22.11.10.254 network 192.33.44.0 exit exit </pre> | [3] – Determination of router commands for routing RIP protocol. |

- 5 (a) Outline the structure of the NDS file system, and how it supports improved fault tolerance on the file system branches. (8)

| Part | Sample answer | Marking schedule |
|------|--|---|
| i | <p>NDS organizes network resources by objects, properties, and values. The two main objects are:</p> <ul style="list-style-type: none"> • Leaf objects – which are network resources such as disk volumes, printers, printer queues, and so on. [1] • Container objects – which are cascadable organization units that contain leaf objects. A typical organizational unit might be a company, department or group. [1] <p>NDS organizes networked resources in a hierarchical or tree structure (as most organizations are structured in this way). The top of the tree is the root object, to which there is only a single root for an entire global NDS database. [2]</p> <p>Servers then use container objects to connect to branches coming off the root object. This structure is similar to the organization of a directory file structure and can be used to represent the hierarchical structure of an organization. [2]</p> <p>To improve fault tolerance, NDS allows branches of the tree (or partitions) to be stored on multiple file servers. These mirrors are then synchronized to keep them up to date. [2]</p> | <p>[6] – NDS file structure [2] – Tolerance</p> |

- (b) Outline how NDS uses context to define the location of an object. What will the context be for the user FRED_B who works for the Fred&Co., in the Test Department, which is within the Engineering Unit? Also define how are relative context names used? (11)

| Part | Sample answer | Marking schedule |
|------|---|------------------|
| i | <p>The location at which an object is placed is called its context. Two objects which are placed in the same container have the same context. [2]</p> <p>If the user FRED_B works for the Fred & Co. (O=FRED_AND_CO), within the Test Department (OU=TEST), which is within the Engineering Unit (OU=ENGINEERING) then his context will be:</p> <p>OU=TEST.OU=ENGINEERING.O=FRED_AND_CO [2]</p> <p>An object is either identified by its distinguishing name. In the name, periods separate the objects. For a complete name, which is referred to from the [ROOT] object, a leading period is used, whereas a relative name does not have a leading period. For example, a complete name for a User object FRED_B could be:</p> <p>.CN=FRED_B.OU=TEST.OU=ENGINEERING.O=FRED_AND_CO [5]</p> | |

| | | |
|--|---|--|
| | Relative distinguishing name (RDN) which defines the relative path with respect to the current context. [2] | |
|--|---|--|

- (c) Why might a network administrator want to restrict the transmission of routing information? How would this be achieved on the router, and how might the network be setup so that the transmission of the routing information might be controlled? (6)

| Part | Sample answer | Marking schedule |
|----------|--|--------------------|
| i | <p>Routing information gives details of the connected networks, which might give some commercial advantages or details of where important information might be stored [2]</p> <p>In the programming of the router the restricted network is not included in the network [2]</p> <p>A network will typically be defined as an autonomous domain [1] with a single gateway, which will not transmit to external networks [1]</p> | [6] – Description. |

Total Marks [25]