NAPIER UNIVERSITY

SCHOOL OF COMPUTING

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 - 6
Number of sections - ONE

INSTRUCTION TO CANDIDATES

Complete any three of the questions from six.

1   The network illustrated in Figure Q1 has the following parameters:

Network address: 46.*x.y.z*
Number of nodes on each subnet: 4094

(a)   Subnet the network by assigning network addresses for NETA, NETB, NETC
      and NETD. Also determine the range of addresses which can be used for NETA,
      and the subnet mask for the complete network.

                                                                          (10)

(b)   Design and apply ACL statements on Router A that would allow the upper half
      of the network host range of NETA access to the FTP_01 server (Staff
      permission), and bar the lower half of the address range.

                                                                          (10)

(c)   Explain a method that could be used to control access to external WWW servers
      for all the users in NETA, and how WWW traffic from outside the network could
      be barred from access to NETA.

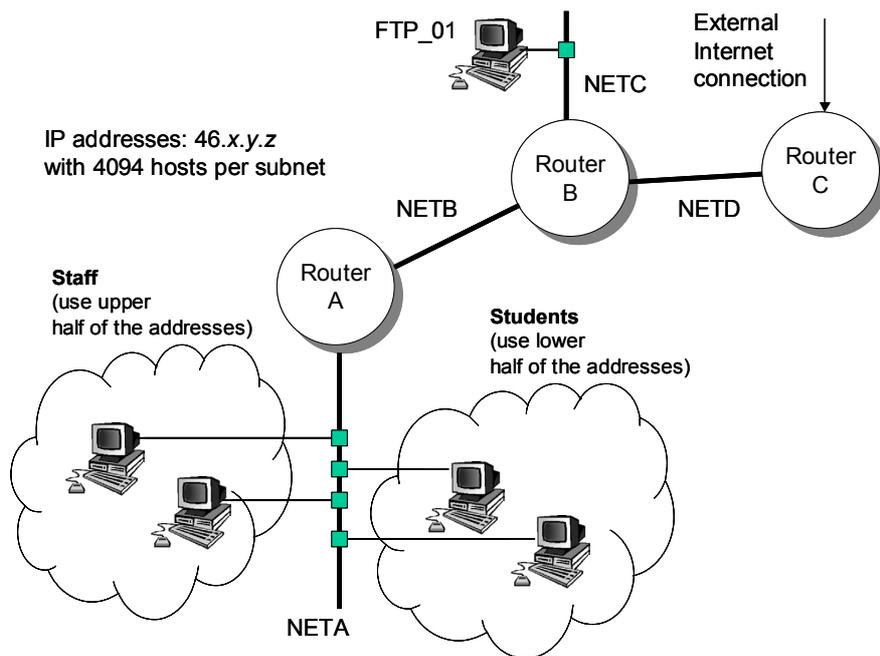   (5)

Figure Q1.

Total Marks [25]

Part	Sample answer	Marking schedule
a	We have a Class A address [1] 4094 hosts requires us to borrow 12 bits from host part [1]. Subnet mask is 255.1111 1111b.1111 0000b.0.0, which 255.255.240.0 [2] NETA = 46.**0000 000**b.**0001** 0000b.0 = 46.0.16.0 [1] NETB = 46.**0000 000**b.**0010** 0000b.0 = 46.0.32.0 [1] NETC = 46.**0000 000**b.**0011** 0000b.0 = 46.0.48.0 [1] NETD = 46.**0000 000**b.**0100** 0000b.0 = 46.0.64.0 [1] NETA = 46.0.16.1 to 46.0.0001 1111b.1111 1110b which is 46.0.16.1 to 46.0.31.254 [2]	As defined.

b	NetA addresses = 46.**0000 000**b.**0001** 000b.0
	
	Lower addresses will be: 46.**0000 000**b.**0001** 0xxxb.x [1]
	
	This we must match to 46.0.16.0 [2]
	with a wild card mark of 0.0.0000 0111b.255 which is 0.0.7.255 [3]
	
	Statements should be something like [3]:
	
	`access-list 102 deny tcp 46.0.16.0 0.0.7.255`
	`host 46.0.48.2 eq ftp`
	`access-list 102 permit ip any any`
	
	Applied to in port of Router A [1].
		As defined.

c	Best method would be to install a WWW proxy server, and the port on Router A should be firewalled so that it only allows out traffic on port 80 that is destined for the proxy. The proxy can then run an audit log. Marks may be granted for other secure methods.	[5] – Explanation.

2   (a)   Explain how interior and exterior routing protocols are used to create a simpler model of the Internet. If a network connects to an external network of 146.176.10.0, and two internal networks of 146.176.11.0 and 146.176.12.0, show the router commands which could be used to setup the RIP routing protocol, so that the routing tables for the internal networks would not be transmitted to the external network.

(6)

       (b)   A network of routers is illustrated in Figure Q2. The error rates on the links are:

Link	Error rate	
A to B	0.15	[15%]
B to C	0.1	[10%]
A to C	0.05	[5%]
A to D	0.2	[20%]
C to D	0.1	[10%]
D to E	0.1	[10%]
C to E	0.3	[30%]

Determine the following:

(i)   The number of possible routes from Router A to Router E, without retracing the same route to go.

(ii)   For RIP, which router(s) would be the next destination for data going from A to E.

(iii)   In a routing protocol based on errors rates, determine the probability of data being sent without error from Router D to Router A. Which route would be chosen?

(iv)   If the link between router B and C has just gone down, what problems might occur in the network, and how could they be overcome?
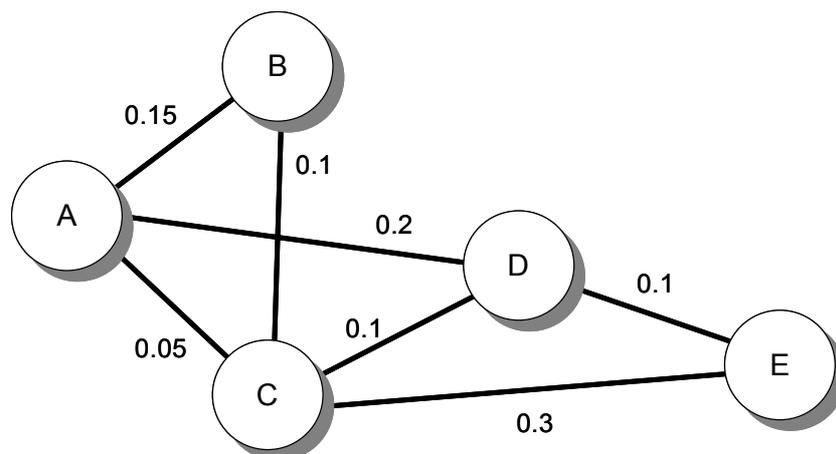
(19)

Total Marks [25]

Figure Q2.

Part	Sample answer	Marking schedule
a	Exterior routing protocols also reduce the complexity of the Internet [1], as they split the high-level structure into domains [1]. Router commands [3] Answer should not include the external network in the routing protocol list [1]	As defined.
b	(i) Routes are: ABCDE, ACE, ACDE, ADE, ADCE, ABCE. [2] (ii) Best routes for RIP are ADE and ACE. The system would load share where half the data would go to C and the other half to D [2]. (iii) Best route calculation [4]. $ABCD = 0.85 \times 0.9 \times 0.9 = 0.69$ $ACD = 0.95 \times 0.9 = 0.69$ $ACED = 0.95 \times 0.7 \times 0.9 = 0.6$ $ABCED = 0.85 \times 0.9 \times 0.7 \times 0.9 = 0.48$ $AD = 0.8$ [Best route] (iv) Routers B and C will tell A that the network that the link between them is down, but Router D could tell A that it can still reach the network, if the message from A was not received in time. [4] It could be overcome with a hold-down timer [2], or setting a split horizon [2]. Student should explain how these could be applied [3].	As defined.

3   (a)   Explain the term RPC (Remote Procedure Call) and its relevance to network file sharing.

(3)

(b)   What is the function of the utility *rpcinfo*?

(3)

(c)   Describe the role of the RPC *port mapper* service and state why it is important.

(4)

(d)   Figure Q3 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.

(10)

(d)   Describe the role of the *.htaccess* file in the file system of a Web Server.
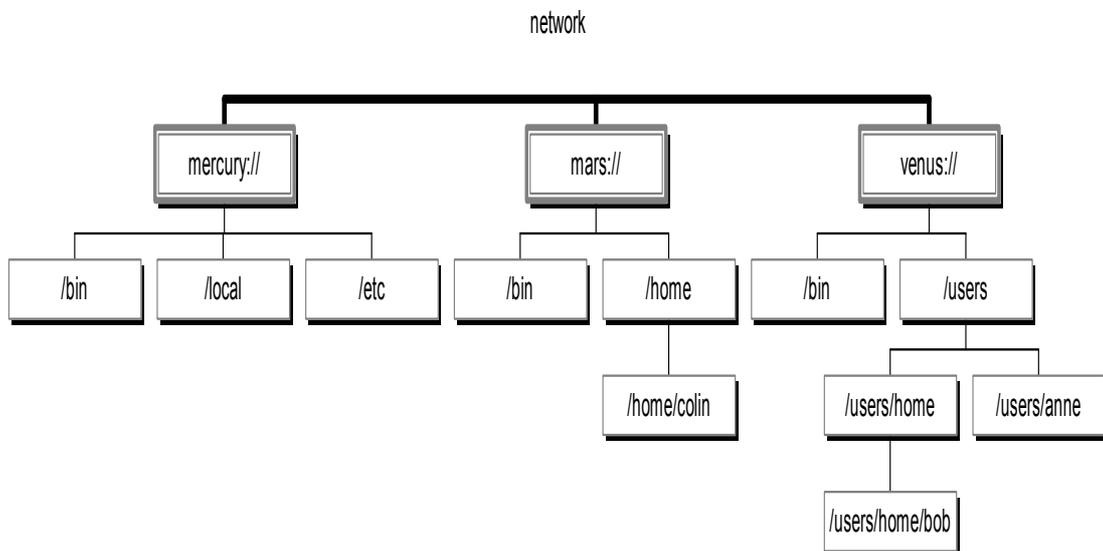
(5)

Total Marks [25]

network

mercury://   mars://   venus://

/bin   /local   /etc   /bin   /home   /bin   /users

/home/colin   /users/home   /users/anne

/users/home/bob

Figure Q3.

Part	Sample answer	Marking schedule
a	This is a mechanism developed by Sun Microsystems which allows a process running on one machine to call a procedure on another using TCP/IP as the transport medium, it is used typically to facilitate file system sharing across a TCP/IP based network.	As defined.
b	rpcinfo allows a system to query its own or other machine's rpc services supported, it can be used to check that a remote node supports the NFS service for example.	As defined.
c	The port mapper maps a TCP port number to an rpc service, only the portmapper service itself is on a fixed port (111) others are not defined. The portmapper service 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.	
d	Firstly a common directory needs to be created on the machines, let's create a /users/home directory on mars and mercury. mars and venus will need to export file systems so they should be configured as servers. All three machines will also be clients. Mars will be set to export it's /home directory whilst venus exports /users. mars will need to mount the following venus://users/anne AS /users/home/anne venus://users/home/bob AS /users/home/bob venus will need to mount the following mars://home/colin AS /users/home/colin mercury will need to mount the following venus://users/home/bob AS /users/home/bob venus://users/anne AS /users/home/anne mars://home/colin AS /users/home/colin Finally a unix soft link can be used to make /home/anne point to /users/home/anne	
	The .htaccess file is read by the web server and typically contains additional configuration information for the directory which contains the .htaccess file. The content of the file can be used to cause the web server to restrict web access to files in the same directory based on the address of the user or request user authentication.	

4   (a)   An encryption technique allocates several alternative ciphertext representations for the same plaintext character for cases where the plaintext character is relatively common (e.g. "E","A", "T" etc.). Explain the benefit of these multiple codes if any exist?

(3)

(b)   In simple Electronic Code Book encryption why would it be inadvisable to use a technique which encrypted individual single bytes rather than large chunks of the message, for example 64 bits at a time.

(3)

(c)   Digital Encryption Standard (DES) uses a combined technique based on several simple encryption methods. Explain the following terms as applied to DES.

(i)   Bit Permutation

(3)

(ii)   XOR

(3)

(iii)   Substitution Boxes

(4)

(d)   Discuss the advantages and disadvantages of making an encryption algorithm public or keeping its details secret.

(5)

(e)   When producing a *message hash* the result is always the same size regardless of the size of the plaintext message, explain.

(4)

Total Marks [25]

Part	Sample answer	Marking schedule
a	The multiple code will effectively mask to increased frequency of the common characters, ideally the frequency of the ciphertext characters should be fairly uniform thus the most common character ("E") will not be recognisable by statistical means.	
b	The frequency of different characters in messages is often predictable, especially for text, the frequency of 8 byte patterns is not so predicable and there are very many more possible combinations to consider so statistical analysis of the ciphertext would not yield a meaningful frequency distribution.	
c	(i) The order of bits in a message block is changed in a particular way to hide the real message content. (ii) Certain bits of the message are inverted wherever a "1" exists in the encryption key, this is a reversible process and very easy to do in hardware or software. (iii) A substitution box is effectively a mini electronic code book applied (in the case of DES) to parts of the message giving an apparently random ciphertext from the plaintext message.	
d	A secret algorithm is more difficult to crack as the hacker would not know how to apply a secret encryption key even it it could be obtained. On the other hand a secret algorithm would have to be protected in the same way that encryption keys are. The technique could never be widely publicly deployed.	
e	A message "hash" is not an encryption of a plaintext message but more of a signature of the message. This signature is a brief code which can be validated against the message so that if the message was changed at all it would no longer match the message hash signature. It should be very difficult to produce a message which matches the hash (signature) of another one so this isgnature cannot be transferred to other fake messages.	

5 (a) What property of the product of two large prime numbers makes this a suitable basis for the creation of an asymmetrical (public key) encryption technique.

(4)

(b) The concept of *non-repudiation* is important in the conduct of e-commerce, explain how public key encryption schemes support this property.

(6)

(c) Describe the *man-in-the-middle* attack as applied to a public key encryption system.

(7)

(d) The following pair of values for *E* and *n* make up a valid RSA public key (*E*,*n*). Show how this key would be used to encrypt the message "8".

Encryption exponent E	Product of primes $n=a \times b$
7	589

(8)

Total Marks [25]

Part	Sample answer	Marking schedule
a	The assymetrical property is the fact that it is relatively easy to find prime numbers and create the product of two of them. It is very very difficult (actually time consuming) however to reverse this to find the factors, the two original prime numbers.	
b	A message encrypted with the private key of the sender can be decrypted by anyone with access to the sender's public key, since these keys are available via key servers the message is not secret. However by decrypting the message, it proves it was encrypted with the sender's private key and since that is secret to the sender only the sender could have created this message. This is a form of authentication or digital signature and also means that the sender cannot repudiate sending such a message, very important for a financial transaction.	
c	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, they could even encrypt it again with the recipient's real public key so that they receive the message which appears to be secure. The solution is to apply caution to the use of any unverified public keys.	
d	Plaintext^7 MOD 589 = Ciphertext 8^7 MOD 589 = 2097152 MOD 589 = 312 Note <table><tr><td>Decryption Exponent D</td><td>$x=(a-1)(b-1)$</td></tr><tr><td>463</td><td>540</td></tr></table>	

6   (a)   Explain how PPP and SLIP can be used to create a Virtual Private Network (VPN). Outline the enhancements that PPP has over SLIP that allows for improved performance and security.

(6)

(b)   Explain how routers are used in a Novell NetWare network to provide services from NetWare servers to NetWare clients on interconnected networks.

(6)

(c)   The following shows an example of a `show ipx route` command. Explain the main elements of this listing.

(7)

```
Myrouter > show ipx route
Codes: C - Connected primary network, c - connected secondary network, R - RIP, E
- EIGRP, S - Static, W - IPXWAN connected
5 total IPX routes

Up to 2 parallel paths allowed. Novell routing protocol variant in use

R Net 2B10 [8/1] via 2B20.0000.0c03.13d3, 40 sec, Serial1
  via 2B30.0000.0000.D101.aa11, 40 sec, Serial 0
C Net 2B30 (X25),  Serial0
C Net 2B20 (HDLC), Serial1
C Net 2B40 (NOVELL-ETHER), Ethernet0
C Net 2B50 (NOVELL-ETHER), Ethernet1
```

(d)   Contrast CHAP and PAP, and outline how they would be setup on a router.

(6)

Total Marks [25]

Part	Sample answer	Marking schedule
a	PPP and SLIP encapsulates most network protocols [1]. PPP allows for: • Data link setup. [1] • Dynamic assignment of IP addresses. [1] • Error detection. [1] • Link configuration and link quality testing. [1] • Negotiation options for capabilities such as network-layer address negotiation and data compression negotiations [1]	
b	Novell servers send out SAP packets [1] which broadcast network services [1], such as a print server [1]. Router do not forward these [1], and store them [1]. When a client requires a service the router send its address to the client [1].	
c	[R] Route learnt through an RIP update. [1] Net 2B10 – Destination network address is 2B10. [1] [8/1] identifies that the network is eight clock ticks away or one hop. The general format is [*delay*/ *metric*], where *delay* defines the number of ticks of the IBM clock to the destination, and *metric* is the number of hops to the network. [1] *Via*. The *via* defines the next hop on the route. The address follows it. [1] 2B20.*etc*. Defines the next hop on the path. [1] *40 sec*. This defines the time that information was last received about the network (age). [1] *Serial1*. Next port is reachable from this port. [1]	
d	CHAP provides for a challenge for the session [1], PAP only verifies once, and does not use encryption (plaintext) [1]. For CHAP, a user account must be setup on the router which is to be connect to [1]. This is setup with a command such as: username fred password mypass [1] The connected ports must then be encapsulated with ppp, with commands such as: encapsulation ppp ppp chap password mypass [1] and so on. pap is setup in a similar way [1]	