Values

INSTRUCTIONS: **Programmable Calculators allowed, No Cheating, Neatness counts (If I Can't read it, I can't mark it)**

Answer in space provided, State any assumptions made. Good Luck

PERMITTED MATERIAL:

Handout: "How Hackers Break In ... and How They Are Caught"

Assume: **$c = 3 \times 10^8$ m/s (signals travel 2/3 c)**
$\tau = 51.2$ usec (maximum round trip delay in ethernet)

Enter NAME and STUDENT NUMBER:

_____
STUDENT NUMBER

_____
WRITE NAME IN FULL ON THIS LINE

_____
PRINT NAME IN FULL ON THIS LINE

_____
EXAMINATION CENTRE

_____
SEAT NUMBER

Values

Part A - Short/Long Answers

(15) One mark for each question/part, except 3 marks for question 4.

1. **True** or **False**:
   [a] Before sending a packet into a datagram network, the source must determine all of the links from source to destination, that the packet will traverse.

   [b] An ARP query packet is broadcast.

   [c] Each LAN adapter should have a unique MAC address.

   [d] Consider a computer network consisting of several interconnected 10BaseT hubs, but no bridges, switches or routers. This network has only one collision domain.

   [e] The entries in a bridge table need to be configured by the network administrator.

2. What type of applications benefit from a connectionless transport protocol?

3. A T3 line multiplexes 28 T1 lines. Each T1 multiplexes 24 64Kbps channels. How many 64 Kbps channels are there on a T3 line? What is the bit rate of a T3?

4. Given the density of prime numbers and the BigInteger constructor that probabilistically generates large prime numbers, how many attempts (iterations) on average are required to generate a 128 bit large number that is very likely prime with certainty $(1-2^{-20})$? How many attempts are required to generate 256 and 512 bit primes?

Hints: BigInteger(int bitLength, int certainty, Random rnd) constructor generates a probably prime number of bitLength bits with probability $(1-2^{-certainty})$. It does this by generating a random number candidate and iteratively checking if the number is prime. If the candidate is not prime an average 2 iterations are required and another candidate is selected. If the certainty is set to 20, 20 iterations are performed and the candidate is considered prime with a probability of $(1-2^{-20})$. The number of prime numbers is n/lnn out of n. ln(2) is about 0.7.

Values

5. Consider a frame of 5 bytes of information to be checked with a 1 byte CRC code, given as:

$$G(x) = x^8 + x^2 + x + 1$$

In hardware the CRC is calculated with LFSRs which represent the CRC polynomial. The CRC operation is equivalent to polynomial division where the 1 bits of the data represent the polynomial coefficients. Calculate the CRC for the following data

D(x) = MSB 00000000 00000000 0000000 00000100 00011100 LSB

[a] What polynomial does D(x) represent, the coefficients are represent by the bit values.

[b] The CRC is the remainder when D(x) is divided by G(x). Calculate the CRC, i.e. the remainder of D(x)/G(x)

Assume that the receiver data stream D'(x) has an error as shown:

D'(x) = MSB 00000000 00000000 0000000 00000100 00011101 LSB

[c] What is the CRC now? Is the CRC able to detect the error? Can it correct the error?

6. What is the difference between congestion control and flow control?

7. Briefly explain both FDM and TDM. List two advantages of TDM?

Values

Part B - Protocol stacks and encapsulation.

(6) One mark each.

8. TCP and IP headers both require a minimum of 20 bytes. Suppose an application generates chunks of 60 bytes of data every second, and each chunk gets encapsulated in a TCP segment and then an IP datagram. What percentage of each IP datagram will contain application data.
   [a] 40%
   [b] 60%
   [c] 80%

9. Wired ethernet adds another 26 bytes of header and trailer. For the same example, assume the underlying physical layer is ethernet. What percentage of each ethernet frame will be application data?
   [a] 26%
   [b] 48%
   [c] 58%

10. Wireless 802.11 adds another 24 byte PLCP for each ethernet frame less the 8 byte preamble of the corresponding wired ethernet frame. What percentage of each 802.11 ethernet frame will be application data across a wireless link?
   [a] 42%
   [b] 40%
   [c] 38%
   [d] none of the above

11. What is the transmission time for the frame on the wireless 802.11b standard LAN. According the 802.11 standard the PLCP is transmitted at 1Mbps while the remainder of the frame will transmit at a higher rate up to 11 Mbps for 802.11b. What percentage of the total transmission time will be for application data.
   [a] 17%
   [b] 7%
   [c] 19%

12. Assume we now are now using IPSec for authentication in the transport mode. That is we are running the AH protocol which introduces another 24 bytes of overhead. What percentage of each IP datagram will now contain application data.
   [a] 48%
   [b] 65%
   [c] 60%

13. Draw and label the layers of the protocol stack representing the transmission of the authenticated data from the previous question over an 802.11 wireless LAN.

Values

Part C - Physical/Network Access Layer (Ethernet)

(19) 14-12, 15-5, 16-2.

14. Assume you are building a CSMA/CD protocol and the network specification calls for a shared medium 1 Km in diameter. That is, from one end of the network to the other the maximum distance is 1 Km.

[a] What is the round trip propagation time?

[b] What does the round trip time imply about the minimum packet size?

[c] What is the minimum packet size if you want to run the network at 10 Mbps.

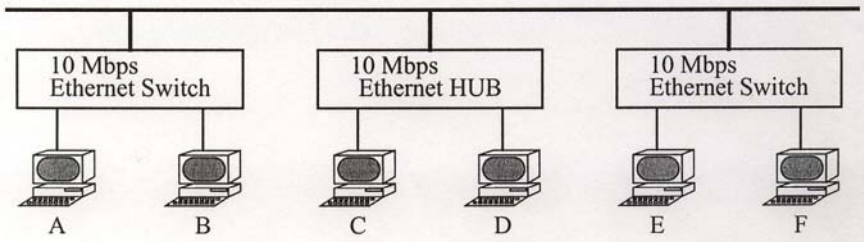
[d] What is the minimum packet size if you want to run the network at 100 Mbps.

[e] What is the maximum packet size for your protocol? Explain your rational.

[f] Does your protocol guarantee any quality of service (QoS)?

Values

15. Given the following Ethernet network:



If two hosts (A and B) on the same ethernet switch want to transmit 10KBytes and 5KBytes respectively. Host A wants to transmit at time t=0 and host B at time t=40 usec. Assuming no other traffic on the network:

[a] Will a collision occur? Explain.

[b] When will B transmit its packet?

[c] If A and B switch transmission times (B at 0 and A at 40 usec) what will happen?

[d] If A and B are on a bus based segment will anything different happen?

[e] If A and B are connected to a hub will anything different happen?

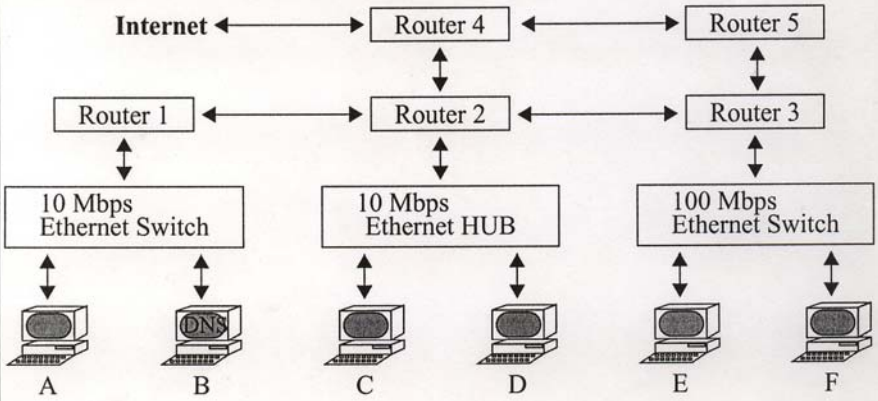
16. In the figure circle the individual ethernet collision domains.

Values

Part D - Network Layer (IP)

(12) 17-2 marks, 18-6 marks, 19-2 marks, 20-2 marks

Given the following network that you are very familiar with.



17. Circle the individual ethernet collision domains.

18. Assuming that all ARP tables are initially empty, the routing tables are stable, and the DNS server can resolve any request. Show the sequence of packets that will occur for **A** to send two ping requests to **D**.

19. Show the sequence of packets that will occur for **A** to send a third ping requests to **D** with with a TTL of 1.

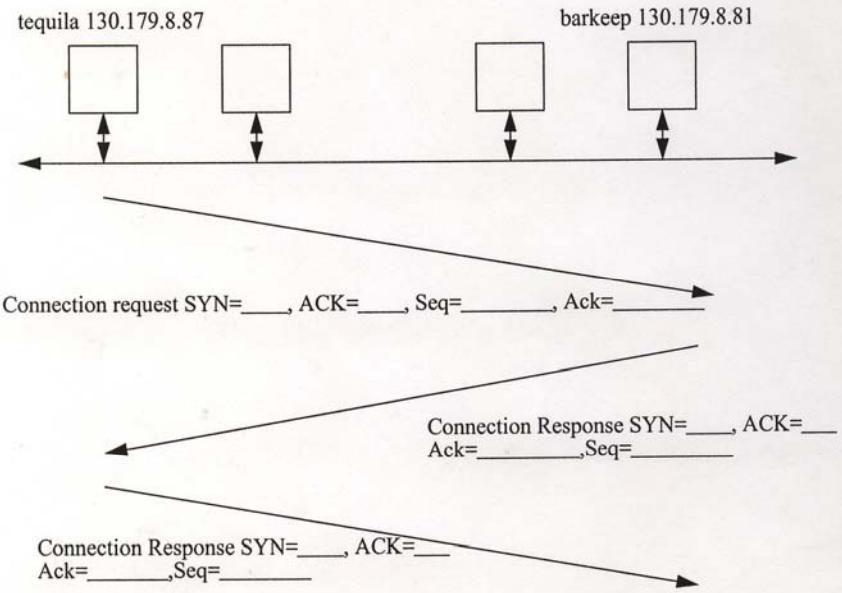
20. If **A** has IP 120.11.22.16 and subnet mask 255.255.128.0, What is the subnetwork address and the hostid portion of the IP address.

Values

Part E - Transport Layer (TCP/UDP)

(14) 21-6, 22 to 25 2 each.

21. Label the TCP/IP three-way handshake. SYN and ACK are message flag BITS, Ack and Syn are 32 bit integers.



22. What are sequence/acknowledge numbers used for in TCP/IP?

23. What is a port number?

24. Can the same service be implemented using either TCP or UDP? If so could they use the same port number?

25. Why is UDP called an 'unreliable' transport service?

Values

Part G - Encryption

(19) 27-8 marks, 28-2 marks, 29-5 marks, 30-4 marks

27. Alice is running a business on the Internet, and wants people to send her credit card numbers encrypted with RSA.

She selects **p** = 11, **q** = 17 as her two large prime numbers.

[a] Which of the following values would be a suitable value for the public encryption key **e**? State the reasons for your selection. (Hint: Only one value is suitable).

5 7 10 15 24 32

[b] Which of the following values would be a suitable value for the secret decryption key **d**? State the reasons for your selection. (Hint: Only one value is suitable).

0 1 9 11 15 23 24

[c] Bob wants to encrypt the number 9. What is the encrypted value of 9?

[d] Alice receives the encrypted message: **0,1,70,0,1,70,0,1,70,0** which represents Bob's credit card number (each digit encrypted separately), What is Bob's credit card number?

28. Could characters (1 byte / character) be encrypted/decrypted one character at a time with these keys? Explain.

Values

29. Answer the following questions on Private Key encryption:

[a] Why are Private key encryption methods also called block ciphers?

[b] List three features that are characteristic of a good block cipher?

[c] Explain what is meant by: "block chaining" in a block cipher, and what it is used for.

30. What are the main advantages and disadvantages of private key encryption compared to public key encryption?