

Calvin Passmore

A02107892

ECE 5600

Final Exam

1

Match the network layer with its function

Name	Answer
Application Layer	c. user programs are part of this layer
Network Layer	f. handles routing through subnet
Physical Layer	e. deals with voltages, frequencies, radiation, etc.
Transport Layer	d. handles framing of data
Presentation Layer	b. converts data to the user's desired format
Data-link Layer	a. provides end-to-end communication

2

Name two classical techniques used to multiplex multiple lower-bandwidth channels onto a single higher bandwidth line.

1. Frequency division multiplexing (FDM)
2. Time division multiplexing (TDM)

3

Assume a telephone line has a bandwidth of 3100HZ and a Shannon limit of 37 kbps, what is the minimum possible signal-to-noise ratio? Express your answer in dB.

```
In [ ]: import math

C = 37e3 # Shannon limit
B = 3100 # Hz

SNR = 2**((C/B) - 1)
SNR_dB = 10 * math.log(SNR, 10)
print(SNR_dB)
```

35.92827765699723

The minimum possible signal to noise ratio is 35.93 dB.

4

How can 56kbps modems seemingly exceed the Shannon Limit?

By removing the local loops at the end, the Shannon limit is seemingly exceeding. However it is really just lower the SNR.

5

How is the following bit string transmitted with (a) bit stuffing and (b) byte stuffing as it is done in PPP: 01111111 11100000 01111110 01111101.

(a) 011111011 111000000 011111010 011111001

(b) 01111111 11100000 ESC 01111110 01111101

6

What is the difference between pure and slotted ALOHA for channel allocation?

In pure ALOHA, a channel may attempt to send whenever it will.

In slotted ALOHA, a channel may only start to send on a slot, or a given time interval.

7

What frequency band does Bluetooth use, (b) How many different frequencies are used, and (c) How often do frequency hops occur?

(a) 2.4 GHz

(b) 79 frequencies are used

(c) There can be 1600 hops/sec

8

What are the four primary "Quality of Service" parameters?

1. What applications need from the network
2. How to regulate the traffic that enters the network

3. How to reserve resources at routers to guarantee performance
4. Whether the network can safely accept more traffic

9

A TCP packet with the FIN + ACK bits set contains 900 data bytes, has a sequence number = 75 and acknowledge number = 98. Assuming no error is detected, what sequence and acknowledge numbers should be returned in the acknowledgement packet?

Sequence = 75 ACK = 900

10

Name the algorithm that coalesces small TCP segments while it waits for an acknowledgement of the previous segment.

Nagle's algorithm

11

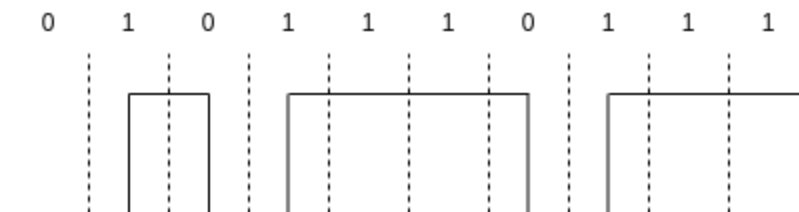
In the PTSN, what is the term for:

- (a) A connection from one office to another - Local Loops
- (b) A connection from the end office to the subscriber - Trunks
- (c) An office that connects to cell phones via base stations - Switching offices

12

Sketch the waveform obtained by encoding 01011011 with 4B/5B then NRZI. Assume an initial state of 0v.

0101 1011 → 01011 10111



13

Four stations (A..D) using Mok & Ward's binary countdown algorithm are currently assigned the values A=1, B=4, C=2, D=3 (0 is not used). If C is ready to transmit one frame and D is ready to transmit two frames, what are the address assignments after all three frames have been sent?

A = 1

B = 2

C = 3

D = 4

14

Using the CRC polynomial x^4+x+1 and an initial value of 0, compute the CRC for the bit sequence 10100101.

```

10011 | 10100101
      10011
      00111
        11110
        10011
        01101
          11011
          10011
          01000

```

01000

15

7-bit Hamming codewords are used to encode 4-bit values. After transmission over a noisy channel, the codeword 1011011 is received. What was the original 4-bit value?

1011011

Check bits: 10 1

Corrected 1011010

Original Message 1010

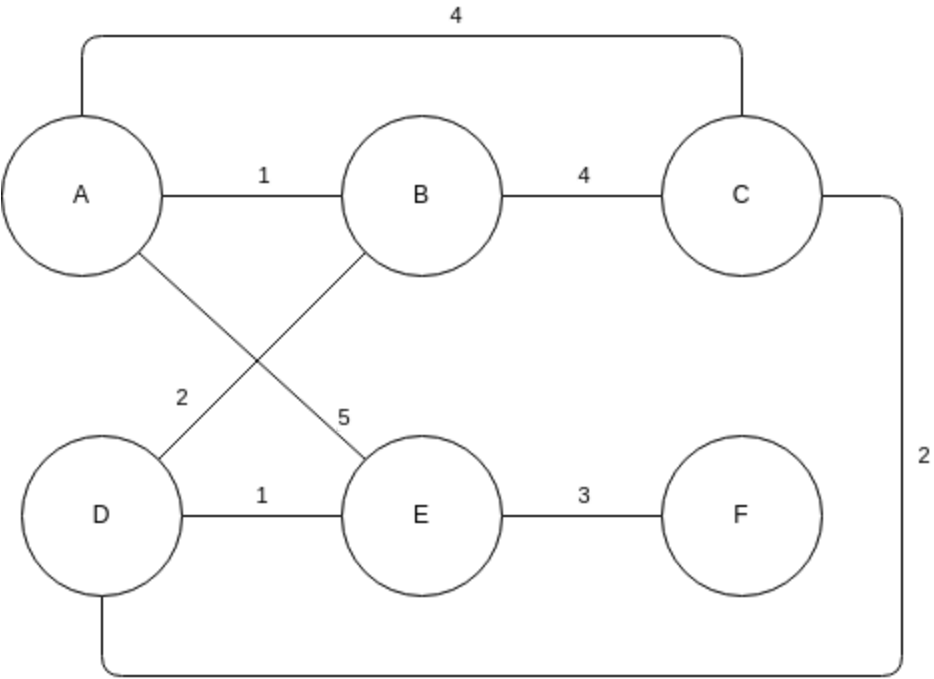
16

What IP protocol numbers are used for each of the following?

- (a) IP in IP = 4
- (b) TCP = 6
- (c) UDP = 17
- (d) ICMP = 1

17

(a) Draw a router diagram. Label each link with its length and each node with its router ID (A-F). If the two routers on either side of a link disagree on its length, take the mean (average) of the two.



(b) Use Dijkstra's Algorithm to find the shortest path from router A to all the other routers. In what order to the “nodes” (routers) become permanent.

A (0), B (1), D (3), E (4), C (4), F (7)

(c)

A Routing Table Base IP address/mask | Line -----|----- 130.0.0.0/19 | LAN
130.0.32.0/21 | B 130.0.40.0/20 | C 130.0.48.0/20 | B 130.0.64.0/20 | E

18

Consider the subnet in the following. Distance vector routing is used, and the following vectors have just come in to router C: from B: (5, 0, 8, 12, 6, 2); from D: (16, 12, 6, 0, 9, 10); and from E: (7, 6, 3, 9, 0, 4). The measured delays to B, D, and E, are 6, 3, and 5, respectively. What is C's new routing table? Give both the outgoing line to use and the expected delay.

C original table

A	B	D	E	F
6	3	5		

C by B table

A	B	C	D	E	F
11	6	14	18	12	8

C by D

A	B	C	D	E	F
19	15	9	3	12	13

C by E

A	B	C	D	E	F
12	11	8	14	5	9

C's new table, below is from who

A	B	C	D	E	F
11	6	9	3	5	8
B	B	E	D	E	F

19

Provide the well-known port number for each of the following application layer protocols:

- http: 80
- telnet: 23
- dns: 53
- pop3: 110
- echo: 7
- ssh: 22
- https: 443
- tftp: 69
- bootp (server): 67

- bootp (client): 68

20

A Diffie-Hellman key exchange uses $p = 43$ and $g = 13$. If one side chooses a random number a of 7 and the other side sends a key exchange message which contains the number 24, what is the secret key?

```
In [ ]: g = 13
        p = 43
        a = 7
        g_b_mod_p = 24

        g_ab_mod_p = (g_b_mod_p ** a) % p

        print(g_ab_mod_p)
```

6

The secret key is 6

21

Captain Picard's public RSA key is ($e=29$, $n=91$). What is his private key? (Note: you will have to factor 91 to get it). To verify that you have the right key, show that the decryption $D(61) = 3$.

```
In [ ]: # To factor 91
        for i in range(2,50,1):
            if (91 % i) == 0:
                print(i)
```

7

13

```
In [ ]: p = 7
        q = 13
        z = (p - 1) * (q - 1)
        print(z)
```

72

$p = 7$

$q = 13$

$z = 72$

factors are 2 & 3, other relatively prime could be any prime number above 5

$d = 5$

```
In [ ]: possible_d_vals = [5, 7, 11, 13, 17, 19, 23, 29, 31, 37] # There are more possible values for d
working_d_vals = []

for d in possible_d_vals:
    for e in range(2, 100):
        if (e * d) % z == 1:
            working_d_vals.append(d)
            break

C = 61 # from problem description
n = 91

for d in working_d_vals:
    if (C*d) % n == 3:
        print(d)
```

5
11
17
23
29

Possible d values for decryption are [5, 11, 17, 23, 29].

$$(61^5) \% 91 = 3$$

$$(61^{11}) \% 91 = 3$$

$$(61^{17}) \% 91 = 3$$

$$(61^{23}) \% 91 = 3$$

$$(61^{29}) \% 91 = 3$$

While there are likely more, the answer your probabaly looking for is 5.