CHAPTER 5

PRACTICE SET

Questions

Q5-1. Communication at the network layer is host-to-host; communication at the data-link layer is node-to-node.

Q5-3. In variable-size framing, flags are needed to separate a frame from the previous one and the next one.

Q5-5. In a single-bit error only one bit of a data unit is corrupted; in a burst error more than one bit is corrupted (not necessarily contiguous).

Q5-7. In this case, $k = 20$, $r = 5$, and $n = 20$. Five redundant bits are added to the dataword to create the corresponding codeword.

Q5-9. The minimum Hamming distance is the smallest Hamming distance between all possible pairs in a set of words.

Q5-11. We have $n = 2^r - 1 = 7$ and $k = n - 3 = 7 - 3 = 4$. A dataword has four bits and a codeword has seven bits. Although it is not asked in the question, we give the datawords and valid codewords below. Note that the minimum distance between the two valid codewords is 3.

Data	*Code*	*Data*	*Code*	*Data*	*Code*	*Data*	*Code*
0000	0000000	0100	0100011	1000	1000110	1100	1100101
0001	0001101	0101	0101110	1001	1001011	1101	1101000
0010	0010111	0110	0110100	1010	1010001	1110	1110010
0011	0011010	0111	0111001	1011	1011100	1111	1111111

Q5-13.

a. The generator has three bits (more than required). Both the rightmost bit and leftmost bits are 1s; it can detect all single-bit errors.

b. This cannot be used as a generator: the rightmost bit is 0.

c. This cannot be used as a generator; it has only one bit.

Q5-15. In this case $r = 7 - 1 = 6$.

a. The length of the error is L = 5, which means L ≤ *r*. All burst errors of this size will be detected.

- **b.** The length of the error is L = 7, which means L = r + 1. This CRC will detect all burst errors of this size with the probability $1 - (0.5)^5 \approx 0.9688$. Almost 312 out of 10,000 errors of this length may be passed undetected.
- **c.** The length of the error is L = 10, which means L > r. This CRC will detect all burst errors of this size with the probability $1 - (0.5)^6 \approx 0.9844$. Almost 156 out of 10,000 errors of this length may be passed undetected. Although the length of the burst error is increased, the probability of errors being passed undetected is decreased.

Q5-17. The value of a checksum can be all 0s (in binary). This happens when the value of the sum (after wrapping) becomes all 1s (in binary).

Q5-19. The address field in the HDLC network defines the address of the secondary station (as the sender or receiver); the primary station, which is always unique, does not need an address.

Q5-21. The transmission rate of this network is T_{fr} = (1000 bits)/(1Mbps) = 1 ms. The vulnerable time in pure Aloha is $2 \times T_{fr} = 2$ ms.

Q5-23. The use of K in the figure decreases the probability that a station can immediately send when the number of failures increases. This means decreasing the probability of collision.

- **a.** After one failure (K = 1), the value of R is 0 or 1. The probability that the station gets R = 0 (send immediately) is 1/2 or 50%.
- **b.** After three failures (K = 3), the value of R is 0 to 7. The probability that the station gets R = 0 (send immediately) is 1/8 or 12.5%.

Q5-25. The last bit is 10 μs behind the first bit.

- **a.** It takes 5 μs for the first bit to reach the destination.
- **b.** The last bit arrives at the destination 10 μs after the first bit.
- **c.** The network is involved with this frame for 5 + 10 = 15 μs.

Q5-27. The answer is theoretically yes. A link-layer address has a local jurisdiction. This means that two hosts in different networks can have the same link-layer address, although this does not occur today because each NIC has a unique MAC address.

Q5-29. We do not need a multiple access protocol in this case. The DSL provides a dedicated point-to-point connection to the telephone office.

Q5-31. ARP Packet Size = 2 + 2 + 1 + 1 + 2 + 6 + 4 + 6 + 4 = 28 bytes (Figure 5. 48).

Q5-33. The preamble is a 56-bit field that provides an alert and timing pulse. It is added to the frame at the physical layer and is not formally part of the frame. SFD is a one-byte field that serves as a flag.

Q5-35. In a full-duplex Ethernet, each station is connected to the switch and the media is divided into two channels for sending and receiving. No two stations compete to access the channels; each channel is dedicated.

Q5-37. The common traditional Ethernet implementations are 10Base5, 10Base2, 10-Base-T, and 10Base-F.

Q5-39. Dial-up modems use part of the bandwidth of the local loop to transfer data. The latest dial-up modems use the V-series standards such as V.90 (56 kbps for downloading and 33.6 kbps for uploading), and V.92 (56 kbps for downloading and 48 kbps for uploading).

Q5-41. For calculating T_p, we need to consider the maximum length of frame transmission between any two stations. In this case, the maximum length is 500 + 700 = 1200 m.

Q5-43. A VLAN saves time and money because reconfiguration is done through software. Physical reconfiguration is not necessary.

Q5-45. A single clock handles the timing of transmission and equipment across the entire network.

Q5-47. A TP (transmission path) is the physical connection between a user and a switch or between two switches. It is divided into several VPs (virtual paths), which provide a connection or a set of connections between two switches. VPs in turn consist of several VCs (virtual circuits) that logically connect two points.

Problems

P5-1. Each escape or flag byte must be pre-stuffed with an escape byte. The following shows the result:

D	**E**	**E**	D	D	**E**	**F**	D	D	**E**	**E**	**E**	**E**	D	**E**	**F**	D

P5-3. We have (vulnerable bits) = (data rate) × (burst duration). The last example shows how a noise of small duration can affect a large number of bits if the data rate is high.

a. **vulnerable bits** = $(1500) \times (2 \times 10^{-3})$ = **3 bits**

b. **vulnerable bits** = $(12 \times 10^{3}) \times (2 \times 10^{-3})$ = **24 bits**

c. **vulnerable bits** = $(100 \times 10^{3}) \times (2 \times 10^{-3})$ = **200 bits**

d. **vulnerable bits** = $(100 \times 10^{6}) \times (2 \times 10^{-3})$ = **200,000 bits**

P5-5. The following shows the results. In the interpretation, 0 means a word of all 0 bits, 1 means a word of all 1 bits, and ~X means the complement of X.

a. (10001) ⊕ (10001) = (00000) Interpretation: $X \oplus X \rightarrow 0$

b. (11100) ⊕ (00000) = (11100) Interpretation: $X \oplus 0 \rightarrow X$

c. `(10011)` ⊕ `(11111)` = `(01100)`   Interpretation: X ⊕ 1 → ~X

P5-7. Answers are given below:

a. error   b. error   c. 0000   d. 1101

P5-9. The following shows the result. Part d shows that the Hamming distance between a word and itself is 0.

a. d (10000, 00000) = 1   b. d (10101, 10000) = 2

c. d (00000, 11111) = 5   d. d (00000, 00000) = 0

P5-11. The CRC-8 is 9 bits long, which means $r = 8$.

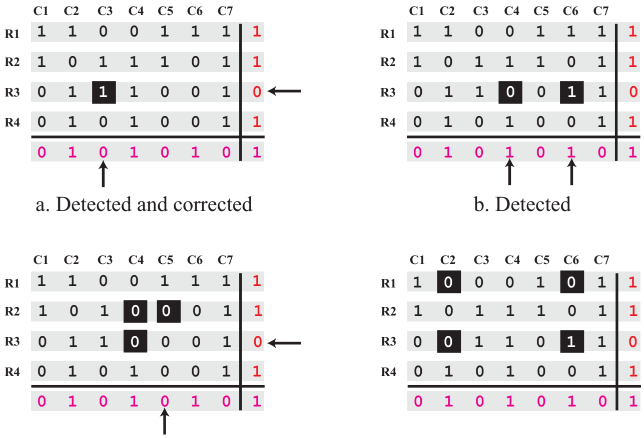
a. It has more than one bit and the rightmost and leftmost bits are 1s; it can detect a single-bit error.

b. Since 6 ≤ 8, a burst error of size 6 is detected.

c. Since 9 = 8 + 1, a burst error of size 9 is detected most of the time; it may be left undetected with probability $(1/2)^{r-1}$ or $(1/2)^{8-1} \approx 0.008$.

d. Since 15 > 8 + 1, a burst error of size 15 is detected most of the time; it may be left undetected with probability $(1/2)^r$ or $(1/2)^8 \approx 0.004$.

P5-13. The following shows the errors and how they are detected.



a. Detected and corrected   b. Detected

c. Detected   d. Not detected

a. In the case of one error, it can be detected and corrected because the two affected parity bits can define where the error is.

b. Two errors can definitely be detected because they affect two bits of the column parity.The receiver knows that the message is somewhat corrupted (although not where). It discards the whole message.

c. Three errors are detected because they affect two parity bits, one of the column parity and one of the row parity. The receiver knows that the message is somewhat corrupted (although not where). It discards the whole message.

d. The last case cannot be detected because none of the parity bits are affected.

P5-15. The following shows the steps:

a. We first add the numbers to get $(0002A3BE)_{16}$. This corresponds to the first loop in Figure 5.17.

b. We extract the leftmost four digits, $(0002)_{16}$, and the rightmost four digits, (A3BE)16, and add them together to simulate the second loop in Figure 5.17. The result is $(A3C0)_{16}$. We stop here because the result does not create a carry.

c. Finally, we complement the result to get the checksum as $(5C3F)_{16}$.

P5-17. The sum in this case is $(FFFF)_{16}$ and the checksum is $(0000)_{16}$. The problem shows that the checksum can be all 0s in hexadecimal. It can be all Fs in the hexadecimal only if all data items are all 0s, which makes no sense.

P5-19. Adler is a byte-oriented algorithm; data needs to be divided into bytes. For this reason, we need to represent each 16-bit data words in the problem into two bytes. The result is $(FB)_{16}$, $(FF)_{16}$, $(EF)_{16}$, and $(AA)_{16}$.

a. We calculate R and L values in each iteration of the loop and then concatenate L and R to get the checksum. All calculations are in hexadecimal and modulo 65521 or $(FFF1)_{16}$. Note that R needs to be calculated before L in each iteration ($L = L_{previous} + R$). Since the result in each iteration is smaller than $(FFF1)_{16}$, modular calculation does not show here, but we need to remember that it needs to be applied continuously.

Initial:	R = 0001	L = 0000
Iteration 1:	R = 0001 + FB = 00FC	L = 0000 + 00FC = 00FC
Iteration 2:	R = OOFC + FF = 01FB	L = 00FC + 01FB = 02F7
Iteration 3:	R = 01FB + EF = 02EA	L = 02F7 + 02EA = 05E1
Iteration 4:	R = 02EA + AA = 0394	L = 05E1 + 0394 = 0975
Checksum =	09750394	

b. The L and R values can be calculated as shown below (D_i is the corresponding bytes), which shows that L is the weighted sum of bytes.

$$R = 1 + D_1 + D_2 + D_3 + D_4 = 1 + FB + FF + EF + AA = 0394$$

$$L = 4 + 4 \times D_1 + 3 \times D_2 + 3 \times D_2 + 3 \times D_2 = 0975$$

P5-21. We recalculate a new checksum with the value of the all fields as shown below. Since the checksum is zero, there is no corruption in the header.

Fields	Decimal	Hex	Binary
4, 5, and 0	17664	4500	01000101 00000000
36	36	0024	00000000 00100100
1	1	0001	00000000 00000001
0 and 0	0	0000	00000000 00000000
4 and 17	1041	0411	00000100 00010001
65207	65207	FEB7	11111110 10110111
180.124	46204	B47C	10110100 01111100
168.110	43118	A86E	10101000 01101110
201.126	51582	C97E	11001001 01111110
145.167	37287	91A7	10010001 10100111
Result	262140	3FFFC	11 11111111 11111100
Sum	65535	FFFF	11111111 11111111
Checksum	00000	0000	00000000 00000000

P5-23. We first calculate the sum modulo 10 of all digits. We then let the check digit to be 10 − sum. In this way, when the check digit is added to the sum, the result is 0 modulo 10.

$$C = [(1 \times 9) + (3 \times 7) + (1 \times 8) + (3 \times 0) + (1 \times 0) + (3 \times 7) + (1 \times 2) + (3 \times 9) + (1 \times 6) + (3 \times 7) + (1 \times 7) + (3 \times 5)] \bmod 10 = 137 \bmod 10 = 7 \quad \rightarrow \quad C = 10 - 7 = 3$$

P5-25. The probability of success for a station is the probability that the rest of the network generates no frame during the vulnerable time. However, since the number of stations is very large, it means that the network generates no frame. In other words, we are looking for *p*[0] in the Poisson distribution.

a. For a pure Aloha network, the vulnerable time is ($2 \times T_{fr}$), which means that $\lambda = 2G$.

$$\mathbf{P\ [success\ for\ a\ frame]} = p[0] = (e^{-\lambda} \times \lambda^0) / (0!) = e^{-\lambda} = e^{-2G}$$

b. For a slotted Aloha network, the vulnerable time is (T_{fr}), which means that $\lambda = G$.

$$\mathbf{P\ [success\ for\ a\ frame]} = p[0] = (e^{-\lambda} \times \lambda^0) / (0!) = e^{-\lambda} = e^{-G}$$

P5-27. We find dS/dG for each network and set the derivative to 0 to find the value of G. We then insert the G in the expression for S to find the maximum. It can be seen that the maximum throughput is the same for each network as we discussed in the text.

a. For a pure Aloha network, $S = Ge^{-2G}$.

$$dS/dG = e^{-2G} - 2Ge^{-2G} = 0 \quad \rightarrow \quad G_{max} = 1/2$$
$$S = Ge^{-2G} \quad \rightarrow \quad \text{If } G = 1/2,\ S_{max} = (e^{-1}) / 2 \approx 0.184$$

b. For a slotted Aloha network, $S = Ge^{-G}$.

$$dS/dG = e^{-G} - Ge^{-G} = 0 \quad \rightarrow \quad G_{max} = 1$$
$$S = Ge^{-G} \quad \rightarrow \quad \text{If } G = 1,\ S_{max} = e^{-1} \approx 0.3678$$

P5-29. We found the success probability for each network type in the previous problem. If we multiply the success probability in each case by N, we have the throughput.

a. In a pure Aloha network with a limited number of stations, the throughput is

$$S = N \times P[\text{success for a particular station}] = Np\,(1 - p)^{2(N-1)}$$

b. In a slotted Aloha network with a limited number of stations, the throughput is

$$S = N \times P[\text{success for a particular station}] = Np\,(1 - p)^{(N-1)}$$

P5-31. We can first find the throughput for each station. Throughput of the network is the sum of the throughputs.

a. The throughput of each station is the probability that the station has a frame to send and other stations have no frame to send.

$$S_A = p_A\,(1-p_B)\,(1-p_C) = 0.2 \times 0.7 \times 0.6 \approx 0.084$$
$$S_B = p_B\,(1-p_A)\,(1-p_C) = 0.3 \times 0.8 \times 0.6 \approx 0.144$$
$$S_B = p_C\,(1-p_A)\,(1-p_B) = 0.4 \times 0.8 \times 0.7 \approx 0.224$$

b. The throughput of the network is the sum of the throughputs.

$$S = S_A + S_B + S_C \approx 0.452$$

P5-33. A slotted Aloha network is working with maximum throughput when $G = 1$.

a. The probability of an empty slot can be found by using the Poisson distribution when $x = 0$:

$$p[\text{empty slot}] = p[0] = (G^0\ e^{-G})/0! = e^{-1} = 0.3679$$

b. To calculate the average number of empty slots before getting a non-empty slot, we can use the Geometric distribution, which tells us that if a probability of an event is *p*, the number of experiments we need to try before getting that event is 1/*p*. The following shows that we should wait on average 2.72 slots before getting an empty slot.

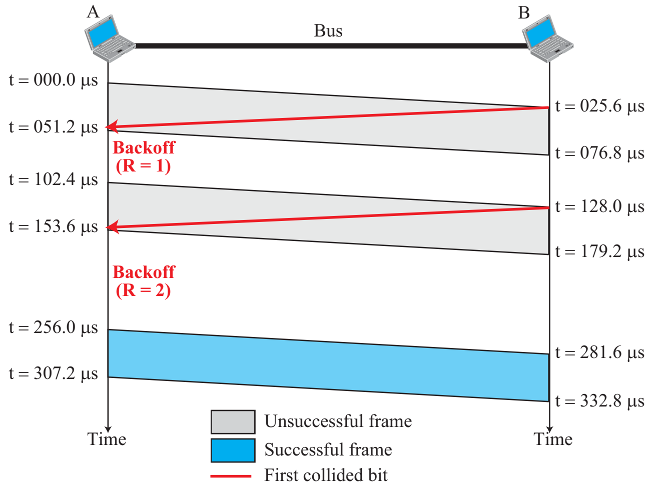
$$n = 1 / p[\text{empty slot}] \approx 2.72$$

P5-35. In the previous problem, we defined the number of bits in one meter of the medium ($n_{b/m}$ = R/V), in which R is the data rate and V is the propagation speed in the medium. If the length of the medium in meters is L_m, then $L_b = L_m \times n_{b/m}$. In this case, we have

$$n_{b/m} = R / V = (1 \times 2^8 \text{ m / s}) / (2 \times 2^8 \text{ m / s}) = 1/2 \text{ m/s}$$
$$L_b = L_m \times n_{b/m} = 200 \times (1/2) = 200 \times (1/2) = 100 \text{ bits}$$

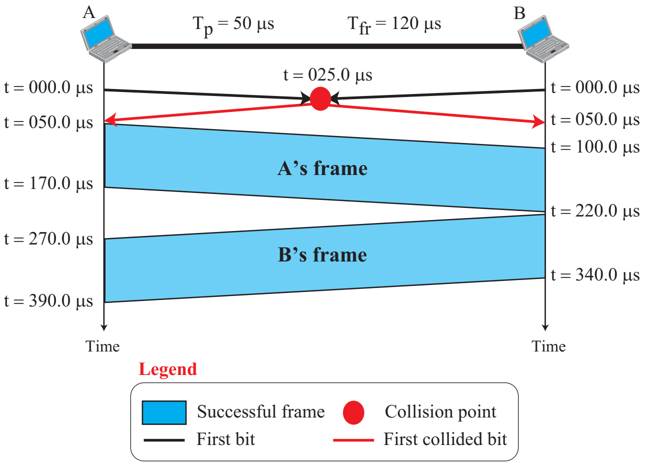
P5-37. For the sender to detect the collision, the last bit of the frame should not have left the station. This means that the transmission delay (T_{fr}) needs to be greater than 40 μs (20 μs + 20 μs) or the frame length should be at least 10 Mbps × 40 μs = 400 bits.

P5-39. See the following figure.



P5-41. Assume both stations start transmitting at t = 0 μs. The collision occurs at the middle of the bus at time t = 25 μs. Both stations hear the collision at time t = 50 μs. Station A (using R = 0) senses the medium and finds it free. It retransmits at time t = 50 μs. The frame arrives successfully. Station B (using R = 1) is scheduled to transmit at time t = 50 + 120 = 170 μs. The channel, however, is busy from t = 50 μs to t = 50 + 50 + 120 = 220 μs. This means that when station B senses the channel at t = 170, it finds it busy. It needs to continuously sense the channel. At t = 220 µs, it finds the channel free. This shows the benefit of creating a random number to make the stations schedule at different times and avoid the collision. See the next figure.

Note: Station B has scheduled to transmit at t = 170.0 µs, but it transmits at t = 220.0 µs because the channel is busy.



P5-43. The probability of a free slot is the probability that a frame, generated from any station, is successfully transmitted. We discussed this in previous problems to be $Np(1-p)^{N-1}$.

a. The probability of getting a free slot is then $P_{free} = Np(1-p)^{N-1}$.

b. As we discussed in previous problems, the maximum occurs when $p = 1/N$ and the maximum of P_{free} is 1/e.

c. The probability that the jth slot is free is the probability that previous $(j-1)$ slots were not free and the next one is free. $P_{jth} = j\ P_{free}\ (1 - P_{free})$.

d. The average number of slots that need to be passed is the average of P_{jth} when j is between 0 and infinity: $n = \Sigma\ P_{jth}$. Since P_{jth} is less than one, the series converges and the result is $n = 1/P_{free}$. The result is somewhat intuitive because, if the probability of the success for an event is P, the average number of times that the event should be repeated before getting a successful result is 1/P.

e. Since $P_{free} = 1/e$ when N is a very large number, the value $n = e$ in this case. In other words, a station needs to wait 2.7182 slots before being able to send a frame.

P5-45. The maximum efficiency in a pure Aloha network is 0.184.

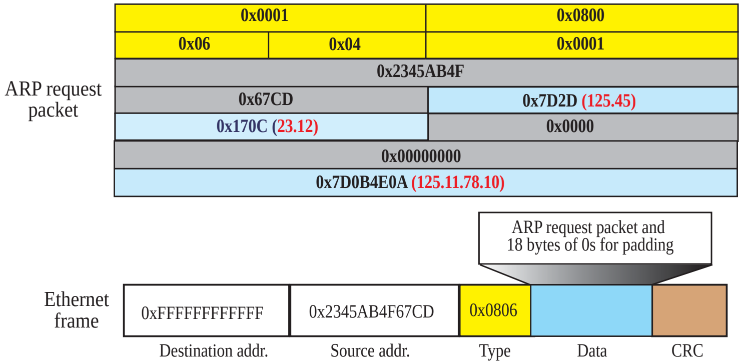
S_{max} = 0.184 × 10 Mbps = 1,840,000 bps
Maximum number of frames per second = 1,840,000 / 1000 = 1840

P5-47. We interpret each four-bit pattern as a hexadecimal digit. We then group the hexadecimal digits with a colon between the pairs:

5A:11:55:18:AA:0F

P5-49. The first byte in binary is 00000111. The least significant bit is 1. This means that the pattern defines a multicast address.

P5-51. The following shows the ARP request packet and its encapsulation in an Ethernet frame (without the preamble and SFD fields for simplicity). Note that all values are in hexadecimal. We have also shown the IP addresses in dotted-decimal notation.



P5-53. The minimum data size in the Standard Ethernet is 46 bytes. Therefore, we need to add 4 bytes of padding to the data (46 – 42 = 4)

P5-55. We can calculate the propagation time as t = (2500 m) / (200,000,000 m/s) = 12.5 µs. To get the total delay, we need to add propagation delay in the equipment (10 µs). This results in T = 22.5 µs.

P5-57. A filtering table is based on link-layer addresses; a forwarding table is based on the network-layer addresses.