1. Show the 4B/5B encoding and the resulting NRZI signal for the following bit sequence
   1110 0101 0000 0011
   Bits: 1 1 1 0 0 0 1 0 1 1 1 1 1 1 0 1 0 1 0 1
   For NRZI let L = low and H = high. For each 1 a transition is made from L to H or H to L. For each 0, there is no transition.
   LH-HL-LH-H-H H-HL-L-LH-HL LH-HL-LH-HL-L LH-H-HL-L-LH

2. Assuming a framing protocol that uses bit stuffing, show the bit sequence transmitted over the link when the frame contains the following bit sequence:
   11010111110101111101011111110

   The stuffed bits (zeros) are underlined: 1101 0111 11$\underline{0}$0 1011 111$\underline{0}$ 1010 1111 1$\underline{0}$11 0

3. Give an example of a 4-bit error that would not be detected by two dimensional parity. What is the general set of circumstances under which 4-bit errors will be undetected?
   If we flip the bits corresponding to the corners of a rectangle in the 2-D layout of the data, then all parity bits will still be correct. Furthermore, if four bits change and no error is detected, then the bad bits must form a rectangle: in order for the error to go undetected, each row and column must have no errors or exactly two errors.

4. Suppose Ethernet physical addresses are chosen at random (using true random bits).

   (a) What is the probability that on a 1024-host network, two addresses will be the same?
   The second address must be distinct from the first, the third from the first two, and so on; the probability that none of the address choices from the second to the one thousand and twenty-fourth collides with an earlier choice is

$$\begin{aligned} (1-1/2^{48})(1-2/2^{48}) &\ \ldots\ (1-1023/2^{48}) \\ \approx 1-(1+2+\ldots+1023)/2^{48} &= 1-1,047,552/(2\times 2^{48}) \\ &= 1.86\times 10^{-9} \end{aligned}$$

   (b) What is the probability that the above event will occur on one or more of 2^{20} networks?
   Probability of the above on $2^{20} \approx 1$ million tries is 1.77×10^{-3}.

   (c) What is the probability that, of the 2^{30}hosts in all the networks above, some pari has the same address? (Hint: for the first and third part, think about the birthday problem from applied probability.)
   Using the method in the first part of this question yields $(2^{30})^2/(2 \times 2^{48}) = 2^{11}$. We are clearly beyond the valid range of the approximation. Suffice it to say that a collision is essentially certain.

5. Suppose that N Ethernet stations, all trying to send at the same time, require $N/2$ slot times to sort out who transmits next. Assuming that the average packet size is 5 slot times, express the available bandwidth as a function of N.
   We alternate $N/2$ slots of wasted bandwidth with 5 slots of useful bandwidth. The useful fraction is: $5/(N/2 + 5) = 10/(N+10)$

6. How can a wireless node interfere with the communications of another node when the two nodes are separated by a distance greater than the transmission range of either node?
   This is the case in the hidden node problem, in which A interferes with Cs communication to B, and C interferes with As communication to B.

7. How can hidden terminals be detected in 802.11 wireless networks?
   802.11 uses the RTS-CTS mechanism to try to address hidden terminals. A node that has data to send begins by sending a short RTS packet indicating that it would like to send data, and the receiver responds with a CTS, which is also likely to be received by nodes that are in reach of the receiver but hidden from the sender. While this doesnt prevent collisions, the fact that RTS and CTS are short packets makes collisions less likely.

8. Having ARP table entries time out after 10 to 15 minutes is an attempt at a reasonable compromise. Describe the problems that can occur if the timeout value is too small or too large.
   If the timeout value is too small, we clutter the network with unnecessary rerequests, and halt transmission until the re-request is answered. When a hosts Ethernet address changes, e.g. because of a card replacement, then that host is unreachable to others that still have the old Ethernet address in their ARP cache. 10-15 minutes is a plausible minimal amount of time required to shut down a host, swap its Ethernet card, and reboot. While self-ARP (described in the following exercise) is arguably a better solution to the problem of a too-long ARP timeout, coupled with having other hosts update their caches whenever they see an ARP query from a host already in the cache, these features were not always universally implemented. A reasonable upper bound on the ARP cache timeout is thus necessary as a backup.

9. IP currently uses 32 bit addresses. If we could redesign IP to use the 6-byte MAC address instead of the 32 bit address, would we be able to eliminate the need for ARP? Explain why or why not.
   The answer is maybe, in theory, but the practical consequences rule it out. A MAC address is statically assigned to each hardware interface. ARP mapping enables indirection from IP addresses to the hardware MAC addresses. This allows IP addresses to be dynamically reallocated when the hardware moves to the different network, e.g. when a mobile wireless device moves to a new access network. So using MAC addresses as IP addresses would mean that we would have to use static IP addresses.

   Since the Internet routing takes advantage of address space hierarchy (use higher bits for network addresses and lower bits for host addresses), if we would have to use static IP addresses, the routing would be much less efficient. Therefore this design is practically not feasible.

10. Suppose hosts A and B have been assigned the same IP addresses on the same Ethernet, on which ARP is used. B starts up after A. What will happen to A's existing connections? Explain how "self-ARP" (querying the network on start-up for one's own IP address) might help with this problem.

    After B broadcasts any ARP query, all stations that had been sending to As physical address will switch to sending to Bs. A will see a sudden halt to all arriving traffic.

(To guard against this, A might monitor for ARP broadcasts purportedly coming from itself; A might even immediately follow such broadcasts with its own ARP broadcast in order to return its traffic to itself. It is not clear, however, how often this is done.)

If B uses self-ARP on startup, it will receive a reply indicating that its IP address is already in use, which is a clear indication that B should not continue on the network until the issue is resolved.