Indian Institute of Technology Bombay

Department of Electrical Engineering

Handout 32 EE 706 Communication Networks

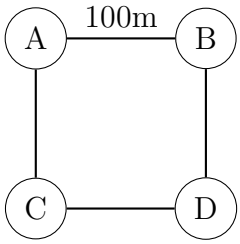
Solutions to Assignment 7 April 19th, 2010

---

1. Consider a four-node wireless network consisting of nodes A, B, C, and D situated on the four corners of a square with side of length 100 m. Each node has a transmission range of 101 m. Assume that all the nodes use the same frequency band to transmit their signals, i.e. a collision occurs if two nodes transmit to the same destination which is in their transmission range. [10 points]

   (a) Give an example of the hidden node problem which arises in this network. How does the RTS-CTS mechanism solve this problem?

   Ans. Since the transmission range of a node is 101 m, it can reach its adjacent nodes but not the diagnolly opposite node. For instance, node A can reach nodes B and C but not node D.



   Suppose A is transmitting to B. This transmission is not heard by D and it may transmit to B thinking that the channel is idle resulting in a collision at B. Thus A is a hidden node with respect to D.

   Suppose the RTS-CTS mechanism is used. Then A sends an RTS to B and B responds with a CTS. The RTS is not heard by D but the CTS is heard by it. So it infers that a hidden node wants to transmit to B and abstains from transmitting to B until it hears an ACK from B acknowledging the frame sent by A.

   (b) Give an example of the exposed node problem which arises in this network. How does the RTS-CTS mechanism solve this problem?

   Ans. Suppose A is transmitting to B and C wants to transmit to D. Since the transmissions from A and C do not reach D and B respectively, these transmissions can potentially happen concurrently. But when C hears A's transmission to B it infers that the channel is busy and abstains from transmitting to D. Thus C is an exposed node in this scenario.

   If the RTS-CTS mechanism is used, C hears the RTS sent from A to B but not the CTS from B to A. Now C can infer that it is out of the transmission range of B. In this specific scenario where all the transmission ranges of the nodes are equal, C can infer that B is also out of its own transmission range and proceed to transmit to D. But this may not be true in general. For example,

if the transmission range of B remains 101 m but the transmission range of C increases to 150 m then the transmission from C to D will cause a collision at B. Now if C sends a RTS to D, it will not get a response because node D has heard the CTS from B to A and knows that it may interfere with the transmission from A to B if it sends a CTS to C. So the RTS-CTS mechanism does not always solve the exposed node problem.

2. The following frames (including the preamble) are observed by a receiving node which is connected to a Ethernet-based LAN. They are shown here in hexadecimal format.

[10 points]

- AAAA AAAA AAAA AAAA FFFF FFFF FFFF 000D 8845 595C 0800 ....
- AAAA AAAA AAAA AAAB 0018 181C 90C1 001C C0AF AD1A 05DC ....
- AAAA AAAA AAAA AAAA 0018 181C 90C1 001C C0AF AD1A 08DD ....
- AAAA AAAA AAAA AAAB 0018 181C 90C1 001C C0AF AD1A 05D0 ....

For each frame, give the following information.

(a) Is the frame format 802.3 Ethernet or DIX Ethernet?

Ans. The first and third frames are DIX Ethernet frames while the second and fourth are 802.3 Ethernet frames.

(b) What are the source and destination MAC addresses in the frame?

Ans. In both 802.3 Ethernet and DIX Ethernet, the first 48 bits following the 64-bit preamble constitute the destination MAC address and the second 48 bits constitute the source MAC address.

(c) Can you decipher the manufacturer of the destination network card for each frame?

Ans. The manufacturer of the destination network card cannot be deciphered in the case of the first frame because the destination MAC address is a broadcast address (all 1s). In the other three frames, the destination MAC address is a unicast address and the first 24 bits in it can be used to identify the manufacturer.

(d) What do the last 2 bytes (which are shown) mean for each frame? Give answers specific to the value of the 2 bytes in each case.

Ans. For the first and third frames which are DIX Ethernet frames, the last two bytes shown represent the network layer protocol to which the frame will be passed on to. For the first frame it is IPv4. For the third frame, there is a typo. It should have been 86DD instead of 08DD. The two bytes 86DD correspond to IPv6.

3. In binary exponential backoff, the nodes involved in the nth collision randomly wait for $0, 1, 2, \ldots, 2^n - 1$ slots before transmitting. So each node involved in the nth collision generates a random number in the set $\{0, 1, 2, \ldots, 2^n - 1\}$. Suppose three nodes A, B and C are involved in collisions and generate the following random numbers to resolve their collision

- A: 0, 2, 1
- B: 0, 2, 5, 2
- C: 0, 2, 5, 9

If the first collision occurs at time $t = 0$ and the slot size is one second, when does the successful transmission for each node complete? [5 points]

Ans. Solved in the last class (Lecture 38). For simplicity, in this question it was assumed that the contention slot and the frame transmission duration are the same. In reality, the contention slot is taken to be the worst case round-trip time (which is 51.2 μs for Ethernet) and the frame transmission duration can be larger than that. Every node transmits a regular frame after a certain number of contention slots but aborts the transmission within a RTT once it hears a collision. If there is no collision, the node continues to transmit its regular frame and effectively "captures" the channel because other nodes sense the channel to be busy in subsequent contention slots.

4. A hypothetical CSMA/CD system has four copper twisted-pair segments connected together by three repeaters. Each segment is 400 metres long. The one-way processing delay at a repeater is 10 microseconds. We wish to operate this system at 10 megabits per second. If the speed of the signal in copper is 2 $\times 10^8$ metres per second, what is the minimum size of the frame in such a system which will ensure that a collision never goes undetected? [5 points]

   Ans. In a CSMA/CD system, a node listens to the channel only when it is transmitting. To always detect a collision it must listen for at least a round-trip time after it starts transmitting. So the minimum size of the frame should be such that the node transmits for the maximum round-trip time.

   The signal takes 2 microseconds to travel through each segment and since each repeater introduces a delay of 10 microseconds, the maximum propagation delay is 38 microseconds. So the maximum round-trip time is 76 microseconds. Since the data rate is 10 Mbps, in order for the frame transmission to last one round-trip time the size of the frame should be at least 10 Mbps $\times$ 76 microseconds which is equal to 760 bits.

5. Suppose an IPv4 packet arrives at a router which is not capable of fragmentation, what are the fields in the IPv4 header which the router can possibly change? If the router is capable of performing fragmentation what are the fields which can possibly be changed? [5 points]

   Ans. When an IPv4 packet arrives at a router, its TTL field is decremented and the checksum if recalculated to account for the changed TTL field. If IPv4 options are used, then the router may insert its own IP address in the variable length options field if the *Record Route* option is enabled or it may insert a timestamp if the *Timestamp* option is enabled. Of course, IP checksum recalculation must be done after all such changes are made. These are the only fields which change if the router is not capable of doing fragmentation.

   If the router is capable of fragmentation, it can also change the Length field, the MF bit in the Flags field and the Offset field.

6. Calculate the Internet checksum of the following bits which are given in hexadecimal format: FFABBCD0 0010EE99 AAAA0000 0000CCDD [5 points]

   Ans. In order to calculate the Internet checksum, group the bits into 16-bit groups, perform one's complement addition and take the bitwise complement of the sum. Taking bitwise complement of 22AF gives DD50 as the checksum.

	11001100	11011101	(CCDD)
	00000000	00000000	(0000)
	00000000	00000000	(0000)
	10101010	10101010	(AAAA)
	11101110	10011001	(EE99)
	00000000	00010000	(0010)
	10111100	11010000	(BCD0)
	11111111	10101011	(FFAB)
100	00100010	10101011	(22AB)
		100	Adding carry bits
	00100010	10101111	(22AF)

7. Suppose a 1520 byte IPv4 datagram which has 1500 bytes of data and 20 bytes of header arrives at a router. It needs to be forwarded along a link which has an MTU of 500 bytes. So the router decides to do fragmentation. Write down the number fragments sent, the number of bytes in each fragment, the specific bytes contained in each fragment (assuming the original data bytes are numbered 1 to 1500), the value of the IPv4 offset field in each fragment's header, and the value of the IPv4 MF flag in each fragment's header. [5 points]

   Ans. If the MTU is 500 bytes, a maximum of 480 bytes of data can be included in the IPv4 fragment. So four fragments will be needed.

Fragment No.	No. of Data Bytes	Bytes	Offset	MF Flag
1	480	1 to 480	0	1
2	480	481 to 960	$\frac{480}{8} = 60$	1
3	480	961 to 1440	$\frac{960}{8} = 120$	1
4	60	1441 to 1500	$\frac{1440}{8} = 180$	0

8. Generate subnetwork addresses and subnet masks to divide a single class C address 192.83.12/24 among four physical networks with 50 hosts each. [5 points]

   Ans. The subnetwork addresses and masks are the following. Each subnetwork can accommodate 62 hosts after we disregard the all zeros and all ones addresses in the host portion which are reserved.

   - 192.83.12.0/26
   - 192.83.12.64/26
   - 192.83.12.128/26
   - 192.83.12.192/26