Homework 3 Solutions

Problem 1.a)

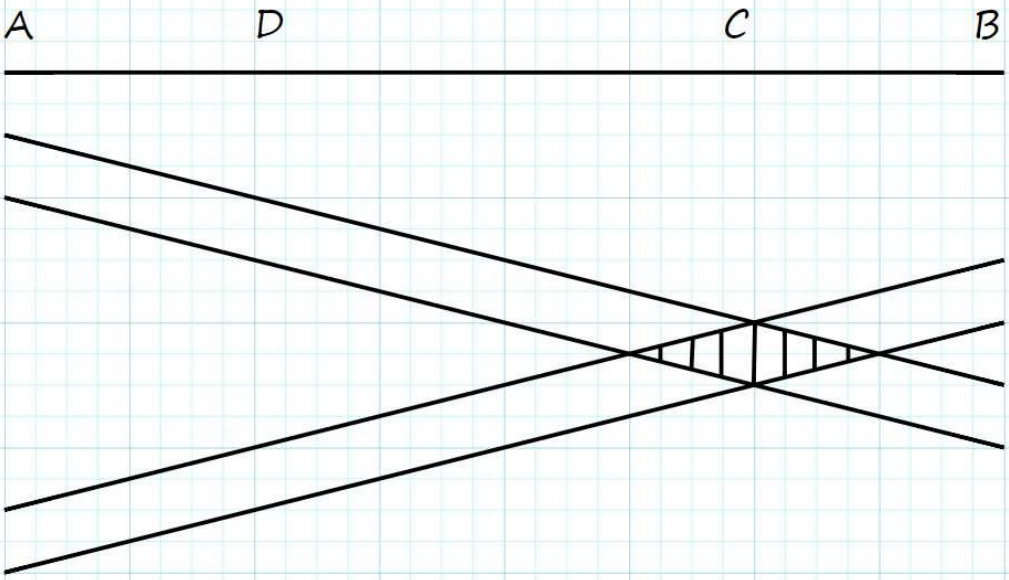
a)Since Nethernet removes the minimum packet size condition then we can eliminate padding

Problem 1.b)

b)No, this rule is no longer valid. Since we are allowing a sender to send a packet without a minimum size criteria, the receiver should not discard a packet less than 64 bytes

Problem 1. c)

c)Consider the following scenario (A send to B and B sends to A)



We need the old mechanism because in this example node C would not detect the collision without the old mechanism

Problem 1.d)

d) Using the same diagram, node D will not be able to detect any collision as it is not transmitting and will not wait for 51.2 microseconds not will there be an increase in voltage

Problem 1.e)

e)If node D is the receiver(i.e. A sends a packet to D in the above example) D will receive the packet correctly as it does not detect collision. A will detect a collision and will retransmit. D will accept the packet again, causing duplicates

Problem 2.a)

B1 learns that packets addressed to V should be forwarded "up" to LAN 1

B2 learns that packets addressed to v should be forwarded "up" to LAN 2

The initial packet should go to every LAN (1,2,3). This is because of the flooding that occurs since the bridges are initially empty

Problem 2.b)

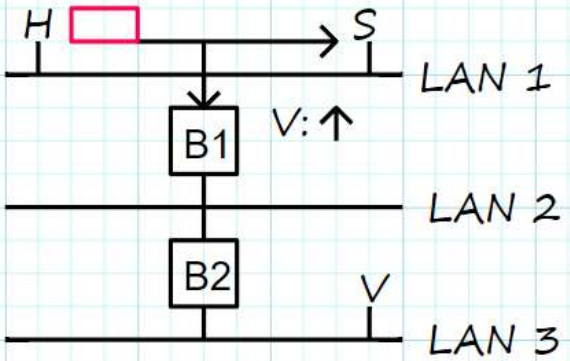
No, the packet will not go to the real victim. This is because B1 now believes that V is located on LAN 1

H will listen in on any packet on LAN 1, so all H must do to accept this packet is accept any packet whose MAC address is V's address

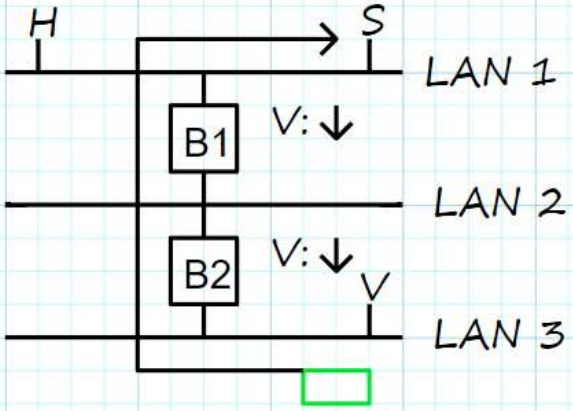
Problem 2.c)

The following sequence of events must occur

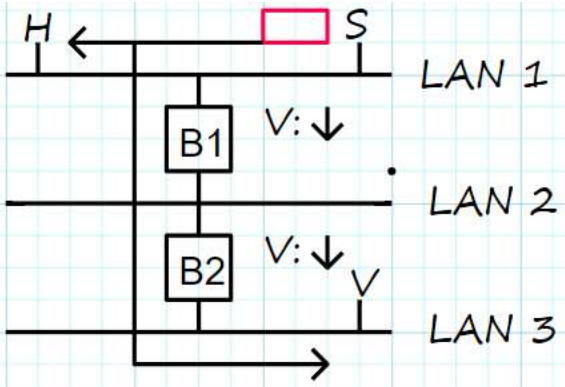
Step 1: H will send a false request to S, causing B1 to refresh it's knowledge that V is up



Step 2: V will send a real request to S, causing B1 and B2 to learn that V is on LAN 2 and 3 respectively. This must occur before S has a chance to reply to H



Step 3: S will send a reply to the false request sent by H. This reply will also reach the real victim V, at which point V will be aware of the hack.



Just the packet Sequence:
1) H sends request to S
2) V sends request to S
3) S sends reply to H

The details for all the points
1) H sends request to S
2) B1 relearns V is on LAN1
3) V sends request to S
4) B2 learns V is on LAN3
5) B1 learns V is on LAN2
6) S sends reply to H
7) V receives S's hacked reply because of 4 and 5

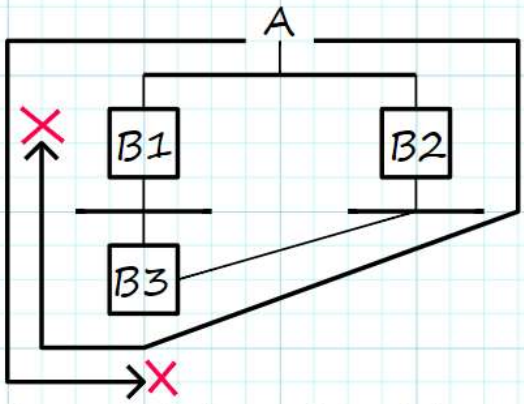
Problem 2.d)

A bridge could maintain statistics on the rate of change for every entry in its forwarding table. If the rate of change is too quick then the bridge will report the problem

The bridge could send a message either to the victim or directly to system admins to report the problem.
If bridge capabilities are minimal, the bridge could "report" the problem by simply flooding hacked messages so that victims could report the problem themselves

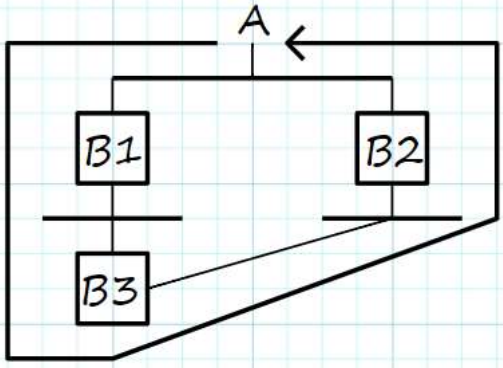
Problem 3.a)

a)Not only should you forward based on destination, you should also NOT forward based on source.
For example, in the drawing the packet would reach B1 and B2 and they would both learn that A is up. Assume the packet reaches B3 from the right first so that B3 learns A is to the right. When the packet reaches B3 from above, it would not be forwarded to the right since the packets source is A and B3 believes A is to the right. Similarly, the packet would not be forward up when it reaches B1 from below, thus preventing loops



Problem 3.b)

b)If the clockwise packet is lost before reaching B2, then the counter clockwise copy will reach B1, B3, and B2 in that order This would create a one-way loop. Furthermore, B2 now believes A is down which would cause it to drop packets from A



Problem 4

(a) Case 1: There is a bridge between the two LANs: (your solution is correct)

Endnode D will do ARP once it find it does not have the destination data-link address in its cache. Endnode A replies with the wrong datalink address of all 1's address. Endnode D then caches this address. Afterwards, whenever endnode D wants to send a packet to endnode A, it will end up broadcasting the packet, causing every endnode on the LAN to receive it. All the other endnodes see that the destination IP address (which is that of A) does not belong to them, but is within the same local network, so they forward the packet within the LAN. However, since every endnode except A and D is forwarding, and all of them do not have the correct IP address, they will forward again once they receive it from another endnode. This will be repeated for all the endnodes, causing a broadcast storm.

Case 2: There is a router between the two LANs: (there are some subtle differences)

The First, if there is a router we assume that the upper LAN has a separate prefix say P1 (so D and E have IP addresses starting with P1) abd the lower LAN has a separate prefix P2 (so A, B, and C have IP addresses starting with P2). So when D wants to talk to A, it first realizes that the prefix of A does not match its own prefix P1, so it decides to send to the router which it has been configured with by say DHCP. D does an ARP for the router (say R) and gets the router MAC address and then sends the frame to A to the router. When router R gets the packet, it realizes it matches the prefix of the lower LAN. Assume R does not have the MAC address of A. Now things get similar to your solution except that R does the ARP that causes the broadcast.

R will do ARP once it find it does not have the destination data-link address in its cache. Endnode A replies with the wrong datalink address of all 1's address. R then caches this address. Afterwards, whenever endnode D wants to send a packet to endnode A, it will end up broadcasting the packet, causing every endnode on the lower LAN to receive it. All the other endnodes see that the destination IP address (which is that of A) does not belong to them, but is within the same local network, sothey forward the packet within the LAN. However, since every endnode except A and R is forwarding, and all of them do not have the correct IP address, hey will forward again once they receive it from another endnode. This will be repeated for all the endnodes, causing a broadcast storm which increases exponentially.

(b) The router will isolate the storm. So before we replace it, there are total $(T-1)^x$ transmission for possibly infinite iteration of x. After the replacement, there are total $(M-1)^x$ transmission. And from the question we know that $T \gg M$, so that's why router did better than bridge.