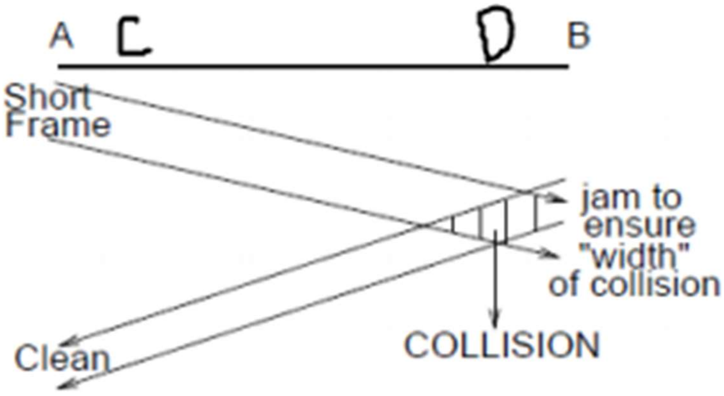
Everett Sheu

704796167

CS 118 – HW #3

1.

a. Because Nethernet no longer requires a minimum packet size, we can remove padding from the original Ethernet protocol.
b. No, because we no longer have a minimum packet size, receivers should not discard "runt packets" because these can now be valid transmissions.
c.

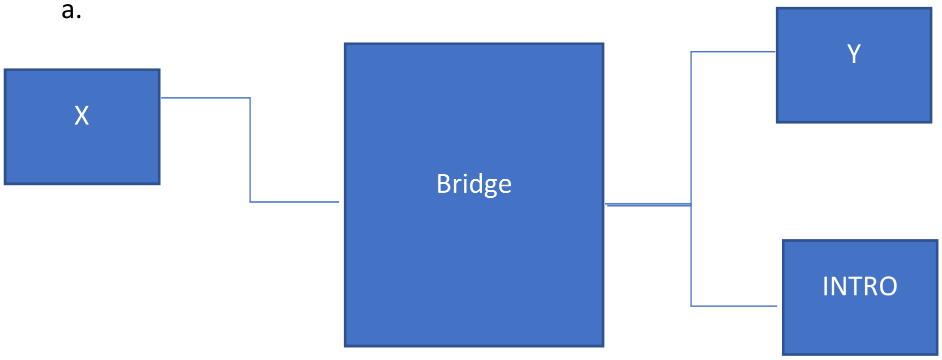


If A were to send a small packet to B and B, just before receiving A's packet, sends his own small packet, D would require the old mechanism to detect the collision as an increase in voltage.

d. Using the same figure as in c), node C will never detect that a collision has occurred in the network because it is not transmitting and will therefore not be waiting the 51.2 usec for collision detection and has no way of seeing the increase in voltage that D is able to.
e. Using the same figure as in c), imagine that node A were to send a small packet to node C and in the 51.2 usec window, B also transmits a packet. C would receive the packet undisturbed. However, because A detects B's packet in the collision detection window, it detects a collision and will retransmit its packet. When it does, C will again accept the packet, resulting in duplicate received packets.

2.

a.



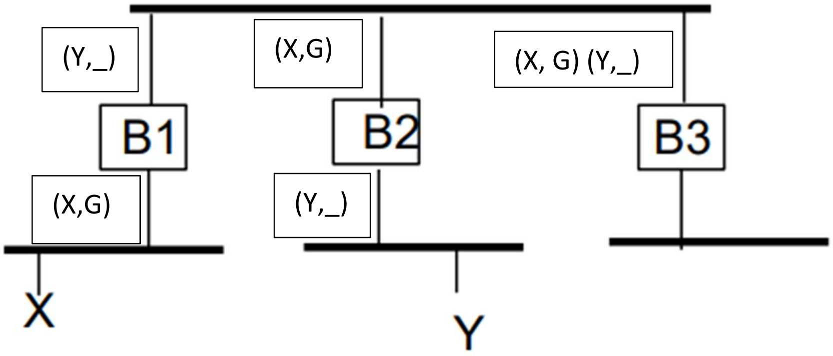
Using this figure as an example, suppose X wants to transmit to Y. He will send a LAN frame to INTRO, where the frame uses X as the source address. In doing this, the Bridge will record that X is on the left side. When INTRO forwards the message to Y, the frame will still have X as the source address. This will cause the bridge to recognize X as having transmitted from the right side and will record that X is on the right side rather than on the left, where he really is.

b. This introduction protocol can easily be fixed by having INTRO send a frame back to X with Y in the data field and INTRO's address as the source address. This way, X can directly message Y.

3.

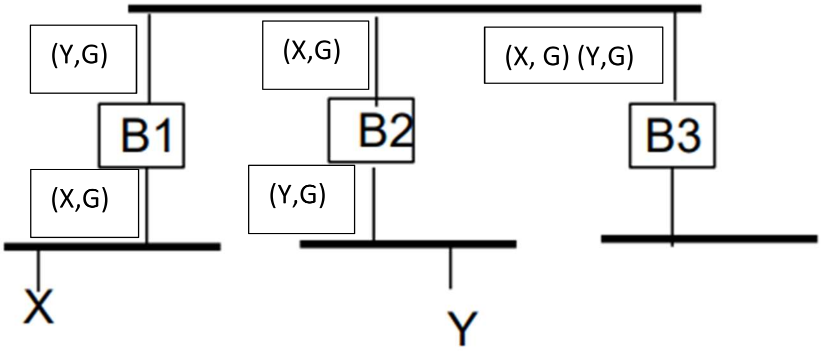
a. Instead of having a port map that stores only stations, the bridge should also store another variable that identifies which, if any, group that the station also belongs in. Thus, the station to port map would become a (station, group) tuple to port map. The bridge would behave as usual for normal messages, but when it recognizes that it has received a multicast message, it should forward the message to all stations that share the group.

b. Suppose that all the bridges have the locations of X and Y. The following picture would show what each bridge knows.



When X multicasts within the group, the bridges will only forward the packet if they find that they have a station in group G on the other end. In this case, the multicast will not extend beyond B1.

Then, assume that Y joins the group G. The bridges will update their port maps to the following:



Now, multicast packets sent to “All Bridges Address” will be forwarded along both B1 and B2 to X and Y. Thus, if any bridge were to receive a multicast packet for group G, it would send it to all ports with G as the second element in the tuple.

c. After a certain amount of time without receiving an “All Bridge Address” multicast to group G from source address Y, the bridges should drop Y from the group G. They should do this by taking out “G” from the second element in the tuple. This timeout period should consider the reliability of the network. If the network is known to be unreliable and often has dropped packets, it should wait a longer timeout before Y should be dropped from the multicast group G.

d. If a bridge gets a multicast address that it has no learnt information about, it should do the following:
   1.) Cache the address to its table. This keeps track of ports that the bridge should forward packets to.
   2.) Send the message to the rest of the bridges. This allows for the rest of the bridges in the network to update their tables.

4.

a. Because B does not have A’s data link address, it will send an ARP request for A’s data link address. A will respond to the ARP request with its incorrectly configured address of all 1’s. Packets that will try to send to A will be sent with all 1’s as the destination link address. Because this is the multicast address as well, all stations will receive the packets. Realizing that the packet is not meant for them, other stations will perform an ARP request to find A and will get back that A has a destination address of all 1’s and transmit the message to that address. This causes an indefinite loop of redirected multicasted messages.
b. If the bridge is replaced by an IP router, the problem “gets better” in that the broadcast storm becomes localized only on the LAN that contains A.