UCLA CS 118 Computer Networks

Homework 3

Due: Nov 16th

Directions: Some of the problems appear long but they are not too hard when you understand them so it will really help if you try them sincerely by yourself. Each problem is meant to teach you something. They are all past exam questions. We will pick 1 out of the 4 problems to grade. Since its appearing on Monday night, it will only be due by **next Tuesday, Nov 16, at midnight** but start early as you also need to start Project 2. Just one more HW, a final and Project 2: so, hang in there!

1. **Ethernet, Min Packet Sizes, and Semi-Reliability**: At Interop 2017, a leading trade show, two members of the 2017 cs118 class have unveiled their new version of the Ethernet. Their product, Nethernet, is identical to standard Ethernet except that it no longer requires a minimum packet size. Recall Figure 1 below that we used to justify the minimum packet size. The problem is that if *A* and *B* sent small frames, they might collide in the middle of the wire and yet neither *A* nor *B* would detect the collision. To fix the problem, Nethernet adds the following rule: if a station like *A* sends a short packet of size less than 64 bytes, *A must* wait for at least 51.2 usec after its first bit is sent; if *A* detects any transmission during this period, *A detect* a collision, and does the usual retransmission.

-a) If Nethernet requires no min packet size, what additional features of the normal Ethernet protocol can be removed as well?

-b) Receivers normally discard runt packets of size less than 64 bytes in normal Ethernet. Is this rule still valid for Nethernet? Explain.

-c) Nethernet also requires the normal means of detecting collisions (i.e., more than one signal at the same point is detected by an increase in voltage) in addition to this new mechanism. Explain with an example why this is still needed so that all stations can detect a collision.

-d) Suppose we use the mechanism in c) (detection via increased voltage) as well as the new Nethernet mechanism to detect collisions. Show using an example that it is still possible for some station to not detect collisions.

-e) Use the results of b) and d) to show that Nethernet collisions can result in duplicate packets being received by a receiver.

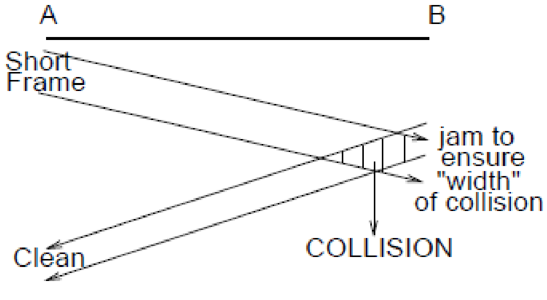
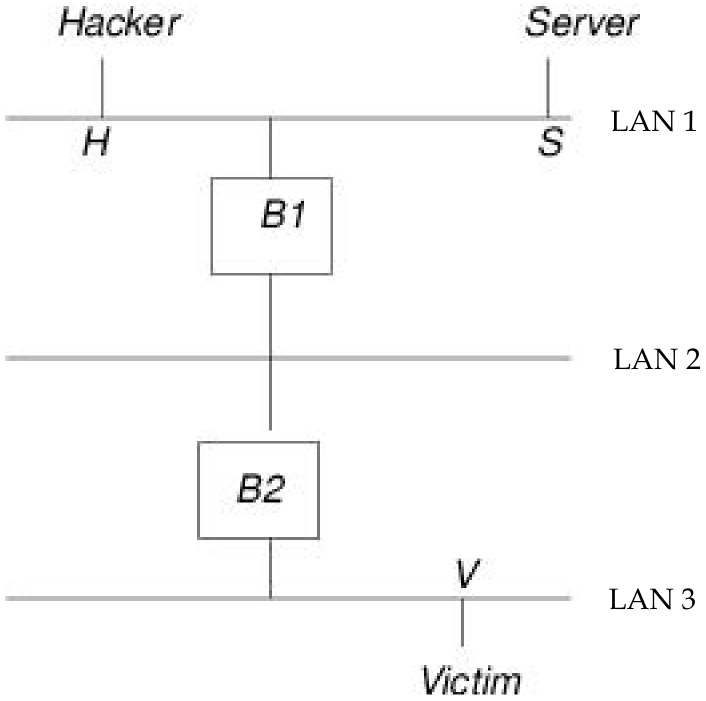


Figure 1:

Do not forget that when A is sending the receiver need not be B. It could be any station C that is anywhere on the Ethernet to cause problems.

2. **Hacking Bridges**: Bridge learning can be affected by wrong (or hacked) behavior of stations. In the figure below assume that a hacker with MAC address H wishes to impersonate a victim with MAC address V when talking to a server with MAC address S. **Assume all bridge tables are initially empty.**



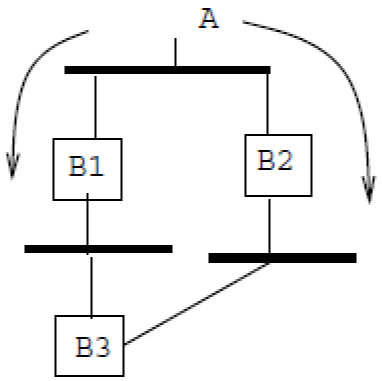
- Suppose H starts by sending an Ethernet packet to S with a forged MAC source address V. What do the bridges learn? Which LANs does this packet go to?

- When S replies to V will the packet go to the real victim? What must H do to pick up the packet?

- Assume that if the real victim V ever gets an unsolicited packet from S, it will send a RESET packet to S that will stop the cozy communication that H is having with S. Describe a scenario (i.e., the sending of some packets) that causes a packet from S to reach the real victim, spoiling the hacker's efforts. Assume that S keeps sending so the bridges never time out their entry for V. Describe the events carefully for more points

- What could a bridge do to detect and report possible attacks such as this?

3. **Bridging and Loops**: Even the Spanning Tree algorithm cannot prevent temporary loops (for example if two separate LANs are connected by a bridge, and then someone plugs together two separate LANs using a repeater). Eventually, the loop will be broken, and the right bridges will turn off, but packets can circulate at very high speeds till the loop is broken.



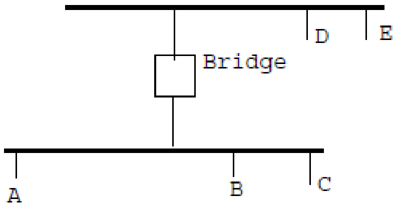
Alyssa P. Hacker has thought of a way to improve the situation during temporary loops. Consider a temporary loop of bridges shown above and assume that bridges B1, B2, and B3 all think they are ON. Suppose A sends a multicast packet. Both B1 and B2 pick up the packet, and so the packet will circulate in *two* directions, both clockwise and anti-clockwise. This will also happen if the destination is unknown.

a) Based on Alyssa's observation, how could you modify the bridge learning and forwarding to prevent multicast and unknown destination packets from circulating continuously in a temporary loop?

b) Alyssa's method is sound if there is no packet loss. What goes wrong with her method if packets can be dropped?

4. IP Broadcast Storms, Bridges versus Routers: (Adapted from Perlman's book) A broadcast storm is an event that causes a flurry of messages. One implementation that caused broadcast storms was the Berkeley UNIX endnode IP implementation. In this implementation, an endnode attempts to forward a packet that it mysteriously receives with a network layer (IP) address that is different from itself. This is what you would do if you found a neighbor's letter wrongly placed in your mailbox. However, this seemingly helpful policy can cause problems.

Consider the figure below which shows 2 LANs connected by a bridge, with several IP endnodes on each LAN. There are no IP routers. All IP endnodes are configured with the same mask and so can tell that they have the same net number/prefix. Suppose IP endnode A is incorrectly configured and incorrectly thinks its data link address is all 1's. The data link address of all 1's is the broadcast address: any packet sent to such an address is received by all stations on a LAN (it is the ultimate multicast address!).



a) What happens when another IP endnode B decides to send a packet to IP endnode A? Assume that B initially does not have A's data link address in its cache, and so must do the ARP protocol. Give the sequence of events.

b) Suppose the bridge is replaced by an IP router. (Of course, the masks at the nodes must be changed so that there are now two masks, one for each LAN. Note a mask is just a bitmap of 1's in the most significant bits that tells you how long the prefix for that subnet is) The problem does not disappear, but it does get a little better. Explain.