UCSD CSE CS 123 | Computer Networks

Exam Review

Directions: Write your name on the exam. Write something for every question. You will get some points if you attempt a solution but nothing for a blank sheet of paper. Problems take long to read but can be answered concisely.

Question	Maximum	Score
1	40	
2	20	
3	20	
4	20	
Total	100	

1, Fundamentals, 40 points total, 4 points each: Give short 1 line answers for each question. If you are asked to give a reason for something, give the most important reason you can think of.

- **Fast Ethernet:** Why Fast Ethernet (which runs at 100 Mbps) has a smaller distance limit (0.15 km) than Ethernet. (Otherwise, Fast Ethernet and Ethernet are very similar.)

- **Bridges versus Routers:** Why its a good idea for bridges to be able to process packets at LAN rates while it is OK for routers to process packets at much slower rates.

- **Hierarchical Addressing:** Why a medium size organization (like Wash U) that is given a Class B address often divides the address space

- **NAPs:** Why NAPs (Network Access points) are essential to a multiprovider Internet.

- **Redirect:** There were once two routers $R1$ and $R2$ on a LAN. For some reason, one of the routers, say $R1$ was upgraded to use buggy software which did not send a Redirect message even when it should have. Traffic on the LAN doubled as a result. Describe in 1 line why this may have happened.

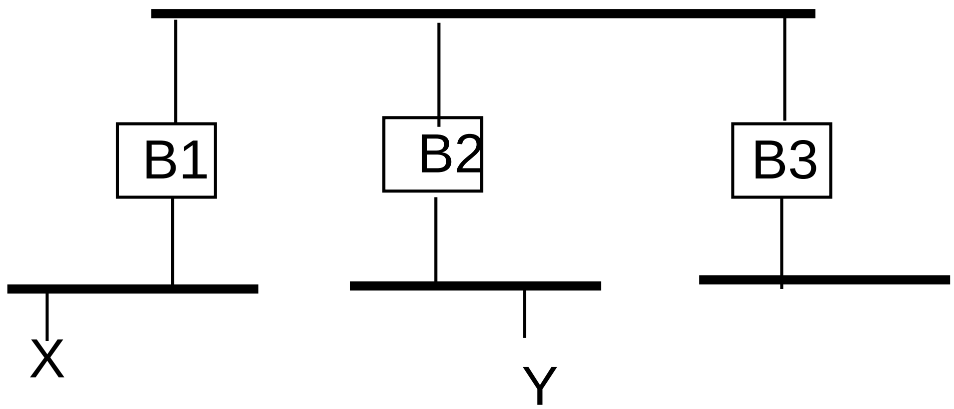
- **Router Forwarding:** Why a router can get away with around 100,000 entries in its forwarding table today though there are millions (if not billions) of assigned IP addresses.

- **Link State Routing:** Why Link State routing is prefered to Distance Vector routing in many ISPs.

- **Distance Vector Routing:** Why when you try to access a web page you sometimes get a message that says "Connection Timed Out" and it takes a long time, while you sometimes get a message that immediately says "Destination Unreachable".

- **Protocol Pragmatics:** Why most protocol headers start with a version number.

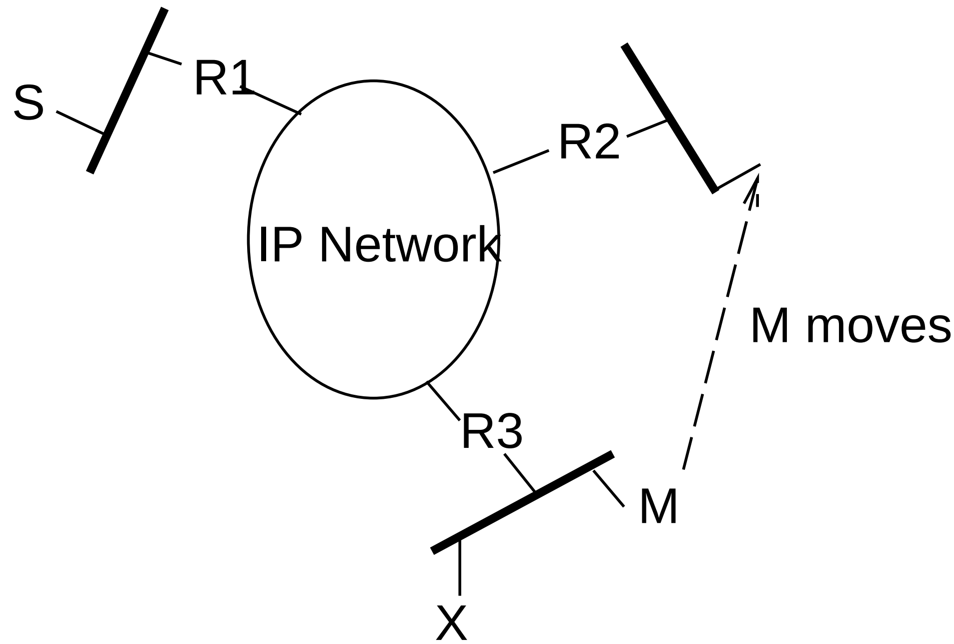
2. Bridging and Pruned Multicast, 20 points: In class, we learnt about IP multicasting and how the multicast trees were "pruned" so that copies of multicast packets were not sent to LANs in which no station was listening to that multicast. We want to offer a similar "pruned multicast" service for Extended LANs by modifying bridges and endnodes slightly. The figure shows two stations X and Y. Assume that initially only X is in group G (G is a multicast data link address). Then when X sends a multicast packet to G bridge $B1$ should (ideally) not forward the packet. Later, assume that Y also joins group G. All bridges should learn this fact. Now when X sends a packet to G, bridge $B1$ should forward the packet on the upper LAN, bridge $B2$ should pick up the packet and forward it to Y's LAN, and bridge $B3$ should not forward the packet.



Thus bridges need to learn all the directions through which a multicast address like G is reachable. To allow bridges to learn, we modify the endnodes that participate in a group G to periodically send a multicast packet to some "All Bridges Address". However, the endnodes put G as the *source address* in such a packet.

- How would you modify the bridge learning algorithm to learn about multicast addresses like G based on the periodic updates sent by the endnodes participating in the group? Describe the new learning algorithm in a few lines. (5 points)
- Explain what each bridge learns in the above example. Assume that initially only X sends updates and show what each bridge learns using a picture. Then show what happens when Y joins the group and begins sending updates using a second picture. (8 points)
- Suppose that Y crashes and stops sending updates. X continues to send updates. Explain precisely how bridges should timeout information asssociated with multicast addresses. (4 points)
- Not all stations participate in this protocol. What should a bridge do when it gets a multicast address that it has no learnt information about? (3 points)

3. Mobility and Routing, 20 points: We now consider the problem of routing to a mobile station that has moved. In the figure below, assume that mobile station M is "homed" (i.e., normally resides) on the LAN that contains $R3$ and X. M has an IP address that contains the prefix corresponding to its home LAN. Sometime later, M moves to the LAN that contains $R2$. Stations S and X may still send packets to M at the old address, even after M has moved. We want to explore how to modify IP routing so that these packets can be delivered to M at its new location.



Lets assume that M (before or after moving) tells its home router $R3$ of the prefix of its new LAN. We assume that M does not get a new host ID at its new LAN because it would take too long to have one assigned. Assume that M has a unique Data Link ID (e.g., Ethernet address) D_M that it carries to the new LAN. Now answer the following 5 questions for 4 points apiece.

- Assume X wants to speak to M. Since it thinks its on the same LAN as M, X may send an ARP for M on the LAN containing X and M. But M has moved. What should router $R3$ do in response?

- Suppose that $R3$ has a packet destined for M that was sent by either S or X. How does $R3$ send the packet to M?

- Assume that the packet for M gets to $R2$. How does $R2$ deliver the packet to M (remember that $R2$ cannot do an ARP because M does not have an IP address with a prefix corresponding to the new LAN. However, you can add info to the packet that can help $R2$.)

- The indirect route can result in sending a large number of extra packets when S is speaking to M. Can you suggest some way of eventually avoiding the indirect route so S can directly send to M in its new location?

- When M eventually moves back to its home LAN, how do you ensure that eventually everyone sends packets to M's home LAN?

4. LSP Propagation, 10 points: There is a subtlety about LSP propagation that we briefly discussed in class. The problem is that after crashes we can sometimes get two LSPs from the same source with the same sequence number and different data. In reality and in the textbook, this is solved by zero age flooding. In this problem, we consider a slightly different approach to solving the problem. As in the HW, please ignore age fields as mentioned in the text.

In the figure below we will concentrate on LSPs sent by router $R1$. Suppose when the network comes up, $R1$ sends its first LSP with sequence number 0 and listing its neighbors as router $R2$ and endnode E. Suppose $R2$ and $R3$ both receive this LSP. Next, $R1$ and E crash and $R1$ comes up (but E does not come up). Thus, $R1$ sends a LSP with sequence number 0 again but listing only $R2$ as its neighbor.

1. (5 points) Does $R1$'s new LSP eventually propagate to the other routers? Does the source jump mechanism help in this case?

2. (5 points) To solve this problem, we can have every LSP carry a checksum along with the sequence number. Two LSPs that have the same sequence number and different checksums are judged to be different. A router that finds that the received LSP has the same sequence number as its stored LSP but has different data, will increment the sequence number in the LSP and send it to all neighbors. Explain how this modification solves the problem above with high probability.

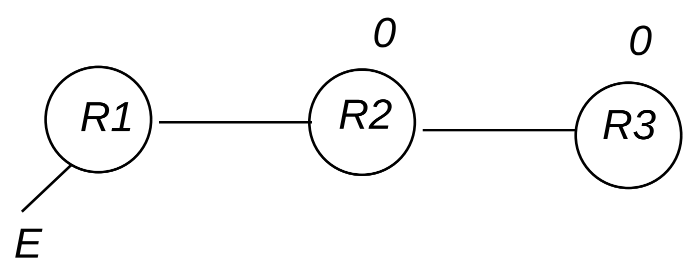


Figure 1:

```
None of us can completely grasp the truth, but none of us can
completely avoid finding a small part of the truth . . . and from
the assembled facts comes a certain kind of grandeur.

                                    --- Paraphrased from Aristotle
```

I hope that this course was more than just a collection of information about networks; instead, that it taught you a little about methods of thought and creativity that apply to many kinds of systems, and to life as well. It was a pleasure knowing you. Happy holidays!