**Luke Pepin - CSE3300: Computer Networking**

Homework 7

Due Date: **Tuesday, December 3, 2024**. Submission through HuskyCT. Full score: 100 for CSE3300 students; 120 for CSE5299 students (will be normalized to 100 when entering the grade in HuskyCT).

1. **Media Access Control (MAC) Protocols.** (30 points) We studied a number of MAC protocols, including (1) TDMA, (2) CSMA, (3) Slotted Aloha, and (4) Token passing. Suppose there are *N* stations on a LAN that has capacity (transmission rate) *C* bps. All frame/packets have a fixed length *L* bits and the end-to-end propagation delay of the broadcast channel is *P* seconds. For each of the protocols listed above, answer the following questions:
   * 1. (12 points) Suppose only one station ever has data to send (i.e., the other *N*−1 stations generate no traffic). What is the maximum possible throughput seen by this single node under each of the protocols above? **Note:** Here the maximum possible throughput refers to the long-term throughput (i.e., the amount of data transmitted successfully per unit time over a period of time) instead of the instantaneous throughput. We assume packets will be transmitted successfully when there is no collision (i.e., we do not worry about other types of bit errors).
2. TDMA: Divides the channel into time slots, and each station is assigned a specific slot. With only one station, it can use the entire channel capacity, so the throughput is C (LAN’s capacity).
3. CSMA: Allows stations to sense the channel before transmitting to avoid collisions. The single station can transmit whenever it wants without waiting, achieving a throughput of C.
4. Slotted Aloha: Divides time into slots and stations can only transmit at the start of these slots. The station can transmit at the beginning of every slot without collisions, resulting in a throughput of C.
5. Token Passing: Involves a token circulating among stations, granting the right to transmit to the station holding the token. The station always has the token and can transmit continuously, giving a throughput of C.
   * 1. (12 points) Suppose now that all stations are trying to send data at the same rate.We are now interested in the aggregate throughput of the LAN. For each of the above protocols, is it possible to achieve a throughput of *C* (i.e., have the channel always be fully utilized with user’s data)? If not, indicate how/why the protocol limits the maximum throughput to less than *C*. **Note:** The aggregate throughput refers to the total amount of data transmitted successfully over all the nodes per unit time. Again we assume packets will be transmitted successfully when there is no collision (i.e., we do not worry about other types of bit errors).
6. TDMA: The aggregate throughput can achieve C because each station gets a specific dedicated time slot, ensuring no collisions.
7. CSMA: Due to the possibility of collisions and the need for backoff periods, the aggregate throughput is going to be less than C. The protocol’s use decreases as the number of stations increases, leading to more collisions and idle times.
8. Slotted Aloha: Once again due to collisions specifically in Slotted Aloha they occur when multiple stations attempt to transmit in the same slot, the aggregate throughput is less than C.
9. Token Passing: Is the closest MAC protocol to getting to C without reaching it. This is a result of the time required to pass the token between stations. The efficiency depends on the token passing delay which nothing is transmitted during transfer of the token.
   * 1. (6 points) In a heavily loaded network, what is the worst case amount of time a node has to wait under each of the protocols, before it can send a message?
10. TDMA: The worst-case wait time is one frame time, as the node has to wait for its assigned time slot to come around. In TDMA, if a node just missed its slot, it must wait for the entire frame to cycle through all other slots before it can transmit.
11. CSMA: The worst-case wait time can be infinite because there is no bound on the number of times the channel can be sensed as busy due to continuous collisions and backoff periods.
12. Slotted Aloha: The node has to wait until the beginning of the next slot to send. However, due to potential collisions, the worst-case wait time can be infinite as there is no bound on the number of times the node might have to retransmit until successful.
13. Token Passing: The worst-case wait time is the time it takes for the token to circulate through all other stations plus the token propagation time. This can be expressed in the formula (N-1)\*(L+P).
14. **ARP and addressing.** (20 points) Consider the network topology shown in Fig. 1. The network interface cards (or network adaptors) are marked in the figure. As used in the textbook and slides, the rectangular forwarding devices are switches, and the circular forwarding device is a router.
    1. (3 points) How many subnets are there in the figure? For each subnet, list a possible subnet address (there can be many possible subnet addresses; listing one is sufficient for this problem).

2 Subnets are in figure 1, left side of the router and right side of the router.

Possible subnet addresses:

Subnet 1, left: 111.111.111.0/24

Subnet 2, right: 222.222.222.0/24

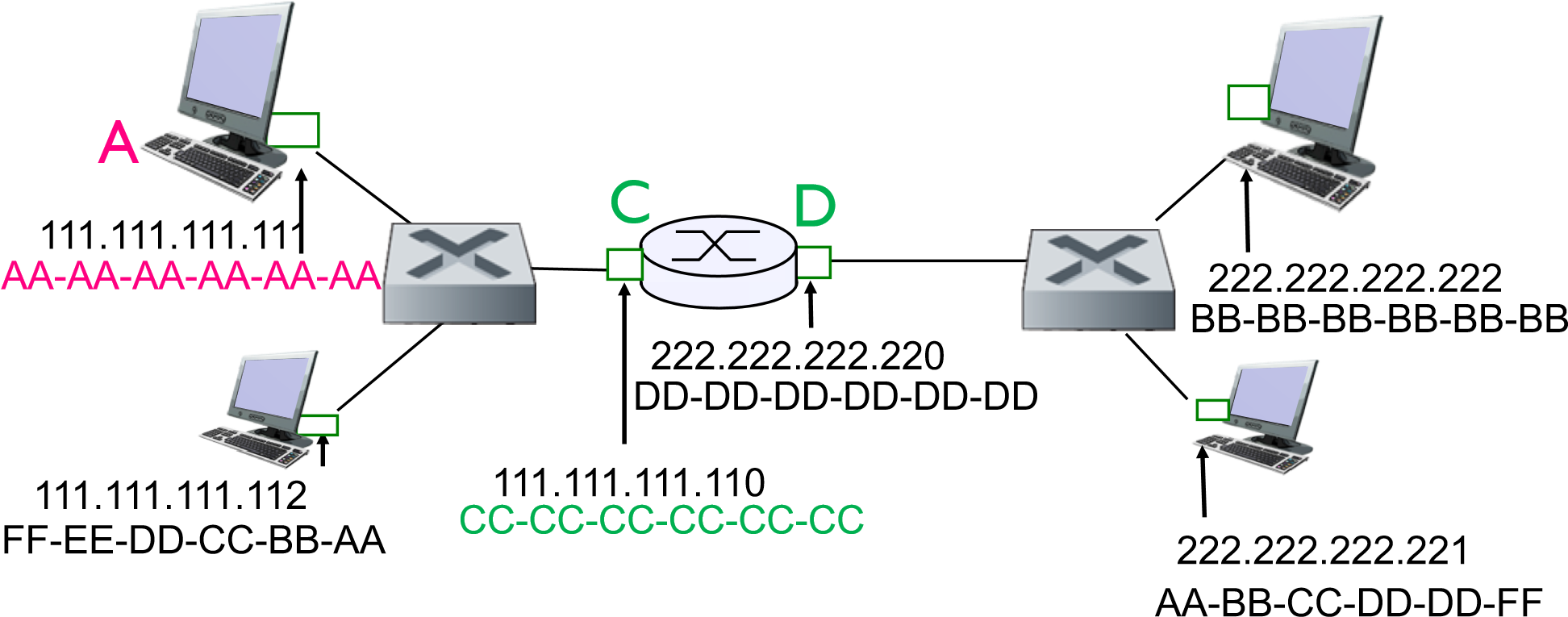
B

Figure 1: Network topology with a router in the middle.

* 1. (14 points) Consider sending an IP datagram from Host *A* to Host *B*. Suppose all of the ARP tables are up to date. In addition, assume the switches have up-to-date forwarding tables and the router has an up-to-date forwarding table.

b1. (6 points) List the source and destination IP addresses as well as the source and destination MAC addresses that are used:

(i) on the hop from *A* to *C*

Source IP 111.111.111.111

Destination IP 111.111.111.110

Source MAC AA-AA-AA-AA-AA-AA

Destination MAC CC-CC-CC-CC-CC-CC

(ii) on the hop from *D* to *B*

Source IP 222.222.222.220

Destination IP 222.222.222.221

Source MAC DD-DD-DD-DD-DD-DD

Destination MAC AA-BB-CC-DD-DD-FF

b2. (4 points) Briefly describe the actions at the switch between *A* and *C*.

The switch betwwen A and C recieves the ethernet frame from A, it looks up the destination of the MAC address given (CC-CC-CC-CC-CC-CC) and finally forwards the frame to the port connected to Router C based on the MAC address table entry.

b3. (4 points) Briefly describe the actions at the router.

The router similarly recieves the ethernet frame, removes the ethernet frame to get the IP datagram, looks up the destination of the IP address in its routing table, encapsulates the IP datagram in a new ethernet fram with the appropriate source and destination MAC address, finally it forwards teh new ethernet frame to the switch connected to B.

* 1. (3 points) Now assume that the ARP table in *A* is empty (and all the other tables are up to date). Will *A* perform an ARP query to find the MAC address of *B*? Why or why not?

No, A will not perform an ARP query to find the MAC address of B. Since the hosts are on a different subnets A will send the datagram to its default gateway the router C. A will only perform a ARP query to find the MAC address of C once it has that MAC address it sends it to C which will then forward it to B.

1. **Switch self-learning.** (30 points) Consider the network topology shown in Fig. 2. As used in the textbook and slides, the rectangular forwarding devices are switches; no router is in this topology. There are three switches, S1, S2 and S3. The ports of each switched are numbered as shown in the figure.
   1. (5 points) How many subnets are there in the figure? For each subnet, list a possiblesubnet address (there can be many possible subnet addresses; listing one is sufficient for this problem).

There is only one possible subnet in figure 2 since the devices are only connected by switches.

“Sub”net Address: 111.111.111.0/24

* 1. (25 points) Consider sending an IP datagram from Host *A* to Host *B*. Suppose that the ARP table in *A* is empty. The forwarding tables of all the switches are also empty. *A* will use ARP to find the MAC address of *B*. Specifically, *A* will send an ARP query with *B*’s IP address. *B* will respond with its MAC address.

B

FF

-

EE

-

DD

-

CC

-

BB

-

AA

AA

-

AA

-

AA

-

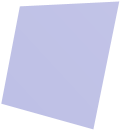
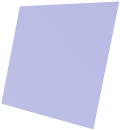
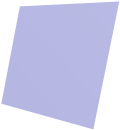
AA

-

AA

-

AA



111.111.111.112

111.111.111.111

A



1

S1

2

S2

1

2

3



111.111.111.120

BB

-

BB

-

BB

-

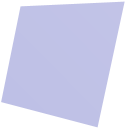
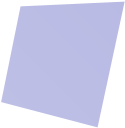
BB

-

BB

-

BB



S3

1

2

3

# 111.111.111.121 AA-BB-CC-DD-DD-FF

Figure 2: Network topology with only switches.

b1. (10 points) What are the source and destination MAC addresses in the ARP query? What will happen at each of the switches along the way (i.e., at S1, S2 and S3)? If a switch adds entry (or entries) to its forwarding table, describe what entry (or entries) is added.

Source MAC address: AA-AA-AA-AA-AA-AA (A)

Destination MAC address: FF-FF-FF-FF-FF-FF (broadcast)

S1: Recieves the query on port 1, adds the entry AA-AA-AA-AA-AA-AA is on port 1, broadcasts the ARP request out of ports 2 and 3.

S2: Recieves the query on port 1, adds the entry AA-AA-AA-AA-AA-AA is on port 1, broadcasts the ARP request out of port 2.

S3: Recieves the query on port 1, adds the entry AA-AA-AA-AA-AA-AA is on port 1, broadcasts the ARP request out of ports 2 and 3.

b2. (10 points) Continuing the above question - What are the source and destination MAC addresses in the ARP response? Describe the actions of the switches similarly as above.

Source MAC Address AA-BB-CC-DD-DD-FF (B)

Destination MAC Address AA-AA-AA-AA-AA-AA (A)

S1: Recieves the reply on port 3, adds the entry AA-BB-CC-DD-DD-FF is on port 3, broadcasts the ARP reply to port 1.

S2: Recieves the reply on port 2, broadcasts the ARP reply to port 1.

S3: Recieves the reply on port 3, broadcasts the ARP reply to port 1.

b3. (5 points) After knowing *B*’s MAC address, *A* sends an IP datagram to *B*. Describe the actions at each of the switches along the way.

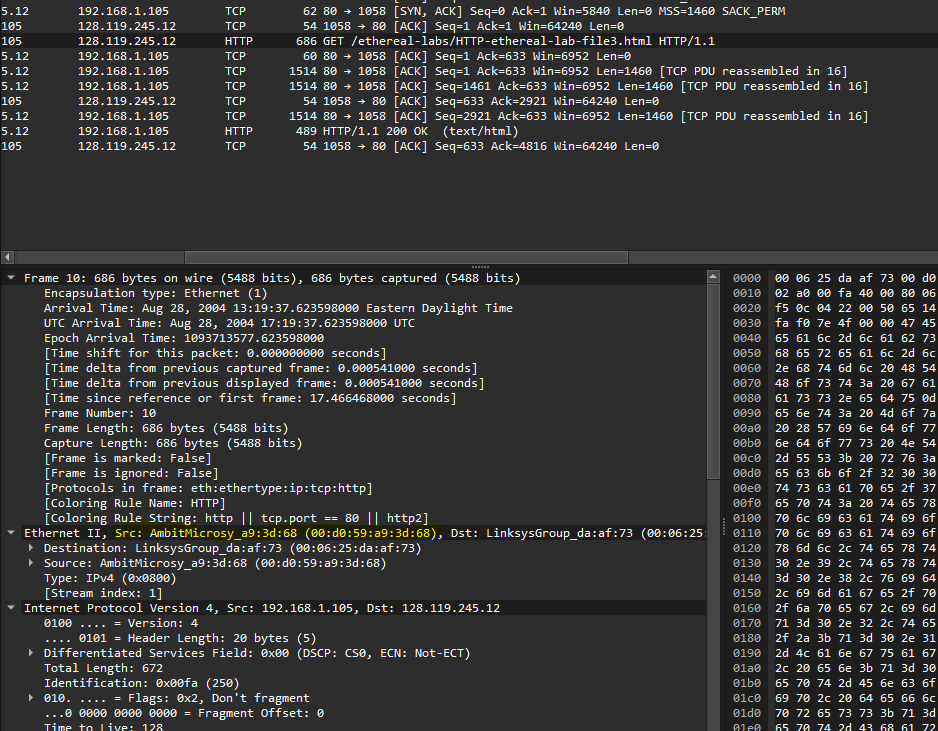
S1: Recieves the IP datagram on port 1, based on fowarding table fowards frame to port 3

S2: : Recieves the IP datagram on port 1, based on fowarding table fowards frame to port 2

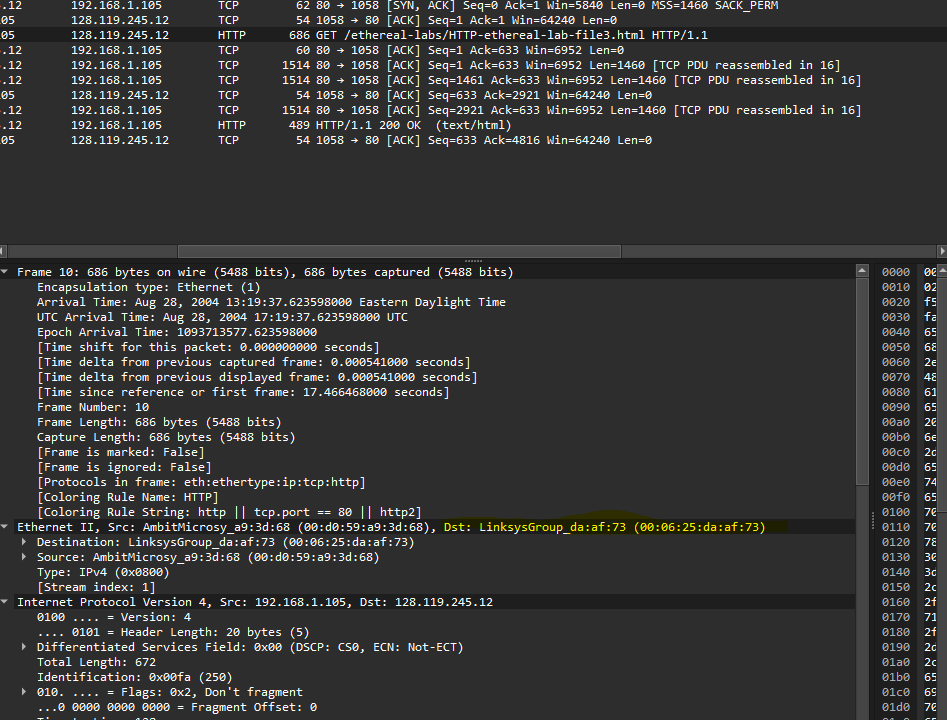
S3: : Recieves the IP datagram on port 1, based on fowarding table fowards frame to port 3

1. **Wireshark Lab (20 points).** Do problems 1-4 in the Ethernet wireshark lab (posted in HuskyCT). Since the capture has to be through Ethernet, while you are most likely using WiFi to access the Internet on your laptop, you may find it easier to just download the trace provided by the author (see footnote 2 on the first page).

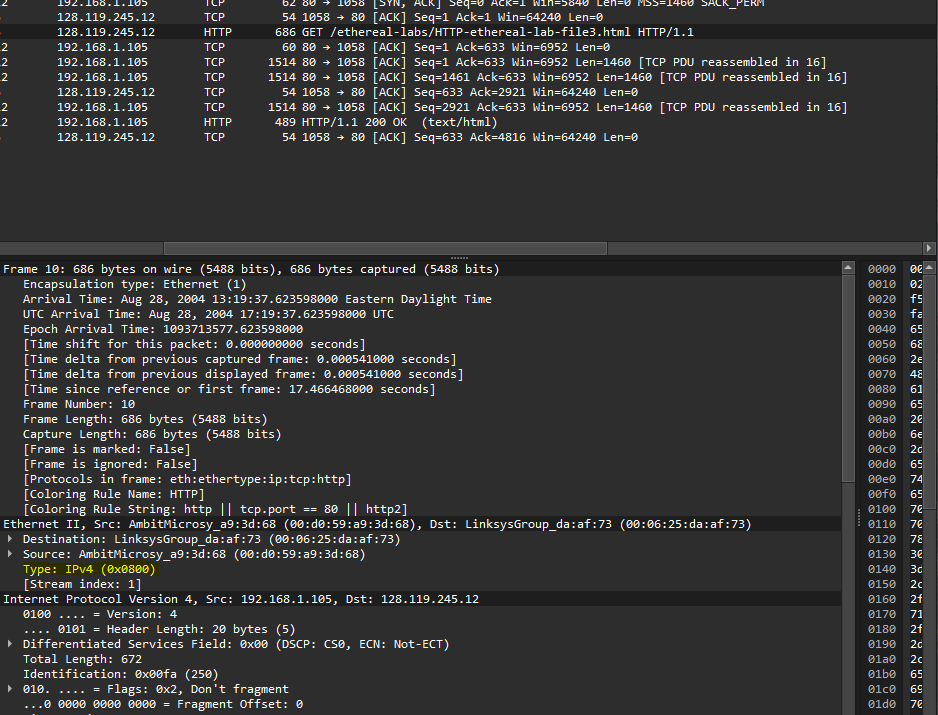
Note using the wireshark downloaded data

1. 

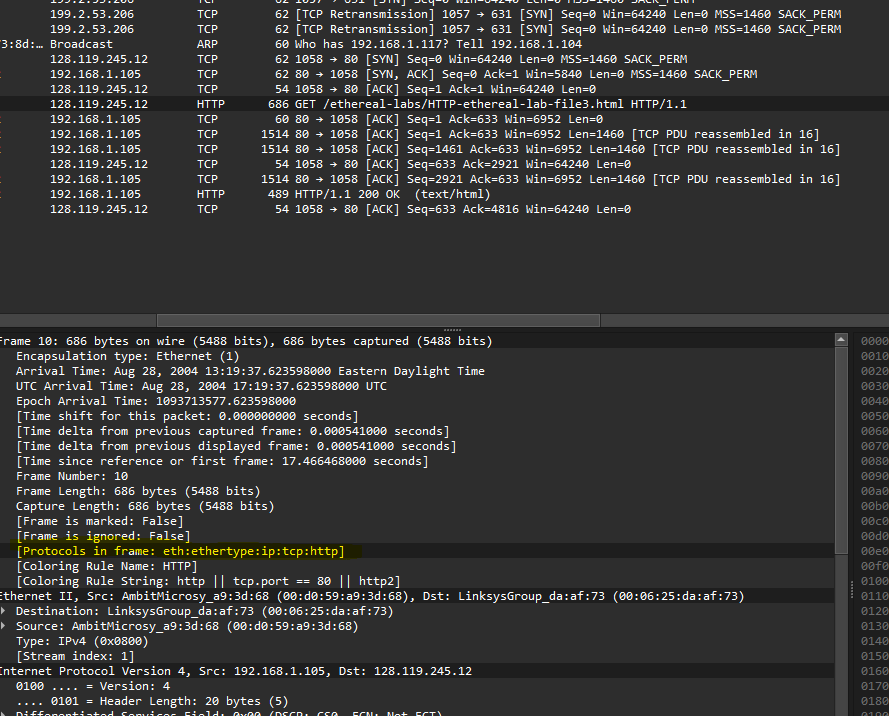
The 48-bit Ethernet address of my computer, is AmbitMicrosy\_a9:3d:68 (00:d0:59:a9:3d:68)

2.

The 48-bit destination address of the Ethernet frame is LinksysGroup\_da:af:73 (00:06:25:da:af:73) this is not the address of gaia.cs.umass.edu, it is the address of the router or gateway.

3.

The hexadecimal value for the two-byte frame type field is 0x0800 the upper level protocol it responds to is IPv4.

4.

From the line [Protocols in frame: eth:ethertype:ip:tcp:http] the ethernet header is 14 bytes, Ip header is 20 bytes, tcp is 20, together “G” in “GET” appears at the (14+20+20 =) 54 offset from the start of the frame.