CSEE 4119 Fall 2022

Homework 5 ANSWER KEY

Uploading course materials, including questions/answers from this homework, to sites such as CourseHero, Chegg or Github is academic misconduct at Columbia (see pg 10).

Question 0 [0 points, but required for credit]

If you wish to submit this homework for credit, the process is as follows:

- You will pick the previous homework (1, 2, 3, or 4, where 4 includes both parts) that you wish to replace with this one. For example, say you wish to replace your homework 1 score. HW1 was out of 83 points.
- We will take the % of points you get on this HW and give you that % on the homework you are choosing to replace. For example, if you receive a 90% on this homework and choose to replace HW1, then your HW1 grade would be counted as 90%*83=75.
- We will replace your previous homework score **even if you do worse on HW5 than on the one you are replacing.** So you should only submit HW5 for credit if you are confident it will increase your score.
- Remember that points within one category ARE on the same scale, so HW3 (120 points) is worth more than HW2 (116 points), which is worth more than HW1 (83 points).

For question 0, please answer which homework you are replacing: HW1, HW2, HW3, or HW4.

Question 1 Multiple Access Protocols

We looked at a number of different multiple access protocols in this course, including TDMA, CSMA, Slotted ALOHA, and Token Passing. Suppose there are N stations on a LAN that has a capacity (transmission rate) R. All packets have a fixed length, and each packet/frame takes up a time L. The propagation delay between any two nodes across the channel is P. Assume that the token-passing protocol allows a maximum of M frames to be transmitted before passing on the token.

For each subquestion:

+1 point answer

+1 point reasonable explanation (even if answer is not quite correct)

a. (8 points, 2 points each) Suppose only one station ever has a message to send (i.e. the other N-1 stations generate no traffic). In terms of the variables provided, give the maximum possible throughput achievable by the following protocols. Be sure to clearly state the reasoning behind your answer, including any assumptions you make.

   i. TDMA

   The one station gets to send every N slots, so the throughput is R/N

   ii. CSMA

   Assuming the station senses the channel immediately after finishing transmission (and finds it idle), it will send another packet. Therefore, it will always be sending, and the throughput is R. This neglects overhead time needed to do channel sensing, which should be very short compared to the transmission time of each packet.

   iii. Slotted ALOHA

Since there will be no collisions, there will be no need for probabilistic retransmissions. Instead, the station will send data continuously, so the throughput will be R.

iv. Token passing

It takes N*P to pass the token all the way around the ring. The one station will transmit for M*L at a time:

Throughput = (M*L)/(M*L + N*P) * R

Note that if the propagation delay is very small, we can approach maximum throughput.

b. (8 points, 2 points each) Suppose now that all of the stations have messages to send. We are interested in finding the total utilization of the link. For each of the following protocols, is it possible to achieve a utilization of 1 (i.e. have the link fully utilized)? If not, describe qualitatively how the protocol limits the maximum utilization.

i. TDMA

This can have a utilization of 1. Each station simply transmits in its own slot.

ii. CSMA

This will have a utilization less than 1. Collisions will still occur due to propagation delays: a station might detect that the channel is clear and not realize that packets are already en route. If the propagation delay is zero, then it can achieve a utilization of 1.

iii. Slotted ALOHA

There will be both collisions and wasted frames, so the utilization will be less than 1.

iv. Token passing

As in (a), there is a propagation delay in sending the token from station to station, so the utilization will be less than 1. Similar to CSMA, if the propagation and transmission times of the token are zero, then it can achieve a utilization of 1.

c. (8 points, 2 points each) In a heavily loaded network, what is the longest (worst-case) amount of time a station has to wait before it can send its next message?

i. TDMA

1 time frame or N time slots. A frame for TDMA is divided into N time slots, one for each node. This is different from the link layer unit of data, which is also sometimes called a frame.

ii. CSMA

Infinite. There is no maximum length of time for which the channel can be detected to be busy.

iii. Slotted ALOHA

When there is a collision, the protocol will wait for the next frame and retransmit with some probability. There is no bound to the number of attempts that will be needed, so this is also infinite.

iv. Token Passing

Each other station will transmit for the maximum time allowed. So any given station might have to wait this long plus the propagation time for each time the token is exchanged. This is ((N-1)*M*L + N*P)

d. [2 points] Explain why slotted ALOHA achieves a higher maximum efficiency than unslotted ALOHA.
In slotted ALOHA a station only conflicts with other stations when they attempt to send at the same time slot (one unit of transmission time), while in unslotted ALOHA, it conflicts with all stations that attempt to send between t0-1 and t0+1.
e. [2 points] Unslotted ALOHA does not require clock synchronization, so nodes do not need to coordinate about their clocks to implement the protocol. Suppose that an unslotted ALOHA network is operating at maximum efficiency. After some time, some nodes have left and some nodes have joined. Can the ALOHA network still operate at maximum efficiency without further coordination among nodes / reconfiguration at nodes?
Assume all nodes always have data to send and that they all calculate retransmission probability the same.
No, each station has to know the total number of stations N in the network since the formulae for optimal probability use this information.

Question 2 ARP, DHCP and Ethernet

1) [6 points] Some warmup T/Fs. For each question, indicate True or False for each index. *Example answer: d) i) True, ii) True, iii) False, iv) False.*
   a) [2 points] ARP requests propagate through:
      i) Switches True
      ii) Links True
      iii) Wireless links True
      iv) Routers False
   b) [2 points] For a switch which has N interfaces, an ethernet frame coming through an interface will be forwarded through:
      i) Exactly 1 interface False
      ii) Exactly N-1 interfaces False
      iii) Exactly N interfaces False
      iv) This is a trick question: it all depends on the state of the forwarding table. True
   c) [2 points] ARP tables contain the following key,value pairs:
      i) IP address, DNS name False
      ii) IP address, forwarding interface False
      iii) MAC address, forwarding interface False
      iv) MAC address, IP address True
2) (4 points)
   i. Why is an ARP query sent within a broadcast frame?
   ii. Why is an ARP response sent within a frame with a specific destination MAC address?

iii. Why is a DHCP Discover sent within a broadcast frame?
iv. Given that the DHCP is intended for a specific client, why might the server need to broadcast the DHCP Offer intended for the client?

i. During the request, the querying host does not know the MAC address that corresponds to the IP that it wants to reach. Thus, it uses a broadcast frame with the hope that it will reach the host with the desired IP.
ii. The host that does the ARP response know which MAC address to send the response to, thus it has a specific destination MAC address. (1 per case)
iii. The client does not know the DHCP server's MAC address, so it broadcasts the discover message, similarly to making an ARP query.
iv. From RFC2131: *A client that cannot receive unicast IP datagrams until its protocol software has been configured with an IP address SHOULD set the BROADCAST bit in the 'flags' field to 1 in any DHCPDISCOVER or DHCPREQUEST messages that client sends. The BROADCAST bit will provide a hint to the DHCP server and BOOTP relay agent to broadcast any messages to the client on the client's subnet.*
Other valid reason: let the other users know that the IP is being assigned.

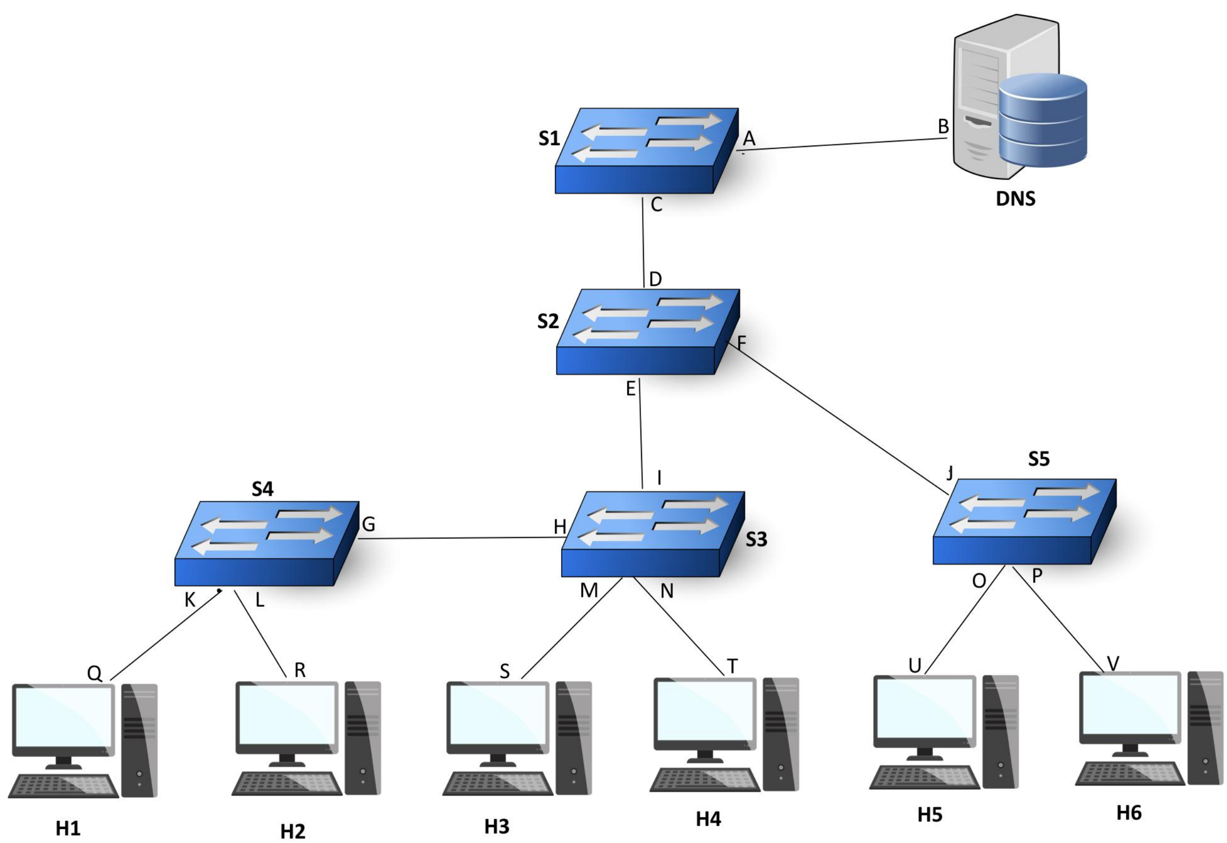


Figure 5. Subnet topology for 4.2

3) [24 points] Consider the subnet topology in Figure 5. All forwarding tables of the switches (S1, S2, S3, S4, S5) start empty. Letters denote interfaces (e.g. switch S4 has interfaces K,L and G). DNS is the local DNS server. Host H3 sends an ethernet frame

df1 to host H6. Then, as a response, host H6 sends an ethernet frame df2 to host H3. df1 has source MAC address s and destination MAC address v. df2 has source MAC address v and destination MAC address s.

a) [8 points] Describe all traffic generated in the network between the moment frame df1 is sent by host H3 and the moment it is received by host H6: <u>which device(s) send or receive which frame(s)</u>?

H3 sends df1 to S3.

S3 doesn't have an entry in the forwarding table. Thus, it forwards df1 to H4, S4 and S2. H4 ignores it. S4 doesn't have an entry in the forwarding table. Thus it forwards df1 to H1 and H2, which all ignore it.

S2 doesn't have an entry in the forwarding table. Thus it forwards df1 to S1 and S5. S1 doesn't have an entry in the forwarding table. Thus it forwards it to DNS.

S5 doesn't have an entry in the forwarding table. Thus it forwards df1 to H5 and H6. H5 ignores it. H6 receives df1.

b) [8 points] Describe all traffic generated in the network between the moment frame df2 is sent by host H6 and the moment it is received by host H3: <u>which device(s) send or receive which frame(s)</u>?

(The forwarding tables are not empty anymore!)

Host H6 forwards df2 to S5.

S5 has an entry in the forwarding table. Thus it forwards df2 to S2.

S2 has an entry in the forwarding table. Thus it forwards df2 to S3.

S3 has an entry in the forwarding table. Thus it forwards df2 to H3. H3 receives df2.

c) [4 points] Assume that the aforementioned traffic is completed (i.e. df1 is delivered, and so is df2). Now, fill the forwarding tables of the switches given below:

Forwarding table of S2

MAC address	forwarding interface
S	E
V	F

Forwarding table of S4

MAC address	forwarding interface
S	G

A common mistake will be having an entry for V in the forwarding table of S4, i.e. <V,G>. That entry should not appear because S3 won't propagate df2!

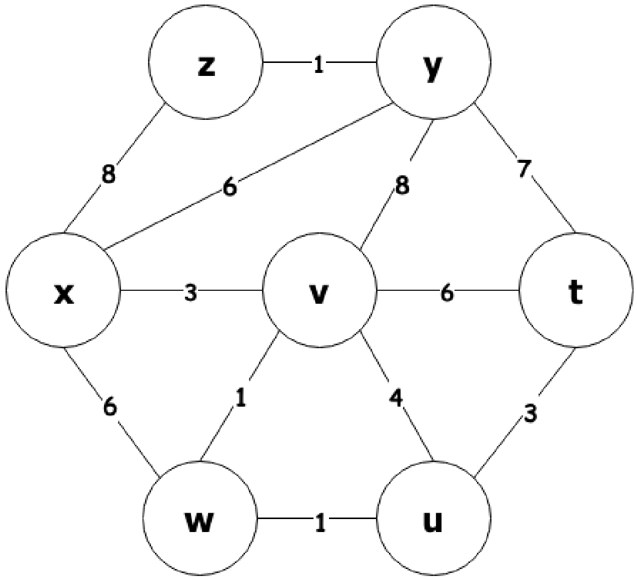
d) [4 points] Host H3 now wants to connect to *courseworks2.columbia.edu* to check for his HW5 grade. Say *courseworks2.columbia.edu/H3gradeHW5.png* contains H3's grade. A classmate, H4, wants to play a bad joke on H3 by tricking him into getting a fake version of *H3gradeHW5.png* which contains a bad grade. Give an ARP-related attack that H4 can perform to achieve this.
Assume that all hosts have just been initially configured (i.e. each host has only i) its own IP, ii) the gateway router's IP, iii) the local DNS server's IP). Assume also that all caches are empty.

Answer: To access the URL is to send a DNS request to the DNS server. Given that we are at the initial setup phase, H3 doesn't know the MAC address of the DNS server and therefore has to make an ARP request. H4 can send ARP replies as soon as it sees the ARP request (which, remember, switch S3 broadcasts to S2, S4 and H4), effectively impersonating the DNS server. The rest is history…

Other answers that will get full credits are: 1) assuming that the URL resolves to an IP inside the Local Area Network, H4 can spoof the web host by flooding ARP responses when H3 does an ARP request to resolve the web host's MAC. 2) Similar logic but assuming that the URL resolves to an IP outside the Local Area Network, H4 can spoof the gateway router...

Question 3 Routing Algorithms

a. [8 points] Consider the following graph model of a computer network, each edge has a value representing its cost. We want to apply link-state (LS) routing algorithm to find out the shortest path from source node x to all the other nodes. Please fill in the following table to show how the algorithm works. (Table is similar to the table 5.1 in the textbook)



Step	N’	D(t), p(t)	D(u), p(u)	D(v), p(v)	D(w), p(w)	D(y), p(y)	D(z),p(z)
0	x						
1							
2							

Step	N’	D(t), p(t)	D(u), p(u)	D(v), p(v)	D(w), p(w)	D(y), p(y)	D(z),p(z)
0	x	∞	∞	3,x	6,x	6,x	8,x
1	vx	9,v	7,v		4,v	6,x	8,x
2	vwx	9,v	5,w			6,x	8,x

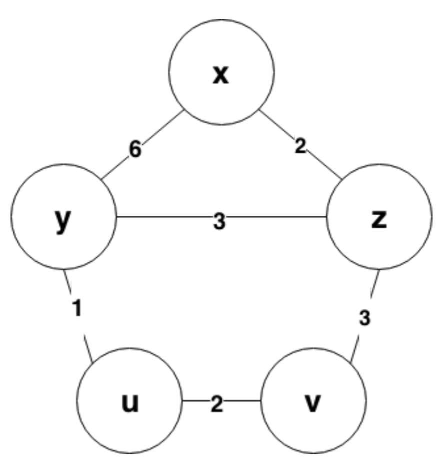
3	uvwx	8,u				6,x	8,x
4	uvwxy	8,u					7,y
5	uvwxyz	8,u					
6	tuvwxyz						

+2 points if correctly add nodes to N’
+1 for each node, if the shortest path is updated correctly

b. [2 points] In the LS routing algorithm, we also record p(v) for each node. How can we construct the least-cost path using p(v)? Also, please figure out the least-cost path from x to t.
After we finish the algorithm, we can construct the least-cost path according to p(v) all the way back to the source node, because we know the predecessor of the final node, then we can also get its predecessor, and so on.
x->v->w->u->t, and the cost is 8

+1 explain how to construct the path using p(v)
+1 correct path from x to t.

c. [8 points] Now we will use the Distance-Vector algorithm to figure out the path. Consider the following network graph. At the beginning, the distance vector of node x is [∞,∞,0,6,2] (the order is [Dx(u), Dx(v), Dx(x), Dx(y), Dx(z)]). Please show how Dx, the distance vector of node x changes in each iteration.
You should write down in the form of [Dx(u), Dx(v), Dx(x), Dx(y), Dx(z)].
For example [∞,∞,0,6,2] -> [?,?,?,?,?] -> ...



At the beginning:

	u	v	x	y	z
x	∞	∞	0	6	2
y	∞	∞	∞	∞	∞
z	∞	∞	∞	∞	∞

y, z tell x their distance vectors

	u	v	x	y	z
x	7 (update)	5 (update)	0	5 (update)	2
y	1	∞	6	0	3
z	∞	3	2	3	0

y, z also updates, and tell x their new distance vectors

	u	v	x	y	z
x	6 (update)	5	0	5	2
y	1	3	5	0	3
z	4	3	2	3	0

Then the result converges.
From the tables, we can found that the distance vector of node x is:

Final answer: [∞,∞,0,6,2] -> [7,5,0,5,2] -> [6,5,0,5,2]

+4 points if [7,5,0,5,2] is correct, Dx(x)=0 doesn't count in points.

+4 points if [6,5,0,5,2] is correct, Dx(x)=0 doesn't count in points.

d. [2 points] As mentioned in the textbook, it is possible that count-to-infinity problem may occur if a link cost increases. What if we connect two nodes where there is no previous

link between them, for example, connect node u and node z in problem d), can this problem occur?
No. We knew that if we decrease the link cost, it won't cause a loop. Connecting two nodes is equivalent to decrease the link cost from infinity to a certain value.

+1 Answer No.
+1 If mentions decrease the link cost, or the student recalculates it and answers correctly.

e. [2 points] Name one scenario (e.g. a type of networks, a certain type of resource such as space or time is limited) that it is more efficient to use the LS routing algorithm.
Small networks (since LS requires global knowledge and O(NE) messages have to be sent to know the costs), very hierarchical networks (since DV is bad in that case), very dynamic networks (since DV is bad in that case), time is limited… (or other reasonable answers)

f. [2 points] Name one scenario (e.g. a type of networks, a certain type of resource such as space or time is limited) that it is more efficient to use the Distance-Vector routing algorithm.
Big networks, flat networks, static networks, space is limited, certain sparse networks (many nodes with few links) … (or other reasonable answers)

Question 4 Measuring Paths through the Internet [20 points]

We learned about one method for measuring paths through the Internet using traceroute. There is another method for measuring paths through the Internet, the 'Record Route' option of IP. Specifying this option indicates that routers along the path should stamp IP addresses of their interfaces in the packet.
Note that there are multiple implementations of Traceroute - please refer to the implementation in the ICMP chapter of the textbook, which matches the standard tool on Linux or MacOS when called with default parameters and is similar to the Traceroute tool you may have used in Project 2.

1. How can we use the record route option to measure the path from a source to a destination? [3 points]
    a. Ans: you activate the record route option in a packet from a source to a destination for which the destination will respond with the IP options of the packet that generated a response to be included in the response (e.g., a ping or something that generates an ICMP error). Then you look at the recorded hops in the returned packet.

(partial credit for get the destination to respond, full credit for specifically what needs to be included)

2. What is one key difference between what traceroute measures and what the record route option measures? [2 points]
    a. Ans: traceroute measures source IP of packets sending TTL exceeded probes, whereas record route measures what record-route-supporting-routers populate the record route field with
    (there are other valid answers)
3. What is one important reason why we might use traceroute vs the record route feature to measure paths (an advantage of traceroute)? [2 points]
    a. Ans: wider support, no limit to the number of hops
4. What is one important reason why we might use the record route feature vs traceroute to measure paths (an advantage of record route)? [2 points]
    a. Ans: unaffected by load balancing / different paths taken between measurements, might get some insight into the reverse path
5. We conducted a record route ping and traceroute measurement between two end hosts. Answer the following questions based on the output shown below. (You may want to skim Ethan's reverse traceroute paper [or watch a video about it] in answering some of the questions.)

```
Ping record route from 4.14.3.38 to 195.89.145.25:
4.69.248.24
195.2.26.30
195.2.1.15
195.2.1.14
195.89.145.25
195.89.145.25
195.2.1.14
195.2.1.24
4.69.186.148
Traceroute from 4.14.3.38 to 195.89.145.25:
4.14.3.1 0.278 ms
195.2.26.29 2.087 ms
195.2.16.133 74.125 ms
195.2.28.170 74.088 ms
195.2.24.66 74.244 ms
195.2.24.177 73.907 ms
195.89.145.25 74.199 ms
```

    a. Why might the first hop be different? [1 point]
        i. Ans: routers might choose different interfaces with either traceroute or record route, first hop does not support record route, first hop doesn't decrement TTL, load balancing

b. What are the extra addresses shown using the record route feature? [2 points]
    i. Ans: hops on the return path
c. To enable the behavior observed in the previous question, with what values does the destination 195.89.145.25 populate the IP header options fields in the return packet to 4.14.3.38? [2 points]
    i. Ans: it copies IP options, so that routers on the return path also record the route
d. Even if all routers along a path support the record route option, why might we not observe absolutely every hop along a path? [1 point]
    i. Ans: (possibly many) too many hops so that the field fills up

6. Thinking more about traceroute:
    a. Why does Traceroute send UDP packets with a destination port that is unlikely to be in use by the destination host? [2 points]
        i. Ans: The packet that reaches the destination causes the destination to send a "port unreachable" ICMP message back to the source, which signifies that no more probe packets need to be sent. The purpose of the unrecognized UDP port number is to ensure that the destination reads the port number as invalid and sends the corresponding message back to the source.
           +1 for explanation of what an unrecognized UDP port number is, +1 for what it is used for
    b. In class, we discussed how routing algorithms find the shortest path. Assume that link costs are symmetric and that the network is stable (no links/nodes are added/removed, and no link costs change). Under these assumptions, both Dijkstra's Algorithm and Bellman-Ford Equation would find that the cost of the shortest path in one direction is the same as the cost of the shortest path in the other direction. Still under these assumptions, suppose you issue a traceroute from a to b and a traceroute from b to a, and they are different (meaning the paths are asymmetric). What is a reason that OSPF could arrive at asymmetric routes? [2 points]
        i. Ans: OSPF can do it because of equal-cost paths. (possibly more answers)
           +2 for mention of equal-cost paths
    c. What is a reason that BGP could arrive at asymmetric routes? [2 points]
        i. Ans: BGP can do it because of policy routing.
           +2 for mention of policy routing