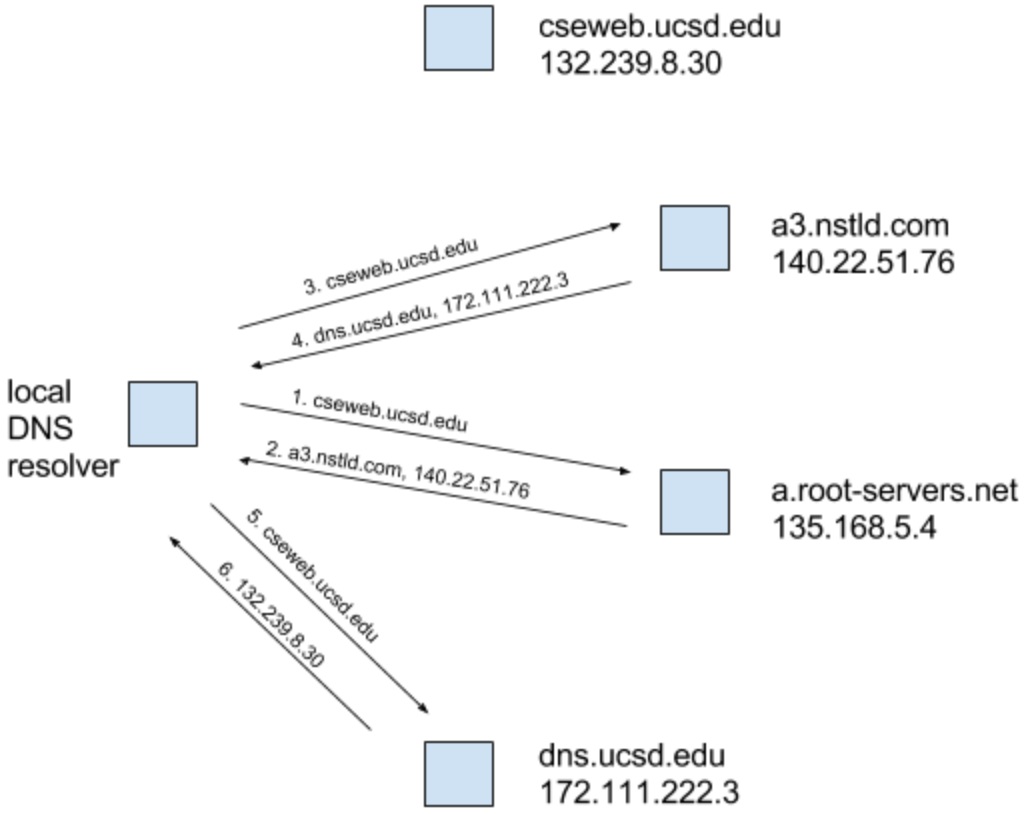
CSE 123: Computer Networks

Homework 2 Solutions

Total points = 50

Problems

1. **The Domain Name System (DNS) [6 points]**
   In the figure below, the first two steps are shown in the process of the local DNS resolver resolving the name “cseweb.ucsd.edu”. Assume that the local DNS resolver is configured to contact a root domain server directly. It would be a good idea to read section 9.3.1 in the book (P&D) before answering this problem.



   a. Complete the rest of the steps in the illustration to finish the resolution of cseweb.ucsd.edu given the records each server contains below. Please refer to figure 9.18 on page 755 of your book if you need to see the expected format of the answer. Note, you may not need to use every server (rectangle) in the illustration above.

```
a.root-servers.net: <edu, a3.nstld.com, NS, IN>
                    <a3.nstld.com, 140.22.51.76, A, IN>
a3.nstld.com: <ucsd.edu, dns.ucsd.edu, NS, IN>
              <dns.ucsd.edu, 172.111.222.3, A, IN>
dns.ucsd.edu: <cseweb.ucsd.edu, 132.239.8.30, A, IN>
```

See the filled in illustration above for the answer.

6 points total

- 1 pt for each arrow with correct information and order (6 in all)
    - -1 total pt if arrows are almost correct, but consistent
    - -1 total pt if accessing cseweb.ucsd.edu

2. **NAT [8 points]**

   NAT, is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. Recall, a NAT capable router essentially translates private addresses within a network to public addresses that can be used publicly on the internet.

   In this question, we look at the inner workings of a simple NAT capable router. The router will have mappings between the private addresses within the network (here, the private addresses all fall within the 172.16.0.0/12 network) to the public address that it uses. Let us assume that the router has a single public address 98.5.23.7 which it uses for all communication with hosts that are not part of the private network. The router multiplexes its public IP address as needed and keeps track of the multiplexing in a NAT translation table.

   Assume that the router multiplexes the public address using ports starting from 4000 and then incrementing by one. For example, if a host in the private network with address 172.16.0.5:9000 sends a message to 132.239.8.45:80 then the entry in the NAT table would be filled in as below. The next time the router will use 4001 after receiving a packet with a new LAN side IP and port pair and so on. Think of a message as a packet (using TCP) in this context.

NAT Translation Table	
WAN Side Address	**LAN Side Address**
98.5.23.7:4000	172.16.0.5:9000
98.5.23.7:4001	172.16.0.6:5000
98.5.23.7:4002	172.16.1.10:6000
98.5.23.7:4003	172.16.5.3:9001
98.5.23.7:4004	172.16.0.10:6000
98.5.23.7:4005	172.20.0.7:7000

a. What would be the entries in the NAT Translation Table at the end of the following global events (keeping the first entry from the table above). Assume the router implementing NAT is connected to the internet and can reach any public IP address and vice-versa.
   i. 172.16.0.6:5000 sends a message to 206.190.36.45:80
   ii. 172.16.1.10:6000 sends a message to 204.79.197.200:80
   iii. 172.16.5.3:9001 sends a message to 206.190.36.45:80
   iv. 172.16.0.10:6000 sends a message to 173.16.0.6:22
   v. 172.16.5.3:9001 sends a message to 74.125.239.33:80
   vi. 172.20.0.7:7000 sends a message to 63.245.215.20:80
   vii. 206.190.36.45:80 sends a message to 172.16.0.6:5000
   viii. 204.79.197.200:7000 sends a message to 74.125.239.33:80

   Note: The NAT Table should be like the one above with the entries generated from the events in (a.) filled in

Only events i, ii, iii, iv, and vi modified the NAT table. Event v just uses the entry that's already in the table for that local ip and port. Events vii and viii were originally meant to be "global events", as mentioned in the part a description, but many perceived this problem as being that the router sees all of the messages from above, so I will grade from that perspective too.

If you took everything as being "global events" then event vii would mean that if some host 206.190.36.45 tried to send to 172.16.0.6 then it would never actually make it through the Internet to get to this NAT enabled router because it is a bogon. As such it

would have no effect on this router's NAT table. If you understood it as the router receiving the messages all listed, then you can assume that the router would do a LPM on its forwarding table and find a match for the private subnet it is attached to, so the message would be forwarded without modification. This would also not cause the NAT table to change. The same arguments basically apply for viii as well. If the message being sent is treated as a "global event" then the message should never reach the router because that's not the router's public IP address. If treated as the router receiving the message, then it would be forwarded back towards the internet because that's what would be matched in the forwarding table. Neither would cause a change to the NAT table.

b. For simplicity, let us assume that message format is MSG<Sender, Receiver>. In that case, if a host in the private network with address 172.16.0.5:9000 sends a message to 132.239.8.45:80 then the message recevied at the router and leaving at the router would look as follows

   Message Received from Host: MSG<172.16.0.5:9000, 132.239.8.45:80>
   Message Sent from Router: MSG<98.5.23.7:4000, 132.239.8.45:80>

   Note: We will need to use the entries from the table we filled in (a.) to do this.

   List out the message received from the host at the router and the message sent from the router (like shown above) for the following messages:

   i. 172.16.5.3:9001 sends a message to 74.125.239.33:80
      Message Received from Host:
         MSG<172.16.5.3:9001, 74.125.239.33:80>
      Message Sent from Router:
         MSG<98.5.23.7:4003, 74.125.239.33:80>
   ii. 172.16.1.10:6000 sends a message to 63.245.215.20:80
      Message Received from Host:
         MSG<172.16.1.10:6000, 63.245.215.20:80>
      Message Sent from Router:
         MSG<98.5.23.7:4002, 63.245.215.20:80>

c. If the router gets a message MSG<204.79.197.200:80, 172.16.1.10:6000>, what would the message look like leaving the router?

   MSG<204.79.197.200:80, 172.16.1.10:6000>
   I will be lenient on grading this problem because realistically the router should not get a message like this that presumably would have come from the Internet. If you mentioned the packet should have been dropped you'll get credit.

d. Finally, if the router gets a message MSG<172.16.1.10:6000, 172.16.5.3:9001>, what would the message look like leaving the router?

   It would look the same because the message is not leaving the private subnet: MSG<172.16.1.10:6000, 172.16.5.3:9001>

8 points total

- 4 pts for part a
  - -1 total pt if not all entries added
  - -1 total pt if extra entries added
- 2 pts for part b
  - 1 pt for part i correctness
  - 1 pt for part ii correctness
- 1 pt for part c for correctness
- 1 pt for part d for correctness

3. **Distance-vector routing [9 points]**
   For the network shown below, give the global distance-vector tables like those in Tables 3.10 and 3.13 on pages 244 and 246 in the book (P&D) when

a. Each node knows only the distances to its immediate neighbors.

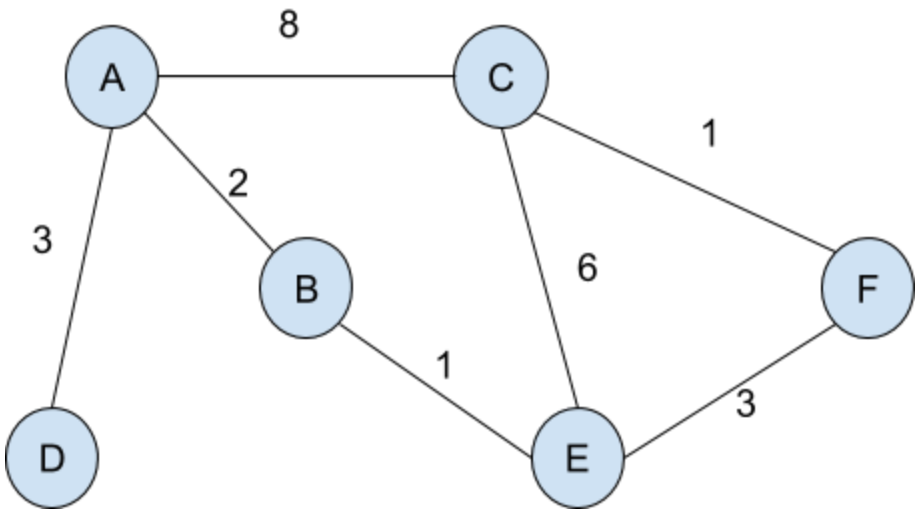
	A	B	C	D	E	F
A	0	2	8	3	Inf	Inf
B	2	0	Inf	Inf	1	Inf
C	8	Inf	0	Inf	6	1
D	3	Inf	Inf	0	Inf	Inf
E	Inf	1	6	Inf	0	3
F	Inf	Inf	1	Inf	3	0

b. Each node has reported the information it had in the previous step to its immediate neighbors.

	A	B	C	D	E	F
A	0	2	8	3	3	9
B	2	0	7	5	1	4
C	8	7	0	11	4	1
D	3	5	11	0	Inf	Inf
E	3	1	4	Inf	0	3
F	9	4	1	Inf	3	0

c. Step “b.” happens a second time.

	A	B	C	D	E	F
A	0	2	8	3	3	6
B	2	0	5	5	1	4
C	8	5	0	11	4	1
D	3	5	11	0	6	12
E	3	1	4	6	0	3
F	6	4	1	12	3	0



9 pts total

- 3 pts for part a
  - -1 total pt if some rows are incorrect
- 3 pts for part b
  - -1 total pt if some rows are incorrect where correctness is based upon the student answer from part a
- 3 pts for part c
  - -1 total pt if some rows are incorrect where correctness is based upon the student answer from part b

4. **Split Horizon and Poison Reverse [9 points]**
   Use the figure from part 3 to answer the following questions assuming the routers are using Distance-vector routing with split horizon and poison reverse. Assume that the network has settled long enough that the routers have all reached a convergence. An example of the vectors that F would receive from its neighbors is shown below.

   Ex. vectors received by F
   C:

A	B	C	D	E	F
Inf	Inf	0	Inf	Inf	Inf

   E:

A	B	C	D	E	F
3	1	Inf	6	0	Inf

   a. Show the vectors A would receive from its immediate neighbors

   D:

A	B	C	D	E	F
Inf	Inf	Inf	0	Inf	Inf

   B:

A	B	C	D	E	F
Inf	0	5	Inf	1	4

   C:

A	B	C	D	E	F
7	5	0	10	4	1

b. Show the vectors E would receive from its immediate neighbors

B:

A	B	C	D	E	F
2	0	Inf	5	Inf	Inf

C:

A	B	C	D	E	F
7	5	0	10	4	1

F:

A	B	C	D	E	F
Inf	Inf	1	Inf	Inf	0

c. Show the vectors C would receive from its immediate neighbors

A:

A	B	C	D	E	F
0	2	7	3	3	6

E:

A	B	C	D	E	F
3	1	4	6	0	3

F:

A	B	C	D	E	F
6	4	Inf	9	3	0

9 points total

- 3 pts for part a
    - 1 pt for each correct distance vector
- 3 pts for part b
    - 1 pt for each correct distance vector
- 3 pts for part c
    - 1 pt for each correct distance vector
- *Note: “correct” is treated as meaning Inf is sent where needed and not sent where not needed. As such, if 11 is put and 10 is expected, no points will be taken. If 11 is put, but Inf is expected, a point will be taken.
    - This helps to be somewhat lenient to those who miscalculated what the global table would be at convergence

5. **Link-state routing [10 points]**
   Using the same network topology as in the figure in problem 3, draw a table like Table 3.14 on page 258 in the book (P&D) that traces the steps for building the routing table for node B.

Confirmed	**Tentative**	**Comments**
(B,0,-)		Initial node
(B,0,-)	(A,2,A) (E,1,E)	B Neighbors
(B,0,-) (E,1,E)	(A,2,A)	Added E
(B,0,-) (E,1,E)	(A,2,A) (C,7,E) (F,4,E)	E Neighbors
(B,0,-) (E,1,E) (A,2,A)	(C,7,E) (F,4,E)	Added A
(B,0,-) (E,1,E) (A,2,A)	(C,7,E) (F,4,E) (D,5,A)	A Neighbors
(B,0,-) (E,1,E) (A,2,A) (F,4,E)	(C,7,E) (D,5,A)	Added F
(B,0,-) (E,1,E) (A,2,A) (F,4,E)	(C,5,E) (D,5,A)	F Neighbors; cheaper path found for C
(B,0,-) (E,1,E) (A,2,A) (F,4,E) (C,5,E)	(D,5,A)	Added C
(B,0,-) (E,1,E) (A,2,A) (F,4,E) (C,5,E)	(D,5,A)	C has no new Neighbors
(B,0,-) (E,1,E) (A,2,A) (F,4,E) (C,5,E) (D,5,A)		Added D; done

Note that C or D can be added first. The order doesn't matter for those two. Also, if you condensed the steps of adding a node to the confirmed list and adding its neighbors to the tentative list, you should get full points assuming it's done correctly.

10 points total

- 1 pt for each addition of a correct node into the confirmed node (except for the last one, so 5 total)
- 1 pt for each update of a node's neighbors (5 total)
- -3 total pts for using link cost of next-hop for total cost rather than adding up the links to get to the destination
- -1 pt for each error
    - I'll try to follow the student through for points on consistency
    - A common error is using F as the next hop for C when the distance to C is shortened after adding F as confirmed. E is still the next-hop from B.

6. **End-to-End Router behavior [8 points]**

For the below topology, rectangles are routers and circles are hosts. The numbers inside the hosts and routers are numbered ports on the host or router. The following lines represent the IP and MAC addresses of each port on the hosts and routers in the topology.

```
A:  1- 78.64.1.5, 74-29-9C-E8-FF-55
R1: 1- 78.64.1.1, E6-E9-00-17-BB-4B
    2- 78.64.2.1, CC-49-DE-D0-AB-7D
R2: 1- 78.64.2.2, 1A-23-F9-CD-06-9B
    2- 78.64.3.1, 88-B2-2F-54-1A-0F
    3- 78.64.4.2, 49-BD-D2-C7-56-2A
B:  1- 78.64.3.5, 2A-1A-CD-DE-E9-74
R3: 1- 78.64.4.1, E9-C7-2F-23-CC-55
    2- 78.64.5.1, DE-D2-B2-1A-4B-FF
C:  1- 78.64.5.5, D2-B2-1A-7D-BB-E8
```

For the parts below assume that there is an ARP cache with no timeout. In other words, if a given host or router has received an ARP reply for an IP they have sent an ARP request for previously, they don't need to send an ARP request again. For each part list each step that occurs to get the packet from source to destination like the example below:

Ex. Say host B sends a packet to R2 (specifically to `78.64.3.1`)
Step 1- B sends an ARP request on port 1 for 78.64.3.1
Step 2- R2 responds on port 2 with 88-B2-2F-54-1A-0F
Step 3- B sends the packet on port 1 with source IP 78.64.3.5, destination IP 78.64.3.1, source MAC address 2A-1A-CD-DE-E9-74, and destination MAC address 88-B2-2F-54-1A-0F

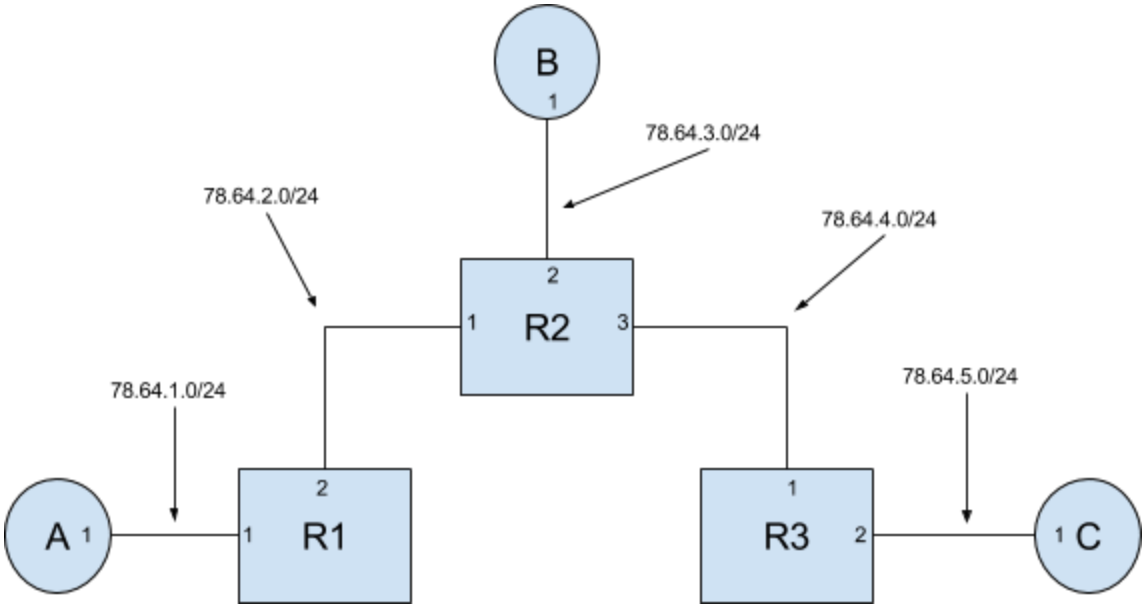
Assume the ARP caches are empty before part a below. Part b will keep whatever was cached from part a.

a. Host A sends a packet to B

Step 1- A sends an ARP request on port 1 for 78.64.1.1
Step 2- R1 responds on port 1 with E6-E9-00-17-BB-4B
Step 3- A sends the packet on port 1 with source IP 78.64.1.5, destination IP 78.64.3.5, source MAC address 74-29-9C-E8-FF-55, and destination MAC address E6-E9-00-17-BB-4B
Step 4- R1 sends an ARP request on port 2 for 78.64.2.2
Step 5- R2 responds on port 1 with 1A-23-F9-CD-06-9B
Step 6- R1 sends the packet on port 2 with source IP 78.64.1.5, destination IP 78.64.3.5, source MAC address CC-49-DE-D0-AB-7D, and destination MAC address 1A-23-F9-CD-06-9B
Step 7- R2 sends an ARP request on port 2 for 78.64.3.5
Step 8- B responds on port 1 with 2A-1A-CD-DE-E9-74
Step 9- R2 sends the packet on port 2 with source IP 78.64.1.5, destination IP 78.64.3.5, source MAC address 88-B2-2F-54-1A-0F, and destination MAC address 2A-1A-CD-DE-E9-74

b. Host A sends a packet to C

Step 1- A sends the packet on port 1 with source IP 78.64.1.5, destination IP 78.64.5.5, source MAC address 74-29-9C-E8-FF-55, and destination MAC address E6-E9-00-17-BB-4B
Step 2- R1 sends the packet on port 2 with source IP 78.64.1.5, destination IP 78.64.5.5, source MAC address CC-49-DE-D0-AB-7D, and destination MAC address 1A-23-F9-CD-06-9B
Step 3- R2 sends an ARP request on port 3 for 78.64.4.1
Step 4- R3 responds on port 1 with E9-C7-2F-23-CC-55
Step 5- R2 sends the packet on port 3 with source IP 78.64.1.5, destination IP 78.64.5.5, source MAC address 49-BD-D2-C7-56-2A, and destination MAC address E9-C7-2F-23-CC-55
Step 6- R3 sends an ARP request on port 2 for 78.64.5.5
Step 7- C responds on port 1 with D2-B2-1A-7D-BB-E8
Step 8- R3 sends the packet on port 2 with source IP 78.64.1.5, destination IP 78.64.5.5, source MAC address DE-D2-B2-1A-4B-FF, and destination MAC address D2-B2-1A-7D-BB-E8



8 points total

- 4 pts for part a
    - -1 total pt for missing any or incorrect ARP requests
    - -1 total pt if used an incorrect MAC Address
- 4 pts for part b
    - -1 total pt for missing any or incorrect ARP requests
    - -1 total pt for adding any unnecessary ARP requests
    - -1 total pt if used an incorrect MAC Address
- -2 total pts for changing ip address in packet
- -2 total pts for omitting details such as source address and destination addresses for either MAC or IP addresses