CS 118 - Homework 6

Kuruvilla Cherian, Jahan
UID: 104436427
Section 1A

November 15, 2016

Problem 1

a

All newly created mappings are labeled as <**IP:port within network, IP:port known in the outside network**>. The basic idea behind the answers are, that if the source is not already in the table, then create an entry with said source, and the outgoing IP with previous port value + 1. If there are messages being sent by IP's outside the internal network, then they have no effect on the NAT Table.

a

10.0.0.6:5000 sends a message to 74.125.239.33:80 - This will create the following mapping <**10.0.0.6:5000, 131.179.128.125:8001**>.

b

10.0.0.10:6000 sends a message to 204.79.197.200:80 - This will create the following mapping <**10.0.0.10:6000, 131.179.128.125:8002**>.

c

10.0.1.101:6001 sends a message to 206.190.36.45:80 - This will create the following mapping <**10.0.1.101:6001, 131.179.128.125:8003**>.

d

10.0.0.10:6000 sends another message to 204.79.197.200:80 - This mapping already exists and so will **not create a new entry**, but instead reuse the entry from part (b) - <**10.0.0.10:6000, 131.179.128.125:8002**>.

e

10.0.1.101:6001 sends a message to 74.125.239.33:80 - Because the source IP Address already exists within the NAT Table thus far, we will **not create a new entry**, even though the destination IP is different from that in part (c). The intuition behind this is that the router responsible for performing the translations will send from the same IP as in part (c) but to a new destination. Thus the entry corresponding to this communication is <**10.0.1.101:6001, 131.179.128.125:8003**>.

f

10.0.0.7:7000 sends a message to 63.245.215.20:80 - This will create the following mapping <**10.0.0.7:7000, 131.179.128.125:8004**>.

g

204.79.197.200:80 sends a message to 131.179.128.125:8002 - This will have **no effect** on the NAT Table, since this communication's source is from outside the network and thus has no need to have a translation associated with it. However, it is worthwhile to mention that this communication is similar to that in part (b), wherein the message from 204.79.197.200:80 will be sent to 10.0.0.10:6000 within the network.

h

204.79.197.200:80 sends a message to 131.179.128.125:8003 - This will have **no effect** on the NAT Table, since this communication's source is from outside the network and thus has no need to have a translation associated with it. However, this message will essentially be sent to the final destination that is 10.0.1.101:6001.

i

204.79.197.200:80 sends a message to 131.179.128.125:8005 - This will have **no effect** on the NAT Table, since this communication's source is from outside the network and thus has no need to have a translation associated with it. Seeing as we have no matching port to 8005, this message will not be sent to any host within the given network.
We see the final table as follows:

IP and port within the network	IP and port known in the outside network
10.0.0.5:5000	131.179.128.125:8000
10.0.0.6:5000	131.179.128.125:8001
10.0.0.10:6000	131.179.128.125:8002
10.0.1.101:6001	131.179.128.125:8003
10.0.0.7:7000	131.179.128.125:8004

Table 1: Final NAT Translation Table

b

a

10.0.0.6:5000 sends a message to 74.125.239.33:80 - Gives us the following:
Message Received from Host: *MSG*<10.0.0.6:5000, 74.125.239.33:80>
Message Sent from Receiver: *MSG*<131.179.128.125:8001, 74.125.239.33:80>

b

10.0.0.10:6000 sends a message to 204.79.197.200:80 - Gives us the following:
Message Received from Host: *MSG*<10.0.0.10:6000, 204.79.197.200:80>
Message Sent from Receiver: *MSG*<131.179.128.125:8002, 204.79.197.200:80>

c

The router will index into its NAT Table and find the mapping between 131.179.128.125:8001 to 10.0.0.6:5000, thus the message will look as follows:
MSG<74.125.239.33:80, 10.0.0.6:5000>.

d

Because both IP Addresses addresses are internal to the network, there is no need to go through the NAT Table, and so the final message will look exactly the same as
MSG<10.0.0.10:6000, 10.0.1.101:6001>.

Problem 2

a

Step	N_{start}	D(y), p(y)	D(t), p(t)	D(x), p(x)	D(v), p(v)	D(w), p(w)	D(u), p(u)	D(s), p(s)
0	z	14, z	2, z	∞	∞	∞	∞	∞
1	zt	6, t	2, z	∞	11, t	∞	4, t	3, t
2	zts	6, t	2, z	∞	11, t	∞	4, t	3, t
3	ztsu	6, t	2, z	∞	5, u	7, u	4, t	3, t
4	ztsuv	6, t	2, z	8, v	5, u	6, v	4, t	3, t
5	ztsuvy	6, t	2, z	8, v	5, u	6, v	4, t	3, t
6	ztsuvyw	6, t	2, z	7, w	5, u	6, v	4, t	3, t
7	ztsuvywx	6, t	2, z	7, w	5, u	6, v	4, t	3, t

Table 2: Link-State step by step table

b

Destination	Link/Interface
y	(z, t)
t	(z, t)
x	(z, t)
v	(z, t)
w	(z, t)
u	(z, t)
s	(z, t)

Table 3: Resulting forwarding table at z

Problem 3

a

We apply a distributed Bellman-Ford algorithm to compute the shortest distance from z to its neighbors (in this case only y and t) and then their shortest distance to the given destination through its neighbors. The bold numbers in the table below, highlight the values we would use to determine the next hop for the forwarding table.

Destination	Nodes through	
	y	**t**
y	14	**6**
t	18	**2**
x	17	**7**
v	15	**5**
u	16	**4**
w	16	**6**
s	19	**3**

Table 4: z's Routing Table

b

As given in 4 the highlighted values are representative of the node to pick for the next hop, giving us 5 below.

Destination	Next Hop
y	t
t	t
x	t
v	t
u	t
w	t
s	t

Table 5: z's Forwarding Table

Problem 4

If we wish to only transfer B's traffic to D through the East Coast, then through eBGP, the only way for C to make such a transfer of traffic possible is to advertise only its route to D through its East Coast peering point with C and ignore its West Coast connection entirely. This way through BGP's routing protocol, B will not pass the traffic that it does not know. Since we can think of C as a customer to B, then we know that C need not advertise the prefixes between providers, and thus can do as mentioned above by ignoring the West Coast. This is known as **Multi-Exit Discriminators (MED)** wherein the AS (in this case ISP C) can choose to show B a preference for the inbound traffic flow (in this case through the East Coast into D).

Problem 5

Yes, BGP will allow for Z to implement the given policy. We know that X, Y and Z are interconnected AS's and thus communicate through eBGP. Because this is interconnected, Inter-AS routing takes over wherein an admin who wants control over how the traffic is routed, can do so by routing through its network. In this case, we can assume Y as the "admin" wherein, under the BGP routing policy, it can tell X that it does not have a path to Z - that is it does not advertise the path to Z, to X, and thus Z wil never receive X's traffic since X will not send its traffic through Y, and thus Z will only get Y's traffic.

Problem 6

A is a dual homed customer to B and C and thus can choose on how to forward the traffic based on its advertisement of its customers.
For X to receive only B's traffic and for Y to receive traffic from either B or C, A will advertise the following routes:

To B:
1.) $X : A \rightarrow X$
2.) $Y : A \rightarrow Y$
3.) $A : A$

To C:
1.) $Y : A \rightarrow Y$
2.) $A : A$

C will receive the following routes:
1.) $B : B$
2.) $A : A$
3.) $A : B \rightarrow A$
4.) $Y : A \rightarrow Y$
5.) $Y : B \rightarrow A \rightarrow Y$
6.) $X : B \rightarrow A \rightarrow X$