Hw #7

#1 a)

	IP:port within private network	IP:port outside private network
	10.0.0.5:5000	128.97.27.37:8000
(1)	10.0.0.6:5000	128.97.27.37:8001
(2)	10.0.0.10:6000	128.97.27.37:8002
(3)	10.0.0.11:6001	128.97.27.37:8003
(6)	10.0.0.7:7000	128.97.27.37:8004

4, 5 are duplicates

7, 8: global, don't get their own entries in the table

b) (1) Message received from Host: MSG <10.0.0.6:5000, 172.217.11.78:80>
Message sent from Router: MSG <128.97.27.37:8001, 172.217.11.78:80>

(2) Message received from Host: MSG <10.0.0.10:6000, 204.79.197.200:80>
Message sent from Router: MSG <128.97.27.37:8002, 204.79.197.200:80>

#2 a) The type of service field in the IP datagram header will specify the correct transport layer protocol that the segment should be passed to. This 8-bit field encodes the upper layer protocol in use, whether TCP, UDP, or other.

b) Yes, a host can have multiple IP addresses. This is because IP address is location dependent. Based on location, a user gets an IP address from a DHCP server, and this can't be reused elsewhere; in a new location, a user gets another IP address, which can be different.
A host will have a unique IP address for each local network with a DHCP server it is connected to, so it can ever have multiple IP's at the same time.

c) Skype works between two hosts behind different NAT boxes using the concept of relaying. Here, a relaying node is used by each side to setup the connection. These nodes set up the connection with the other client behind the NAT, which believes that the client is using the public IP of the node. All information from the client is sent to the relaying node, and then redirected to the NAT router and then to the host behind the NAT router. Thus, the information is "relayed" from the node to the client to complete the connection.
(See slide 65 for Chapter 4 for the diagram).

d) NAT is not needed if IPv6 is globally deployed, in my opinion. This is because NAT is used to solve the issue of the lack of IPv4 space, meaning that there are a lot of devices that need IPs and the number available is running out. IPv6 does not have this issue because there are 128 bits for IP addresses in IPv6, so there are 2^{128} possible addresses compared to the 2^{32} possible IPv4 addresses. Therefore, NAT should not be needed to extend the addressing space of IPv6.

break ties: t > u > v > w > x > y ; u > w, add u before w if tied

#3

step	N'	D(t),p(t)	D(u),p(u)	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)
0	z	∞	∞	∞	∞	8, z	12, z
1	z, x	∞	∞	11, x	14, x		12, z
2	z, x, v	15, v	14, v		14, x		12, z
3	z, x, v, y	15, v	14, v		14, x		
4	z, x, v, y, u	15, v			14, x		
5	z, x, v, y, u, w	15, v					
6	z, x, v, y, u, w, t						

u, w tied, so 2 iterations

Shortest paths to each node from z:

z → t : z x v t cost = 15
z → u : z x v u cost = 14
z → v : z x v cost = 11
z → w : z x w cost = 14
z → x : z x cost = 8
z → y : z y cost = 12

#4 a) eBGP learns about x through border router 4c in AS4, different AS, so eBGP

b) iBGP; learns about x from 3b, which is an internal router in the same AS

c) eBGP; learns about x from 3a, a border/gateway router in a different AS

d) iBGP; learns about x from 1a, an internal router in the same AS

#5 ☆ Hot-potato routing: select the local gateway / border router w/ least cost

Customer 1 to 2: J → H → I → Exchange point → F → D → C → B

5 + 5 + 5 + 10 + 35 + 20 + 5 = 85 msec one-way propagation delay from customer 1 to 2

Customer 2 to 1: B → C → A → G → H → J

5 + 10 + 5 + 10 + 5 = 35 msec one-way propagation delay from customer 2 to 1

Thus, the routing between two customers is asymmetric

This is because for customer 1 to get to customer 2, of the two routes specified by ISP 1's gateway routers, it is faster to get to router I. Thus, it will use the path that includes I to go from 1 to 2. In the opposite direction, the path specified by gateway router C in ISP 2 is clearly the closest for customer 2, so it will use this followed by OSPF once within ISP 1 to reach customer 1. All in all, this creates a separate path for each direction of propagation.