# Problem 1

Suppose that the NAT-capable router has a single public address `128.97.27.37` which it uses for all communication with hosts that are not part of the private network. The private network used is subnet `10.0/16`. The router multiplexes its public IP address(es) 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 `8000` and then increments the port number by one for each new entry. For example, if a host behind the router with address and port `10.0.0.5:5000` sends a message to an external server `8.8.8.8:53`, then the entry in the NAT table would be filled in as below.

Table 1: NAT Translation Table

| `IP:port` within private network | `IP:port` outside private network |
|---|---|
| `10.0.0.5:5000` | `128.97.27.37:8000` |
| ... | ... |

The next time the router will use port `8001` to establish a new connection and so on.

(a) Draw the resulting NAT Translation Table at the end of the following message exchanges following the format of Table 1 (including the original entry):

(1) `10.0.0.6:5000` sends a message to `172.217.11.78:80`

(2) `10.0.0.10:6000` sends a message to `204.79.197.200:80`

(3) `10.0.1.101:6001` sends a message to `206.190.36.45:80`

(4) `10.0.0.10:6000` sends a message to `204.79.197.200:80`

(5) `10.0.1.101:6001` sends a message to `172.217.11.78:80`

(6) `10.0.0.7:7000` sends a message to `63.245.215.20:80`

(7) `204.79.197.200:80` sends a message to `128.97.27.37:8002`

(8) `204.79.197.200:80` sends a message to `128.97.27.37:8003`

(b) For simplicity, let us assume that message format is `MSG <Sender, Receiver>`. In that case, if a host in the private network with IP address and port `10.0.0.5:5000` sends a message to `132.239.8.45:80`. Then the message received at the router and leaving at the router would look as follows:

Message Received from Host: `MSG <10.0.0.5:5000, 132.239.8.45:80>`

Message Sent from Router: `MSG <128.97.27.37:8000, 132.239.8.45:80>`

List the messages, in the same format shown above, received from the host at the router and the message sent from the router for the following messages:

(1) `10.0.0.6:5000` sends a message to `172.217.11.78:80`

(2) `10.0.0.10:6000` sends a message to `204.79.197.200:80`

Assume the entries from your NAT Translation Table in (a) to do this.

Problem 1 continued on next page. . .

Write your solution to Problem 1 in this box

a)

| IP : Port within Private Network | IP : Port outside Private Network |
|---|---|
| 10.0.0.5 : 5000 | 128.97.27.37 : 8000 |
| 10.0.0.6 : 5000 | 128.97.27.37:8001 |
| 10.0.0.10 : 6000 | 128.97.27.37 : 8002 |
| 10.0.1.101 : 6001 | 128.97.27.37 : 8003 |
| 10.0.0.7 : 7000 | 128.97.27.37 : 8004 |

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>

## Problem 2

Answer the following questions regrading to IP.

(a) Can a host have more than one IP address? Justify your answer briefly.

(b) How does Skype work between two hosts which are behind two different NAT boxes?

(c) Do you think NAT is still needed if IPv6 is globally deployed?

Write your solution to Problem 2 in this box

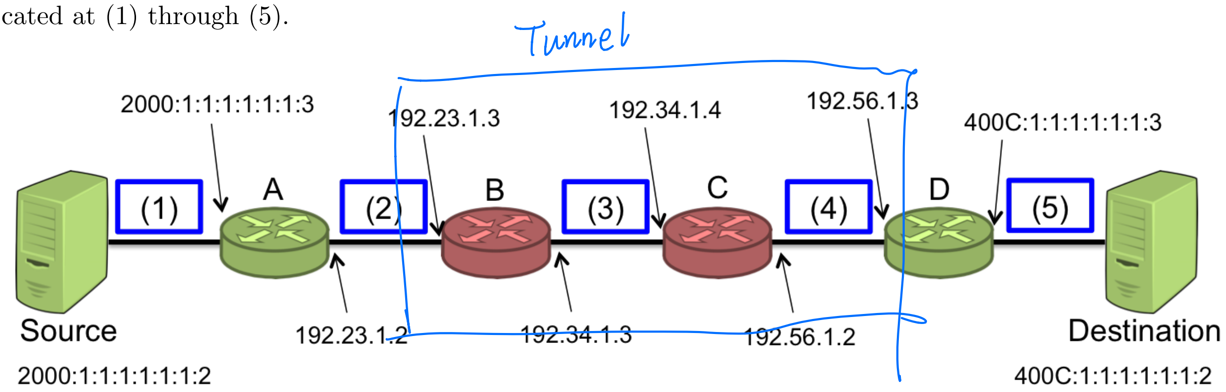
a) Yes.
If a host has multiple NICs, then the host can have more than one IP address.

b)
The hosts behind NAT boxes can be found by each other since they are first connected to the Skype server. The server then helps each user make a connection to the other users by providing connection information.

c)
Yes.
NAT can provide additional security, protect the hosts within the network from malicious attacks from external network.

## Problem 3 IP Tunneling

Consider a network with four routers. Router A and D are IPv6 routers while router B and C are IPv4 routers. Assume that the source host sends an IPv6 packet to the destination host. The blue boxes in the figure represent the packet's location. Show source IP address and destination IP address of the packet located at (1) through (5).



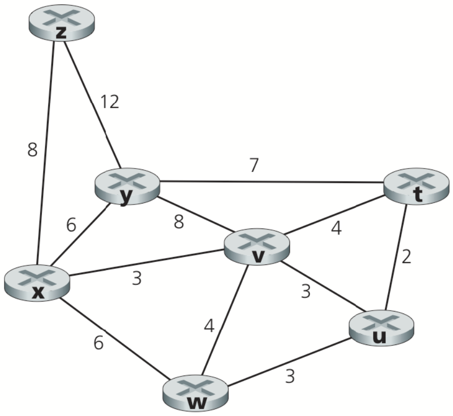
Write your solution to Problem 3 in this box

| | Source IP | Dest IP |
|---|---|---|
| 1) | 2000:1:1:1:1:1:1:2 | 400C:1:1:1:1:1:1:2 |
| 2) | 192.23.1.2 | 192.56.1.3 |
| 3) | 192.23.1.2 | 192.56.1.3 |
| 4) | 192.23.1.2 | 192.56.1.3 |
| 5) | 2000:1:1:1:1:1:1:2 | 400C:1:1:1:1:1:1:2 |

## Problem 4

Consider the following network. With the indicated link costs, use Dijkstra's shortest-path algorithm to compute the shortest path from **z** to all network nodes. Show how the algorithm works by computing a table similar to the table in chapter 5 lecture slide 12 (Dijkstra's Algorithm: example).

**Note**: When there is a tie, you should select the node with order $t > u > v > w > x > y$. For example, when u and w appear to have the same cost, you should add u into $N'$ in your next iteration.



Write your solution to Problem 4 in this table.

| 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 | zx | ∞ | ∞ | 11, x | 14,x | | 12, z |
| 2 | zxv | 15, v | 14,v | | 14, x | | 12, z |
| 3 | zxvy | 15, v | 14,v | | 14, x | | |
| 4 | zxvyu | 15,v | | | 14,x | | |
| 5 | zxvyuw | 15,v | | | 14,x | | |
| 6 | zxvyuwt | 15,v | | | | | |

Reference: https://docs.oracle.com/cd/E19253-01/816-4554/dhcp-overview-3/index.html

## Problem 5

- Please download and install Wireshark (`https://www.wireshark.org`). If your computer does not support Wireshark, you can use `tcpdump`. The difference is that Wireshark supports UI while tcpdump not. Both can be used to capture and analyze packets for this lab.
- Please learn how to use Wireshark (or tcpdump). You can find a lot of online resources useful, for example, Wireshark Cheat Sheet (e.g, https://www.comparitech.com/net-admin/wireshark-cheat-sheet/) and tcpdump cheat sheet (or man tcpdump).
- Please capture DHCP packets for IP address allocation via Wireshark. Hint: You need to start packet capturing before DHCP runs. Think about how to invoke IP address allocation via DHCP.
- Please answer the following questions using the trace captured. Please show the screenshoot of relavant packets and filelds in the answer.

  (a) Do you observe all the DHCP messages in this allocation instance (DHCP discover, DHCP offer, DHCP request, DHCP ack)? If no, what types of DHCP messages are observed in the above instance?

  (b) Which transport layer protocol is used? Please choose one DHCP message as an example to show the screenshot with its source port and destination port numbers.

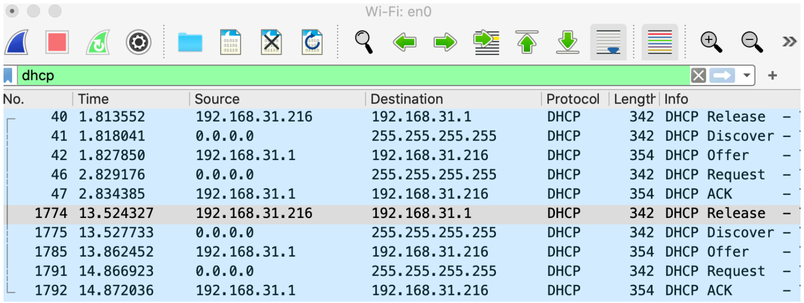
  (c) Check the source IP addresses and destination IP addresses used in all the DHCP messages observed in your case. Are they the same as those illustrated in the lecture? If not, what is the difference and why is this difference allowed for DHCP?

  (d) What is the IP address of the DHCP server? What is the IP address allocated to the host? How do you know that?

  (e) What is the subnet mask and DNS server IP address?

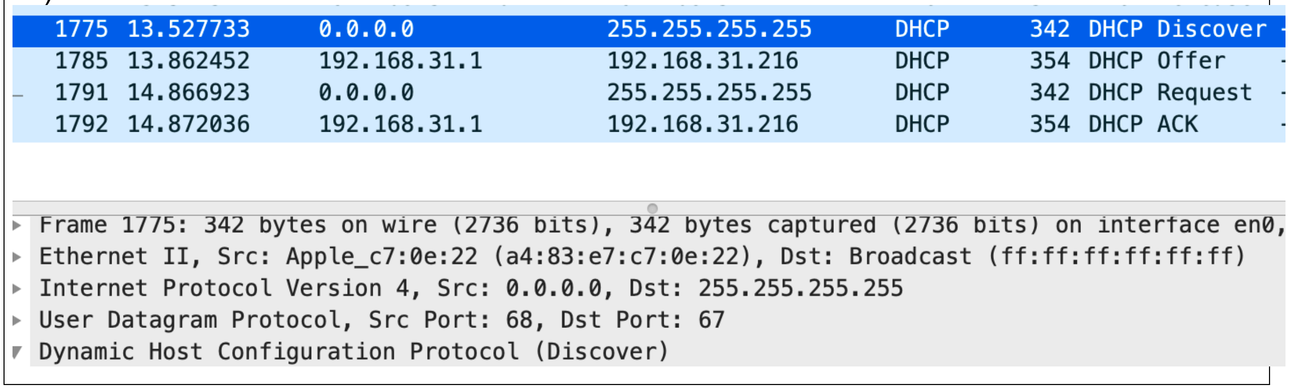
Write your solution to Problem 5 in this box

a) Yes, I observed all the DHCP messages.



```
dhcp
No.   Time       Source          Destination      Protocol Length Info
   40 1.813552   192.168.31.216  192.168.31.1     DHCP     342 DHCP Release  –
   41 1.818041   0.0.0.0         255.255.255.255  DHCP     342 DHCP Discover –
   42 1.827850   192.168.31.1    192.168.31.216   DHCP     354 DHCP Offer    –
   46 2.829176   0.0.0.0         255.255.255.255  DHCP     342 DHCP Request  –
   47 2.834385   192.168.31.1    192.168.31.216   DHCP     354 DHCP ACK      –
 1774 13.524327  192.168.31.216  192.168.31.1     DHCP     342 DHCP Release  –
 1775 13.527733  0.0.0.0         255.255.255.255  DHCP     342 DHCP Discover –
 1785 13.862452  192.168.31.1    192.168.31.216   DHCP     354 DHCP Offer    –
 1791 14.866923  0.0.0.0         255.255.255.255  DHCP     342 DHCP Request  –
 1792 14.872036  192.168.31.1    192.168.31.216   DHCP     354 DHCP ACK      –
```

b) UDP is used.



```
1775  13.527733   0.0.0.0        255.255.255.255   DHCP   342  DHCP Discover
1785  13.862452   192.168.31.1   192.168.31.216    DHCP   354  DHCP Offer
1791  14.866923   0.0.0.0        255.255.255.255   DHCP   342  DHCP Request
1792  14.872036   192.168.31.1   192.168.31.216    DHCP   354  DHCP ACK

▸ Frame 1775: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0,
▸ Ethernet II, Src: Apple_c7:0e:22 (a4:83:e7:c7:0e:22), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Dynamic Host Configuration Protocol (Discover)
```

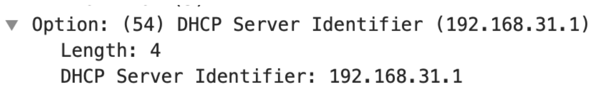
c) They are not the same as in the lecture.

The difference occurs in the DHCP Ack and DHCP offer. The difference is allowed, since they mean different dynamic IP address assigned to the host (which is unique) and the ip address of the DHCP server.  DHCP servers are multiple, the ip address could be different.

The host discovers a DHCP server by broadcasting a discover message to the limited broadcast address (255.255.255.255) on the local subnet.  Since the subnet network i am using is different from the one in the lecture, so the ip address of the DHCP server would be different.

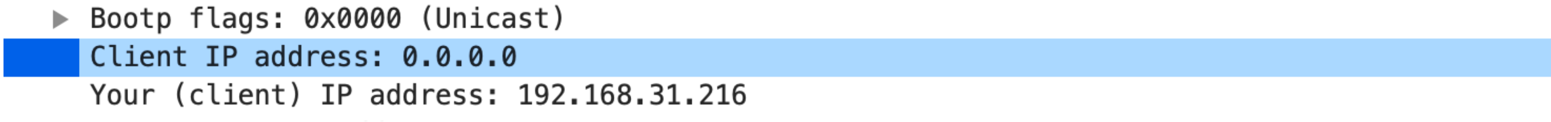
d)

DHCP IP address: 192.168.31.1



```
  ▼ Option: (54) DHCP Server Identifier (192.168.31.1)
        Length: 4
        DHCP Server Identifier: 192.168.31.1
```

IP address allocated: 192.168.31.216, know it from the DHCP message.

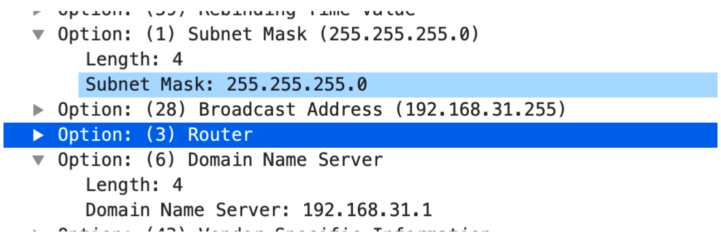


```
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.31.216
```

e)

subnet mask: 255.255.255.0

DNS server IP address: 192.168.31.1



```
 ▶ Option: (59) Rebinding Time Value
 ▼ Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
 ▶ Option: (28) Broadcast Address (192.168.31.255)
 ▶ Option: (3) Router
 ▼ Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 192.168.31.1
 ▶ Option: (43) Vendor-Specific Information
```