# 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` → 8001

(2) `10.0.0.10:6000` sends a message to `204.79.197.200:80` → 8002

(3) `10.0.1.101:6001` sends a message to `206.190.36.45:80` → 8003

(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` → 8004

(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: <10.0.0.6:5000, 172.217.11.78 : 80>
Message sent from router: <128.97.27.37 : 8001, 172.217.11.78:80>

2) Message received from host: <10.0.0.10:6000, 204.79.197.200:80>
Message sent from router: <128.97.27.37: 8002, 204.79.197.200:80>

## Problem 2

Answer the following questions regrading to IP.

(a) Suppose Host A receives an IP datagram. How does the network layer in Host A know it should pass the segment (that is, the payload of the datagram) to TCP rather than to UDP or to something else?

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

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

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

Write your solution to Problem 2 in this box

(a) The 8-bit protocol field in the IP datagram tells the network layer which transport layer protocol to pass the segment to.

(b) Yes, it depends on the number of network interfaces in the host. For example, your laptop can have 2 IP addresses — one corresponding to the IP network interface, and another corresponding to a LAN/Ethernet network interface.

(c) Skype uses relaying for NAT traversal. Each client maintains a host cache with the IP address and port numbers of reachable supernodes. The NATed client who initiates the call establishes a connection to the supernode. The NATed client who receives the call also connects to the supernode. The supernode bridges packets between these two connections.

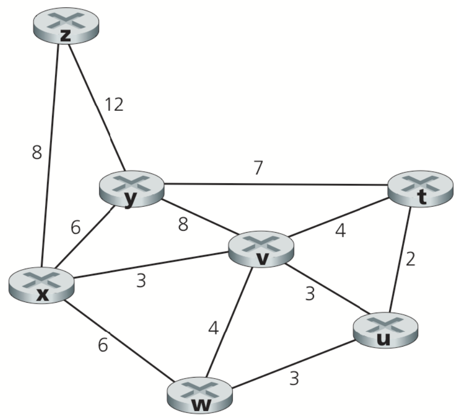
(d) One of the reasons NAT was developed was to overcome the shortage of IPv4 addresses. Therefore, since there is no shortage of IPv6 addresses, there is no reason to actually have NAT. However, we would lose some benefits NAT provides

1. Changing addresses of devices in a local network
2. Changing ISP without changing addresses of devices in the local network
3. Devices inside a local network not explicitly being visible to the outside world, improving their security.

# Problem 3

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.



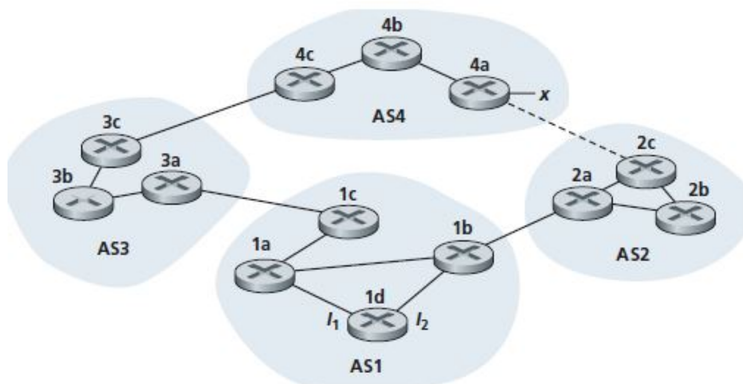

Write your solution to Problem 3 in this table.

| 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 | | | | | |
| 6 | zxvyuwt | | | | | | |

← tie: pick u since u>w

# Problem 4

Consider the network shown below. Suppose AS3 and AS2 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.




At some time T, the prefix $x$ appears in AS4, adjacent to the router 4a. From which routing protocol (OSPF, RIP, eBGP, or iBGP):

(a) Router 3c learns about prefix $x$?

(b) Router 3a learns about prefix $x$?

(c) Router 1c learns about prefix $x$?

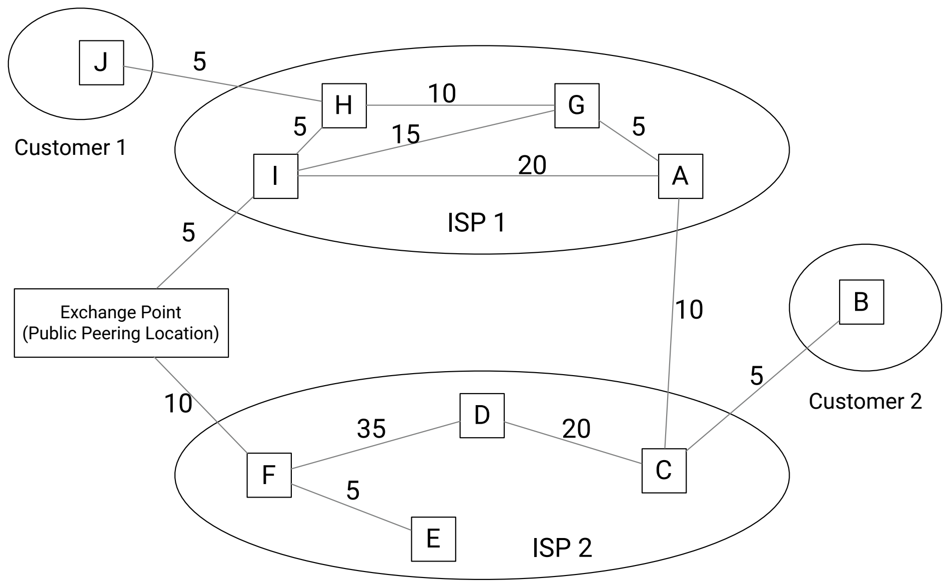
(d) Router 1d learns about prefix $x$?

Write your solution to Problem 4 in this box

(a) eBGP (receives from AS4)
(b) iBGP (receives from AS3)
(c) eBGP ( receives from AS3)
(d) iBGP (receives from AS1)

# Problem 5

Consider the following topology. The cost metric of a link denotes the one-way propagation delay on the link in msec (assuming the delays are symmetric). The two ISPs ISP 1 and ISP 2 are peers. CIDR is used for addressing and BGP is used for inter-domain routing. Assume that both ISPs always try to enforce hot-potato routing above all other routing policies. What is the one-way propagation delay between Customer 1 and Customer 2? Is the routing between two customers symmetric or asymmetric?




Write your solution to Problem 5 in this box

Since Hot Potato routing is enforced, from among all possible routes, the route chosen is the one with the least cost to the NEXT-HOP router beginning at that route.

Propagation delay from Customer 1 to Customer 2:

$5+5+5+10+35+20+5 = 85$ msec

J-H-I-Exchange Point-F-D-C-B

Propagation delay from Customer 2 to Customer 1:

$5+10+5+10+5 = 35$ msec

B-C-A-G-H-J

Since the propagation delays are not the same, the routing between the two customers is asymmetric.