Problem 1

Suppose that the NAT-capable router has a single public address `128.97.36.96` 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`	`128.97.36.96:8000`
...	...

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) `10.0.0.7:7001` sends a message to `63.245.215.20:80`

(7) `204.79.197.200:80` sends a message to `128.97.36.96:8002`

(8) `204.79.197.200:80` sends a message to `128.97.36.96:8003`

(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 <128.97.36.96:8000, 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) NAT Translation Table

IP: port within private net	IP: port outside private net
10.0.0.5 : 5000	128.97.36.96 : 8000
10.0.0.6 : 5000	128.97.36.96 : 8001
10.0.0.10 : 6000	128.97.36.96 : 8002
10.0.1.101 : 6001	128.97.36.96 : 8003
10.0.0.7 : 7001	128.97.36.96 : 8004

b)

1) msg rcv from host: MSG<10.0.0.6 : 5000, 172.217.11.78 : 80>
msg snt from router: MSG<128.97.36.96 : 8001, 172.217.11.78 : 80>

2) msg rcv from host: MSG<10.0.0.10 : 6000, 204.79.197.200 : 80>
msg snt from router: MSG<128.97.36.96 : 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) network layer uses upper layer header field

↳ next header : describes next header is UDP or TCP.

b) yes. ex: host is laptop or arduino; multiple network ports like ethernet + wifi each diff connection to link layer is a diff IP

c) Skype uses relaying in order to connect clients.

both hosts are NATed

1) establish connection to relay so can bridge/relay packets btwn connection

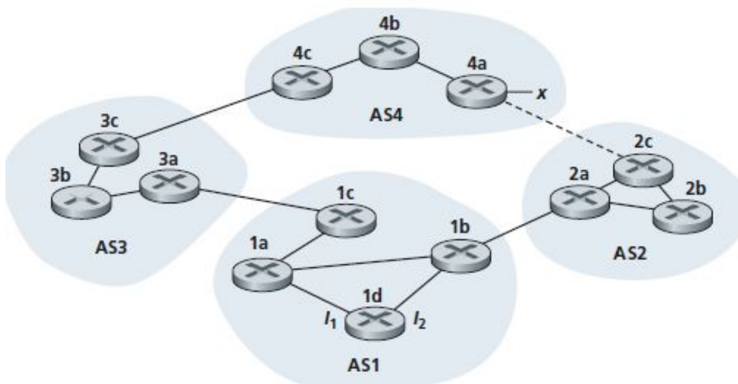
d) No. Point of NAT is security + limited IP from IPv4

IPv6 solves this.

NAT doesn't really solve this. NAT is actually very vulnerable b/c all traffic through 1 router → 1 router can collect private data.

Problem 3

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 4b learns about prefix x?

(b) Router 3c learns about prefix x?

(c) Router 3b learns about prefix x?

(d) Router 1d learns about prefix x?

Write your solution to Problem 3 in this box

a) iBGP

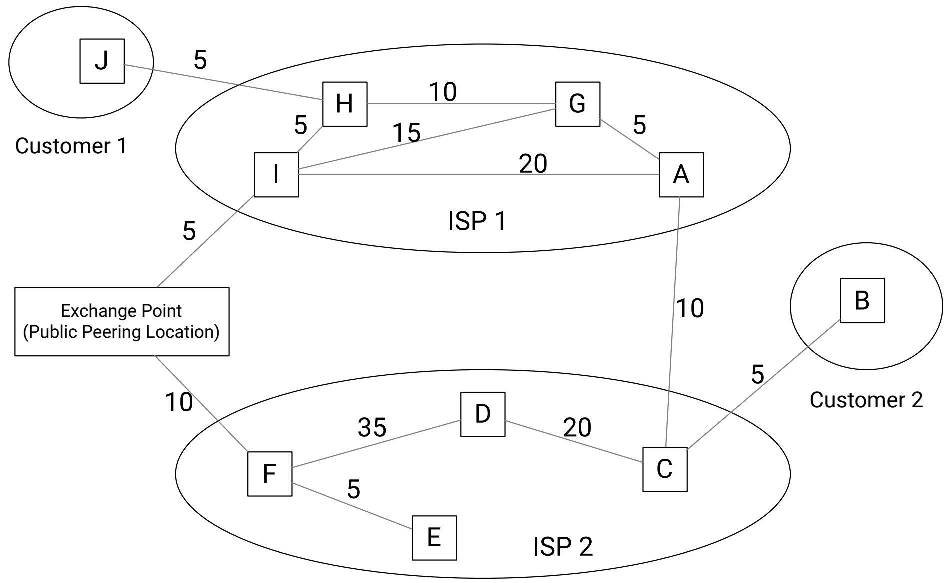
b) eBGP

c) iBGP

d) iBGP

Problem 4

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 4 in this box

a) 1 way prop delay = 8+5+5+10+35+20+5 = $\boxed{\text{85 msec,}}$ b/w 1 & 2

b) asymmetric, between 2 and 1 is: 5+10+5+10+5 = 35 ms.

c) Hot potato routing chooses local gateway w/ least intradomain cost. → cost metric organization affects propagation delay

Problem 5

In this problem, you will derive the efficiency of a CSMA/CD like multiple access protocol. In this protocol, time is slotted and all adapters are synchronized to the slots. Unlike slotted ALOHA, however, the length of a slot (in seconds) is much less than a frame time (the time to transmit a frame). Let S be the length of a slot. Suppose all frames are of constant length $L = kRS$, where R is the transmission rate of the channel and k is a large integer. Suppose there are N nodes, each with an infinite number of frames to send. We also assume that $d_{prop} < S$, so that all nodes can detect a collision before the end of a slot time. The protocol is as follows:

- If for a given slot, no node has possession of the channel, all nodes contend for the channel; in particular, each node transmits in the slot with probability p. If exactly one node transmits in the slot, that node takes possession of the channel for the subsequent $k - 1$ slots and transmits its frame.
- If some node has possession of the channel, all other nodes refrain from transmitting until the node that possesses the channel has finished transmitting its frame. Once this node has transmitted its frame, all nodes contend for the channel.

Note that the channel alternates between two states: the productive state, which lasts exactly k slots, and the non-productive state, which lasts for a random number of slots. The channel efficiency is defined as the ratio of $k/(k + x)$, where x is the expected number of consecutive non-productive slots.

(a) For fixed N and p, determine the efficiency of this protocol.

(b) For fixed N, determine the p that maximizes the efficiency.

Write your solution to Problem 5 in this box

a) P(success for one time slot)

$$S = Np(1-p)^{N-1} \rightarrow P(Z = m) = S(1-S)^{m-1}$$

$$E[X] = E[Z] - 1 = \frac{1-S}{S} = \frac{1 - Np(1-p)^{N-1}}{Np(1-p)^{N-1}}$$

$$\mathcal{E} = \frac{k}{k+X} = \frac{k}{k + \frac{1-Np(1-p)^{N-1}}{Np(1-p)^{N-1}}}$$

b) $\max \mathcal{E} \Rightarrow \max S$

$$\downarrow$$

$$\frac{d}{dp}\left(Np(1-p)^{N-1}\right) = 0 \rightarrow N(1-p)^{N-1} = Np(1-p)^{N-2}(N-1)$$

$$\downarrow$$

$$1-p = p(N-1)$$

$$\boxed{p_{max} = \frac{1}{N}}$$