1. On the left are listed three ways of identifying computers for network communication. Match them to a correct description from the right:

- a. MAC address
- b. IP address
- c. domain name

1. can be changed, used by the Internet Layer
2. easy for people to remember, but cannot be used directly to communicate between hosts
3. unchangeable, used by the Link Layer

2. Consider the following two hosts:

<table>
<thead>
<tr>
<th>Host A</th>
<th>Host B</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address: 145.38.22.11</td>
<td>IP address: 145.38.20.75</td>
</tr>
<tr>
<td>Subnet mask: 255.255.252.0</td>
<td>Subnet mask: 255.255.252.0</td>
</tr>
</tbody>
</table>

Use the Network Address Calculator found on the course Resources page to answer the following: Are A and B on the same network? Explain how you arrived at your answer!

3. Pull up the demo page [http://rona.cs.usna.edu/~si110/resources/netdemo/Networking.html](http://rona.cs.usna.edu/~si110/resources/netdemo/Networking.html) and click on Host 1 and Host 3. Then step carefully through the demo. Note: you may want to use ctrl-minus to shrink the text size until everything fits nicely on your screen.

Consider the following three hosts.

<table>
<thead>
<tr>
<th></th>
<th>Host X</th>
<th>Host Y</th>
<th>Host Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>145.38.22.11</td>
<td>145.38.20.75</td>
<td>87.210.100.17</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.252.0</td>
<td>255.255.252.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway Router</td>
<td>145.38.20.75</td>
<td>145.38.20.75</td>
<td>87.210.100.5</td>
</tr>
</tbody>
</table>

If host X wants to send the message "foobar" to host Z, which of the below describes what X sends to its switch? Explain your answer!

a. packet 145.38.20.75:foobar to MAC address EE-46-02-72-39-B3
b. packet 87.210.100.17:foobar to MAC address E6-00-6A-FB-39-1D
c. packet 87.210.100.17:foobar to MAC address EE-46-02-72-39-B3
d. packet 145.38.20.75:foobar to MAC address E6-00-6A-FB-39-1D
4. Pull up the network address translation demo at

http://rona.cs.usna.edu/~si110/resources/netdemo/privateIP.html

and step carefully through the demo. Now, here’s the question: Midshipman X and Midshipman Y point their browsers at ipchicken.com at the same time. What each of them sees is shown below.

Midshipman X sees this

Midshipman Y sees this

a. The IP Address of the USNA server that’s doing the network address translation

b. The ipchicken.com webserver sends the packet shown here back to USNA. This packet is being sent back to which host? (I.e. is it Mid X or Mid Y)? How do you (and, more importantly, the network address translation server!) know?

5. Consider the network shown below, with four regular hosts and a router all connected to a switch. Suppose a bad guy is able to observe all the traffic along the cable from the switch to the router.

**Scenario A:** one host contacts an external webserver using HTTPS. Recall, this means that HTTP data is encrypted before it’s given to the transport layer to send to a webserver host on port 443.

**Scenario B:** once again, one host contacts an external webserver using HTTPS, but in this scenario all data is also encrypted as it is passed between the Internet and Link layers, which means the entire packet is encrypted before it is sent across the wire to the switch. What information can the attacker learn in Scenario A that he can’t in Scenario B? Hint: review the demo page from #3.