1. Do a page check: you should have 8 pages including this cover sheet.
2. You have 50 minutes to complete this exam.
3. A calculator may be used for this exam.
4. This is a closed book and closed notes exam. You may use two single-sided hand-written pages of notes.
5. Turn in your two single-sided hand-written pages of notes with your exam.
6. This exam may be given as a makeup exam to several midshipmen at a later time. No communication is permitted concerning this exam with anyone who has not yet taken the exam.

Name:  

Instructor:  

| 4-bit pattern | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
|---------------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| hex digit     | 0    | 1    | 2    | 3    | 4    | 5    | 6    | 7    | 8    | a    | b    | c    | d    | e    | f    |
| Dec Hex Char  |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
| 32           | 00   | 01   | 02   | 03   | 04   | 05   | 06   | 07   | 08   | 09   | 0a   | 0b   | 0c   | 0d   | 0e   | 0f   |
| 20           | 10   | 11   | 12   | 13   | 14   | 15   | 16   | 17   | 18   | 19   | 1a   | 1b   | 1c   | 1d   | 1e   | 1f   |
| !            | 20   | 21   | 22   | 23   | 24   | 25   | 26   | 27   | 28   | 29   | 2a   | 2b   | 2c   | 2d   | 2e   | 2f   |
| "            | 30   | 31   | 32   | 33   | 34   | 35   | 36   | 37   | 38   | 39   | 3a   | 3b   | 3c   | 3d   | 3e   | 3f   |
| #            | 40   | 41   | 42   | 43   | 44   | 45   | 46   | 47   | 48   | 49   | 4a   | 4b   | 4c   | 4d   | 4e   | 4f   |
| $            | 50   | 51   | 52   | 53   | 54   | 55   | 56   | 57   | 58   | 59   | 5a   | 5b   | 5c   | 5d   | 5e   | 5f   |
| %            | 60   | 61   | 62   | 63   | 64   | 65   | 66   | 67   | 68   | 69   | 6a   | 6b   | 6c   | 6d   | 6e   | 6f   |
|             | 70   | 71   | 72   | 73   | 74   | 75   | 76   | 77   | 78   | 79   | 7a   | 7b   | 7c   | 7d   | 7e   | 7f   |
|             | 80   | 81   | 82   | 83   | 84   | 85   | 86   | 87   | 88   | 89   | 8a   | 8b   | 8c   | 8d   | 8e   | 8f   |
|             | 90   | 91   | 92   | 93   | 94   | 95   | 96   | 97   | 98   | 99   | 9a   | 9b   | 9c   | 9d   | 9e   | 9f   |
|             |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |      |
Question 1 (16 pts). Suppose you know that one of your organization’s IP addresses is \textit{205.16.37.39/28}.

(a) (4 pts) What is the network mask in dotted decimal notation? Show work.

**Mask is /28.** Mask in binary is \textit{11111111.11111111.11111111.11110000}.

Converting to decimal: \textit{255.255.255.240}.

Use judgment on the "show work" portion.

(b) (4 pts) What is the network address (the network ID) in dotted decimal notation? Show work.

**Mask falls in the last octet.**

Last octet of IP address: \textit{39} = \textit{0 0 1 0 0 1 1 1}.

Last octet of mask: \textit{1 1 1 1 0 0 0 0}.

Bitwise AND-ing: \textit{0 0 1 0 0 0 0 0}.

Last octet is decimal 32.

Network ID is \textit{205.16.37.32}.

Use judgment on the "show work" portion.

(c) (4 pts) How many total addresses are available for assignment to hosts on this network? Show work.

There are 4 bits in the host-ID portion of the address.

Thus there are \textit{2^4 - 2 = 14} addresses available for assignment.

\textbf{1 point deduction} for an answer of 15 or 16.

Use judgment on the "show work" portion.

(d) (4 pts) Assume that host IP addresses are assigned sequentially from lowest to highest on your network. What is the last valid IP address that can be assigned to a host on your network expressed in dotted decimal form? Show work.

Focus on the last octet.

Last octet in Network ID is 32 and the mask falls between the fourth and fifth bits in this octet:

\begin{center}
\begin{tabular}{c c c c c c c c c c}
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{tabular}
\end{center}

Network ID Host ID

Filling the host bits with 1's except for the rightmost bit yields the last address available for a host:

\begin{center}
\begin{tabular}{c c c c c c c c c c}
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0
\end{tabular}
\end{center}

Network ID Host ID

Converting this to decimal: 46. Last address assignable to a host is: \textit{205.16.37.46}.

\textbf{1 point deduction} for an answer of \textit{205.16.37.47}. 
Question 2 (6 pts). Consider the small network shown below. The network has 4 users, for which the IP addresses and Ethernet addresses are shown.

The ARP cache for all users is shown in the table below:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Ethernet Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>W</td>
</tr>
<tr>
<td>B</td>
<td>X</td>
</tr>
<tr>
<td>C</td>
<td>Y</td>
</tr>
<tr>
<td>D</td>
<td>Z</td>
</tr>
</tbody>
</table>

MIDN Evil Jose would like to launch an ARP spoofing attack on MIDN Joyous, thereby stealing MIDN Joyous's traffic. Make the necessary change(s) to the table above that would cause all of MIDN Joyous's traffic to flow to MIDN Evil Jose instead.

Answer:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Ethernet Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>W</td>
</tr>
<tr>
<td>B</td>
<td>Z</td>
</tr>
<tr>
<td>C</td>
<td>Y</td>
</tr>
<tr>
<td>D</td>
<td>Z</td>
</tr>
</tbody>
</table>

3-point deduction for any answer that has Ethernet address Z in multiple columns, for example:
**Question 3 (8 pts).** Construct the full routing table for Router RA in the network shown. Show your answer in the table below (filling in the Next-Hop Address if applicable). Note that your answer might not require filling in every line of the table.

<table>
<thead>
<tr>
<th>Mask</th>
<th>Network Address</th>
<th>Next-Hop Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>/28</td>
<td>1.1.1.0</td>
<td>--</td>
<td>m1</td>
</tr>
<tr>
<td>/26</td>
<td>2.2.2.0</td>
<td>--</td>
<td>m2</td>
</tr>
<tr>
<td>/24</td>
<td>3.3.3.0</td>
<td>--</td>
<td>m3</td>
</tr>
<tr>
<td>/0</td>
<td>0.0.0.0</td>
<td>2.2.2.2</td>
<td>m2</td>
</tr>
</tbody>
</table>

Award 0.5 points for each correct answer for each of the 4 entries in columns 1, 2 and 4.

For column 3: Award 1 point for correct last entry (2.2.2.2) and 1 point for the correct answer for the first three entries in this column.

If entries are correct except rows are not ordered in descending-mask order: 3 point deduction.
**Question 4 (10 pts).** Consider the network shown below, where the numbers on the edges indicate the cost of using that edge. For example, the cost of using the link from Router A to Router B is 10. The network uses link state routing.

(a) (2 pts) Which routers in the network ultimately receive the Link State Packet sent by Router G?

Answer: **All of them. NPC.**

(b) (8 pts) Sketch the routing table for Router A. Your table should have three columns: "Destination", "Total Cost" and "Next Hop".

Answer:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Total Cost</th>
<th>Next-Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>6</td>
<td>G</td>
</tr>
<tr>
<td>C</td>
<td>4</td>
<td>C</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
<td>D</td>
</tr>
<tr>
<td>G</td>
<td>1</td>
<td>G</td>
</tr>
</tbody>
</table>
**Question 5 (19 pts).** An attacker is located on the 3.4.5.0/25 network and wants to prevent midshipmen from reaching a website at 8.9.7.104. He turns his computer into a router using Loki and advertises a false network to router RA.

In the table below, under the target's network (8.9.7.64), the bit values corresponding to each octet have been filled in. Additionally, under the target's IP address (8.9.7.104), the bit values corresponding to each octet have been filled in.

(a) (3 pts) In the table below, draw a dashed vertical line showing where the mask for the target's network divides the address (i.e., draw a dashed line showing where the network-ID bits end and the host-ID bits begin).

![Diagram](image)

<table>
<thead>
<tr>
<th>Target’s Network</th>
<th>8 .</th>
<th>9 .</th>
<th>7 .</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00001000</td>
<td>00001001</td>
<td>00001110</td>
<td>10000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target’s IP Address</th>
<th>8 .</th>
<th>9 .</th>
<th>7 .</th>
<th>104</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00001000</td>
<td>00001001</td>
<td>00001110</td>
<td>10101000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attacker’s Lie</th>
<th>. . .</th>
</tr>
</thead>
</table>

Answer: Line is drawn here! NPC.
(b) (8 pts) Design the false network! Specifically, state the network ID for the false network you would use. Use the table above to show your work. Your answer should be of the form W.X.Y.Z/n.

Answer:

One correct answer is 8.9.7.96/27 where students show their work by filling in the table showing:

- The mask (shown below as a vertical line) (2 pts – but give the student full credit if they simply give the mask in the CIDR notation for the fake network’s address)
- The proper bit entries in the first three octets (1 pt)
- The entries in the fourth octet where the bits match the target’s IP address up to the mask, and are zeros after the mask (5 pts – use judgment in awarding points, realizing that the student must somehow convey their reasoning.)

<table>
<thead>
<tr>
<th>Target's Network</th>
<th>8</th>
<th>9</th>
<th>7</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>000011000000100100000111010000000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target's IP Address</td>
<td>8</td>
<td>9</td>
<td>7</td>
<td>104</td>
</tr>
<tr>
<td>000011000000100100000111011010000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attacker's Lie</td>
<td>8</td>
<td>9</td>
<td>7</td>
<td>96</td>
</tr>
<tr>
<td>000011000000100100000111011010000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The answer 8.9.7.96/28 should also be accepted (where the proper work is shown).

(c) Briefly explain why your attack as specified in part (d) is successful. Specifically:

(i) (3 pts) Why does router RA believe the attacker's fake network advertisement?

Answer:

Use judgment in grading. Student must convey the idea: "Routers trust each other… Routers trust the information received from other routers."

(ii) (3 pts) Why does the fake network information that is entered into the routing table for router RA override the target network?

Answer:

Use judgment in grading. Student must convey the idea: "The fake network has a larger mask, so will appear higher in Router RA's routing table. Since routers make routing decisions starting at the top of the routing table and working downward, packets destined for 8.9.7.104 will be routed to the fake network which appears higher in the routing table."

(d) (2 pts) Ward Hall detects that traffic is being misdirected by an attacker and decides to protect router RA by establishing a passive interface on one of router RA's ports. Which port should ITSD establish the passive interface on (chose one from the list below)?

(i) eth0
(ii) eth1
(iii) eth2
(iv) None of the above
Question 6 (8 pts). There are four users on a Linux system: root, midshipman, jose and joe. Consider the long listing for two files shown below. Note that the program note2.exe writes to the file named /tmp/notes.

```
midshipman@EC310:/work $ ls -l /tmp/notes note2.exe
-rwsr-xr-x 1 midshipman midshipman 7525 2014-10-17 08:05 note2.exe
-rw------- 1 midshipman midshipman 10 2014-10-17 08:02 /tmp/notes
```

(a) (4 pts) Can jose read the file /tmp/notes by entering: `cat /tmp/notes`? Briefly explain.

Answer:

No. jose does not have read permission for this file.

Award 2 points for the answer "No" and award two points for the correct reasoning.

(b) (4 pts) Examining the permissions above, explain how the permissions to the files either do or do not allow jose to somehow successfully write to the file /tmp/notes without using sudo?

Answer:

Use judgment in grading. The student's thought process should somehow convey the following reasoning (hopefully more succinctly):

- Notice that note2.exe (which writes to /tmp/notes) has the setuid flag set.
- This means that anyone executing note2.exe is executing this program as though they were the owner of the program.
- The owner of note2.exe is midshipman.
- midshipman has permission to write to /tmp/notes.
- Thus jose is able to write to the file /tmp/notes via execution of note2.exe.
Question 7 (15 pts). Consider the C program shown below on the left. Evil Jose is running this program.

```c
#include<stdio.h>
void fun( int value )
{
    char mid_name[ 10 ];
    printf( "Enter your name: ");
    scanf( "%s" , mid_name );
}
int main( )
{
    int value = 2016;
    fun( value );
}
```

Evil Jose would like to launch a buffer overflow attack by entering an evil exploit into memory, and then causing his evil exploit to execute. Evil Jose decides that when he sees the prompt

```
Enter your name:
```

he will enter his evil exploit into memory. The evil exploit is 12-bytes long.

The stack at the point in time where Evil Jose is prompted to enter his name is shown below. Since we are in the function `fun`, this is the stack frame for `fun`. Note the location where `mid_name` is stored.

(a) (3 pts) Suppose Evil Jose has perfect knowledge of the stack shown on the left. Evil Jose starts entering his 12-byte exploit at the location where `mid_name` is stored. The correct value of the return address is stored at `bffff80c`. If Evil Jose wishes to execute a buffer overflow and cause his 12-byte exploit to run, what address must be used to overwrite the correct return address stored at location `bffff80c`? Choose one:

(i) `bffff7d0`  
(ii) `bffff7d8` **NPC**  
(iii) `bffff7e0`  
(iv) `bffff804`  
(v) `bffff80c`

(b) (8 pts) In real life Evil Jose does not have perfect knowledge of the stack (he does not know exactly where the return address is stored on the stack and does not know the exact value to place in the return address field). List and briefly describe two tools that Evil Jose can use to successfully execute his buffer overflow. Place your answer in the table below.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Table Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOP Sled (2 pts)</td>
<td>The NOP sled lets the hacker be a little bit off with the return address. The return address just has to point anywhere within the NOP sled. (2 pts – use judgment).</td>
</tr>
<tr>
<td>Repetition of the return address (2 pts)</td>
<td>Repeating the return address gives the hacker a number of chances to get the address correctly positioned in the return address field. (2 pts – use judgment).</td>
</tr>
</tbody>
</table>
(c) (4 pts) Now, continuing this problem, suppose that the programmer is using a canary to guard against a buffer overflow attack. Referring to the picture of the stack, select from the choices below the best address where the canary should be stored (choose one):

(i) bffff7d0
(ii) bffff7d8
(iii) bffff7e0
(iv) bffff804 **NPC**
(v) bffff810
Question 8 (18 pts total; 2 pts each part). Consider the 10 Mbps Ethernet used by the ten users shown below. Note that users A and B are marked below.

(a) What layer of the TCP/IP reference model does the **hub** operate at? Answer:

**Physical (NPC)**

(b) What is the effective data rate seen by User A? Answer:

\[
\frac{10 \text{ Mbps}}{10 \text{ users}} = 1 \text{ Mbps} \quad \text{(NPC)}
\]

(c) What is the effective data rate seen by User B? Answer:

1 Mbps (NPC, but give full credit if the student provides the same incorrect answer as in part (a))

Suppose now the hub is replaced by a bridge.

(d) What layer of the TCP/IP reference model does the **bridge** operate at? Answer:

**Data Link (NPC)**

(e) What is the effective data rate seen by User A? Answer:

\[
\frac{10 \text{ Mbps}}{4 \text{ users}} = 2.5 \text{ Mbps} \quad \text{(1 point deduction for the answer 3.33 Mbps. Otherwise, NPC)}
\]

(f) What is the effective data rate seen by User B? Answer:

\[
\frac{10 \text{ Mbps}}{3 \text{ users}} = 3.33 \text{ Mbps} \quad \text{(1 point deduction for the answer 5 Mbps. Otherwise NPC)}
\]

**Question 8 Continues on Reverse Side of this Page**
An Ethernet frame now arrives at the bridge from User A. Shown below is a Wireshark capture of this frame. Neglecting the bits added by the physical layer, the Ethernet frame begins:

```
ff ff ff ff ff ff 00 04 75 c8 d5 dc 08 06 00 01
```

(g) How many bits are in User A's Ethernet address? Answer: 48 bits (NPC)

(h) What is User A's Ethernet address in hexadecimal? Answer: 00 04 75 c8 d5 dc (NPC)

(i) Explain what the bridge does with this received frame.

Answer:

Since the destination is the broadcast address, the bridge will forward the frame to the other three ports so that all users receive the frame.

Give full credit for words to the effect: The bridge forwards the frame on all ports/outgoing lines.

Turn in your equation sheet with your exam!