# ISEC 325 Homework 01

Answer the following questions based on your reading of the text books, the module key points, and the instructor's presentation this week.

1. [10 points] For each layer of the TCP/IP model (layers 7, 4, 3, and 2 in the OSI model) describe the following
    - The responsibilities of that particular layer
    - Significant protocols at that layer (only for 4 and 3)
    - The protocol data unit name and pertinent fields of that layer
    - Addressing and delivery methods of that layer
    - The standards body most relevant to the layer

**Layer 2**- Network Access Layer, the Data Link and Physical Layers in OSI model

- Formats data into frames, interfaces network adapters and error checks
- The protocol data units are Frames and Bytes
- Physical addressing converting MAC addresses into IP addresses
- Uses ARP (Address Resolution Protocol) and RARP(Reverse Address Resolution Protocol)

**Layer 3**- Internet Layer, is the Network Layer in OSI

- Where addresses are applied so that routing is possible, attaches an IP header onto the data
- Significant protocols for the layer are IP, ICMP, IPsec, and IPv6
- The protocol data unit is the packet or datagram
- Addresses with the Internet Protocol
- The Internet Layer uses ARP and RARP standards

**Layer 4**- Transport Layer

- Ensures reliable delivery of packets and error recovery, where segmentation occurs
- Significant protocols for the layer are TCP, UDP
- The protocol data unit is the segment
- Addresses with Ports and Sockets
- TCP (transmission control protocol) and UDP (User datagram protocol)

**Layer 7**- Application or Application, Presentation and Session layer in OSI model

- Provides enhanced session services, where encryption and encoding occurs, where applications interface with the user.
- The protocol data unit is data

- Addresses with Application Programming Interface or API
- DNS, HTTP, FTP and STMP

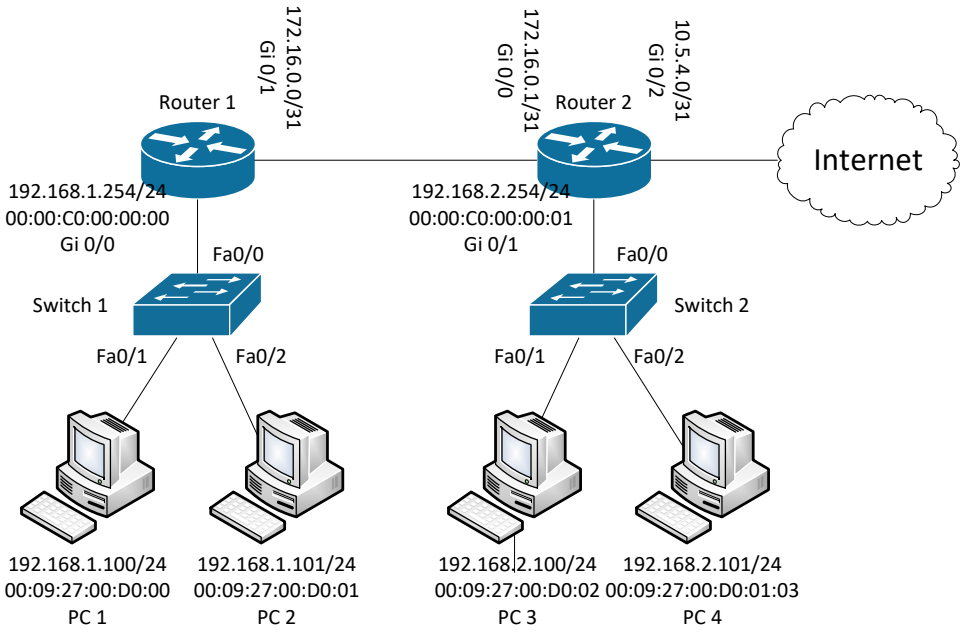
2. [3 points] Each layer of the TCP/IP model has a different addressing schema. For each layer of the TCP/IP model (layers 7, 4, 3, and 2 in the OSI model), how are addresses resolved and PDUs delivered? Frame your answer in the context of an HTTP GET request on an Ethernet network for http://cs.franklin.edu/isec/chart.php.
   Application- (data) has no addressing schema
   Transport- (segments) addresses with the http in the address
   Internet- (packets) addresses with the ip address assigned to cs.franklin.edu/isec/chart.php which is 199.30.211.241-1
   Network- (frames) addresses to the mac addresses of the physical components used.

3. [2 points] What is the binary subnet mask for the IP address of 172.16.55.131/25? What is the decimal subnet mask?

   The binary subnet mask would be 10101100. 00010000. 00110111. 1 00011001

   The decimal subnet mask would be 255.255.255.128 = 25

4. [10 points] Consider the following diagram of a small network




- Describe the mechanism and path (e.g. any lookups, switching, routing, resolutions, etc.) for PC1 to communicate with PC2.

PC1 192.168.1.100/24 looks up PC2 192.168.1.101/24 using ARP and goes from Fa0/1 Switch 1 which looks up PC2 by its MAC address 00:09:27:00:D0:01 using ARP to Fa0/2 to PC2 192.168.1.101.

- Describe the mechanism and path (e.g. any lookups, switching, routing, resolutions, etc.) for PC1 to communicate with PC3.
  PC1 192.168.1.100/24 looks up PC 3 192.158.2.100/24 with ARP and goes from Fa0/1 to Switch 1 which looks up PC3 with ARP and sends the datagram to Router 1 00:00:C0:00:00:00 to Fa0/0 to Router 1 192.168.1.254/24 which looks up PC3 192.168.2.100/24, 00:09:27:00:D0:02 with ARP which has the next step route of Router 2 192.168.2.254/24,00:00:C0:00:00:01 and goes from gateway 172.16.0.0/31 to gateway 172.16.0.1/31 to Router 2 192.168.2.254/24, 00:00:C0:00:00:01 which looks up PC3 192.168.2.100/24,00:09:27:00:D0:02 with ARP to Switch 2 through Fa0/0 Switch 2 looks up PC3 by MAC address 00:09:27:00:D0:02 with ARP to Fa0/1 to PC3 192.168.2.100/24.
- Show the routing table for Router 2 with columns for port, network, and gateway

| Port | Network | Gateway |
|---|---|---|
| Gi 0/1 | 192.168.1.100/24 | 172.16.0.0/31 |
| Gi 0/1 | 192.168.1.101/24 | 172.16.0.0/31 |
| Fa 0/1 | 192.168.2.100/24 | Direct delivery |
| Fa 0/1 | 192.168.2.101/24 | Direct delivery |

- Show the switching table for Switch 1 with columns for destination address and destination port.

| Destination Address | Port |
|---|---|
| 00:00:C0:00:00:00 | Gi 0/0 |
| 00:09:27:00:D0:00 | Fa 0/1 |
| 00:09:27:00:D0:01 | Fa 0/2 |

- What might the ARP cache of PC3 look like?
  Interface 192.168.2.100.124

| Internet Address | Physical Address | Type |
|---|---|---|
| 192.168.1.100/24 | 00:09:27:00:D0:00 | Dynamic |
| 192.168.1.101/24 | 00:09:27:00:D0:01 | Dynamic |
| 192.168.2.101/24 | 00:09:27:00:D0:01:03 | Dynamic |
| 192.168.2.254/24 | 00:00:C0:00:00:01 | Dynamic |

5. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you're still confused about. In other words, you should think and write critically not just

about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

This class week has been a nice review of the OSI/ TCP/IP models and the protocols that they use to communicate and deliver information. I have an associate's degree from ITT Tech in Network Systems Administration. We did not go as far in-depth term/verbiage book wise of the OSI model and how the process is laid out. We did cover it, but it seems like more of a brush over than this review. We spent most of our time in lab environments, the book side was very light. I wish I would have taken all my classes here to be honest. I am not lost I understood everything, but it is a bit rusty as I worked with this stuff two years ago. I have a deeper understanding of each of the layers and how they work. I have several questions to ask you at next weeks meet to make sure I am clear. I don't have a textbook to look back at, so I did most of my research from your MEET presentation.

We covered the OSI model and the TCP/IP model. We went through each layer explaining their responsibilities and the protocols that they follow. It was the first time that I understood how data/bytes are formed into packets with headers and then segments to be transmitted between two computers and the first time that windowing was explained to me. We covered binary and subnetting at ITT, but I never clearly understood it. I understand it a bit more now, but I did use an ip to subnet calculator for my answers. I am very interested to see how to protect attackers from packet injection and how attackers use malicious packets to gain access into a network. It was cool to look at routing tables and see how they worked. The ARP table was interesting as well and I can now see how they accomplish an ARP poisoning attack.

I am looking forward to the rest of this class, I really love cyber security. I may end up asking a lot of questions. I don't have any formal IT experience I am a technician at a company that makes bottled water and trying to change my career to something I am interested in and enjoy doing. I don't have the same background as many of the others and may need insight to draw the big picture in my head. I read a lot of cybersecurity books and follow cyber security pages on Instagram and reddit so I am pretty familiar with the subject coming back and looking at the OSI/ TCP/IP models with a cybersecurity eye is pretty cool it makes the subject matter much more interesting.

# References

Jodies, K. (2000-2011). *IP Calculator*. Retrieved from IP Calculator: http://jodies.de/ipcalc

Quine, A. (2008, January 27). *How the Network Access Layer Works*. Retrieved from ITPRC IT Professional's Resource Center: https://www.itprc.com/the-network-access-layer/

*tcp-flash-cards*. (2020). Retrieved from Quizlet.

*Whois Lookup*. (2020). Retrieved from Whois Lookup.