## **Activity File: Networking Review**

### **Part One: HTTP**

Open reviewpackets.pcap.

* Filter for HTTP traffic.
* Make sure Name Resolution for Resolving Network Addresses is enabled.
* There should be four HTTP packets.

A. Answer the following questions on HTTP:

1. What does HTTP stand for?
   1. Hyper Text Transfer Protocol
2. What is the port number for HTTP?
   1. Port 80
3. What types of services does HTTP provide?
   1. Communicating and accessing resources on the internet
4. Which OSI layer does HTTP exist in?
   1. Layer 7: Application
5. What website is being accessed?
   1. example.com
6. What is the source port being used?
   1. 58424
7. What is the the port number range that this port is part of?
   1. This is a private port

B. Select packet number 419, which should be the first HTTP packet. View the packet details to answer the following questions:

* Under Ethernet II is a value of Destination: Technico\_65:1a:36 (88:f7:c7:65:1a:36)  
  1. What does this value represent?
     + Mac address
  2. Which OSI layer does this exist in?
     + Layer 2 data link
  3. What networking devices use these values?
     + Switches and NICs

### **Part Two: ARP**

Continue viewing the same PCAP.

* Filter for ARP traffic.
* There should be 115 ARP packets.

A. Answer the following questions on ARP:

1. What does ARP Stand for?
2. What service does ARP provide?
3. Which OSI layer does ARP exist in?
4. What type of networking request does ARP first make?

B. Use a filter to find the count of ARP responses, and answer the following questions:

1. What is the IP of the device that is responding?
2. To what IP is the device responding to?
3. Write out in simple terms what has taken place, describing the request and response.

### **Part Three: DHCP**

Continue viewing the same PCAP.

* Filter for DHCP traffic.
* There should be four DHCP packets.

A. Answer the following questions on DHCP:

1. What does DHCP stand for?
2. What service does DHCP provide?
3. Which OSI layer does DHCP exist in?
4. What are the four steps of DHCP?

B. Use a filter to view the DHCP Discover, and answer the following questions on that packet:

1. What is the original source IP?
2. Why does it have that value?
3. What is the original destination IP?
4. What does that value signify?

C. Use a filter to view the DHCP ACK, and answer the following questions on that packet.

1. Explain in simple terms what is happening in this packet.
2. Define the term "DHCP lease."
3. What is the DHCP lease time provided in this packet?

### **Part Four: TCP and UDP**

Continue viewing the same PCAP.

* Filter for the following IP Address: 185.42.236.155.
* There should be five packets.

A. Answer the following questions on TCP:

1. What does TCP stand for?
2. Is TCP connection-oriented or connection-less?
3. Which OSI layer does TCP exist in?
4. What are the steps in a TCP connection?
5. What are the steps in a TCP termination?
6. What steps appear in the packets displayed?
7. What type of activity/protocol is TCP establishing a connection for?
8. What is the website name being accessed after the TCP connection?

B. Answer the following questions on UDP:

1. What does UDP stand for?
2. Is UDP Connection oriented or connection-less?
3. What type of services would UDP provide a benefit for?

### **Part Five: Network Devices, Topologies, and Routing**

Open reviewdoc.pdf and answer the following questions:

* **Topologies**
  1. What are the Topologies for A, B, C?
  2. What are the advantages and disadvantages for each?
* **Network Devices**
  1. In the network devices illustration, what are numbers one through four?
  2. What does the dashed line represent in number five?
  3. What is a load balancer?
  4. Where would you place a load balancer?
* **Network Routing**
  1. Which routing protocols use distance as criteria?
  2. Which routing protocols use speed as criteria?
  3. Using the shortest number of hops, determine the shortest path from A to O.
  4. Using the least time, determine the shortest path from A to O.

### **Part Six: Network Addressing:**

Answer the following questions.

1. Define binary.
2. What are the two binary states?
3. What are IP addresses used for?
4. What are the two primary versions of IP addresses?
5. How many octects are in a IPV4 address?
6. Use a web tool to determine the IP of the following binary representation: 11000000.10101000.00100000.00101011
7. What is the difference between primary and public IP addresses?
8. What is CIDR?
9. What is the range of IP addresses in: 192.18.65.0/24?