Layer 3 Lab

Please use your VMs for this Lab  
In this lab, students will use Wireshark to learn more about:

• DHCP

* Host Routing Logic
* Routing Between LANs • DNS

Part 1 – DHCP

When your host boots, it uses the DHCP protocol to obtain networking configuration information including:

* IP Address
* Subnet Mask
* Default Gateway
* DNS Servers
* Domain Name

When the networking services are initialized during the boot process, your host broadcasts a DHCP **Discover**. This sends a broadcast to everything in your LAN that requests any listening DHCP servers to offer a set of configuration parameters. Any listening DHCP servers will reply to your host with a DHCP **Offer**. This offers a set of network configuration parameters for your host. Your host replies with a DHCP **Request** that lets the DHCP server know that your host would like the offered network configuration parameters. (Interestingly, this request is broadcast because if multiple DHCP servers send an offer, they will all get to find out which one your host selected.) Finally, the DHCP server sends a DHCP **Acknowledge** that lets your host know that its request has been confirmed. You can remember the sequence of events with the mnemonic DORA (Discover, Offer, Request, Acknowledge). To recap the sequence:

* 1. The client broadcasts a DHCP **Discover**
  2. The DHCP server sends a DHCP **Offer** to the client
  3. The client broadcasts a DHCP **Request**
  4. The DHCP server sends a DHCP **Acknowledge** to the client

In this part of the lab, you are going to use the dhclient command to release your current network parameters and then use dhclient again to request a new set using the DORA sequence. We’ll use Wireshark to see the details of this interaction.

1. Start a capture in Wireshark
2. Issue the following command in a terminal window:

sudo dhclient –r ens32

This command releases the IP address currently associated with interface ens32 on your virtual machine.

1. Next, issue a new DHCP request with the command:
2. sudo dhclient ens32
3. Stop the Wireshark capture and save the capture file. Name this file “dhcp”.
4. Find the frames associated with the DHCP request. You are looking for frames using the DHCP

protocol issuing the Discover, Offer, Request, and Acknowledge (DORA). If you want, you can filter the packets by entering bootp for the filtering criteria to help narrow down your search. DHCP is basically an extended version of the old BOOTP protocol.

1. Select the DHCP Offer frame and expand the Bootstrap Protocol information in the Wireshark Packet Details window.

**Q1.1: What IP address was offered to your client? (Look for “Your (client) IP address”.)**

**10.2.58.158**

**Q1.2: What Subnet Mask was offered to your client?**

**255.255.248.0  
Q1.3: What is the IP address lease time?**

**(777600s) 9 days  
Q1.4: What DNS servers are included in the offer? (List all of them.)**

**172.28.102.11**

**172.28.102.13**

**10.11.0.51**

**10.14.1.10**

**Q1.5: What is the default gateway? (It’s labeled “Router” in the Packet Details Window.)**

**10.2.56.1**

**Q1.6: What is the domain name?**

**hh.nku.edu**

Part 2 –Host Routing Logic

In this part of the lab, we are going to ping a VM in another LAN and examine the contents of the layer 2 and layer 3 addresses.

1. Open a terminal window by right-clicking on your VM’s desktop and select Open Terminal. Find your IP address.

**Q2.1: What is the IP address that is assigned to your ens32 interface?**

**10.2.58.158**

1. Start a new Wireshark capture on ens32.
2. From your terminal window, ping -c 1 10.2.64.11. This is the IP address of a VM that is in a different LAN from yours.
3. Stop and save the Wireshark capture. Name it “hostrouting”.

**Q2.3: Locate the ICMP echo request and echo reply in your Wireshark capture. Provide the following information:**

* **Source MAC address of the echo request:** 
  + **00:50:56:b9:03:5a**
* **Source IP address of the echo request:** 
  + **10.2.58.158**
* **Destination MAC address of the echo request:** 
  + **00:1d:71:f4:b0:00**
* **Destination IP address of the echo request:** 
  + **10.2.64.11**

1. **Q2.4:  What device is associated with the source IP address in the echo request?** 
   1. **Your computer**
2. **Q2.5:  What device is associated with the source MAC address in the echo request?** 
   1. **Your computer**

**Q2.6: What device is associated with the destination IP address in the echo request? (Hint: Look in step 3.)**

**A VM that is in a different LAN from yours**

**Q2.7: What device is associated with the destination MAC address in the echo request? Be careful here. It is not the same device that is associated with the destination IP.**

**The servers that the VM is running on**

**Q2.10: What is the IP address of the device associated with the destination MAC address of the ping?**

**10.2.64.11**

Part3–DNS

1. Start a new Wireshark capture on ens32.
2. In a terminal window, ping -c 1 example.com. Note that example.com is the name of an actual domain.
3. Stop your Wireshark capture and save it using the file name “dns”.
4. Examine the DNS requests and responses that were generated in your Wireshark capture. You may see several. This is because DHCP gave your computer more than one DNS server to use. Choose one DNS request and its associated response and answer the following questions:

**Q4.1: What is the Wireshark frame number for the DNS request?**

**Frames 218-221  
Q4.2: What is the Wireshark frame number for the DNS response?**

**Frame 222-226  
Q4.3: What is the IP address that the DNS response provided for example.com?**

**93.184.216.34**

**Please submit your Wireshark files as a single zipped file on Canvas**