Individual Assignment

Experiment 1 on DHCP

In order to observe DHCP in action, you will perform the following six steps and capture the DHCP messages exchanged as a result of executing these steps.

Below is the step-by-step procedure to down a wireless interface, start collecting packets using Wireshark, bring up the interface, stop capturing packets, and analyze DHCP IP address assignment using Wireshark commands:

Step-by-Step Procedure:

1. Disable Wireless Interface:

- Open a terminal on your Unix machine.
- Disable the wireless interface using the following command:

  sudo ifconfig `<wireless_interface_name>` *down*

  (Replace `<wireless_interface_name>` *with the name of your wireless interface (e.g., wlan0))*

2. Start Wireshark Capture:

- Open Wireshark on your Unix machine.
- Start capturing packets on the disabled wireless interface:
  - Go to Capture > Options.
  - Select the interface corresponding to the wireless interface.
  - Configure capture filters to capture DHCP packets only if desired.
  - Start the capture.

3. Enable Wireless Interface:

- After starting the capture, re-enable the wireless interface using the following command:
  sudo ifconfig `<wireless_interface_name>` *up*
  (Replace `<wireless_interface_name>` with the name of your wireless interface.)

4. Continue Capturing Packets:

- Let Wireshark continue capturing packets for a desired duration, during which DHCP packets will be captured as well.

5. Stop Wireshark Capture:

- After capturing packets for the desired duration, stop the Wireshark capture:
- Go to Capture > Stop.

6. Save Captured Packets:

- Save the captured packets to a file for analysis:
  - Go to File > Save As.
  - Choose a location and filename as <*RollNo_DHCP.pcapng*> to save the capture file.

Answer the following questions from the captured packet trace:

1. Are DHCP messages sent over UDP or TCP?

2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicate the source and destination port numbers.

3. What is the link-layer (e.g., Ethernet) address of your host?

4. What values in the DHCP discover message differentiate this message from the DHCP request message?

5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What is the purpose of the Transaction-ID field?

6. For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

7. What is the IP address of your DHCP server?

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

9. Explain the purpose of the lease time. How long is the lease time in your experiment?

10. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

You need to upload Deliverables in Eduserver as a tarball with the following:

- Captured wireshark packet trace.
- A readable PDF Report (with name “WiresharkDHCP-<RollNo>.PDF”) with the answers for the aforementioned questions on the captured packet trace.