Kadejha Jones

Shane McDonough

Shawn Ching

Lab 4

Our address 10.100.100.140

Link ether: f4:4d:30:6a:a4:76

Name of the interface for the 10.100.100 network enp3s0

1. View your ARP table on the `main` NUC, save it in the qanda
   a. 10.31.0.1 dev wlp2s0 lladdr 94:24:e1:ae:bc:db STALE
      10.100.100.120 dev enp3s0 lladdr f4:4d:30:6a:9c:db STALE
      10.31.254.250 dev wlp2s0 lladdr 00:1a:1e:05:09:00 STALE
2. Start capturing in Wireshark on the ethernet interface on the NUC
3. Make sure the table in front/behind you is ready and is also capturing packets
4. Ping your neighbors `main` NUC
   a. Stop the ping after a few successes (Ctrl-C)
   b. Stop your wireshark capture
5. View your ARP table again, save it in the qanda
   a. 10.31.0.1 dev wlp2s0 lladdr 94:24:e1:ae:bc:db REACHABLE
      10.100.100.120 dev enp3s0 lladdr f4:4d:30:6a:9c:db STALE
      10.31.254.250 dev wlp2s0 lladdr 00:1a:1e:05:09:00 STALE
6. Does the IP address match what you have pinged?

    a. Yes, it does still match.
7. What is the ethernet address for the new IP address?
    a. f4:4d:30:6a:9c:db
8. Does it match your neighbors?
    9. Wireshark
        a. Write a filter to show both `arp` and `icmp` packets (probably an OR statement)
            1. arp || icmp
        b. What was the ARP request and response sent *before* your ICMP ECHO?
            1. Who has 10.100.100.120? Tell 10.100.100.140
            2. 10.100.100.120 is at f4:4d:30:6a:9c:db
        c. If you have no ARP data, it's possible the ARP entry was already in your table. Let me know if this happens to you
            1. Didn't happen in our experience.