FIT9137 Workshop Week 8

Topics

- Network Layer:
  - Address Resolution
  - Dynamic Addressing of IP addresses

Covered Learning Outcomes:

- Analyse and formulate the functions and architectures of (wireless) local area networks, wide area networks and the Internet.
- Examine networks using the underlying fundamental theories, models, and protocols for data transmission.

Instructions

- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 4-5 students to work through the exercises. If met a problem, try to solve it by asking direct questions to your peer. If the issue was not solved within peers, ask your tutor. If did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

ACTIVITY A: Address Resolution

1. Explain how application layer addresses (e.g. `www.monash.edu` or `jsmith@foo.com`) are resolved to IP addresses and why is this necessary.

2. Explain how IP addresses are resolved to MAC addresses (in Ethernet) and why is this necessary.

3. Download the `fit9137_w8.imn` file from Moodle week 8 and save it in the shared folder on your host machine (laptop or PC). Open the core in VM and from the file open the downloaded file from the shared folder (under `/media/sf_NAME_OF_YOUR_SHARED_FOLDER`). While performing the following steps also observe how the address range `10.1.1.0/24` is divided into 4 subnets and 3 of these subnets assigned to the three interfaces of node `phoenix`.

   Start the emulation (click on the green play button) and wait until the emulation boots emulated nodes. Open Wireshark on `eth0` interface of the node named `phoenix` by *Right* clicking on the node `phoenix` then move the mouse over Wireshark and select `eth0` from the list. Wait until Wireshark window opens and starts capturing. Open a terminal on the node named `selene` and issue the following command:

```
lynx www.argos.edu
```

This command uses the text-based web browser to visit the page `www.argos.edu`. Select the Wireshark window and stop the capture.

a) Can you identify any application layer address resolution in captured traffic?

b) Can you identify any MAC address to IP address resolution in the captured traffic? *(Hint: check out the address resolution protocol for mapping datalink address to IP address in linux checkout* ***`man arp`*** *or in windows* ***`arp /?`*** *)*

ACTIVITY B: Dynamic Assignment of IP Addresses

The Dynamic Host Configuration Protocol is used to automate the process of assigning network addresses and other network related settings such as the address of the default gateway, DNS server etc. The core configuration file `FIT9137_w8.imn` has a DHCP server configured on node `phoenix`. It has also configured a packet capture on the node `selene` that starts as soon as the emulation starts which allows the DHCP traffic to be captured. If you have completed the previous exercise you should find a captured traffic file under `/home/muni/` named `selene.eth0.pcap`.

Note: For Cloud VM users, you will find the `selene.eth0.pcap file in the /tmp folder, cp the file to your home directory`.

Now open the file in Wireshark and answer the following questions:

a) What source and destination addresses are used in the `DHCP Discover` message? Why?
b) What are the source and destination address in `DHCP Offer`? What parameters are provided by the server? Did the server offer every option requested by the client?
c) Identify and explain the next two steps in the DHCP protocol in the captured traffic.

Stop the configuration and open the services on the node `phoenix` and then click on the wrench icon of `DHCP` service. Compare the values offered in the captured DHCP traffic with the settings. Check out the page

https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

for more information on DHCP protocol.