FIT9137 Workshop Session
Week 8

Topics

- Data Link Layer: Wireshark packet analysis & CORE simulation

Covered Learning Outcomes:

- Analyze 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 targets of workshops is to anchor the learner into the session and create many opportunities to reinforce the learning in different ways – individually and in small groups. Sometimes we also teach key practical/theoretical concepts to you during these sessions.
- Form groups of 4-5 students to work through the exercises. If you meet a problem, try to solve it within your group by discussing it with your group members. If not resolved within the group, ask one of the support tutors to help you.
- You still have a question? Jump into one of many consultation hours run by our experienced tutors and seek help. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

Activity A: Data Link Layer – Ethernet Frame

In this activity you will use Wireshark to capture the live network traffic into and out of the VM. Recall from the textbook/lecture notes that Ethernet frames have the following structure:

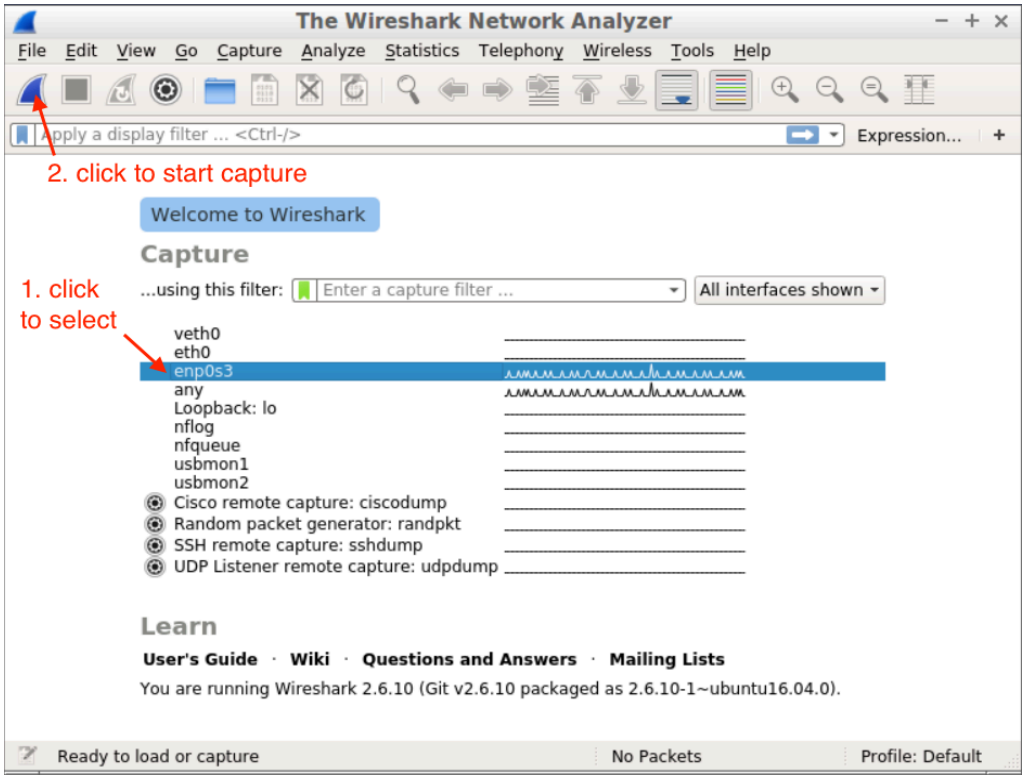
The description of the fields is as follows:

- Hardware fields, invisible in Wireshark:
  - 7-byte **preamble**: repeating pattern of ones and zeros
  - 1-byte **start of frame** delimiter (SFD): `10101011`
  - 4-byte CRC-32 frame **check sequence**

- Fields visible in Wireshark:
  - 6-byte **destination** and 6-byte **source** MAC addresses
  - 2-byte length or type of frame field. If value is ≤1500 (`=0x05DC`) this is the length of the data. If value is ≥1536 (`=0x0600`), then, this value represents the "type of frame". The length is then determined dynamically, by listening for the end of the packet (no signal) and determining the correct FCS. E.g.: a type of `0x0800` means the frame contains an IPv4 packet, `0x86DD` means IPv6, and `0x0806` indicates an ARP frame (we'll learn about these protocols later).

- Variable length **data** field - 46 to 1500 bytes.

1. In the VM open Wireshark. We are going to capture the live network traffic of the VM. From the Wireshark list of available interfaces click on `enp0s3` to select (blue line identifies selected interface) and then click on the blue shark fin on the Wireshark panel to start capturing. Alternatively double click on the interface name to select and start capturing traffic.



Capturing traffic on `enp0s3` interface

2. After starting the capture in Wireshark, open Firefox and browse to the following page:

   http://www.bom.gov.au

   The page contains texts and images. As soon as the page has finished loading, you can stop the capturing in Wireshark. Analyze the captured packets to identify the different requests and responses. Select the Ethernet frame containing the `HTTP GET` message.

3. Answer the following questions, based on the contents of the Ethernet frame containing the `HTTP GET` message (`GET /HTTP/1.1..`).

   a) What is the value of the Ethernet source address?

      `Hint: Example Ethernet Address (or MAC Address): 12:40:63:46:EF:9D`

   b) What is the destination address in the Ethernet frame? Is this the Ethernet address of http://www.bom.gov.au?

      Hint: It is the MAC address (i.e. `52:54:00:12:35:02`) of VBox playing the role of the default gateway of the VM. Again, if you are using the Machine's O.S then it will be the Mac address of the modem router.

   c) Give the hexadecimal value for the two-byte Frame type field.

      `Hint:` See under the Ethernet II, Source Type.

   d) How many bytes from the very start of the Ethernet frame does the ASCII "`G`" in `GET` appear in the Ethernet frame?

   e) What is the total size of each header for Datalink, Network and Transport layers?

4. Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message (the first `HTTP/1.1 200 OK` after the `GET` request, part of this HTTP stream).

   a) What is the value of the Ethernet source address? Is this the address of your computer (VM), or of http://www.bom.gov.au ?

      Hint: It is the MAC address of VBox (i.e. `52:54:00:12:35:02`,) playing the role of the router, the default gateway of the VM.

   b) What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer (VM)?

   c) Give the hexadecimal value for the two-byte Frame type field.

Activity B: Data Link Layer – MAC Addresses

The data link layer transfers data between nodes on a network segment across the physical layer. Its function is to provide means to transfer data between network entities and detect errors in the physical layer, concerned with delivering frames between nodes on the same level of the network hence its local delivery of frames within the LAN.

(i) Frame Structure: Data link frames typically contain: (a) A header with source and destination MAC addresses, (b) The encapsulated data (payload), (c) A trailer with error checking information.

(ii) Addressing Purpose: MAC addresses allow frames to be directed to specific devices on the same network segment. They enable communication between directly connected nodes without needing higher layer addressing.

(iii) Scope: MAC addresses are only used for local delivery within a single network segment. If you need to communicate between network boundaries - ***routers strip off and replace the MAC addresses when forwarding packets between networks.***

By using MAC addressing, the data link layer can efficiently deliver frames between devices on a local network segment, providing the foundation for higher-layer network communication. To understand how a data link layer functions, let's construct a simple network and examine the data link layer (Ethernet II) functionality and observe the layer 2 addresses playing the role of frame forwarding. We will be using the Wireshark tool to capture the frames to understand the layer-2 addressing.

Step 1

Create a simple network with two pc (let's call them "**Alice**" & "**Bob**" nodes) connected via a **router** as shown in figure-2 below. Assign IP address as shown by selecting the default 10.0.0.0/24 network address, remove the ipv6 addresses for sake of simplicity.

Note that the switches are not "addressed" in data transmission. That means, switches do not reveal the layer-2 MAC addresses, hence layer-2 switches are ignored in our explanations.

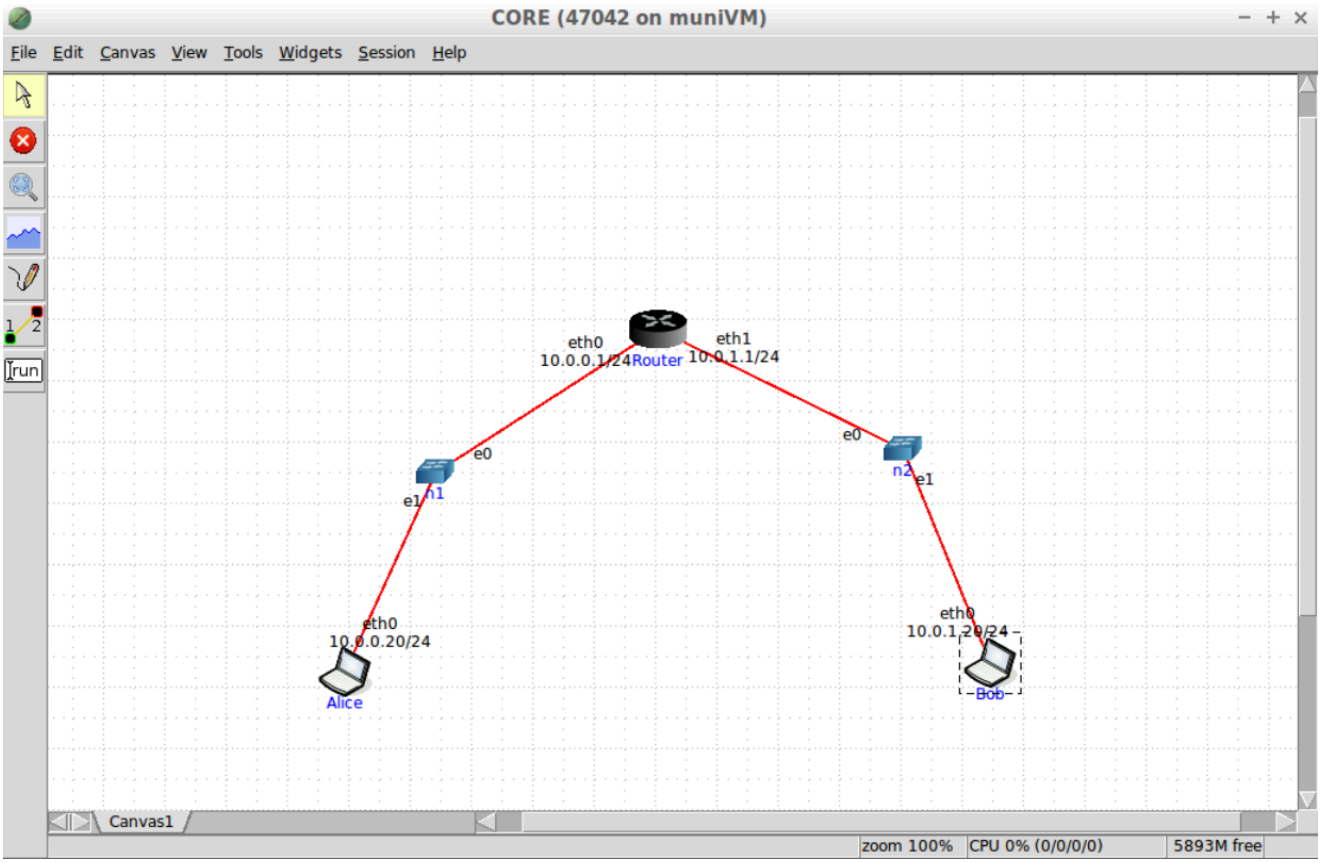


Figure 2: Data Link Layer activity

Next save the network as **`week-8-ActivityB.imn`** file.

Step 2

Now start the simulation, by clicking on the "**start the session**" button.

Step 3

Next open a terminal on each node and run "**`ifconfig`**" command and make a note of their Hardware Address: "**`HWaddr`**" For the nodes Alice, Bob & the Router, please make a note of both the Ethernet Interface **`eth0, eth1`** addresses. Please, answer the question (A) below.

Question A: List all the Hardware addresses of all the devices and their ethernet interface cards: note: Hardware address is also known as MAC address / Physical Address / NIC address / Ethernet address.

Sample Hardware Addresses are as follows: -

```
Alice node:  MAC address =   00:00:00:aa:00:02
Bob node:    MAC address =   00:00:00:aa:00:03

Router Node eth0: MAC address =   00:00:00:aa:00:00
Router Node eth1: MAC address =   00:00:00:aa:00:01
```

Step 4

We need to create traffic from node **Alice** to node **Bob**, using ping command (from **Alice** to **Bob)** generating ICMP packet-flow between these two end-hosts**.** Assuming the IP address of Bob PC is 10.0.1.20, type the following command @ Alice PC terminal.

[@ Alice] Ping 10.0.1.20

Step 5

Once the frames have been initiated, the traffic will be successfully sent and received indefinitely; we are now ready to capture the frames in the network stage by stage starting from **Alice** to **router** interface eth0, then from **router** interface eth0 to eth1 interface, and then the frames on the receiver's pc **Bob** eth0 interface.

Step 6

Capture the frames on **`Alice interface eth0`** and observe the source and destination MAC address to answer the question (B) below. You should see the Ethernet II data link layer information similar to the data shown as below:

Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
Destination: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
Source: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.1.20
Internet Control Message Protocol

Question B: While the simulation is running, use the Wireshark tool to capture the traffic on the `Alice interface eth0.` What is the Source and Destination MAC address on a frame captured at Alice PC? Explain the rationale behind these source and destination MAC addresses in this captured ethernet frame? Note: Select a frame going from Alice PC to Bob PC.

Step 7

Capture the frames on **`router interface eth0`** and observe the source and destination MAC address to answer the question (C) below. You should see the Ethernet II data link layer information similar to the data shown as below:

Ethernet II, ……
Destination: ….
Source: …
Type: IPv4 (0x0800)
Internet Protocol Version 4, …..
Internet Control Message Protocol

Question C: While the simulation is running, use Wireshark to capture the traffic on `the router interface eth0.` List the Source and the Destination MAC address on a frame captured in `Router interface eth0`? Do you see the change in source or destination MAC address? If so, please explain? Note: Select a frame going from Alice PC to Bob PC.

Step 8

Now Capture the frames on **`router interface eth1`** and observe the source and destination MAC address to answer the question (D) below. You should see the Ethernet II data link layer information similar to the data shown as below:

Ethernet II, ……
Destination: ….
Source: …
Type: IPv4 (0x0800)
Internet Protocol Version 4, …..
Internet Control Message Protocol

Question D: While the simulation is running, use Wireshark to capture the traffic on `the router interface eth1.` List the Source and the Destination MAC address on a frame captured in the `Router interface eth1`? Do you see the change in source or destination MAC address? If so, please explain? Note: Select a frame going from Alice PC to Bob PC.

Step 9

Finally Capture frames on **`Bob interface eth0`** and observe the source and destination MAC address to answer the question (E) below. You should see the Ethernet II data link layer information similar to the data shown as below:

Ethernet II, ……
Destination: ….
Source: …
Type: IPv4 (0x0800)
Internet Protocol Version 4, …..
Internet Control Message Protocol

Question E: While the simulation is running, use Wireshark to capture the traffic on the `Bob interface eth0.` What is the Source and Destination MAC address on a frame captured at Bob PC? Do you see the change in source or destination MAC address? If so, please explain? Note: Select a frame going from Alice PC to Bob PC.