FIT9137 Applied Session
Week 8

Topics

A. **A simple network in the CORE Emulator**
    i. Design a network with two LANs and a router.
    ii. Enable Web and Email services
B. **Addresses in LANs and in routed backbone Networks**
    i. Analyse pre-captured network traffic
    ii. Understand the change of addresses at different sections of the network.

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 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 2 students (peers) to work through the exercises. If you meet a problem, try to solve it by asking direct questions to your peers. If the issue was not solved within peers, ask your tutor. If you 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: (i) Network Design and (ii) Enabling Web and Email services in the CORE Emulator

In this activity we discuss the design of two simple LANs connected via a router, with the use of two servers in each LAN. And we learn how to configure the WEB and EMAIL services on the servers in the CORE.

Here we introduce the Layer-2 device Ethernet "Switch" and Layer-3 device "Router" necessary for design. Switch will be used to create two simple switched LANs with multiple

users. We will call these Local Area Networks as EAST_LAN and WEST_LAN, We will use two ethernet switches to create the LANs and these LANs will be interconnected by a layer-3 router using the CORE network emulator. Follow these steps given below (see also the network structure figure in the next page).

Creating two LANs and connecting them with a Router:

1. From the available tools in the left column, select an "ethernet switch" and place it to the **left** of your screen. Name it "**East-Switch**".
2. From the available tools in the left column, select "PC object". Then select and add 3 PCs close to the east-switch.
3. From the top menu, select "Tools" and then "IP Addresses". Select for example 192.168.0.0. Discuss the other options with your group.
4. From the left column tools, use "link" to draw 3 lines between the created east_switch in the first step and each PC(3) in the second step.
5. Check your current network by selecting "start a session" from the left column. If everything goes green eventually, your EAST_LAN is ready. Annotate the LAN with EAST_LAN.
6. Use the "two-node tool" again from the left column. Assign random sources and destinations on top of the page and use "Ping" and "Traceroute" to check the network. Discuss what you see with other members of your group.
7. Stop the session.
8. Now: Repeat steps 1-6 and create another independent network and call the network WEST_LAN to the **right** of your screen.
9. Now select from the available tools in the left column, select an "router" and place it in the **Middle** of your screen. Name it "router".
10. From the left column tools, use "link" to connect the router to east_switch & the west_switch. This will give network connectivity between the LANs.
11. Check your current network by selecting "start a session" from the left column. If everything simulation status goes green eventually, your EAST_LAN & WEST_LAN should communicate with each other.

Check the connectivity between the LANs:

12. Use the “two-node tool” again from the left column. Select a random source PC and a destination PC from each of the LAN’s and use “Ping” and “Traceroute” option to check the two networks' communication. Discuss what you see with other members in your group.
13. Stop the session.

Adding Servers in the LAN and enabling web and email services:

14. Now from the left column tools, use “server object” to place one server in EAST_LAN and one in the WEST_LAN. Now connect the servers to the respective switches in each LAN using the link object. Name the servers as “email” and the other as “web” server.
15. Now we need to enable the email and web server with these services respectively. This will give access to these services to the entire network.
16. You should see the following structure of your network as shown in the below figure:

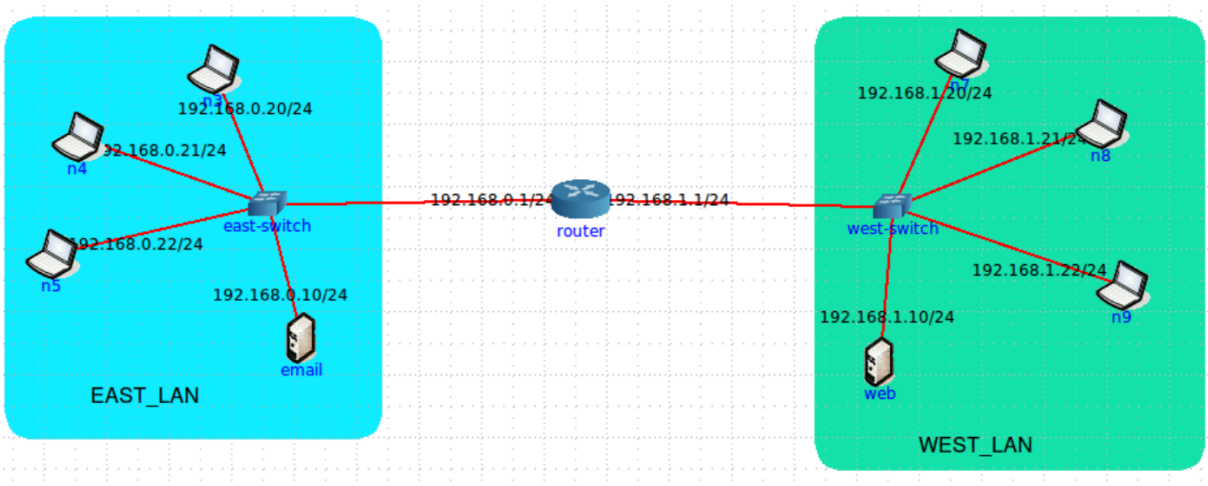
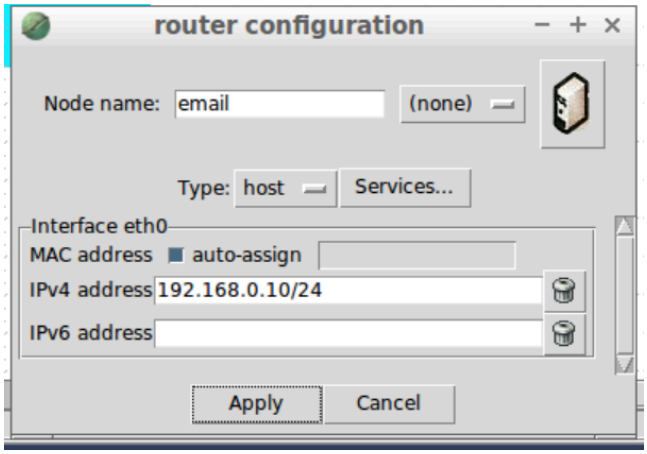
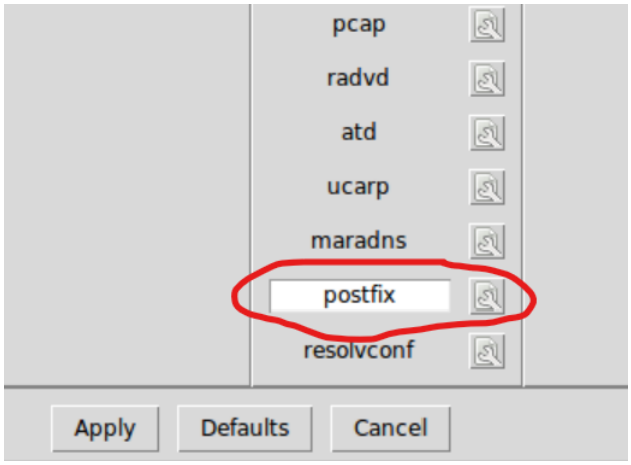


Figure 1: Two LANs connected with a Router

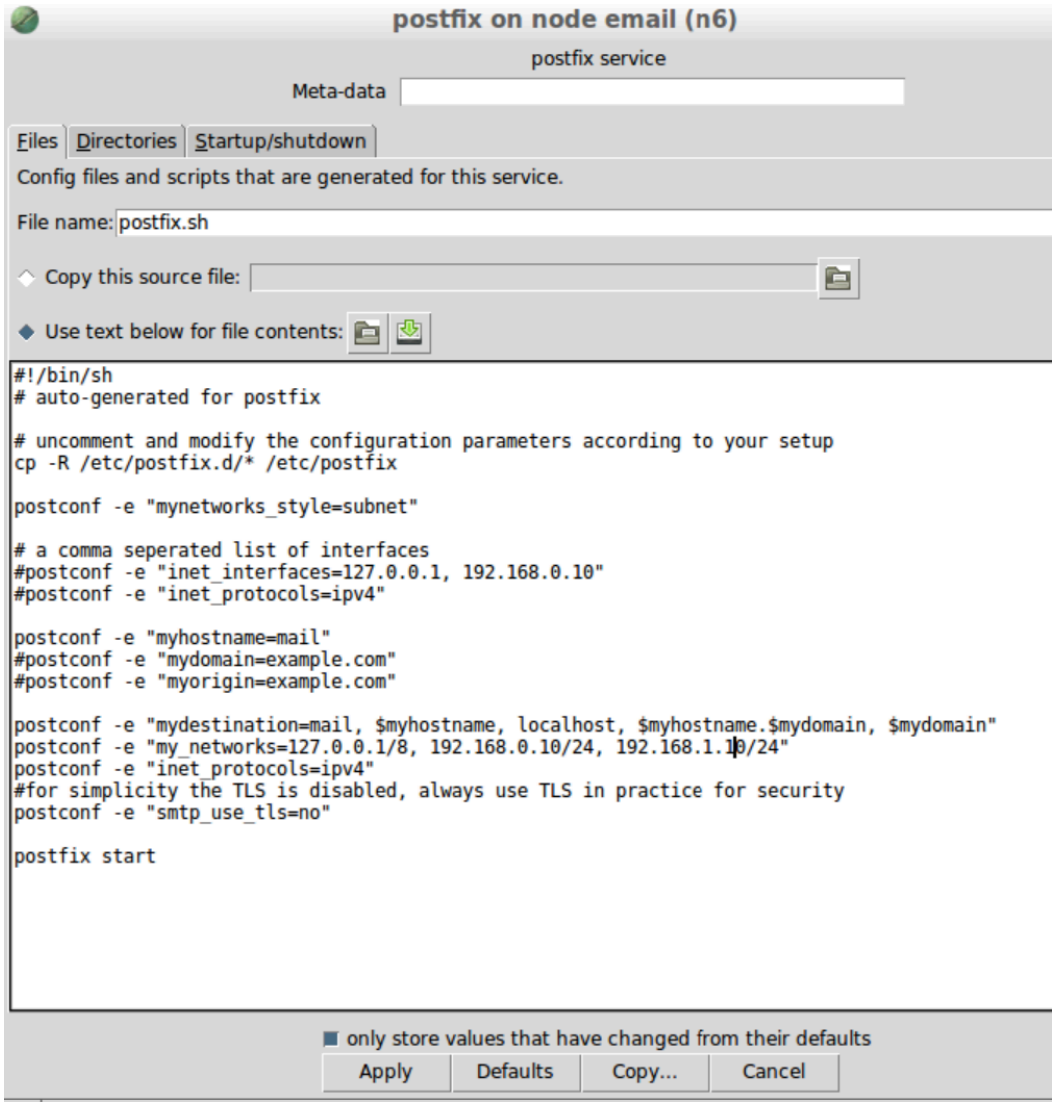
17. Now double click on the email server to configure email services.



Click services and select postfix (email services)

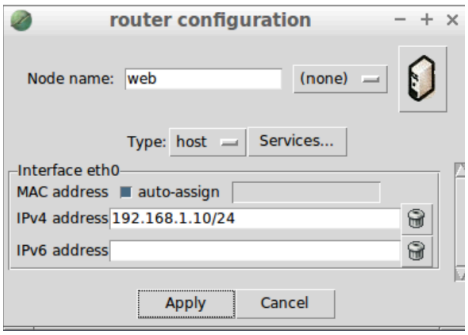


And configure the settings as follows: -

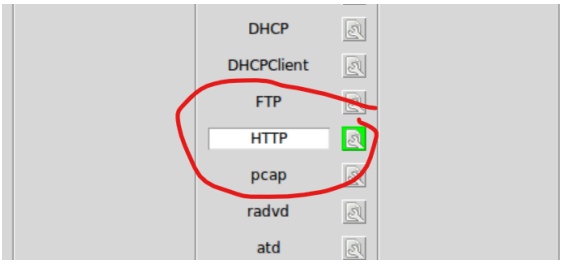


Click "apply" to all settings screen and save the imn file as FIT9137-Applied-W8-Activity-A.imn.

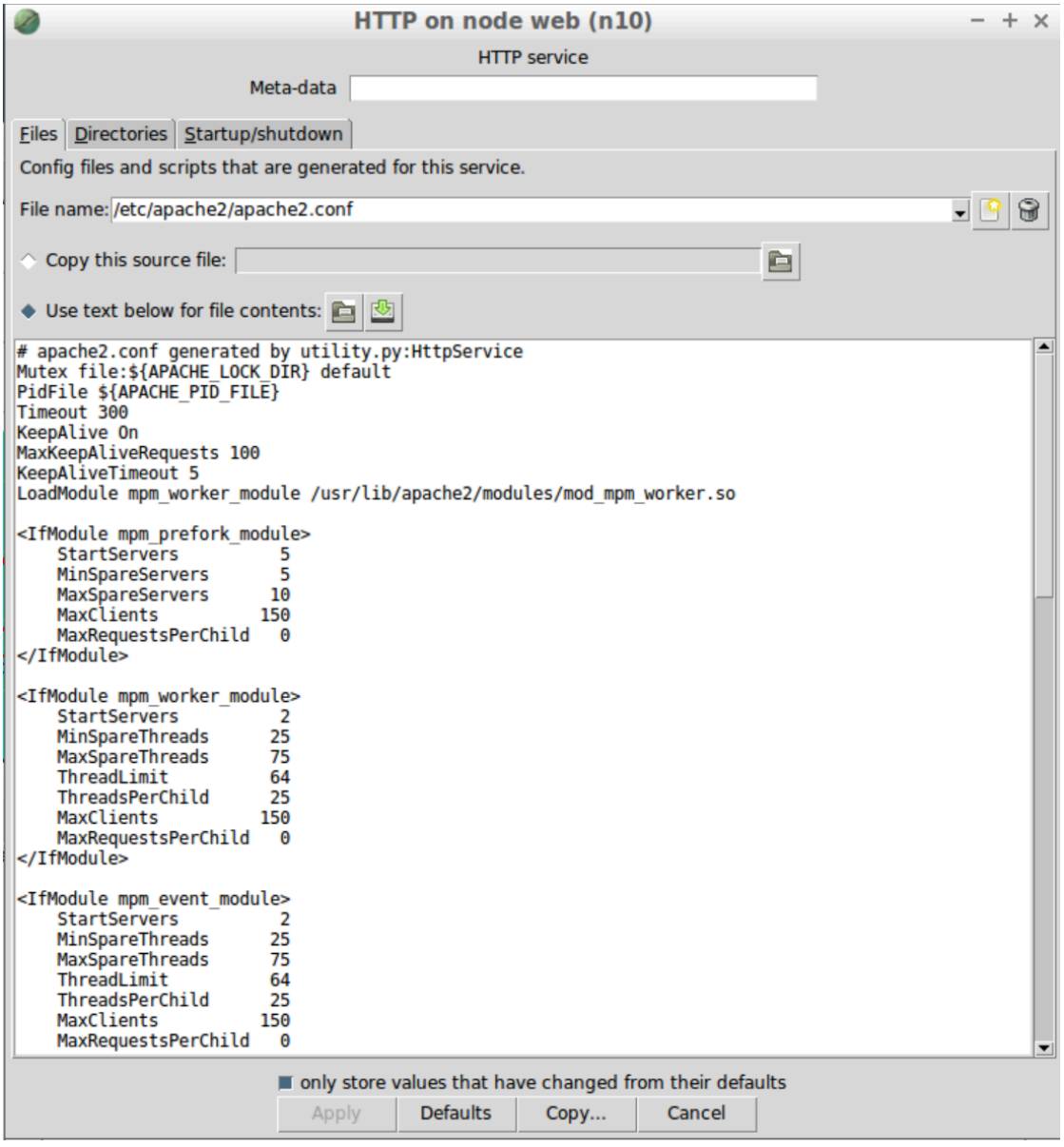
18. Now double click on the web server to configure web services.



Click services and select Http (Web services)



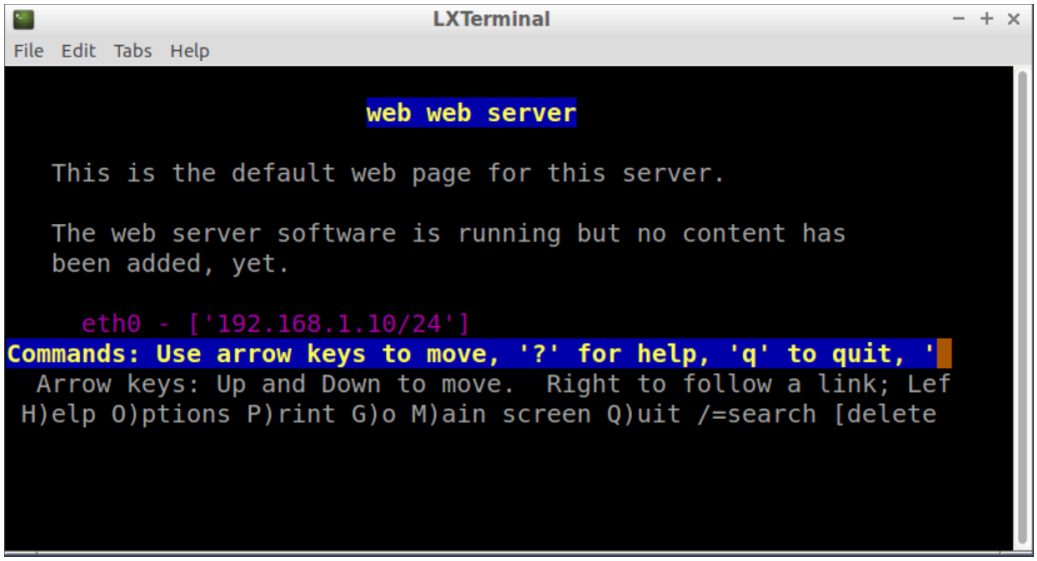
And leave the DEFAULT settings as it is: -



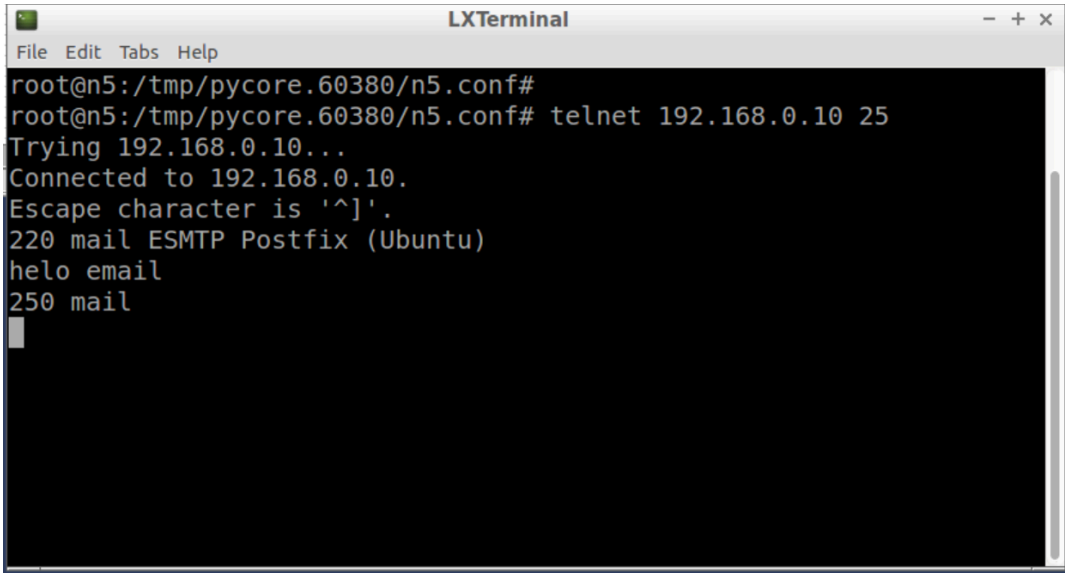
Click “apply” to all the settings screen and save the imn file again.

19. Now check your current network by selecting “start a session”

20. To check the running web services on “web” server, select a random client PC (example node-n5) open a terminal prompt on n5 and type in “lynx 192.168.1.10” The output should be as follows:



21. To check the running email services on “email” server, select a random client PC (example node-n5) open a terminal prompt on n5 and type in “telnet 192.168.0.10 25 ” The output should be as follows:



22. These outputs will show that you have successfully configured the two LAN’s with a router and setup the Email and Web services in each LAN and were able to connect to those services using a random client node n5.

Activity B: Addresses in LANs and in routed backbone Networks

In this activity, we will analyse traffic captured at different points in a Client-Server communication that took place in the network shown in Figure 2. These captured traffic (by Wireshark) are available in a zip-file (FIT9137-Applied-W8-Activity-B.zip) in the Moodle week 8 page. This zip-file contains four different capture files containing traffic data collected from four segments of this network (Figure 2).

We will analyse traffic captured at different points in the network (Figure 2). The packets that originated from the Client computer went through the backbone network (routers R-1, R-2 and R-3) reaching the server computer. We used Wireshark to capture network traffic at different sections of the network while a Client-Server packet exchange was going on.

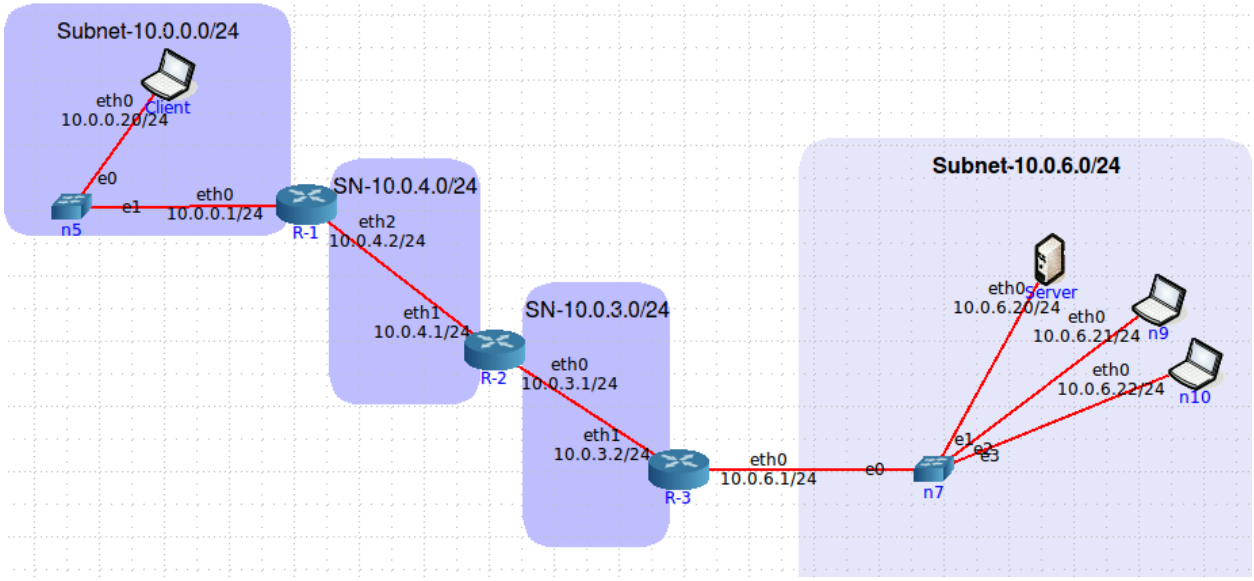


Figure 2: A Client-Server pair with supporting networks

The list of IP and MAC addresses used in the above network are listed below (Table 1). The end-host computers (the client and the server) and the routers use these addresses to forward or route packets in the network.

Table 1: Addresses Used in the network in Figure 2

Device	Interface	MAC	IP
Client	eth0	00:00:00:aa:00:08	10.0.0.20
Router R-1	eth0 eth2	00:00:00:aa:00:09 00:00:00:aa:00:03	10.0.0.1 10.0.4.2
Router R-2	eth0 eth1	00:00:00:aa:00:00 00:00:00:aa:00:02	10.0.3.1 10.0.4.1

Router R-3	eth0 eth1	00:00:00:aa:00:07 00:00:00:aa:00:01	10.0.6.1 10.0.3.2
Server	eth0	00:00:00:aa:00:04	10.0.6.20

We will investigate the addresses present in the frames captured in different network sections. Please download the zipped file containing the Wireshark captures from week 8 Moodle page to perform the following tasks.

(i) Use Wireshark to open the file "FIT9137-Applied-W8-Q2a.pcapng" which captures packets at the interface *eth0* of the Client PC. Analyze the frame no. 1 and answer the following questions. *Please note that this file captured packets in the subnet 10.0.0.0/24.*

a. What is the value of the Ethernet address of the client computer?

b. What is the destination address in the Ethernet frame? Is this the Ethernet address of the Server or a router?

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

d. What are the source and destination IP addresses?

(ii) Use Wireshark to open the file "FIT9137-Applied-W8-Q2b.pcapng" which captures packets at the interface *eth2* of the router R-1. Analyze the frame no. 1 and answer the following questions. *Please note that this file captured packets in the subnet 10.0.4.0/24.*

a. What is the value of the Ethernet source address? Is this the address of the client computer, or of a router?

b. What is the destination address in the Ethernet frame? Is this the Ethernet address of a router?

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

d. Are there any changes in the source and destination IP addresses?

(iii) Use Wireshark to open the file "FIT9137-Applied-W8-Q2c.pcapng" which captures packets at the interface *eth0* of the router R-2. Analyze the frame no. 1 and answer the following questions. *Please note that this file captured packets in the subnet 10.0.3.0/24.*

a. What is the value of the Ethernet source address? Is this the address of a router?

b. What is the destination address in the Ethernet frame? Is this the address of a router?

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

d. Are there any changes in the source and destination IP addresses?

(iv) Use Wireshark to open the file "FIT9137-Applied-W8-Q2d.pcapng" which captures packets at the interface *eth0* of the Server PC. Analyze the frame no. 1 and answer the following questions. *Please note that this file captured packets in the subnet 10.0.6.0/24.*

a. What is the value of the Ethernet source address? Is this the Ethernet address of the client computer?

b. What is the destination address in the Ethernet frame? Is this the address of the server, or of a router?

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

d. Are there any changes in the source and destination IP addresses?

Additional Note: Ethernet frames have the following structure:

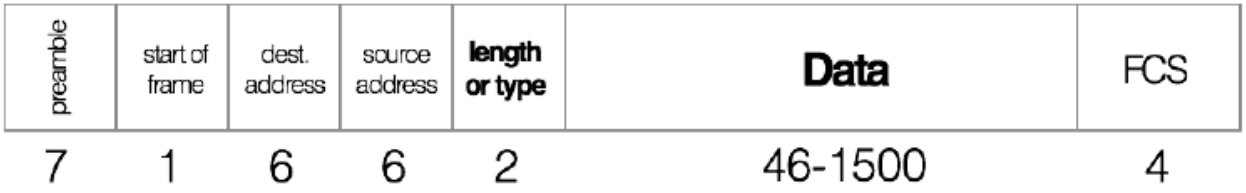


Figure 3: Ethernet Frame

Fields visible in Wireshark: (i) 6-byte destination and 6-byte source MAC addresses, (ii) 2-byte length or type of frame field (Example: a type of 0x0800 means the frame contains an IPv4 packet, 0x086dd means IPv6, and 0x0806 indicates an ARP frame), (iii) Variable length data field – 46 to 1500 bytes. The following hardware fields are not visible in any Wireshark capture: (i) 7-byte preamble: repeating pattern of ones and zeros, (ii) 1-byte start of frame delimiter (SFD): 10101011, (iii) 4-byte CRC-32 frame check sequence.