Lab 4: Ethernet and Datalink Layer

# What you will do:

* Learn about the data-link layer
* Learn about Ethernet types.
* Learn how to use xcap Packet Builder (xcap)
* Use Wireshark to receive constructed Ethernet frames

# Things that you will need to know or learn:

* How to use xcap Packet Builder
* How to configure IP addresses and subnet masks, both statically and dynamically, using both the command line and the GUI, under Windows 7(see References below)
* How to copy text from the command line window (aka DOS box)
* How to enable and disable the Windows Firewall
* How to use Wireshark to see actual network traffic (Skill acquired during lab time)

# What you need to submit and when:

* Complete the “Lab 4 Pre-lab” exercise on Blackboard before 8am on the day of your lab
* Complete the in-lab part of the exercise (see below) before the end of your lab period.
* Complete the “Lab 4 Post-lab” exercise on Blackboard before 8am on the day of your lab

# Required Equipment:

* Network cables from your kit
* USB memory stick to save results for post-lab questions – share all results with your partner

# Marks:

* Each of the three lab parts identified above are weighted equally, even though they may have a different number of points assigned to them.
* 20% of your final mark is for labs done during the course of the semester.

# References and Resources:

* Packet Tracer (for help on correct cabling; view of packets similar to Wireshark)
* How IP in Windows 7 (on Blackboard, Labs and Assignments -> Lab 03)
* How to Wireshark (on Blackboard, Labs and Assignments -> Lab 03)
* How to Cable (on Blackboard, Labs and Assignments -> Lab 03)
* How to Build a packet in Xcap (on Blackboard, Labs and Assignments -> Lab 04)

# Task 1: Craft a Frame

1. Download the xcap\_1\_0\_2.zip from Blackboard You will use this to craft frames and packets
2. Extract the files and remember the location
3. Go to the folder containing xcap. Launch the program (xcap.exe)
4. On the left side of the screen, right click on “Interfaces” and select “Refresh interfaces”
   1. Examine the Interface List, locate the interface that is your “Ethernet Adapter”
   2. Right Click on this interface and select “Start interface”
5. Locate the “Packet group”
   1. Right Click on the “Packet group” and select “Create packet group”
   2. Name this group “Lab 04”
6. You should now see a table in the right pane of the app. Locate the “Interface” drop down list and choose the interface you started in step 4
7. Click on the “+” sign button to add a new packet. Name this packet this “Task 1”
   1. The packet name will now appear in the table.
   2. Enable the packet by clicking on the check box in the “Enabled” column
   3. Double click on the “Task 1” packet name to open the configuration window, Configure your packet as follows
      1. Destination Mac : your partner's MAC address
      2. Source MAC: your MAC address
      3. VLAN: none
      4. Type: Ethernet II (radio button)
      5. Type field: Enter 0x0899
      6. Select “Append FCS at end of packet”
   4. Now click “Next”
      1. Open “Notepad” and type a short message to your partner. Something like *Hi John, How are you? from Susan.*
      2. Count the number of characters in your message (including spaces).
      3. In the “Length” box enter your character count
      4. Copy you message from Notepad.
      5. Select all the “00” in the data area and use CTRL-V to paste in you message. The “00”s should change to the hexadecimal numbers representing the message you typed. The right hand portion of the window should contain the ASCII text you wanted to send.
      6. Save your packet and then click “Close”
8. Have your partner start a Wireshark capture and then right click on your “Task 1” packet and select “Send selected packets”. You may want to do this a few times
9. Each partner needs to send one frame and receive one frame.
10. You might want to filter your capture using the string eth.type == 0x0899

# Checkpoint 1 : Show the crafted frames and the captured frames.

# Task 2: Experiment with frames

1. You now going to craft 4 more packets as outlined below. Do not send them until you are instructed to do so. The easiest way to do this is to make 4 copies the packet you created in Task 1 and then modify them. You can do this by right clicking on the packet and selecting “copy” and then right click anywhere on the packet table and select “paste”
2. Rename the second packet to “Task 2.2” by right clicking on the packet and selecting “Rename”
   1. Verify everything in the Ethernet header is the same as in Task 1 then click next
   2. Change the length of the data field to 10
   3. Save and close
3. Rename the third packet to “Task 2.3”
   1. Verify everything in the Ethernet header is the same as in Task 1 then click next
   2. Change the Length value to 1500
   3. Ensure that the “Append FCS” box in un-checked
   4. Click on the “Fill” button and change the value to 0XAB
   5. Save and close
4. Rename the fourth packet to “Task 2.4”
   1. Verify everything in the Ethernet header is the same as in Task 1 then click next
   2. Change the Length value to 3000
   3. Click on the “Fill” button and change the value to 0XBC
   4. Save and close
5. Rename the fifth packet to “Task 2.5”
   1. Verify everything in the Ethernet header is the same as in Task 1 but this time change the value of the Ethernet type to 0x500 then click next
   2. Change the Length value to 40
   3. Click on the “Fill” button and change the value to 0X61
   4. Save and close
6. Start a wireshark capture on the destination PC. Set your filter to the sender’s (your partner's) MAC address (ex: eth.src == A1:B2:C3:D4:E5:F6 use upper case letters)
7. Send the 4 frames you just created. You can just select them and click send.
8. Stop the Wireshark capture and filter for the sender's MAC address. EXAMPLE: eth.src == A1:B2:C3:D4:E5:F6 (change to the correct MAC address)
9. You might want to save your crafted packets
10. What frames were received by the destination?
    1. The small frame (less than 46 bytes)? (Yes) What happened to the frame? Is it the same size as the frame that was sent?
    2. The 1500 byte frame? (yes)
    3. The 3000 byte frame? (no) Why?
    4. The 40 byte frame with the type of 0x0500? (Yes) But what happened? Expanded the captured packet in Wireshark

# Checkpoint: Explain what happened with each frame

# Task 3: Determine MAC of a computer.

1. Working with other students in your row. Develop a protocol that would allow you to find the MAC address of another computer in your pod without talking to the student at the workstation. You are trying to exchange messages with the other student. You are allowed to know the name of the person whose MAC address you are trying to find. Everything needs to be done with Wireshark and Packeth. Hint: Think about the layers of addressing you are using in this lab. What are the logical and physical layer addresses.
2. Exchange messages with a student in your row. You can’t know the MAC address of the students workstation when you start the process. This may take more than one step.

# Checkpoint: Explain your protocol to the instructor and show the xcap Packet(s) and the Wireshark captures that prove your protocol works (2 marks)

# Task 4: Clean up and Post-lab

1. Return all cables to the rack at the back of T111
2. Be sure to complete the post-lab questions before the beginning of your next lab period.