Lab 3: Introduction to Wireshark, Packet Tracer and the Lab

What you will do:

- Learn about your lab environment
- Learn how to determine and set your IP address.
- Learn how to test basic network connectivity (Layer 3)
- Learn to use Wireshark and Packet Tracer (PT)
- Learn to relate Wireshark captures to the OSI and TCP/IP models

Things that you will need to know or learn:

- Topology of the existing lab infrastructure (ie. Where do all those wires go? Done in lab.)
- How to recognize & identify the lab equipment (ie. PCs, switches, routers. Done in lab)
- The correct type of cabling to use when connecting network devices (From pre-lab)
- What a valid IP address looks like; what a valid subnet mask looks like (From lectures)
- How to configure IP addresses and subnet masks, both statically and dynamically, using both the command line and the GUI, under Windows 8(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 3 Pre-lab” exercise and preparation tasks 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 3 Post-lab” exercise on Blackboard before the start of your next lab

Required Equipment/Software:

- Network cables from the rack
- Packet Tracer 6.1.1 installed and working (done in Lab 01)
- Wireshark installed and working (done in Lab 01)
- Lab document downloaded to your laptop
- **T113 only** - 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 to IP in Windows (on Blackboard in Labs/ Lab 03)

- How to Wireshark (on Blackboard in Labs/ Lab 03)
- How to Cable (on Blackboard in Labs/ Lab 03)
- Packet Tracer My First PT Lab (Parts I to VII)

T113 Lab connectivity information

T113 Patch panel connections

- Blue Jack - From the Lab's PC "Realtech" add-on network card. If the PC is used for the lab, this is the NIC to configure.
- Green Jack - From the Lab's PC serial port. This is your console connection
- Black Jack - From the Lab's PC on-board NIC – Unused in semester 1.

T111 Lab connectivity information

T111 Patch panel connections

- Blue Jack – this is connected to the college network and when your laptop is connected to it you have Internet Access
- Red Jack – this is connected to a private network for T111, we call it the Eagle Network because we often use it to connect to a standard topology used in the course that includes a server we call the Eagle server.

Cable types:

- You will be using 3 types of cables; straight through, crossover, and rollover.
- A straight through cable is used for connecting different (electrically) types of devices (e.g. PC to switch, router to switch)
- A crossover cable is used for connecting "like" devices (e.g. PC to PC, PC to router, router to router, switch to switch)
- A rollover cable is used to connect from a serial port (using a USB to serial adapter) on your PC to the console port of the router or switch

Identify the type of cable required for the following connections. Confer with your classmates if necessary. For cabling purposes, you should think of a router as a specialized PC. Complete the table at the top of the next page by placing a check in correct box.

From	To	Straight Through	Crossover	Rollover
PC Ethernet	PC Ethernet			
PC Ethernet	Switch Ethernet			
PC Ethernet	Router Ethernet			
Router Ethernet	Router Ethernet			
Router Ethernet	Switch Ethernet			
PC Serial	Router Console			
PC Serial	Switch Console			

Task 0: Preparation

1.1 All Lab 03 pre lab tasks must be completed prior to beginning the activities described in this document.

1.2 Confirm you have downloaded the following from BB "Labs - > Lab 03" to your computer:

1.2.1 CST8103 "Lab 03 – In-Lab Activies.pdf" (this document)

1.2.2 Resource files

1.2.2.1 HowToIP_Win7.pdf

1.2.2.2 HowToWireShark.pdf

1.2.2.3 Cables.pdf

1.2.2.4 ICMP.pdf

1.2.3 The packet tracer file: T113-Simulation.pkt file.

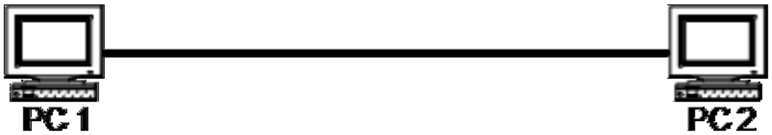
1.3 Tasks 1 and 2 require that you work in groups of two (2)

1.4 Do not start until you have completed ALL steps in this task.

Task 1: Create a directly-connected network of two PCs using static addressing

1.1 Disable the Wireless Interface of your Mobile computer. Your only network connection must be via the Wired (Ethernet) interface.

1.2 Using the correct cable and the jack colour specified by your instructor, directly connect your PC to your partner's PC at the **patch panel**. This is the smallest possible network; 2 PCs directly connected to each other.



1.3 Using the document "*How to IP in Windows 7*," (Downloaded from Blackboard) assign static IP addresses to each PC as per the following:

PC1: 192.168.1.XXX (XXX= jack number)

PC2: 192.168.1.YYY (YYY= Add 100 to jack number)

Use a subnet mask of 255.255.255.0.

Example: If PC1 is connected to jack number 25, the IP address for PC1 will be 192.168.1.25. If PC2 is connected to jack number 26, the IP address for PC2 would be 192.168.1.126.

Disable the Windows Firewall (Start -> Control Panel -> Windows Firewall -> Turn Windows Firewall on or off). You may also be required to disable other 3rd party Firewalls such as Norton.

1.4 Test that you can reach your partners computer by using the ping command from a windows CMD prompt (ping a.b.c.d where a.b.c.d is your partner's IP address). Each partner should ping the other.

NOTE: You should be able to successfully ping your partner. If you don't get any response, be sure to turn off any anti-virus or other 3rd party firewalls (during this lab).
A successful ping will look similar to this:

```
Pinging 192.168.1.25 with 32 bytes of data:
```

```
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
```

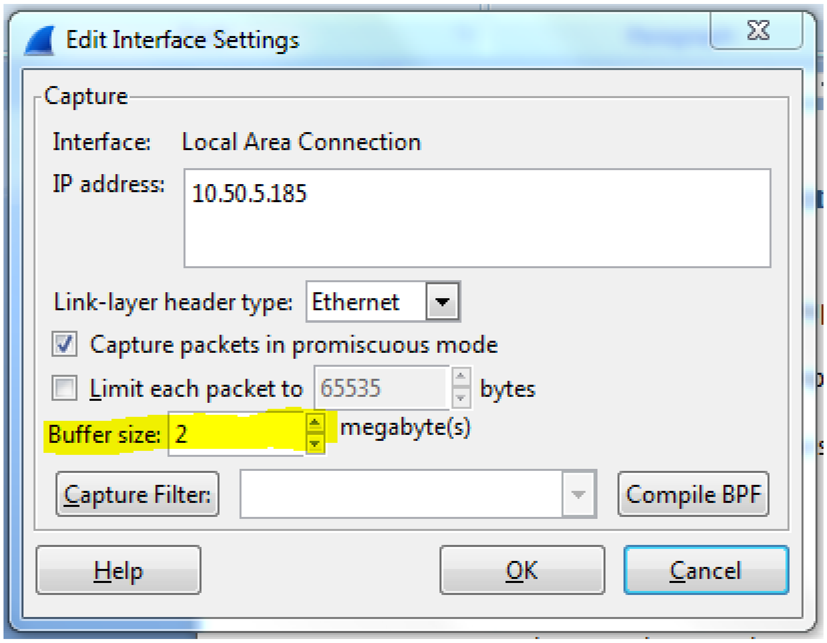
1.5 Copy and paste the output of the ping command to a text file. You'll need to save the file so that you can answer questions in the post-lab. Make sure to add your name, course, and lab section to the original text file so that you'll know that it's yours!

NOTE: To copy from a CMD prompt, right click inside the black area of the CMD prompt window and click "Mark." Then highlight the area you wish to copy by dragging the curser. Press enter to copy. Paste into notepad.

Task 2: Use Wireshark to view network activity

2.1 Prepare Wireshark to capture network traffic on your Ethernet adapter:

2.1.1 Open Wireshark
2.1.2 From Wireshark's menu, click Capture –> Options
2.1.3 From the Capture Options window, highlight and select the Ethernet adapter with the correct IP address. BE SURE TO SELECT THE CORRECT ADAPTER!
2.1.4 Double click the entry selected in step 2.1.3. This will bring up the Edit Interface Settings window.
2.1.5 From the Edit Interface Settings window, change the value of the Buffer size to 10 and click OK (see screen capture below). This change will ensure the capture buffer is large enough as to not discard the packets of interest should there be a lot of traffic on the wire.



Edit Interface Settings

Capture

Interface: Local Area Connection

IP address: 10.50.5.185

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

☐ Limit each packet to 65535 bytes

Buffer size: 2 megabyte(s)

Capture Filter:

2.1.6 Before moving to step 2.2, click Start (on Capture Options window) to begin capturing network traffic

2.2 Ping your partners PC, and stop the capture when you have BOTH successfully completed and captured each other pings! A successful ping consists of four echo requests and four echo reply.

2.2.1 Examine the output, noting the three windows, each one with increasing amounts of detail.
2.2.2 Compare the output of your capture with the output of your partners capture. Do you see any

differences?

2.2.3 What other traffic, if any, was captured by Wireshark?

2.2.4 You can filter specific “packets” in your Wireshark. Type “**icmp**” in the filter box and click *apply* to view just your “ping” traffic. Click *clear* after examining the results as simply erasing the field content with the erase or delete keys will NOT clear the filter. Hint: ping uses the ICMP protocol!

2.2.5 Save the output for later examination and to answer post lab questions. Save the file from Wireshark as “**Lab03 Task 2.2 ping.pcap**".

CHECKPOINT 1

You are ready for instructor sign off if you have filtered the capture to show only packets resulting from the ping command (Hint: enter icmp in the filter box), and both you and your partner MUST see at least 8 captured ICMP packets containing the following in the capture’s Info column:

i. Echo ping request
ii. Echo ping reply

Task 3: Connect to the Eagle Network with Dynamic Addressing

3.1 Connect your PC using the correct cable type to the jack on your desk (jack colour to be specified by your instructor). This jack is connected to a switch labelled “S1-Central” which in turn is connected to the Eagle network. What type of cable should you use? Is there an exception to this?

3.2 Using the instructions in “How to IP in Windows 7”, configure both PCs to use dynamic addressing (Dynamic Host Control Protocol – DHCP). Be patient while your PC attempts to obtain an address. It may take as long as 30 seconds.

3.3 At the windows command prompt, type **ipconfig.** Locate and note the IP address assigned to the “*Ethernet Local Area Connection*” network adapter. From the IP address you just noted, you can determine if you are connected to the correct network. Remember, you want to be connected to the Eagle Network. From the table below, determine which network you are connected to:

IP for college network :	10.x.x.x	College services, Internet access, lab printer access
IP for “Eagle” network:	172.16.254.x	Lab’s Internal Eagle server – Lab only
No DHCP server responding:	169.x.x.x	Nowhere! (Check your connections)
Any other IP:	192.168.1.x	Check that your Ethernet network adapter is configured to obtain an IP address automatically.

Once you have confirmed you are connected to the correct network, you will use the PING command to confirm connectivity with the “Eagle Server”. The Eagle Server is at the following address:

eagle-server.example.com

DO NOT PROCEED TO THE NEXT STEP UNTIL YOU HAVE CONFIRMED BOTH LAPTOPS ARE CONNECTED TO THE “Eagle Network”.

Here are useful commands:

ipconfig /release	To release the automatically assigned addresses on ALL adapters.
ipconfig /renew	To request new IP addresses for each adapter.

3.4 Launch Wireshark and start a new Wireshark capture on the Ethernet adapter.

3.4.1 Open Wireshark

3.4.2 From Wireshark's menu, click Capture –> Options

3.4.3 From the Capture Options window, highlight and select the Ethernet adapter with the correct IP address. BE SURE TO SELECT THE CORRECT ADAPTER!

3.4.4 Double click the entry selected in step 3.4.3. This will bring up the Edit Interface Settings window.

3.4.5 From the Edit Interface Settings window, change the value of the Buffer size to 10 and click OK. This change will ensure the capture buffer is large enough as to not discard the packets of interest should there be a lot of traffic on the wire.

3.4.6 Before moving to step 3.5, click Start (on Capture Options window) to begin capturing network traffic

3.5 Open your web browser and connect to http://eagle-server.example.com . Leave your Wireshark capture running for at least 30 seconds and then stop the capture.

3.6 Examine the captured traffic. How many different protocols can you identify? What are their names? Do all protocols use an IP address?

3.7 Save your Wireshark capture as "**Lab03 Task 3.4.pcap**". You may need it for post-lab questions.

CHECKPOINT 2

Filter your capture to only display "http, dns and arp" traffic by entering the following expression in the Filter box: http || dns || arp You know you are good if your capture includes at least one of each of the packets having the following characteristics:

- Client request for Web page
  - Source IP address corresponding to your PCs IP;
  - Destination IP address corresponding to the eagle-server's IP address of 192.168.254.254;
  - Protocol is HTTP.
- Server response for Web page
  - Destination IP address corresponding to your PCs IP;
  - Source IP address corresponding to the eagle-server's IP address of 192.168.254.254;
  - Protocol is HTTP.

You are ready for instructor sign-off!

Task 4: Packet Tracer Exercise

4.1 Download the Lab03.pka file from Blackboard. Open the file in Packet Tracer.

4.1.1 Make sure you fill in you name and email address when prompted.

Name: *First_name Last_name (ex: Susan Smith)*
Email: Your Algonquin email address (ex: smit0999@algonquinlive.com)

4.2 Locate the "Activity Instructions Window", it's labelled PT Activity , follow the instructions to complete the activity.
Ensure that you enter your Lab section and your Student Number in the Instruction Window. Then click "Update", this will store the information for submission to the server. **Note:** The activity needs to be completed in a single sitting. Your results are uploaded to the server only when you click the "Submit for Grading" in the quiz window. You would be wise to record your answers to the questions so you can reenter them quickly if you need to stop and restart the activity.

CHECKPOINT 3

Checkpoint 3 is checked automatically by the Packet Tracer activity. You must complete the activity before doing the post lab. Be sure to save a copy of the activity and upload it to the Lab 03 Dropbox

Challenge

(Optional) Connect your computer back to the college network. Note that you might need to issue and ipconfig/release followed by ipconfig/renew in order to force your PC to acquire an IP address. Close any open web browsers. Start a new Wireshark capture. Start a browser and go to http://www.algonquincollege.com/ then stop the capture. Can you filter the capture to see just the web packets? (Hint: what is the acronym for the actual name of the web browsing protocol?)

Task 5: Clean up and Post-lab

5.1 Make sure you have saved or printed all the results you got during this lab period. Always share your results with your lab partner.

5.3 Make sure that the network wiring for your station (and your partner's station) is back to its default configuration.

5.4 Re-enable your Wireless Network and all anti-virus and firewall software you may have disabled.

5.5 Be sure to complete the post-lab questions before the start of your next lab.