
VANIER COLLEGE – Computer Engineering Technology – Winter 2021

Network Fundamentals (247-409-VA)

Leonardo Fusser (1946995)

LABORATORY EXPERIMENT 5

Basic Network Debugging

NOTE:

To be completed in one lab session of 3 hrs + Started at home

To be submitted: Non formal lab report, Hand in:

- this document with screen shots and the answers to all questions in another color (not red)

This exercise is to be done individually.

OBJECTIVES:

After performing this experiment, the student will be able to:

1. Use `ping` and `tracert` to verify and debug the connectivity from source to destination.
2. Explain the purpose of protocol analyzer (Wireshark).
3. Perform basic PDU capture using Wireshark.
4. Perform basic PDU analysis on straightforward network data traffic.
5. Experiment with Wireshark features and options such as PDU capture and display filtering.

BACKGROUND

Labs are designed to reinforce computer networking concepts that are taught in curriculum. The labs provide discovery and experience in configuring Cisco switches and routers to construct a functional computer network. In addition to the simulated network labs used with Packet Tracer, students also gain valuable hands-on experience with real equipment.

The lab environment is self-contained and requires no outside connectivity to the Internet to perform labs. Student labs consist of configuring host computers to connect different devices on the local area network (LAN), configure connectivity to the wide area network (WAN), and use typical network services such as DNS to access network services.

The lab environment is designed to be separate from a production network, and requires no additional connectivity to any other network to complete student labs. All resources that the students will use to complete labs are shown in the topology as shown in Figure 1. Some network client software for host computers such as Wireshark will be used.

Eagle Server Topology

Eagle Server allows students to access and use applications and services in the lab as if they were connected to the internet. Students are required to configure PC hosts to access the model network and server as shown in Figure 1. The rest of the interconnections to Eagle Server have been pre-configured.

Purpose of the lab devices

Host computer

Host computers provide students with network access and services. The computer is used as a client for popular network services, enabling the student to analyze those protocols. As a data capture tool, the computer is used to monitor data communication between itself and a network server. The data communication is examined to give an understanding of the underlying protocols. Finally, the host computer is used as a troubleshooting tool in labs that teach troubleshooting skills.

S1-Central switch

S1-Central switch provides LAN connectivity in the lab environment. The switch routes frames between the host computers and network end devices.

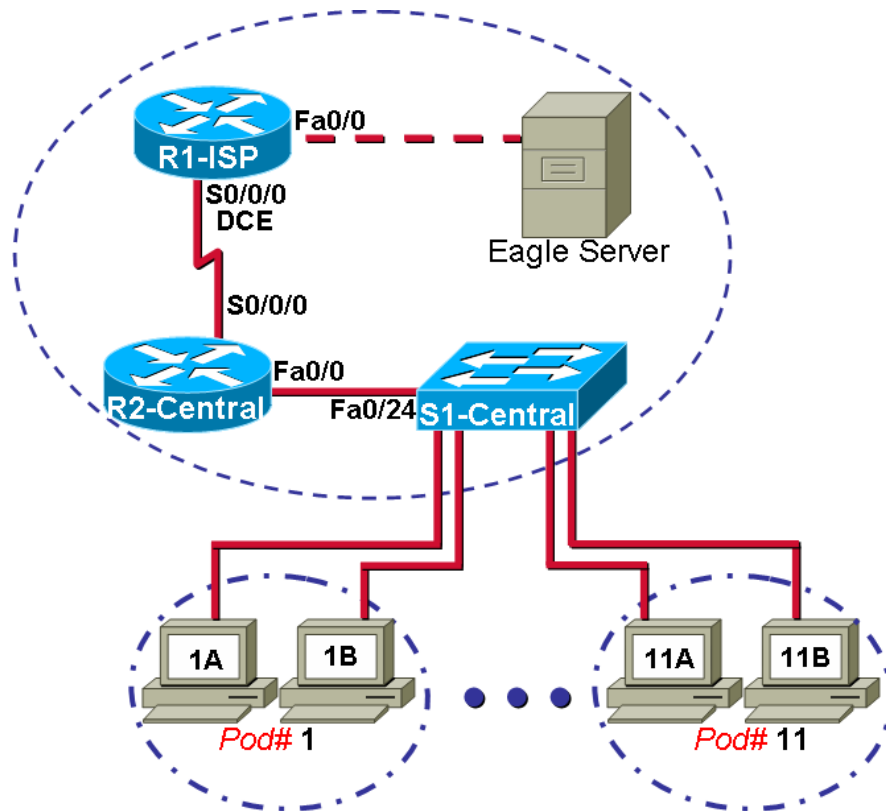


Figure 1 Eagle Server Topology

Addressing table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	N/A	172.16.Pod#.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

R2-Central router

R2-Central router acts as the LAN gateway, enabling host computers to connect to devices outside of the LAN. The router may be configured as a DHCP server, responding to host computer DHCP requests for IP addresses. The router may be configured with additional IP addresses to simulate different computer networks prior to accessing the network edge router, R1-ISP. Finally, the router has an enabled web-server that students use for router configuration and connectivity testing.

R1-ISP router

R1-ISP router is the classroom edge router, simulating the Internet service provider (ISP) role in a computer network. Additional IP addresses may be configured on R1-ISP to simulate external Internet sites, test correct routing protocol configuration, and as another link in the data communication path during troubleshooting exercises. Finally, the router has an enabled web-server that students use for router configuration and connectivity testing.

Eagle Server

The Eagle Server has several roles in the lab:

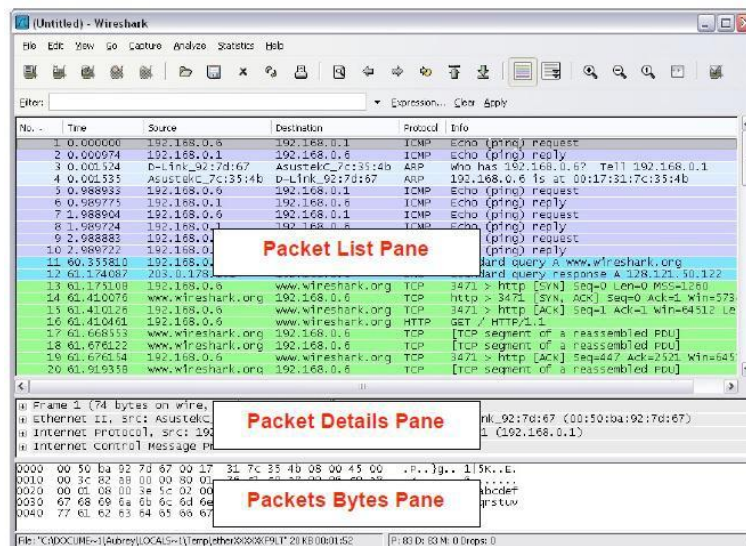
- It acts as network server for the class, enabling students to connect host computer client applications to the network service.
- It is a name server (DNS), translating lab domain names to IP addresses. When the host computer has networking correctly configured, students may use a web client application such as Mozilla Firefox, enter URL <http://eagle-server.example.com>, and receive a web page from Eagle Server.
- Email servers, SMTP and IMAP, permit students to configure an Email client on the host computer and send Email to each other.
- FTP and TFTP servers are enabled.

Wireshark

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. Before June 2006 Wireshark was known as Ethereal.

A packet sniffer (also known as a network analyzer or protocol analyzer) is computer software that can intercept and log data traffic passing over a data network. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is programmed to recognize the structure of different network protocols. This enables it to display the encapsulation and individual fields of a PDU and interpret their meaning.

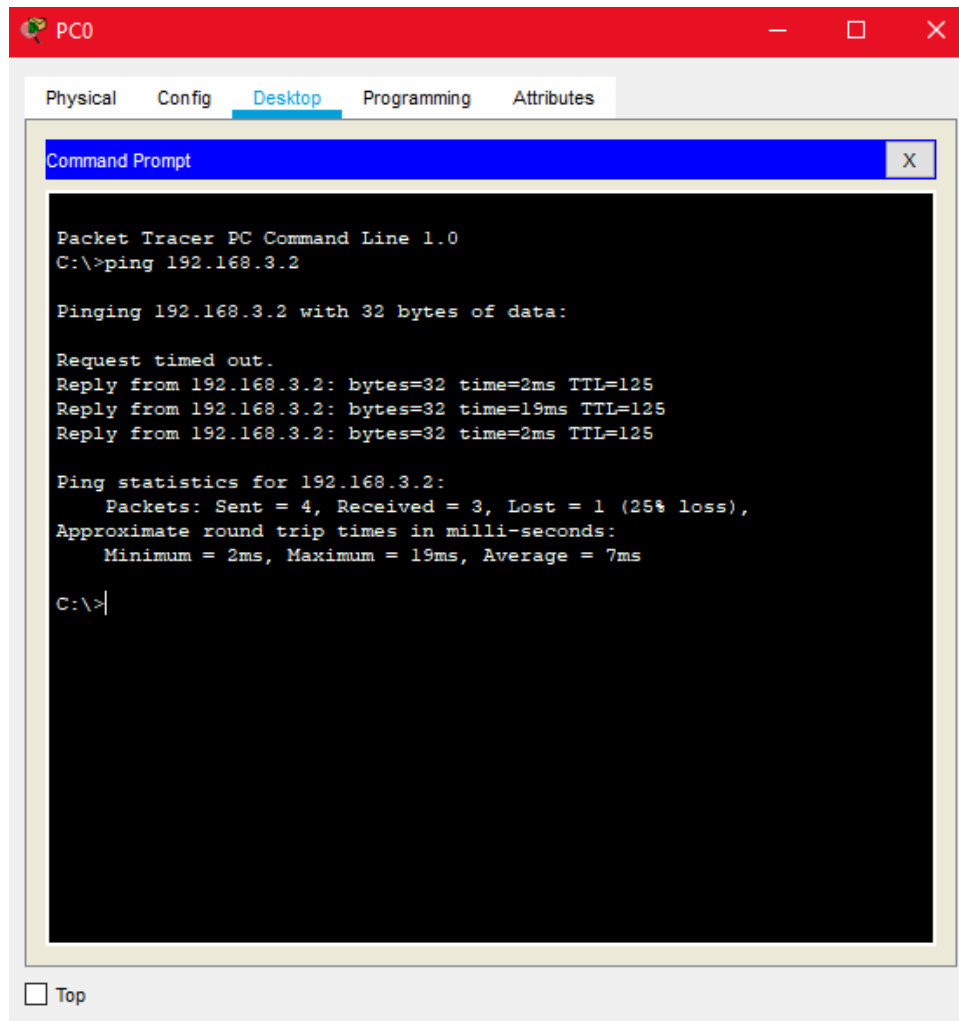


PROCEDURE

Part of the Lab that can be done at home

Part A: Observing packets using ping and tracert

1. Run the packet tracer activity file, "247-413 Lab4-ping and tracert.pka" attached in this lab assignment. **** DO NOT FOLLOW the instructions in the activity.**
2. Verify the connectivity from the source host (**PC0**) to the destination host (**PC1**) using ping command. Show your result.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

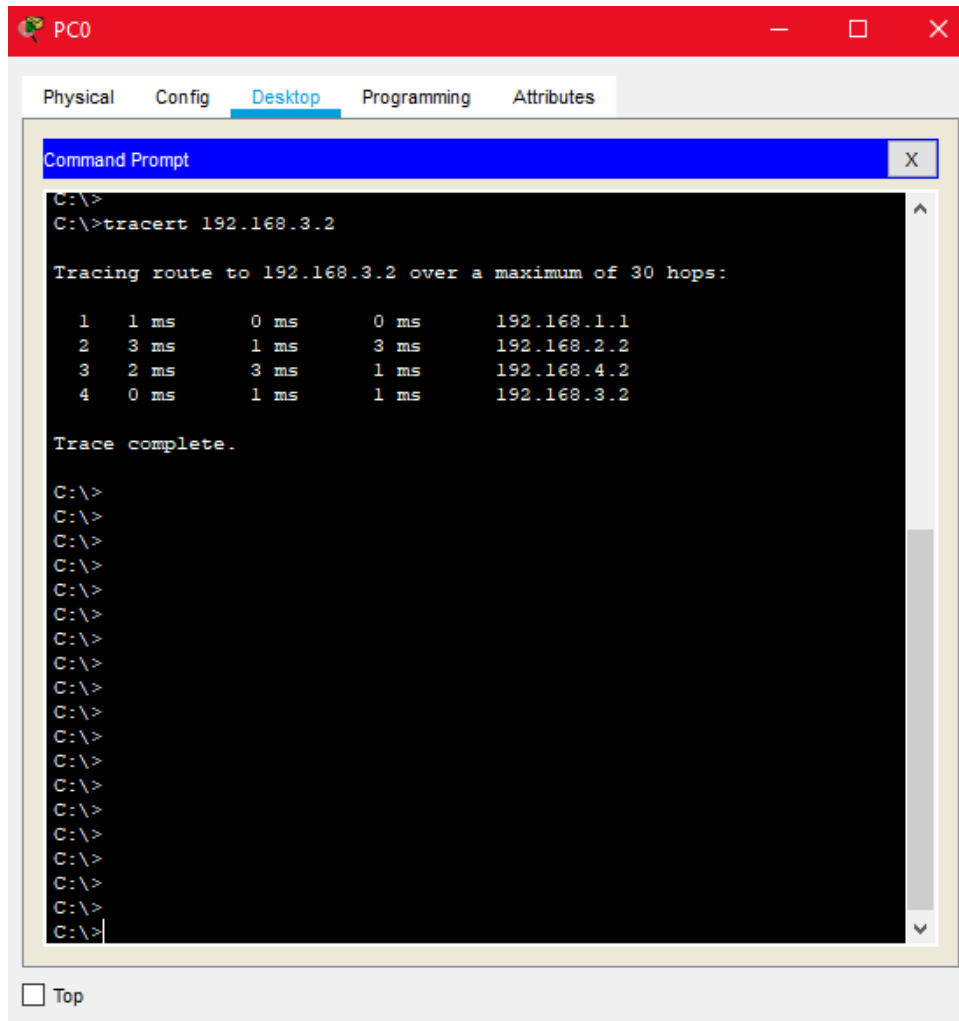
Request timed out.
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=19ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 19ms, Average = 7ms

C:\>
```

Result of ping command sent to PC1 (192.168.3.2) shown above. Despite saying there was a "25% loss", a second run of the ping command yielded a 0% loss as well with a third and fourth time of running the command. Result shows that there is a successful communication between PC0 and PC1.

3. At the same command prompt window, type in the command `tracert <ip address of PC1>`. Show your result. Perform some research on internet to understand the function of `tracert`.



The screenshot shows a Packet Tracer PC0 window with a red title bar. Inside, there are tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt has a blue title bar and contains the following text:

```
C:\>
C:\>tracert 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    192.168.1.1
  2  3 ms    1 ms    3 ms    192.168.2.2
  3  2 ms    3 ms    1 ms    192.168.4.2
  4  0 ms    1 ms    1 ms    192.168.3.2

Trace complete.

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

At the bottom of the Command Prompt window, there is a checkbox labeled "Top" which is currently unchecked.

Result of tracert command sent to PC1 (192.168.3.2) from PC0 shown above. This shows the path of how many routers the command must pass through before reaching PC1 (known as "hops"). There were only four hops that occurred once the command was done executing. There will be different results if the tracert command was to be initiated from PC1 to go to PC0 (shown in next few steps below).

a. **What is the general function and purpose** of `tracert`? (explain in detail)

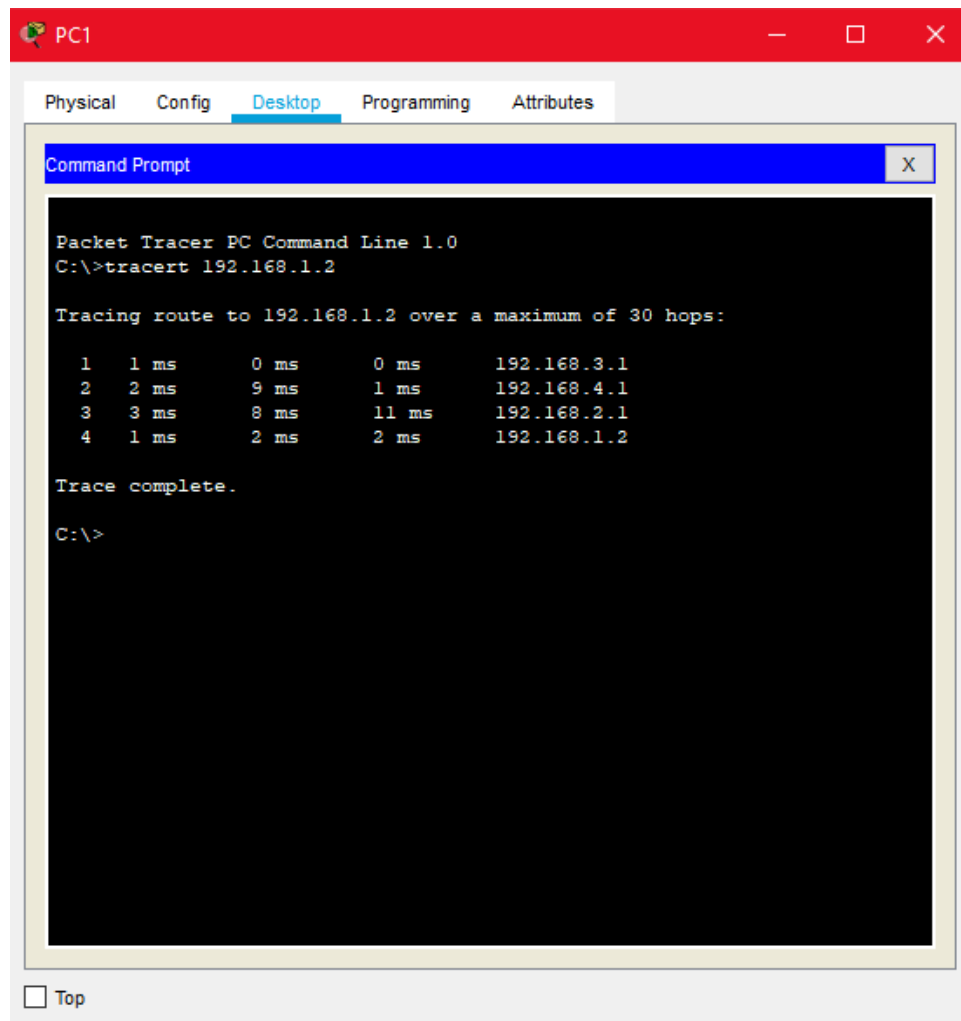
- In a nutshell: TRACERT (trace route), is a command-line utility that you can use to trace the path that an Internet Protocol (IP) packet takes from its source all the way to its destination. The TRACERT command determines the route to from a source to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT command uses varying IP Time-To-Live (TTL) values. Since each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer. TRACERT command sends the first echo packet with a TTL of 1 and increments the TTL by 1 on each subsequent transmission, until the destination responds or until the maximum TTL is reached. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. TRACERT command prints out an ordered list of the intermediate routers that return ICMP "Time Exceeded" messages. TRACERT command is also used for troubleshooting networks.

<https://support.microsoft.com/en-us/topic/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows-e643d72b-2f4f-cdd6-09a0-fd2989c7ca8e>

b. **Analyze and interpret your results from** `tracert`, based on the network under test. (You should get 4 hops). Double click on the "network connection" cloud.

- Based on the results after the `tracert` command was done executing, it took a total of four hops before the `tracert` command reached PC1. The path of which the `tracert` command is following (from PC0 to PC1) is as follows: 192.168.1.1 (interface Fa0/0 on Router0) -> 192.168.2.2 (interface Se0/0 on Router2) -> 192.168.4.2 (interface Se0/0 on Router1) -> 192.168.3.2 (PC1).

4. On **PC1** try **tracert** to **PC0**.



Result of **tracert** command sent to PC0 (192.168.1.2) from PC1 shown above. Similar as before when **tracert** command was initiated from PC0 to go to PC1, there are still four hops that occur before **tracert** command reaches PC0. The only difference here is that the path in which the command takes is slightly different (they reach different interfaces on the routers).

- a. Look well at *Figure 2: Packet Tracer Topology* and explain why the 2 **tracerts** are not hopping to the same addresses.
- The reason why the two outputs from the two **tracert** commands being executed is different is because the path that the two takes before reaching the destination will differ. The number of hops will remain the same. This behaviour can be seen clearly by looking at the network diagram below. You'll notice that the IPs (for direction 1: PC0 to PC1) will be different than for the other (for direction 2: PC1 to PC0) since they will be hitting up different interfaces on the routers.

- b. In *Figure 2: Packet Tracer Topology* all the green dots are different interfaces. Put the address to the proper interface. (I'll give you a png of the image)

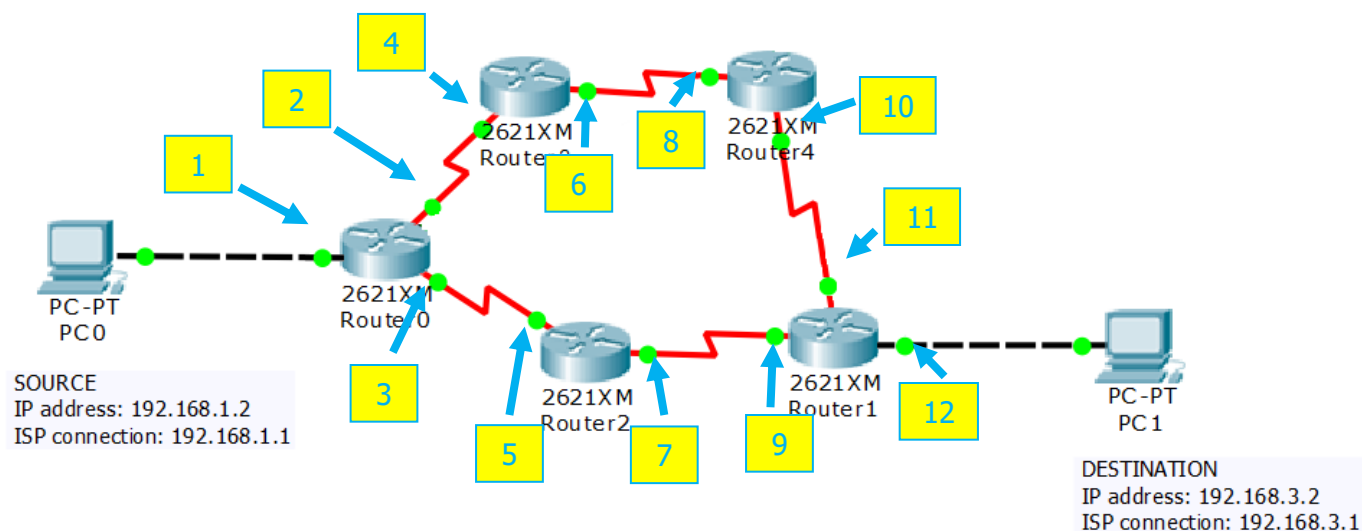


Figure 2: Packet Tracer Topology

Number (shown above)	IP address
1 (Interface Fa0/0 on Router0)	192.168.1.1/24
2 (Interface Se0/1 on Router0)	192.168.10.1/24
3 (Interface Se0/0 on Router0)	192.168.2.1/24
4 (Interface Se0/0 on Router3)	192.168.10.2/24
5 (Interface Se0/0 on Router2)	192.168.2.2/24
6 (Interface Se0/1 on Router3)	192.168.12.1/24
7 (Interface Se0/1 on Router2)	192.168.4.1/24
8 (Interface Se0/0 on Router4)	192.168.12.2/24
9 (Interface Se0/0 on Router1)	192.168.4.2/24
10 (Interface Se0/1 on Router4)	192.168.15.1/24
11 (Interface Se0/1 on Router1)	192.168.15.2/24
12 (Interface Fa0/0 on Router1)	192.168.3.1/24

5. Next, using the technique learned from the previous lab, try to view the packet path in simulation mode of Packet Tracer. Ensure that only ICMP is checked in your filter list.

In the work area window, click the network cloud to expand it and view router devices connected within the cloud. The source and destination devices are off screen. The focus is on the Routers within the network cloud only and packets forwarded between these devices.

Submit a screen shot after the completion of your simulation. Your event list should clearly show list of paths taken by the packet.

The screenshot shows a Packet Tracer simulation in Logical mode. The network topology consists of five 2621XM routers: Router0, Router1, Router2, Router3, and Router4. Router0 is connected to Router2 via Fa0/0 and Fa0/0. Router2 is connected to Router1 via Se0/0 and Se0/1. Router1 is connected to Router4 via Se0/0 and Se0/1. Router4 is connected to Router3 via Se0/0 and Se0/1. Router3 is connected to Router0 via Se0/0 and Se0/1. A network cloud is present, containing PC0 and PC1. The Event List panel on the right shows the path of an ICMP packet from PC0 to PC1 via the routers.

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Router0	ICMP
	0.002	Router0	Router2	ICMP
	0.003	Router2	Router1	ICMP
	0.004	Router1	PC1	ICMP
	0.005	PC1	Router1	ICMP
	0.006	Router1	Router2	ICMP
	0.007	Router2	Router0	ICMP
	0.008	Router0	PC0	ICMP

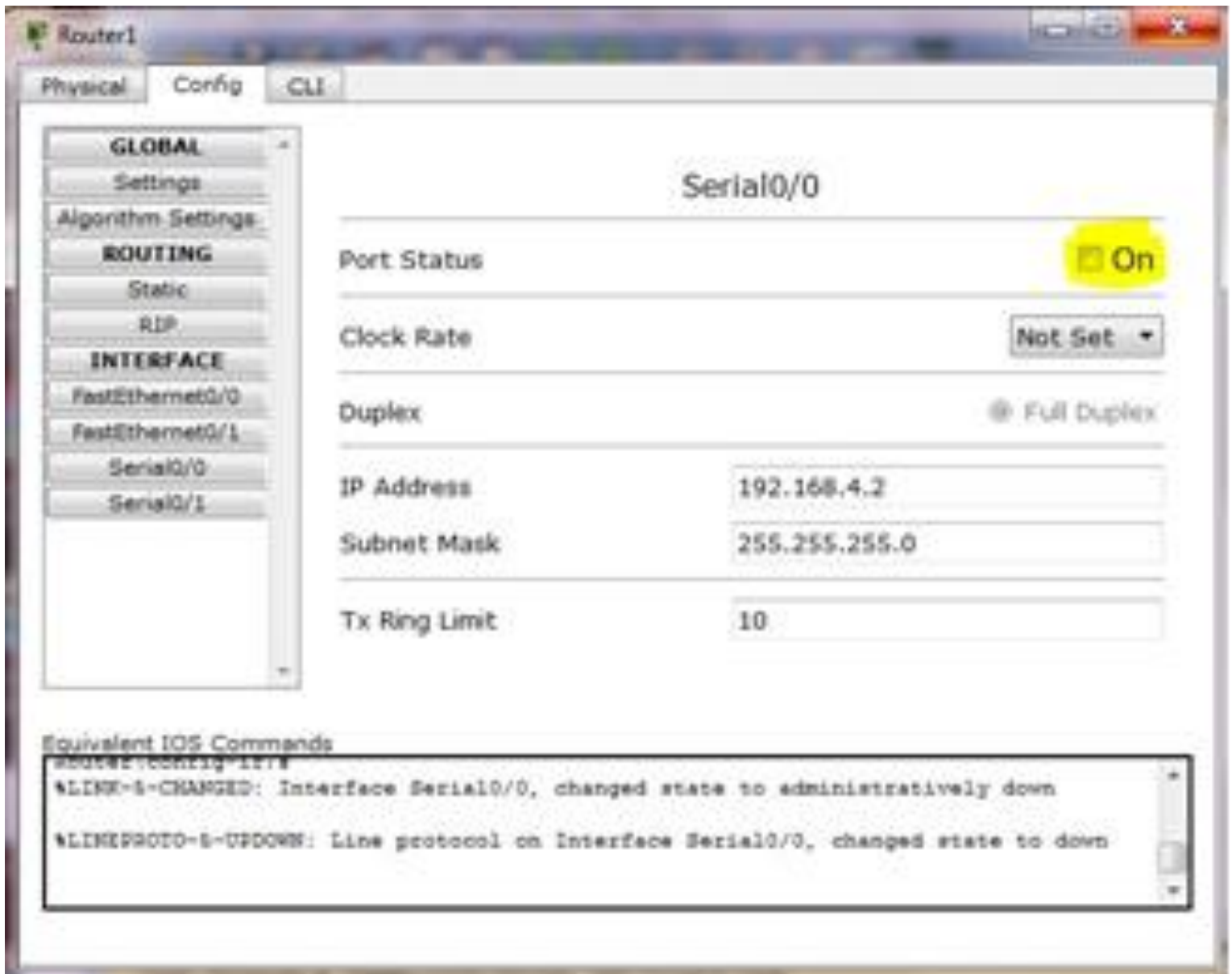
Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Router0	ICMP
	0.002	Router0	Router2	ICMP
	0.003	Router2	Router1	ICMP
	0.004	Router1	PC1	ICMP
	0.005	PC1	Router1	ICMP
	0.006	Router1	Router2	ICMP
	0.007	Router2	Router0	ICMP
	0.008	Router0	PC0	ICMP

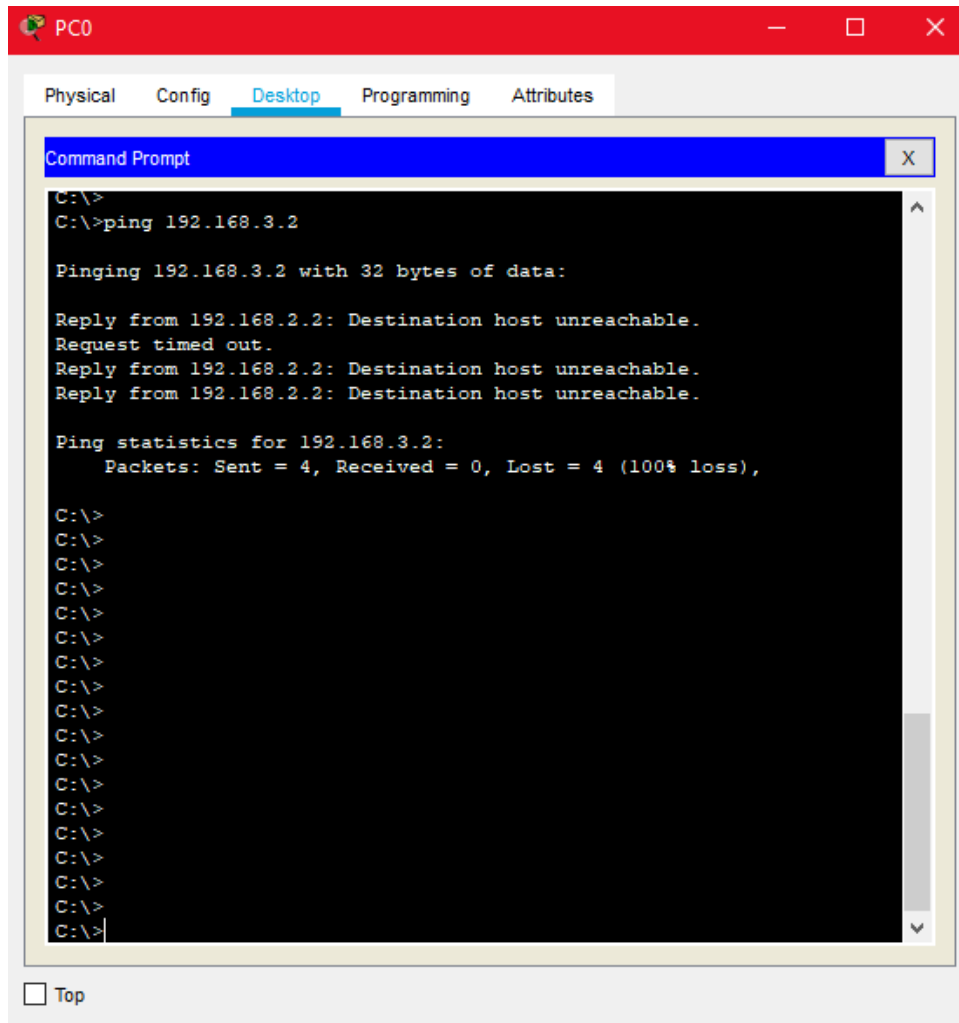
Result after sending ping request to PC1 from PC0 shown above. Results similar to tracert command output.

6. Introducing an error in the routing path.
 - a. In the network cloud, click on **Router1**. Select **Config > Serial0/0**. Uncheck the **Port Status** (turn it off). Close the configuration windows.



Config tab for Router1 shown above.

- b. Perform a `ping` from PC0 to PC1. What is the output of your `ping` command? Explain your result.



- c. Run a `tracert` command. Observe what is the different between this output, and your previously results from `tracert`. Analyze and explain your results and observation.

```

PC0
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>
C:\>tracert 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    192.168.1.1
  1  0 ms    2 ms    1 ms    192.168.2.2
  2  1 ms    *        9 ms    192.168.2.2
  3  *        1 ms    *        Request timed out.
  4  6 ms    *        1 ms    192.168.2.2
  5  *        6 ms    *        Request timed out.
  6  1 ms    *        1 ms    192.168.2.2
  7  *        2 ms    *        Request timed out.
  8  1 ms    *        1 ms    192.168.2.2
  9  *        3 ms    *        Request timed out.
 10  1 ms    *        0 ms    192.168.2.2
 11  *        2 ms    *        Request timed out.
 12  0 ms    *        0 ms    192.168.2.2
 13  *        1 ms    *        Request timed out.
 14  2 ms    *        1 ms    192.168.2.2
 15  *        2 ms    *        Request timed out.
 16  2 ms    *        2 ms    192.168.2.2
 17  *        1 ms    *        Request timed out.
 18  5 ms    *        0 ms    192.168.2.2
 19  *        1 ms    *        Request timed out.
 20  1 ms    *        1 ms    192.168.2.2
 21  *        0 ms    *        Request timed out.
 22  1 ms    *        0 ms    192.168.2.2
 23  *        0 ms    *        Request timed out.
 24  1 ms    *        0 ms    192.168.2.2
 25  *        5 ms    *        Request timed out.
 26  1 ms    *        0 ms    192.168.2.2
 27  *        3 ms    *        Request timed out.
 28  1 ms    *        1 ms    192.168.2.2
 29  *        1 ms    *        Request timed out.
 30

Trace complete.


C:\>
  
```

Result after running `tracert` command from PC0 to PC1 shown above. Between the output of this `tracert` command and the other one, this one shows that the `tracert` command is not reaching PC1. Similar to the explanation above, with the link down between Router1 and Router2, the command cannot execute as expected. When the `tracert` command is initiated, it assumes to follow the path as follows: Router0 -> Router2 -> Router1 -> final destination (since the routers haven't acknowledged that the link was down between Router1 and Router2). Since the link between Router1 and Router2 is no longer present, when the `tracert` command is run it can only travel up to Router2 (the IP 192.168.2.2 is interface Se0/0/0 on Router2). If the routers acknowledged that the link between Router1 and Router2 was down, an alternative path would have been chosen and the `tracert` command would reach the final destination (in this case PC1).

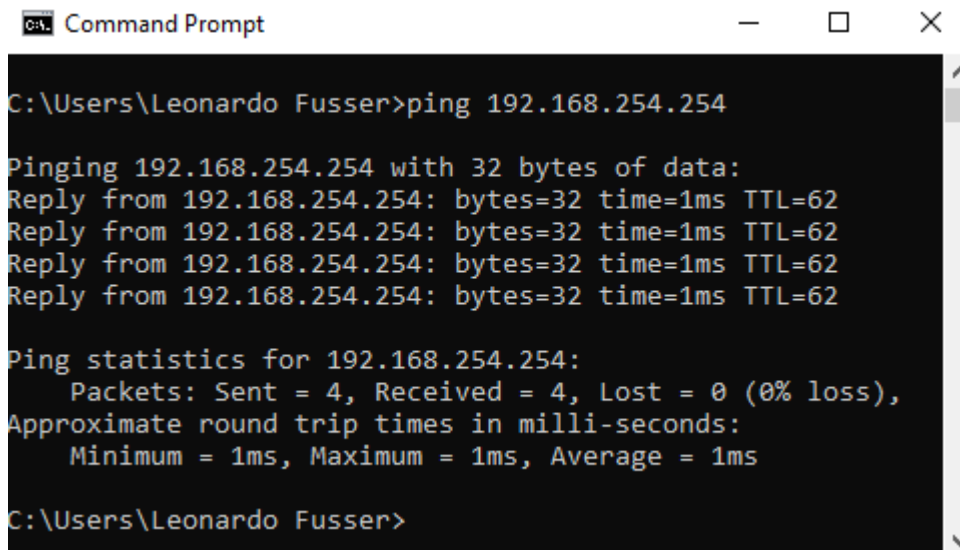
In school part of the Lab**Part B: Introduction to Wireshark**

7. Host computer preparation.

- Ensure that you have downloaded and installed Wireshark (do not use the portable version).
- Setup the IP configuration (IP address, subnet mask, default gateway) of your computer according to addressing table shown in Figure 1, to connect to Eagle Server. Pod# is the number of your computer station.

- Double click  ENG 4:4
CMS 2021
- Click on Network and internet settings.
- Click on Change adapter options.

- What cable should you use to connect between your host computer to S1-Central switch? ____
 - The cable that should be used is a copper straight-through cable due to the switch having an MDI-X interface and the PC having an MDI interface for their respective network adapters. The transmit and receive lines don't have to be crossed over because of the two devices that are being used (otherwise copper cross-over cable would have to be used like in P2P network).
- Once both hardware and software are properly configured, perform a ping operation to ensure the host computer is linked to Eagle server properly. What is the output of your ping command? (screen shot)



```
C:\Users\Leonardo Fusser>ping 192.168.254.254

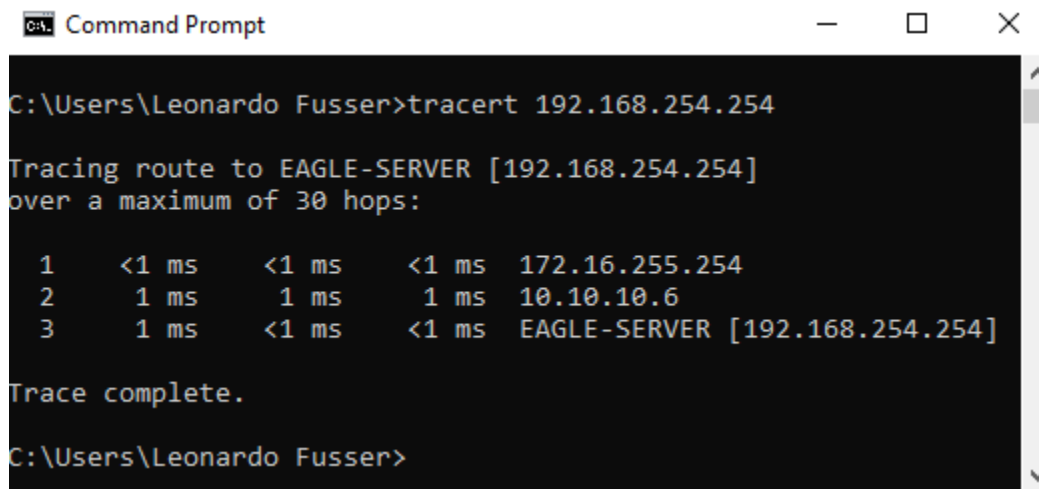
Pinging 192.168.254.254 with 32 bytes of data:
Reply from 192.168.254.254: bytes=32 time=1ms TTL=62
Reply from 192.168.254.254: bytes=32 time=1ms TTL=62
Reply from 192.168.254.254: bytes=32 time=1ms TTL=62
Reply from 192.168.254.254: bytes=32 time=1ms TTL=62

Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Leonardo Fusser>
```

Output of ping command to Eagle server (192.168.254.254) shown above. Result shows that there is a successful communication between the server and my computer. This hints that the network settings are configured correctly on my computer and, possibly, that the network itself is configured and operating correctly.

- e. Perform a tracert to Eagle Server. (screen shot) Explain and analyze your result.



```
C:\Users\Leonardo Fusser>tracert 192.168.254.254

Tracing route to EAGLE-SERVER [192.168.254.254]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    172.16.255.254
  1  1 ms      1 ms      1 ms      10.10.10.6
  2  1 ms      <1 ms     <1 ms     EAGLE-SERVER [192.168.254.254]

Trace complete.

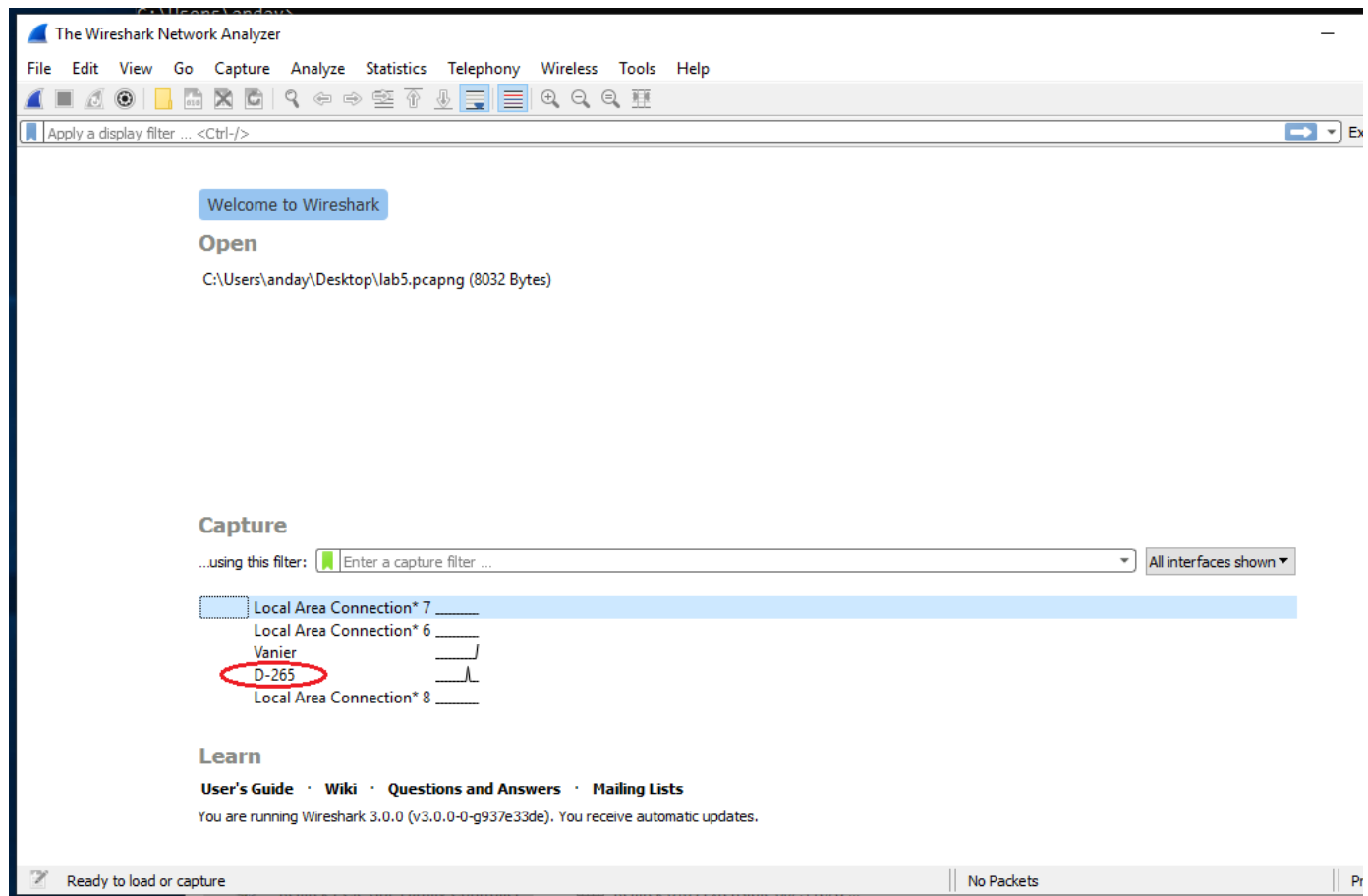
C:\Users\Leonardo Fusser>
```

Output of tracert command above. As discussed above in Part A, tracert command shows the logical path of passing through routers the command takes (hops) to reach the destination (specified IP address). From above, we can see that three hops were done in order to reach the Eagle server from my computer. The path that is taken is as follows: 172.16.255.254 (interface Fa0/0 on R2-Central) -> 10.10.10.6 (interface S0/0/0 on R1-ISP) -> 192.168.254.254 (Eagle server).

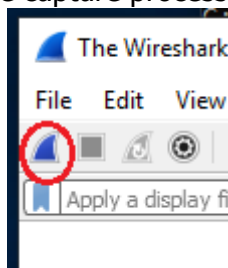
- f. If you had access to the Eagle server and you performed a tracert to your PC, what would be the output?

- Knowing that three hops occurred from executing tracert command from my computer to the Eagle server, there will be three hops going from the Eagle server to my computer as well. But, the path will be different and it will look something like this: 192.168.254.253 (interface Fa0/0 on R1-ISP) -> 10.10.10.5 (interface S0/0/0 on R2-Central) -> 172.16.22.1 (my computer). Theoretically, this can be easily found by looking at the Eagle server network overview diagram from above (under "Background" section).

8. Launch Wireshark on the host computer. To start data capture it is first necessary to go to the Capture menu to ensure that Wireshark is set to monitor the *correct interface based on your host configuration*.



Start the capture process.



9. From the command line of the computer, ping the Eagle Server, using the command `ping 192.168.254.254`. After receiving the successful replies to the ping in the command line window, stop the packet capture.

10. Examine the packet list pane on Wireshark, which should look something like this:

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
276	376.0009010	Cisco_25:44:17	Cisco_25:44:17	LOOP	60	Reply
277	376.9151060	Cisco_25:44:17	Spanning-tree-(for STP	60	Conf. Root = 32768/1/00:23:ea:25:44:00 Cost = 0 Port	
278	377.6432760	172.16.23.1	192.168.254.254	ICMP	74	Echo (ping) request id=0x0001, seq=63/16128, ttl=128
279	377.6439480	192.168.254.254	172.16.23.1	ICMP	74	Echo (ping) reply id=0x0001, seq=63/16128, ttl=62
280	378.6498350	172.16.23.1	192.168.254.254	ICMP	74	Echo (ping) request id=0x0001, seq=64/16384, ttl=128
281	378.6504730	192.168.254.254	172.16.23.1	ICMP	74	Echo (ping) reply id=0x0001, seq=64/16384, ttl=62
282	378.9238440	Cisco_25:44:17	Spanning-tree-(for STP	60	Conf. Root = 32768/1/00:23:ea:25:44:00 Cost = 0 Port	
283	379.6638220	172.16.23.1	192.168.254.254	ICMP	74	Echo (ping) request id=0x0001, seq=65/16640, ttl=128
284	379.6644600	192.168.254.254	172.16.23.1	ICMP	74	Echo (ping) reply id=0x0001, seq=65/16640, ttl=62
285	380.6778150	172.16.23.1	192.168.254.254	ICMP	74	Echo (ping) request id=0x0001, seq=66/16896, ttl=128
286	380.6784590	192.168.254.254	172.16.23.1	ICMP	74	Echo (ping) reply id=0x0001, seq=66/16896, ttl=62
287	380.9250880	Cisco_25:44:17	Spanning-tree-(for STP	60	Conf. Root = 32768/1/00:23:ea:25:44:00 Cost = 0 Port	
288	382.9303170	Cisco_25:44:17	Spanning-tree-(for STP	60	Conf. Root = 32768/1/00:23:ea:25:44:00 Cost = 0 Port	

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
5	3.611880	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
14	5.622656	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
20	8.736214	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
22	9.630181	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
27	10.747731	172.16.22.1	192.168.254.254	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 28)
28	10.748719	192.168.254.254	172.16.22.1	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=62 (request in 27)
30	11.750715	172.16.22.1	192.168.254.254	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 31)
31	11.751774	192.168.254.254	172.16.22.1	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=62 (request in 30)
33	12.758131	172.16.22.1	192.168.254.254	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 34)
34	12.759016	192.168.254.254	172.16.22.1	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=62 (request in 33)
35	13.765474	172.16.22.1	192.168.254.254	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 36)
36	13.766445	192.168.254.254	172.16.22.1	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=62 (request in 35)
40	15.761347	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
43	17.641247	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
51	23.776464	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
71	42.957149	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
79	45.973793	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
84	49.086444	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
86	49.978357	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
92	52.101033	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
97	56.106553	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
102	57.990405	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)
114	64.106637	10.10.10.6	172.16.22.1	ICMP	70	Destination unreachable (Host unreachable)

> Frame 5: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{F46C336C-16C4-40CE-BF3A-ABEE5B4E3CDE}, id 0
 > Ethernet II, Src: Cisco_6b:d2:88 (00:19:56:6b:d2:88), Dst: Dell_a2:ce:bd (d4:be:d9:a2:ce:bd)
 > Internet Protocol Version 4, Src: 10.10.10.6, Dst: 172.16.22.1
 > Internet Control Message Protocol

0000 d4 be d9 a2 ce bd 00 19 56 6b d2 88 08 00 45 00Vk....E-
 0010 00 38 2c 10 00 00 fe 01 ba 93 0a 0a 0a 06 ac 10 .8,.....
 0020 16 01 03 01 c2 f9 00 00 00 45 00 00 34 45 b7E..4E-
 0030 40 00 7e 06 c4 60 ac 10 16 01 0a 01 26 9a fd 88 @.....&...
 0040 1e 00 fa 58 24 23X\$#

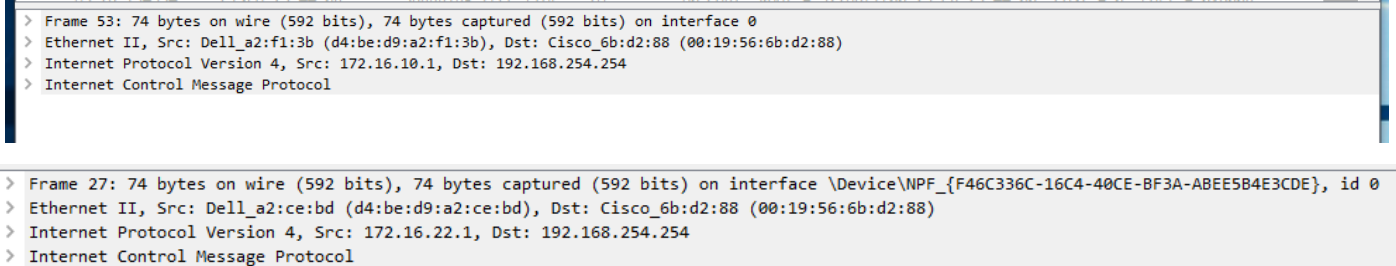
Wireshark packet capture output after ping command execution shown above. Results in pink are caused when the ping command was sent to the Eagle server's IP address.

- What protocol is used by ping? What is the full protocol name?
 - The protocol used by ping command is the ICMP (internet control message protocol).
- What are the names of the two ping messages?
 - The names of the two ping messages are request and reply.

c. Are the listed source and destination IP addresses what you expected? Why?

- The listed source and destination IP addresses are what I expected because they are originating from the origins I expect them to come from. For instance, if I was expecting a reply, I would be expecting it to come directly from the Eagle server's IP address (in this case it is 192.168.254.254) and if I was sending the ping command, I would expect the request to come directly from my computer (in this case 172.16.22.1). As it shows in the screenshot above, this is the case therefore my assumptions are correct.

11. Select the first echo request packet on the list with the mouse. Check the Packet Detail pane which looks like this:



The screenshot shows two sections of the Wireshark Packet Detail pane. The top section is for Frame 53, showing Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol details. The bottom section is for Frame 27, also showing Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol details. The text in the screenshot is as follows:

```
> Frame 53: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Dell_a2:f1:3b (d4:be:d9:a2:f1:3b), Dst: Cisco_6b:d2:88 (00:19:56:6b:d2:88)
> Internet Protocol Version 4, Src: 172.16.10.1, Dst: 192.168.254.254
> Internet Control Message Protocol

> Frame 27: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F46C336C-16C4-40CE-BF3A-ABEE5B4E3CDE}, id 0
> Ethernet II, Src: Dell_a2:ce:bd (d4:be:d9:a2:ce:bd), Dst: Cisco_6b:d2:88 (00:19:56:6b:d2:88)
> Internet Protocol Version 4, Src: 172.16.22.1, Dst: 192.168.254.254
> Internet Control Message Protocol
```

Details of first request packet originating from my computer shown above.

Click each of the four greater than sign (>) buttons to expand the information. Spend some time to scroll this information and understand the information displayed.

- a. Locate the two different types of "Source" and "Destination" addresses. Why are there two types?
 - Two different types of "Source" and "Destination" addresses are the MAC addresses and IPv4 addresses.
- b. What protocols are in the Ethernet II frame?
 - Under the Ethernet II frame, there is only the IPv4 protocol that is being used.

12. Quit Wireshark without saving.