|  |
| --- |
| Image result for unc charlotte college of computing and informatics |
| Network Security  ITIS 6167 |
| Homework #  Lab 1: cisco lab routers  RUCHIRA POKHRIYAL |

Table of Contents

[1.0 Introduction 3](#_Toc19737693)

[2.0 Activity Log 3](#_Toc19737694)

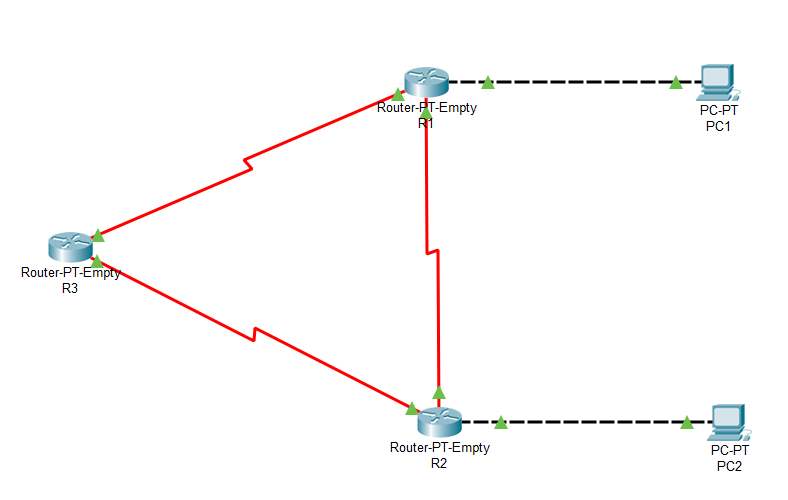
[3.0 Lab Results 3](#_Toc19737695)

# 1.0 Introduction

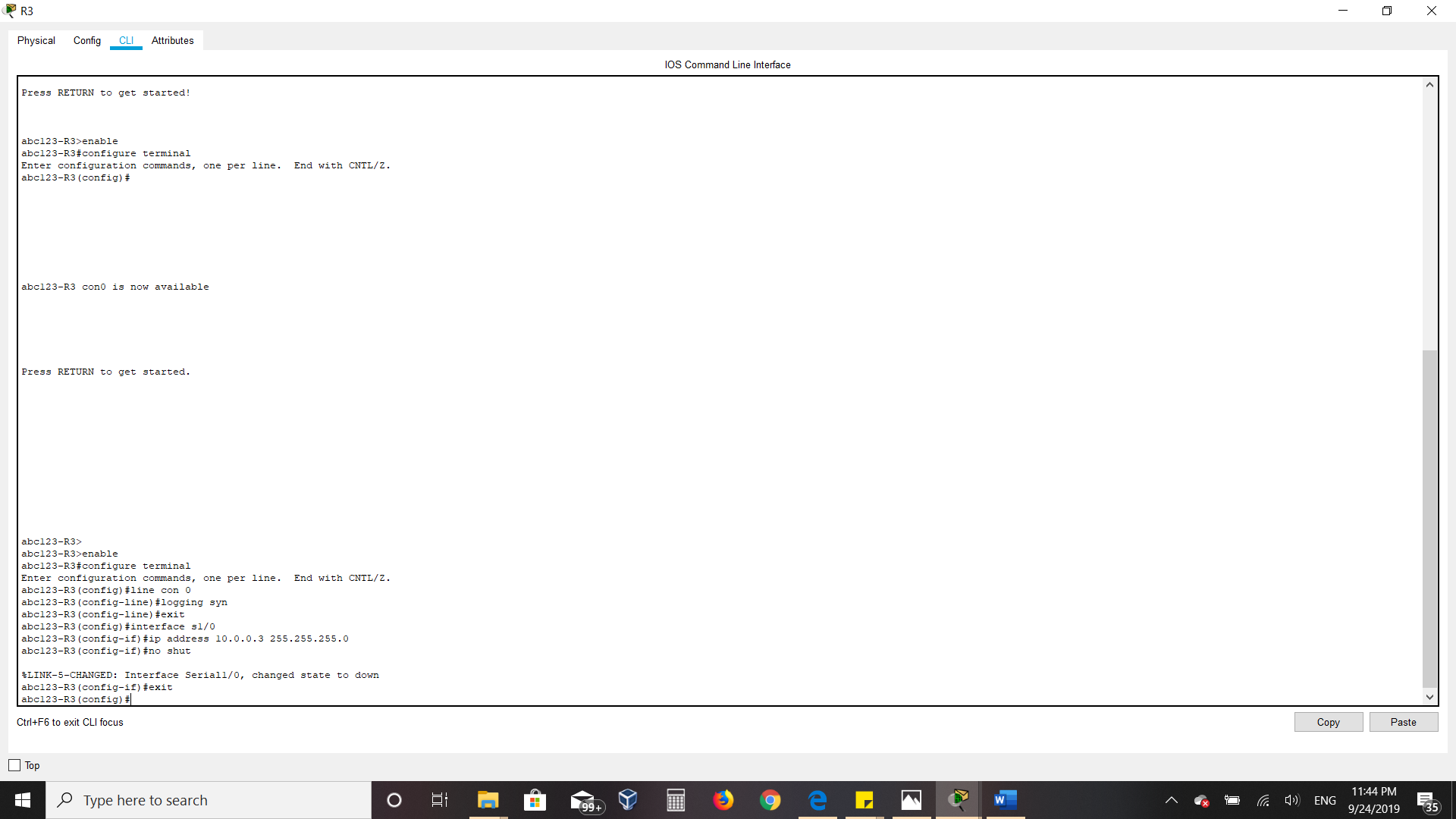
The primary motivation for this lab is to use Cisco Packet Tracer- a cross-platform, visual simulation tool owned by Cisco to set up a VPC, containing three routers and two PC's. The next goal is to connect all the devices together and facilitate communication. For this, we will connect the routers and PC's using serial and cross over cable respectively. Next, we will learn how to configure routing on each router, so that the packets are forwarded to the next router correctly. After the router and cable configuration is complete, all the devices on the network would be connected in such a way that PC1 will able to communicate to PC2 and vice versa.

In this lab, I would be implementing the installation of Routing Information protocol AKA RIP, which is a dynamic protocol that uses hop count as a routing metric to find the best path between the source and the destination network. Through RIP, traffic will always be routed through the shortest path in our network. Additionally, in this I would also be implementing and testing ACLs (Access Control Lists) to permit and restrict data flows into and out of network interfaces.

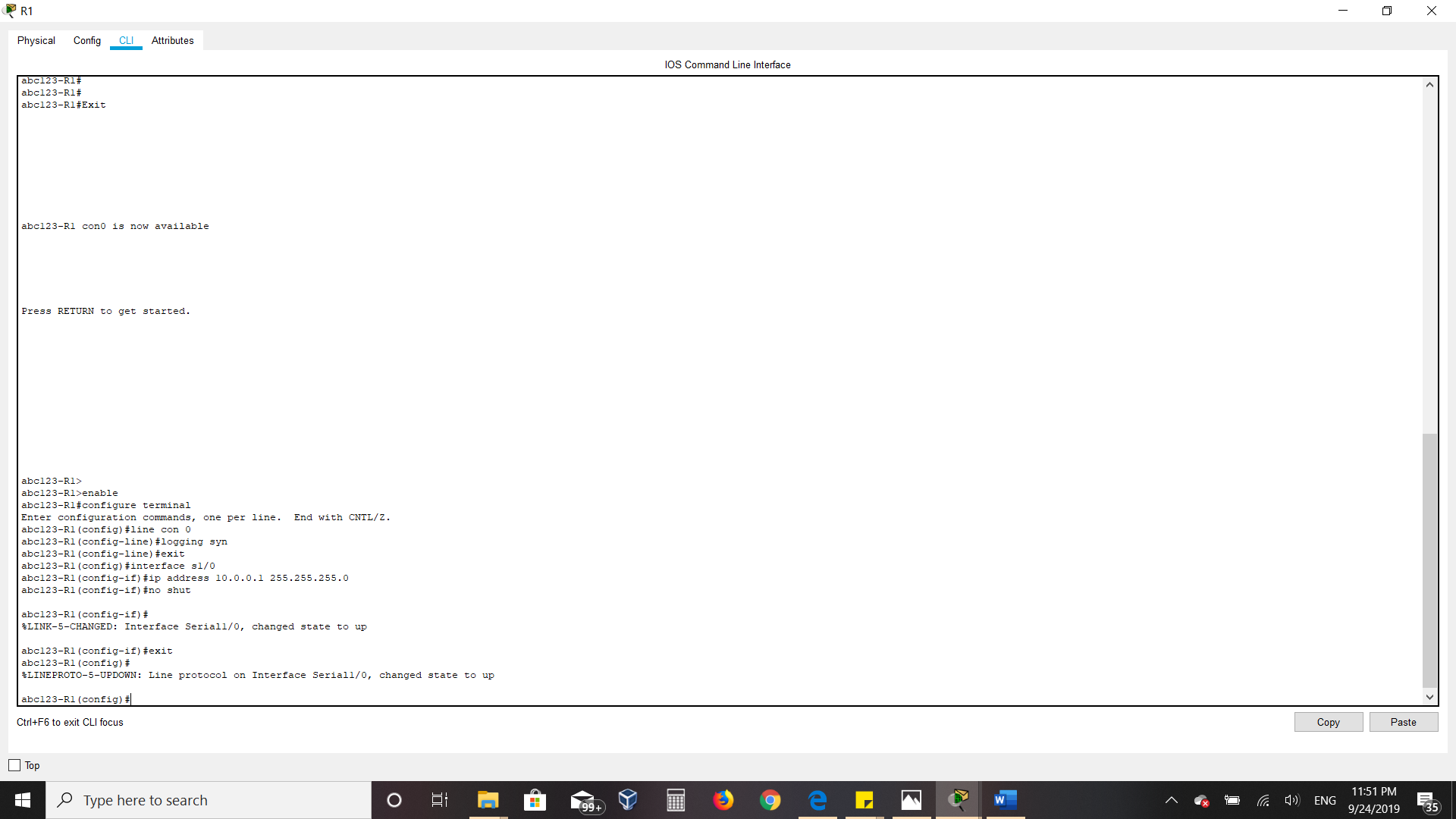
# 2.0 Activity Log



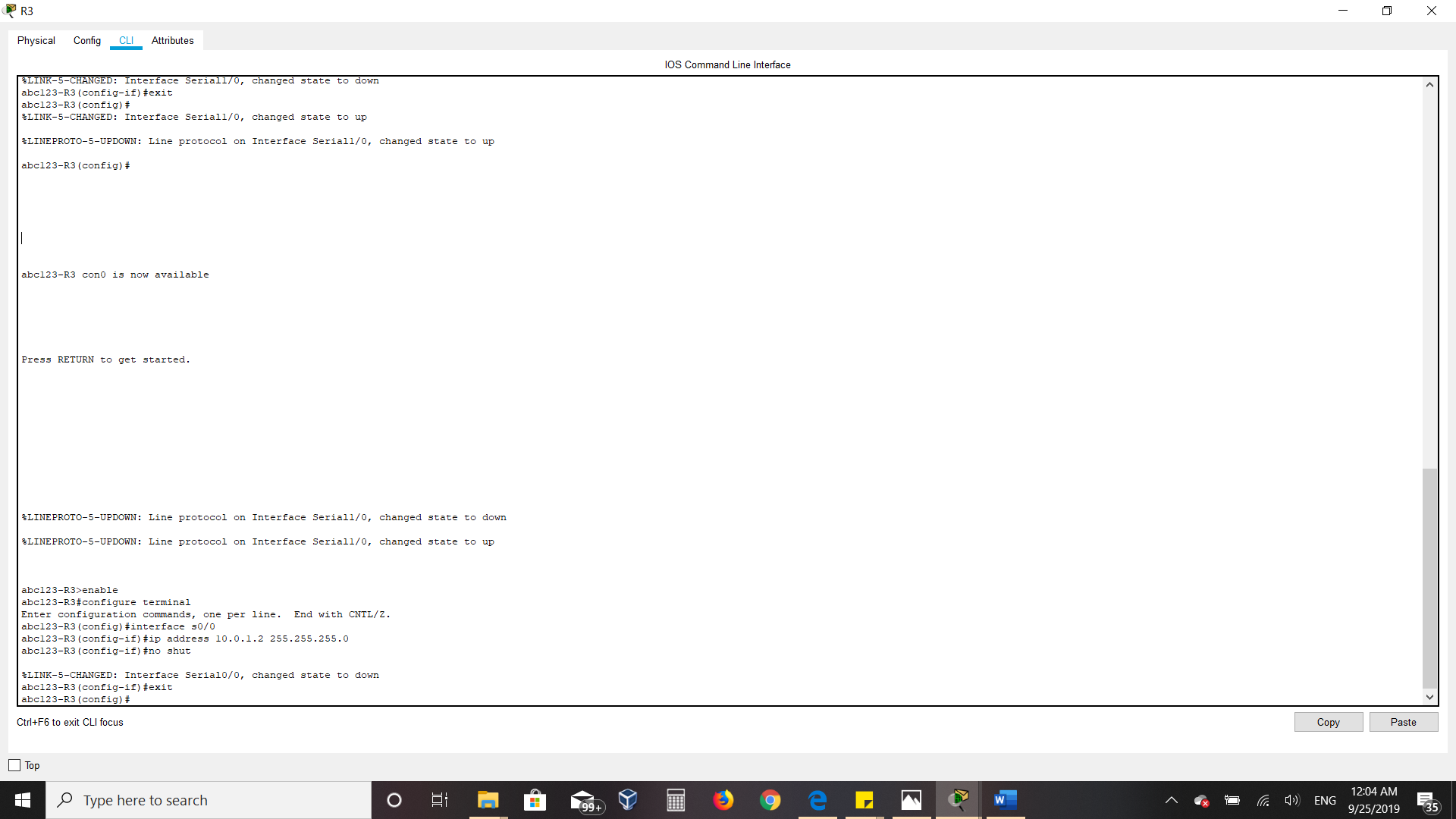
* First, I dragged and dropped three “Router-PT-Empty” type routers from Network devices into the logical view. Then double clicked each router and under the Config tab, renamed the routers display name to R1, R2, and R3 and also renamed their host names to ‘abc123-R1’,’ abc123-R2’ and ‘abc123-R3’ respectively.
* Next, I added two PCs from End Devices into the logical view. After adding PC’s double-clicked on each PC and under the Config tab, renamed the display names to PC1 and PC2 respectively.
* After adding and renaming all the chosen devices, the next step was to connect the routers with each other using serial interface and routers to PC using cross over fast ethernet cable. To add the interfaces, routers were first shut down, the interface was added then again, the routers were powered on.
* I started by adding two serial interfaces: S0/0, S1/0 and one Faster ethernet interface: F2/0 in Router 2.
* Similarly, I added two serial interfaces: S0/0, S1/0 and one Faster ethernet interface: F2/0 in Router 1.
* Finally, added two serial interfaces: S0/0, S1/0 and one Faster ethernet interface Faster ethernet interface and F2/0 in Router 3.
* The next step is to connect the three routers via serial and cross over cable. So, I started by using serial cable to connect Router 3 S1/0 interface to Router 1 S1/0 interface, Router 3 S0/0 interface to Router 2 S0/0 interface and Router 1 S0/0 interface to Router 2 S1/0 interface.
* Next, I connected Router 1 via Fast Ethernet F2/0 to PC1 on Fast Ethernet F2/0. Then connected Router 2 via Fast Ethernet 2/0 to PC2’s Fast Ethernet 0/0.
* Next step was to move on to the configuration part, so I started configuring Router 3 so that the traffic can flow from Router 3 to Router 1, I assigned an IP addresses to the interfaces. The screenshots below show all the configuration details:



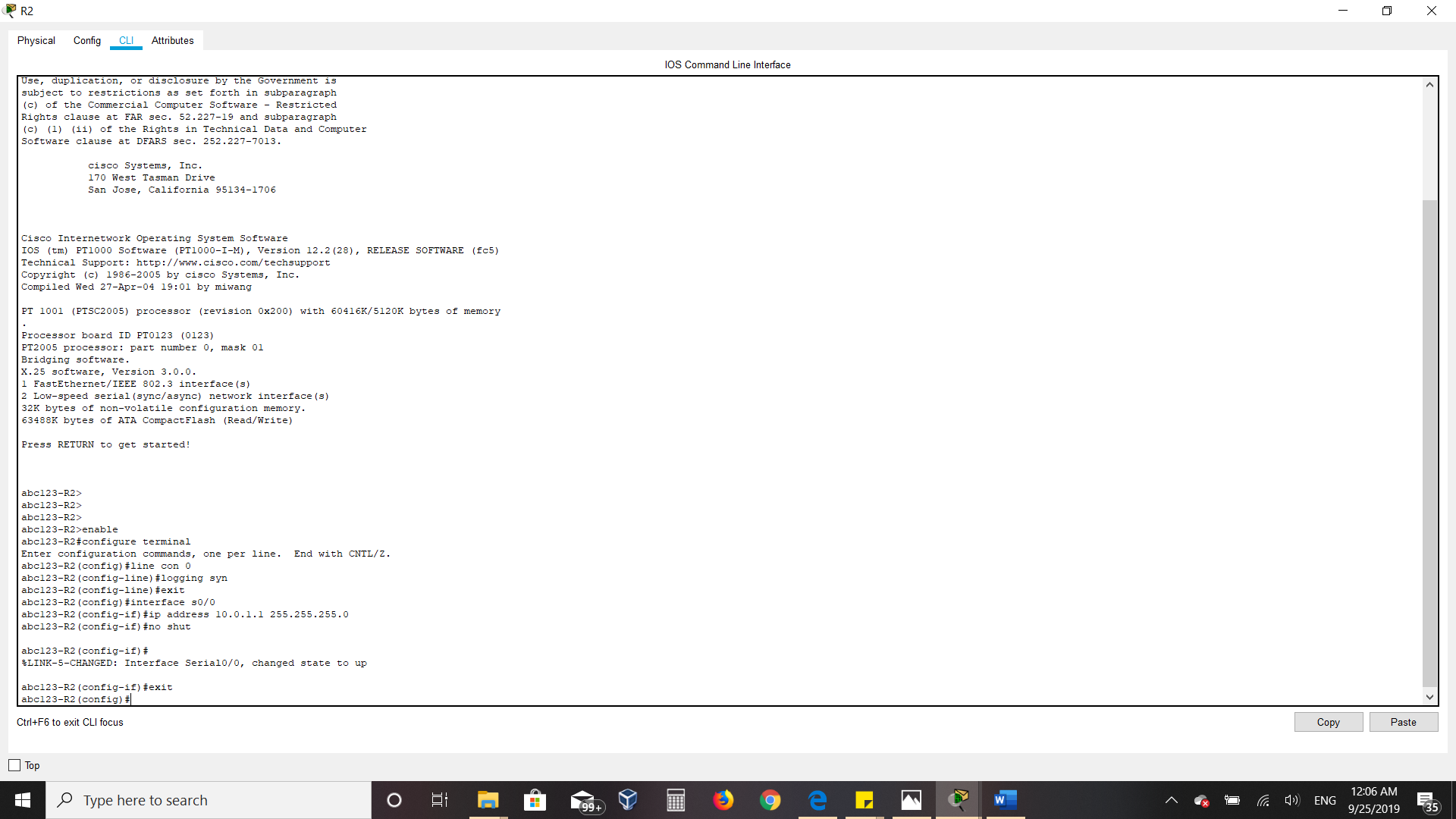
* Then I configured Router 1 so that the traffic can flow from Router 1 to Router 3, assigned an IP addresses to the interfaces. The screenshot below shows all the configuration details:



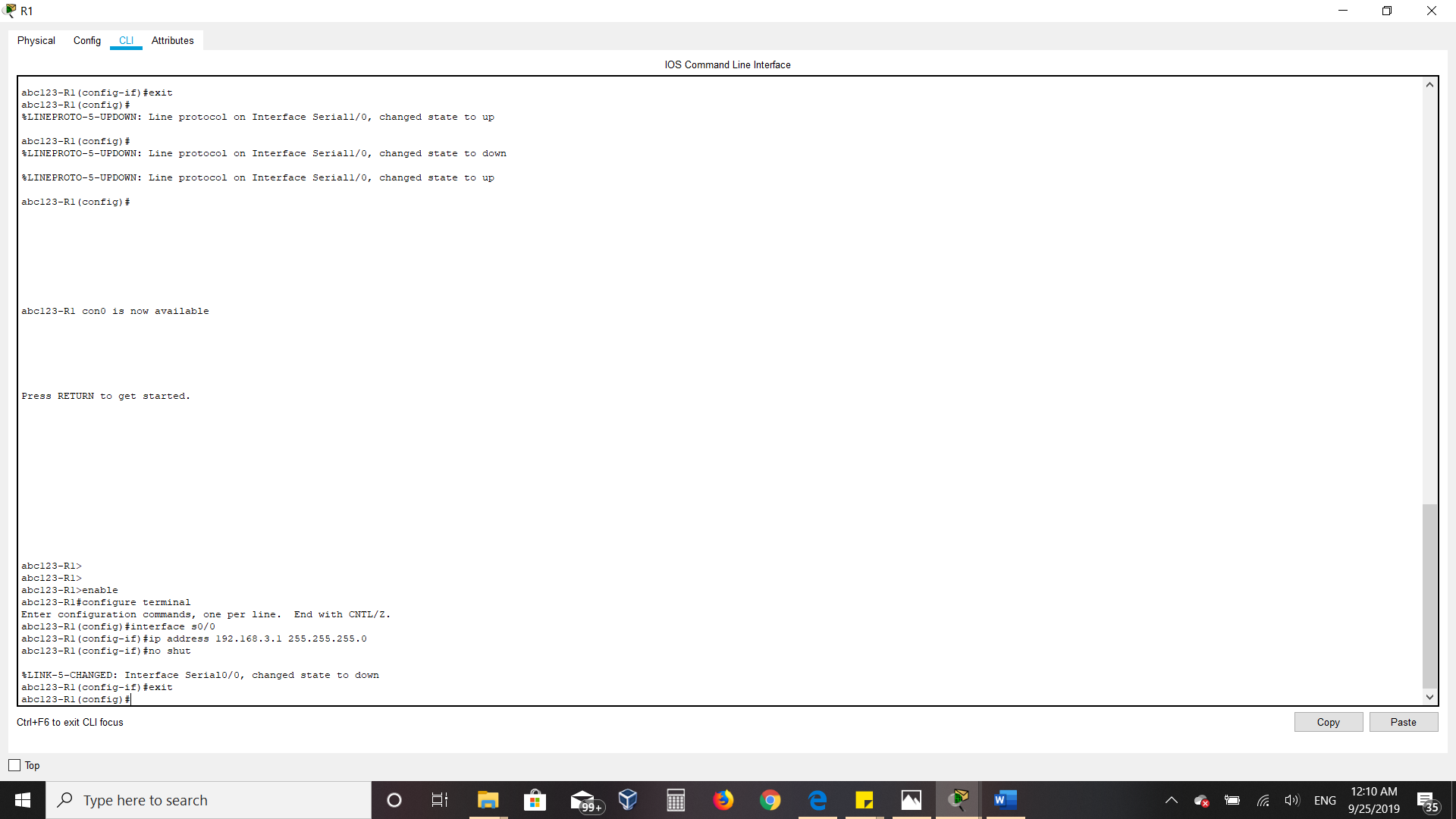
* I configured Router 3 so the traffic can flow from Router 3 to Router 2 and assigned IP address to the interface. The screenshot below shows all the configuration details:



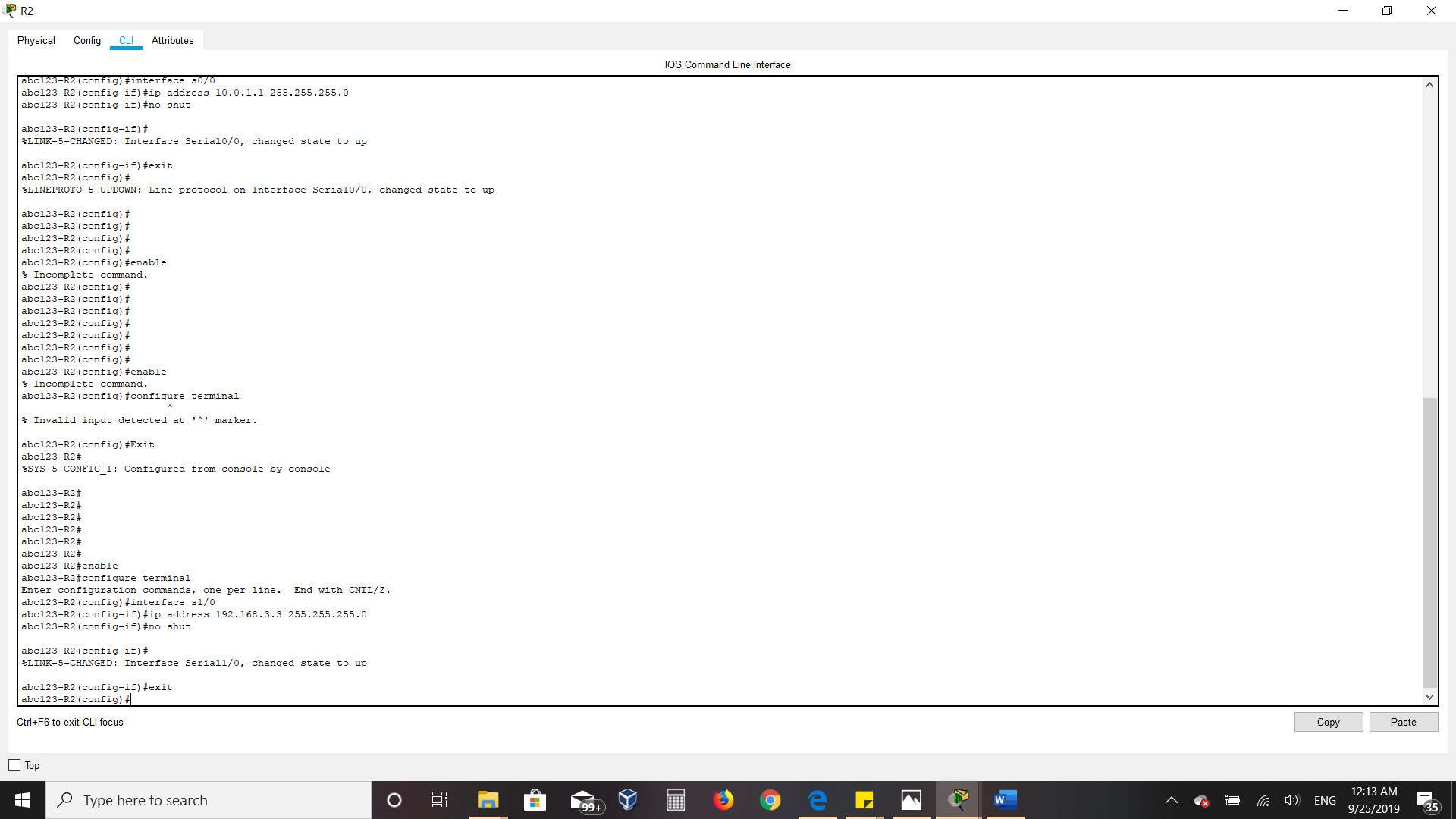
* Now, again on Router 2, we configure traffic flow between Router 2 and Router 3 as shown below:



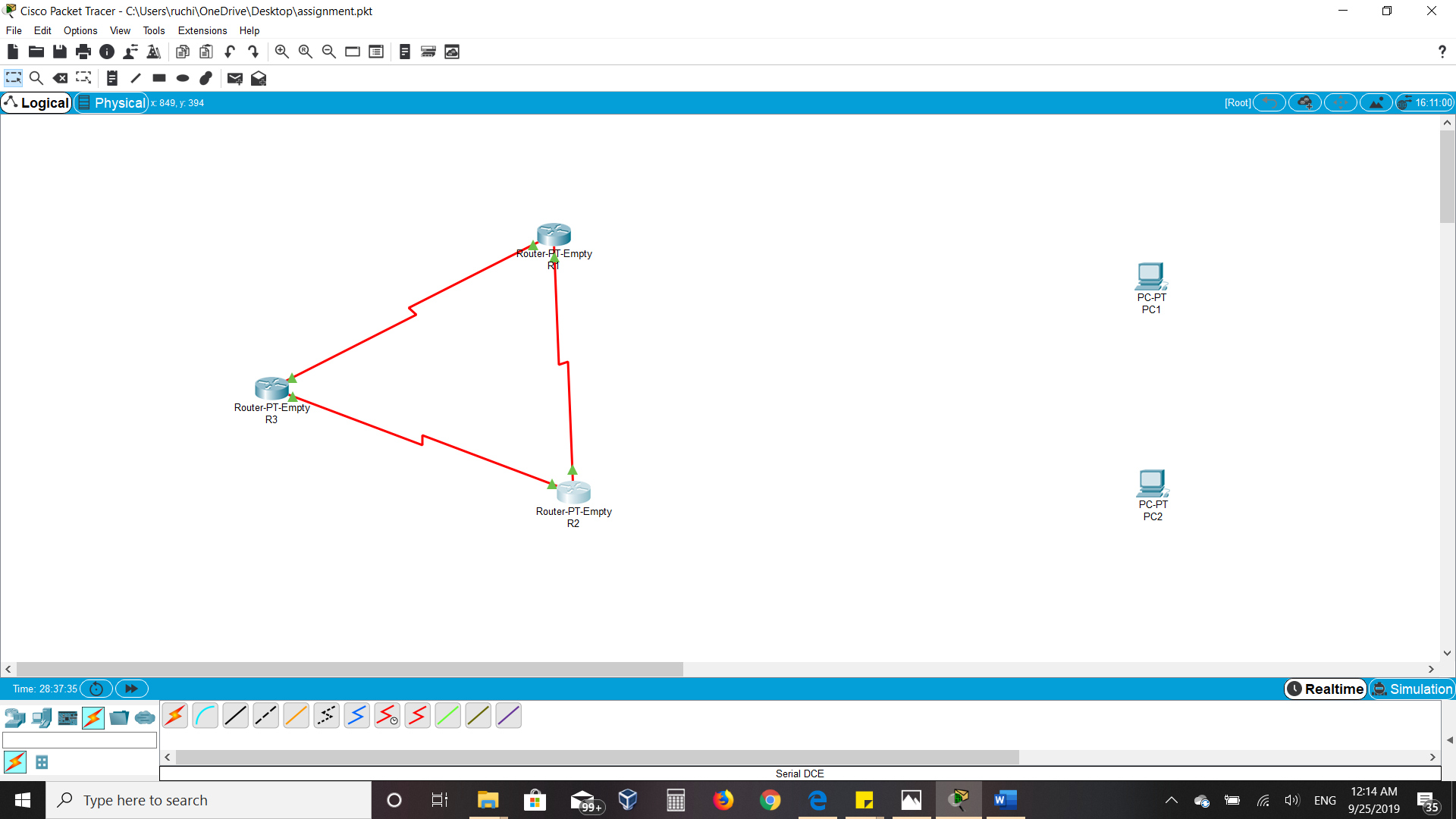
* Again, moving back to Router 1 to configure routing between Router 1 and Router 2:



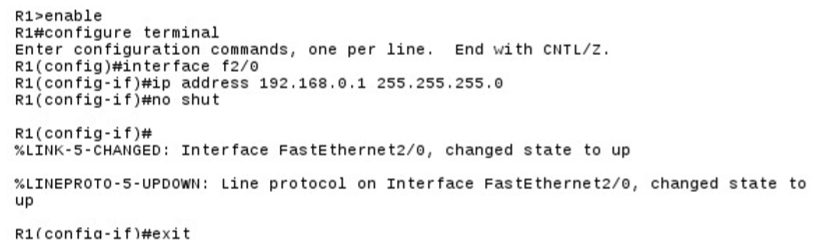
* Finally, configured routing between Router 2 and Router 1. Details are shown below:



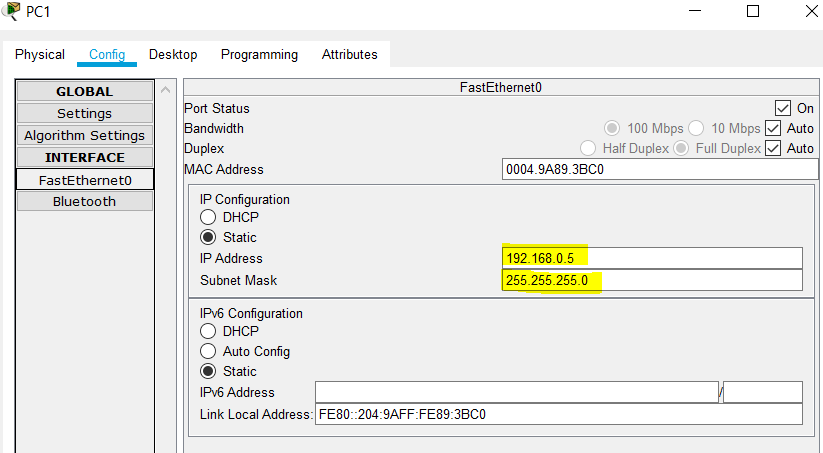
* After enabling routing on all routers, the data flow arrows turned green indicating that routing has been enabled successfully between all the routers. Below is the LAN network after configuring routing:

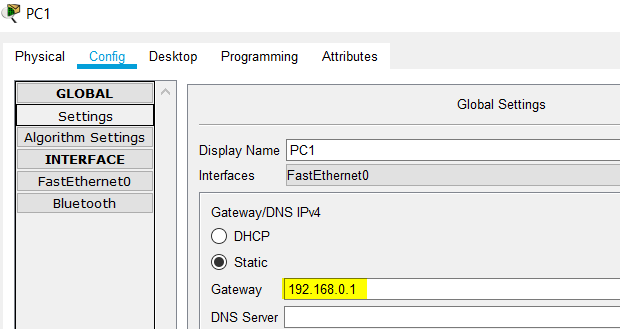


* After routing, the next steps were to install RIP version 2 on all three routers so that they choose the shortest route for traffic flow.
* To start, I first connected PC1 with R1 using cross over cable on fast ethernet interface then ran the following commands on the Config pane of Router 1 to enable routing between PC 1 and Router 1:
* Now we have to enable routing between Router 1 and Pc1 which was achieved by running following config on Router 1:

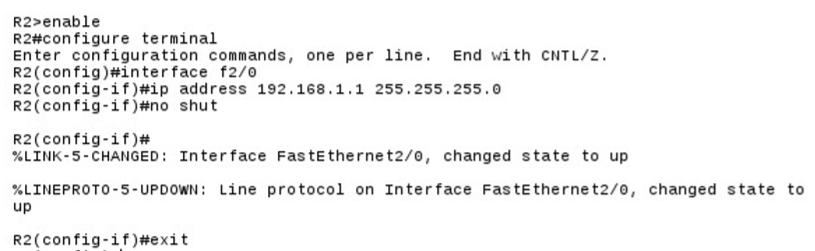


* Assigning static IP and gateway to PC1:

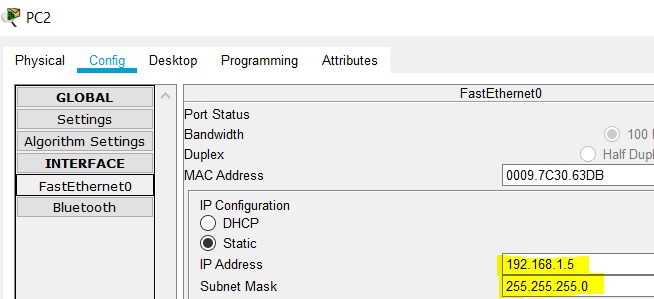


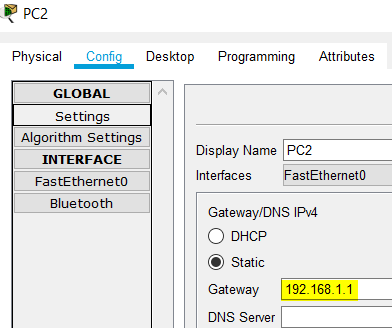


* Similarly, connected PC2 with R2 using cross over cable on fast ethernet interface then ran the following commands on the Config pane of Router 2 to enable routing between PC 2 and Router 2:

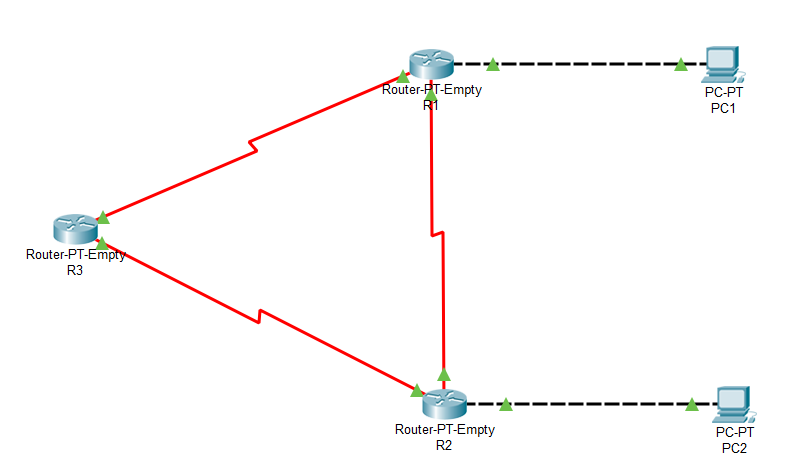


* Assigning static IP and gateway to PC2:

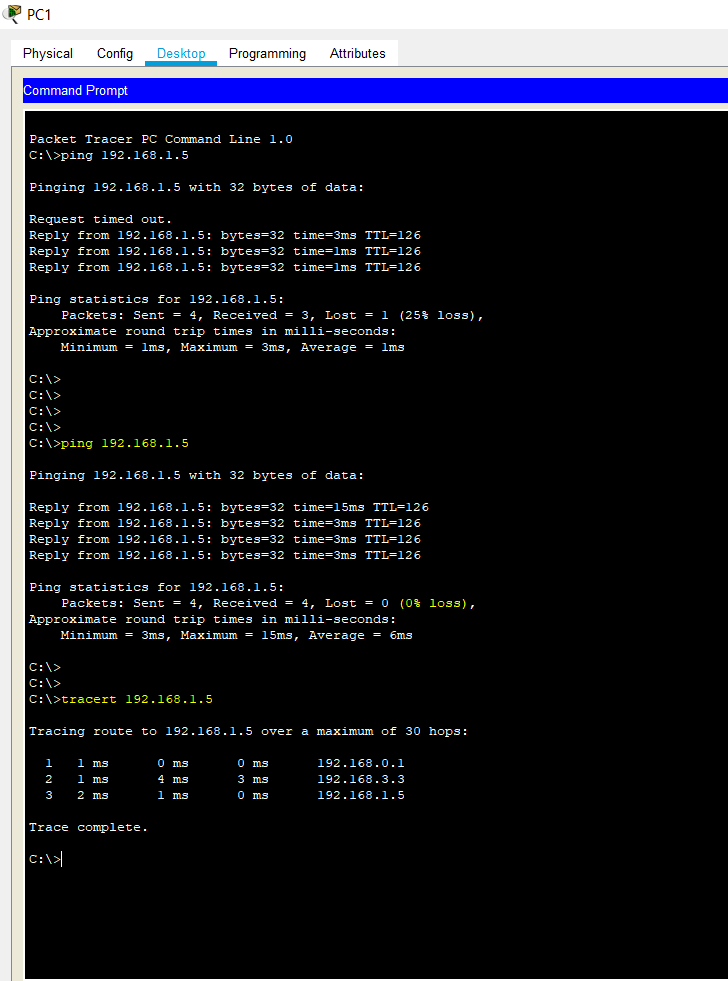




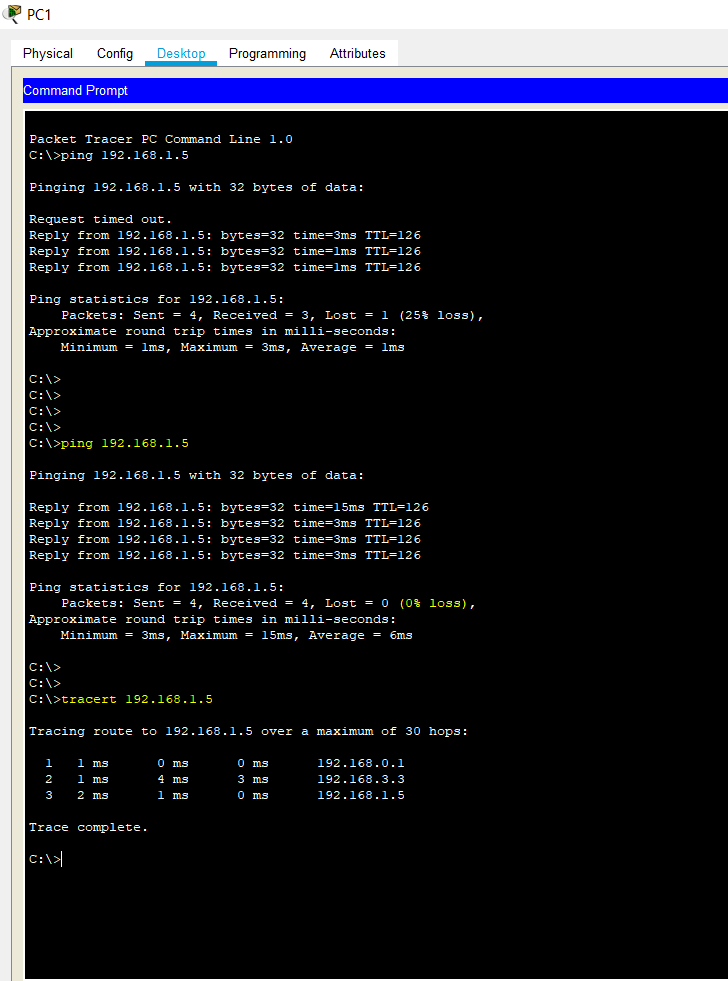
* Ultimately, The Logical View looks like below when all the cables are connected, routers have been configured, and static IPs have been assigned to PC’s:



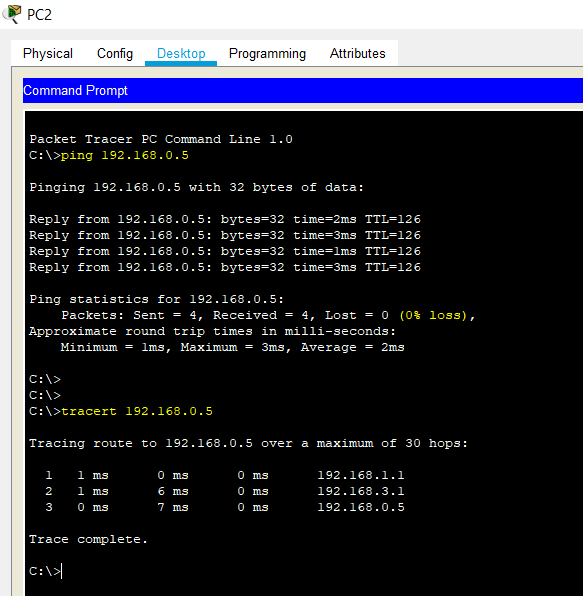
* Now to examine the traffic flow, I pinged PC2 from PC1 and straight away and could get a response back as shown below:



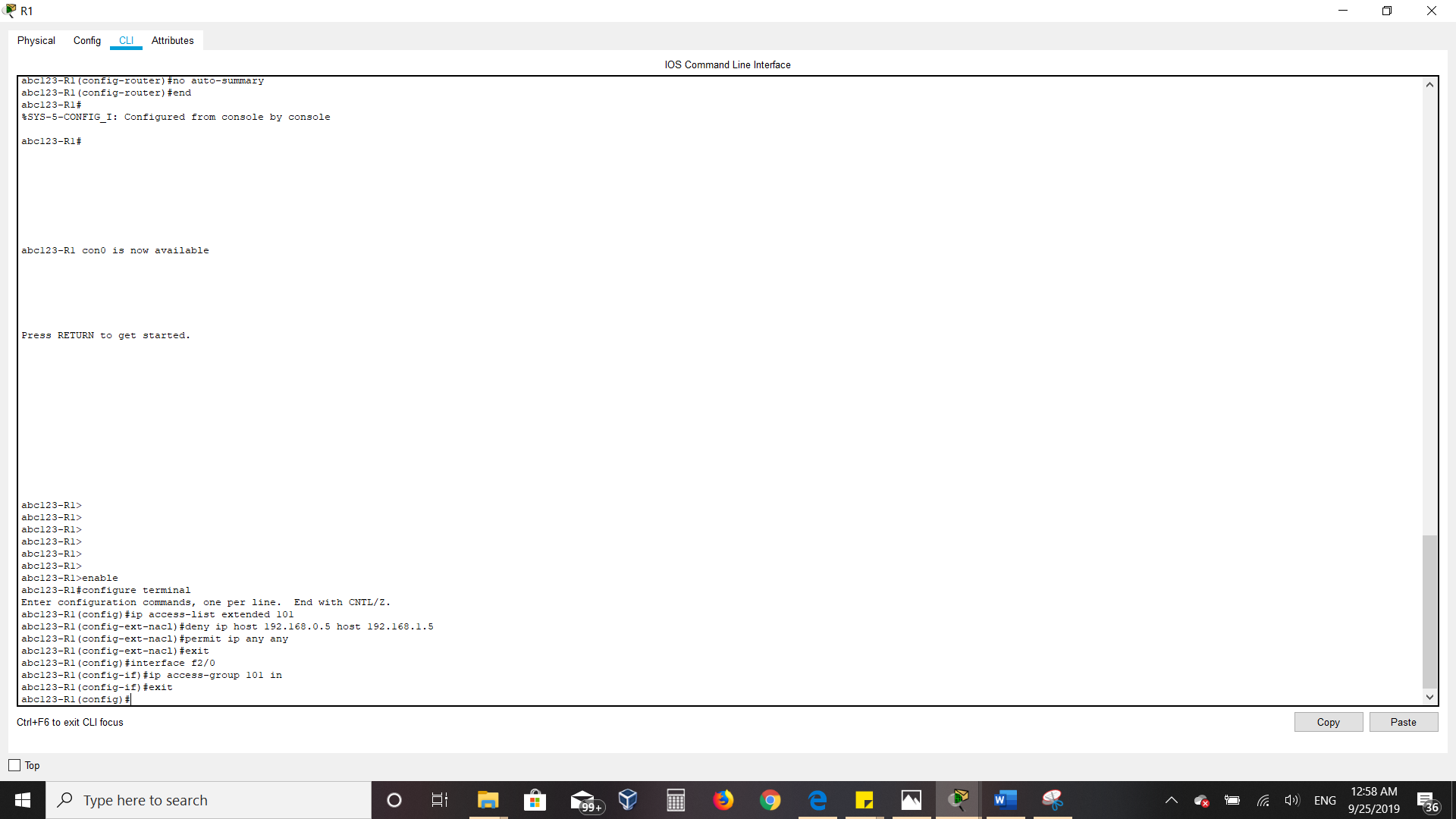
* I also executed the **Tracert** command which gave out all the routes the packet took to reach the destination PC2. Due to the presence of RIP, the packet traversed from the shortest path: R1 to R2, skipping R3:



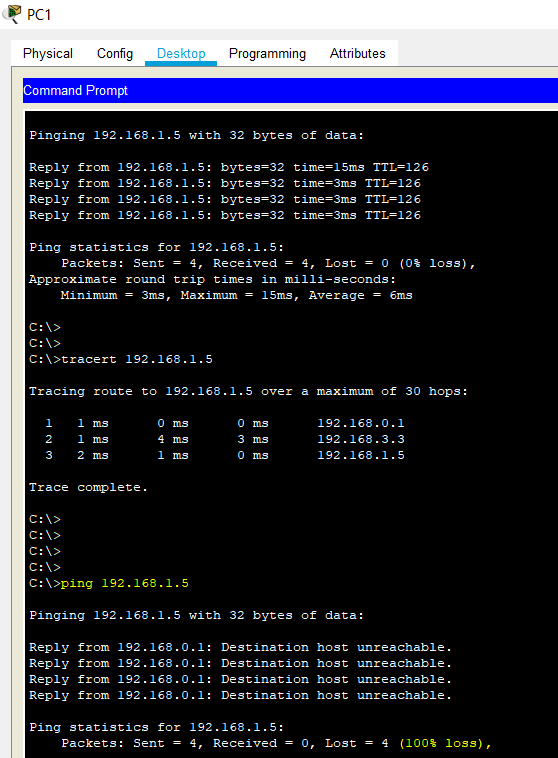
* Performed the same Two steps on PC2: Pinged PC1 from PC2 and obtained the same results: Destination was reached and due to RIP, shortest path was followed:



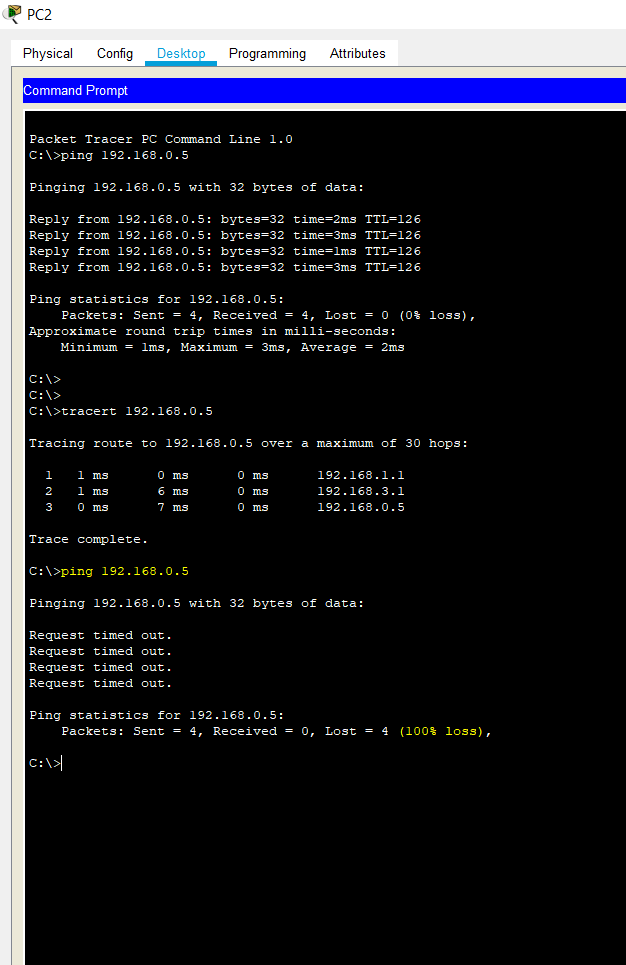
* Now for part 2 of the lab, I configured ACL (access control list) to deny traffic coming from PC1 and going towards PC2. This was done using the following commands:



* Now, to test the ACL, I pinged PC2 from PC1s terminal. This time, instead of getting a response back from PC2, I received a “Destination unreachable” message. This implied that ACL is functioning correctly:



* Next, I pinged PC1 from PC2. The traffic reached PC1 but PC1s response was discarded at Router 1, thereby giving a “Request Timed Out”; this again implied that the ACL was functioning correctly:



By the end of this lab, I learnt a bunch of things which I was expecting to cover:

**Basics of Cisco Packet Tracer:** It is a simulation software owned by Cisco which can be used to build complex network typologies. With Cisco Packet Tracer, one has the ability to create a network with almost unlimited number of devices, experiment with network behavior and troubleshoot before actual deployment can happen in production.

**The purpose of VPC:** It is a logical virtual data center in cloud which provide an isolated section to host your machine. It enables an enterprise to achieve the benefits of private cloud while still taking advantage of public cloud resources. **Features of RIP and its implementation:** A dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.   
**What are ACLs and how to implement one:** ACLs are a network filter utilized by routers and some switches to permit and restrict data flows into and out of network interfaces.

# 

# 3.0 Lab Results

1. What is a Virtual Private Cloud (VPC) and when might you use one? What are some large VPC providers?

A [virtual private cloud](https://www.sciencedirect.com/topics/computer-science/virtual-private-cloud) (VPC) offers public cloud users the privacy of a private [cloud environment](https://www.sciencedirect.com/topics/computer-science/cloud-environment). While the infrastructure remains public in a VPC, the provider allows the customers to define a [virtual network](https://www.sciencedirect.com/topics/computer-science/virtual-networks), by letting them select their own [subnets](https://www.sciencedirect.com/topics/computer-science/subnet), route tables, network gateways and IP address ranges. Additionally, VPNs can be optionally provided to further secure the virtual networks. Furthermore, in VPCs, the Stored data can be protected by assigning ACLs. One use-case to explain VPCs is **Amazon Virtual Private Cloud (VPC)**, which allows its users to use AWS resources in a virtual network. With Amazon VPC, the users can customize their virtual networking environment as they like, such as selecting own IP address range, creating subnets, and configuring route tables and network gateways—benefits of a private as well as a public cloud. With Amazon VPC, one could Use the VPC wizard to create a VPC for running a single-tier, public-facing web application such as a blog or simple web site and also for extending one’s data center into the cloud.

One might consider using VPCs for the following reasons:

* **Private Cloud Benefits:** VPCs provide enterprises some benefits of private clouds such as granular network control, while they are still using off-premises public cloud resources, in a highly scalable, pay-as-you-go model.
* **VPCs provide high level of uptime and Security: Since all the customers** operate on the same back-end infrastructure, VPC providers ensure that they keeping things running smoothly and securely, while maintaining [high levels of uptime](https://www.dsm.net/it-solutions). All the information passed through a VPC stays within a customer’s control without crossing the internet. VPC providers invest a lot of time in ensuring high level of reliability and security.
* **Easy integration and cost-efficient.** A VPC can be integrated with the public cloud, an on-premise-infrastructure or even with other VPCs. Once, this is done, it becomes a [hybrid cloud](https://www.dsm.net/it-solutions-blog/what-is-the-hybrid-cloud-and-how-can-it-benefit-me), which is more than one cloud working in synchronization. Since VPCs are within a public cloud, customers benefit a lot by sharing costs with other organizations, without compromising on security.

**Some major VCP providers are Amazon, Google, Microsoft, Digital Ocean, IBM etc.**

1. What is the difference between a Serial Interface and a Fast Ethernet Interface?

|  |  |
| --- | --- |
| **SERIAL INTERFACE** | **FAST ETHERNET INTERFACE** |
| Used by ISP to provide WAN connections as a frame relay, T1, T3, etc. | Used in LAN and WAN connections. |
| The port used is V.35 or RS-232. | The port used is RJ45 |
| Used in long distance communication such as Wide Area Networks. Hence, ideal for longer links. | Based on Ethernet and operates at speeds as high as 100 Mbps with the media standard 100Base T. Hence, ideal for links up to 100 meters. |
| A serial connection is a layer 1 connection. | An Ethernet connection is a layer 2 connection. |
| point-to-point link. | Shared medium. Bus connecting many-to-many. |

1. When would you use a Serial Interface? When would you use a Fast Ethernet Interface?

The serial interface is used in long distance communication such as WAN connections as a frame relay, T1, T3, etc. Therefore, serial interface is ideal for creating links between devices that are more than 100 meters apart. Furthermore, Serial interfaces can be configured either as Data Communication End or Data Terminal End. Two serial ports must be synchronized with appropriate clock frequency and proper bandwidth must be allocated, if they are to communicate with each other.

On the other hand, Fast Ethernet is ideally used to connect devices in LAN. It’s used for links of up to 100 meters. Workstations with existing 10 megabit per second [ethernet](https://searchnetworking.techtarget.com/definition/Ethernet) [card](https://whatis.techtarget.com/definition/card-or-expansion-card-board-or-adapter) can be connected to a Fast Ethernet network. Devices at distance longer than 100 meters can be connected using ethernet too but with degraded performance.

1. Why did you use a cross over cable to connect the router to the PC? Why not use a straight through cable?

Devices such as Routers-PCs, Switch-Switch, use the same pins or cables, to send and receive information, therefore, it needs to be "flipped" to avoid occurrence of collision. Therefore, devices that transmit and receive on the same pins require connection via cross-over cable. Similarly, devices that transmit and receive on opposite pins require straight-through cable, i.e. devices such as switch-PC, Switch-Router. We could have used a straight through cable only if a switch or a hub was placed between the routers and PCs.

So, in conclusion, when you need to connect two devices of different types together, use a straight through cable. But when you need to connect two devices of the same type together, use a crossover cable. If you insert a network device between two devices of the same type, all cables are straight through.

1. Why do you receive a “Destination Host Unreachable” when pinging PC2 (192.168.1.5) from PC1 (192.168.0.5) but receive a “Request Timed Out” when pinging PC1 (192.168.0.5) from PC2 (192.168.1.5)?

In general, a “Destination Host Unreachable” could mean that something is blocking the way from or to your destination. Such as, an ACL that filters bad IPs. In part two of this lab, we are setting an ACL on Router 1. We use:

**#deny ip host 192.168.0.5 host 192.168.1.5**

Because of this, the ACL denies all the traffic from 192.168.0.5 to 192.168.1.5. This is the reason why we receive a “Destination Host Unreachable” when pinging PC2 (192.168.1.5) from PC1 (192.168.0.5).

Now, “Request Timeout" means that the ICMP packet reached from one host to the other host/destination but the reply could not reach the requesting host. We received this because we have denied traffic from PC1 To PC2. So, the response from the destination- PC2 never reaches PC1.

**References:**

1. [**https://www.comparitech.com/net-admin/difference-between-straight-through-crossover-rollover-cables/**](https://www.comparitech.com/net-admin/difference-between-straight-through-crossover-rollover-cables/)
2. [**https://www.tutorialspoint.com/amazon\_web\_services/amazon\_web\_services\_virtual\_private\_cloud.htm**](https://www.tutorialspoint.com/amazon_web_services/amazon_web_services_virtual_private_cloud.htm)
3. [**https://study.com/academy/lesson/access-control-lists-acls-definition-purpose.html**](https://study.com/academy/lesson/access-control-lists-acls-definition-purpose.html)
4. [**https://searchnetworking.techtarget.com/definition/Routing-Information-Protocol**](https://searchnetworking.techtarget.com/definition/Routing-Information-Protocol)