# **Department of Computing**

# **EE353: Computer Networks**

# **Class: BESE-13AB**

**Lab 12: (Open Ended Lab)**

**Date: 06-12-2023**

# **Time: 10:00 to 01:00 and 2:00 to 05:00**

**Course Instructor: Dr. Humma Gafoor**

# **Lab Engineer: Syed Muhammad Ali Musa**

|  |  |
| --- | --- |
| **Group Members** | **CMS ID** |
| Aimen Munawar | 415867 |
| Hadia Ali | 410865 |

# 

**Lab12: Open Ended Lab**

**Task:**

Troubleshooting a Network Outage Scenario: You are a network administrator for a medium-sized company, and you have received reports from multiple users that they are unable to access the internet or critical internal resources. Your task is to identify and resolve the network outage, ensuring minimal downtime for users.

**Objective:** The objective of this simulation task is to challenge students to troubleshoot a network outage scenario and restore network connectivity.

**Materials:** This is an Open-ended Lab and students can choose on their own Network simulation software/Programming language.

**Network Outage Scenario 1: Network Devices Security Issue**

In this scenario, the network is facing a security issue related to the configuration and management of network devices. The security of these devices is paramount to ensure the integrity, confidentiality, and availability of the network infrastructure. The identified security problem requires a systematic troubleshooting approach to identify, address, and mitigate the underlying issues.

**Problem 1: Troubleshooting Network Devices Security Problem\**

Network security problems can manifest in various ways, such as unauthorized access, potential vulnerabilities, or misconfigurations. In this specific case, the troubleshooting focus is on ensuring that network devices, including routers and switches, are configured securely. Potential issues could range from weak passwords and open ports to misconfigured access control. The objective is to investigate and rectify these issues to fortify the network against security threats.

**Tools:**

* **Network Configuration Tools in Packet Tracer:** Utilize the graphical user interface (GUI) features of Packet Tracer for visualizing and configuring network components. This includes drag-and-drop functionality for devices, connections, and configurations.
* **Command-Line Interface (CLI) on Routers and Switches:** Utilize the command-line interface to access the configuration and management capabilities of routers and switches. The CLI provides a powerful way to interact with devices, configure settings, and troubleshoot issues through direct commands.

**Solution:**Configuring and securing network devices is a crucial aspect of maintaining a robust and reliable network infrastructure. A systematic approach involves implementing a series of well-thought-out measures to enhance the overall security posture of the network. This not only safeguards against potential threats but also ensures the smooth functioning of the network. Here's a breakdown of key components within this systematic approach:

* **Access Control and Authentication:**
  + Username and Password Policies: Enforce strong username and password policies to authenticate access to network devices. This includes specifying password length, complexity, and expiration policies.
  + Privilege Levels: Assign appropriate privilege levels to users, limiting access to critical configurations based on roles and responsibilities.
* **Encryption and Secure Protocols:**
  + SSH (Secure Shell): Implement Secure Shell for encrypted communication, especially for remote management. This ensures that sensitive information, including login credentials, is transmitted securely over the network.
  + Password Encryption: Encrypt all passwords stored on network devices to prevent unauthorized access in case of security breaches.
* **Network Monitoring and Logging:**
  + Logging Configuration: Set up comprehensive logging to monitor network activities. This includes logging login attempts, configuration changes, and potential security events.
  + Syslog Servers: Configure devices to send logs to external syslog servers for centralized monitoring and analysis.
* **Banner Messages:**
  + MOTD (Message of the Day) Banners: Display warning messages to users upon login. This serves as a deterrent and informs users about the consequences of unauthorized access.
* **Session Timeout and Security Measures:**
  + Session Timeout Settings: Configure session timeout parameters to automatically close idle sessions, preventing unauthorized access in case of user inactivity.
  + Security Measures Against Brute Force Attacks: Implement mechanisms, such as account lockout policies, to counteract brute force login attempts, enhancing security against malicious activities.
* **Network Segmentation and VLANs:**
  + VLAN Implementation: Create Virtual Local Area Networks (VLANs) to segment the network logically. This enhances security by isolating broadcast domains and controlling access to resources.
  + Default Management Interface Configuration: Configure default management interfaces to accept connections only from trusted networks, restricting access to authorized entities.
* **Switch Port Management:**
  + Administratively Down Unused Ports: Deactivate unused switch ports to minimize potential security risks and prevent unauthorized access through unused interfaces.

**Steps:**

**Step 1:**

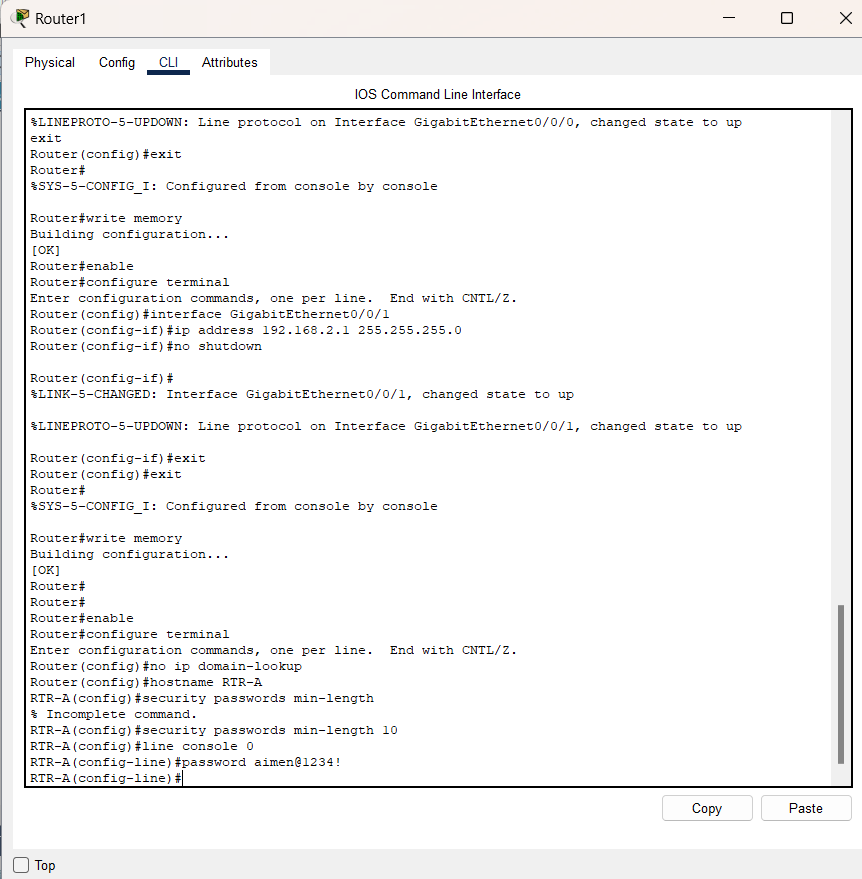
**Creating the Network:**

A diagram of a computer network

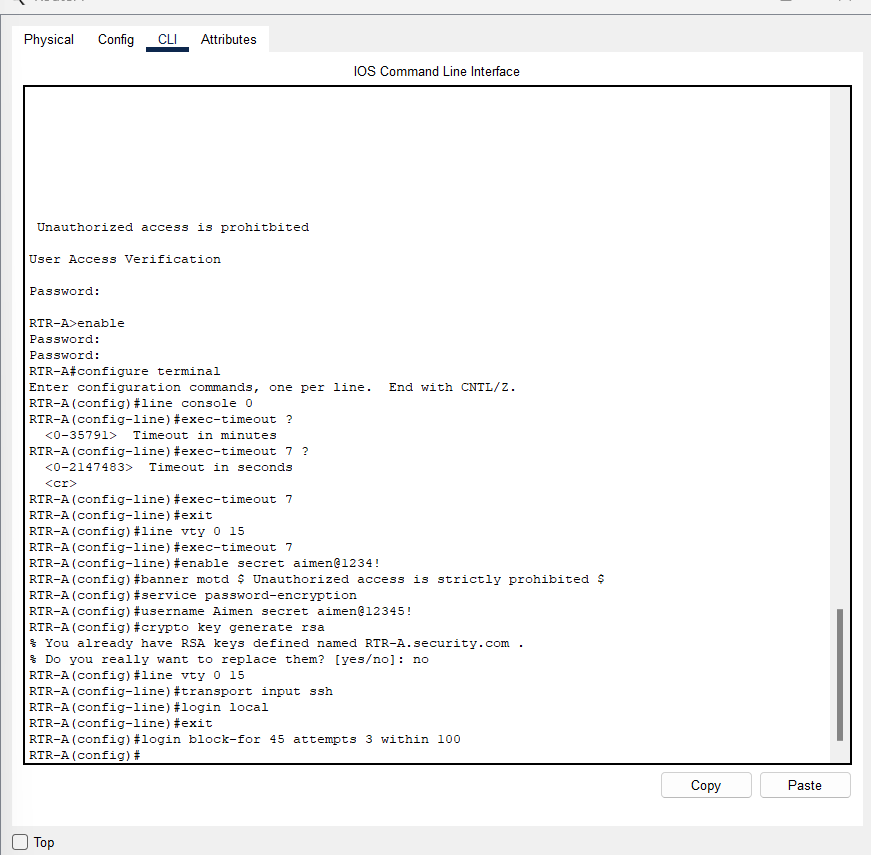
Description automatically generated

**Step 2: Router Configuration**

* Preventing IOS from attempting to resolve mistyped commands to domain names.
* Assigning Hostname
* Requiring Newly Created Password to be at least 10 characters in length.
* Creating a string ten-character password for the console.

****

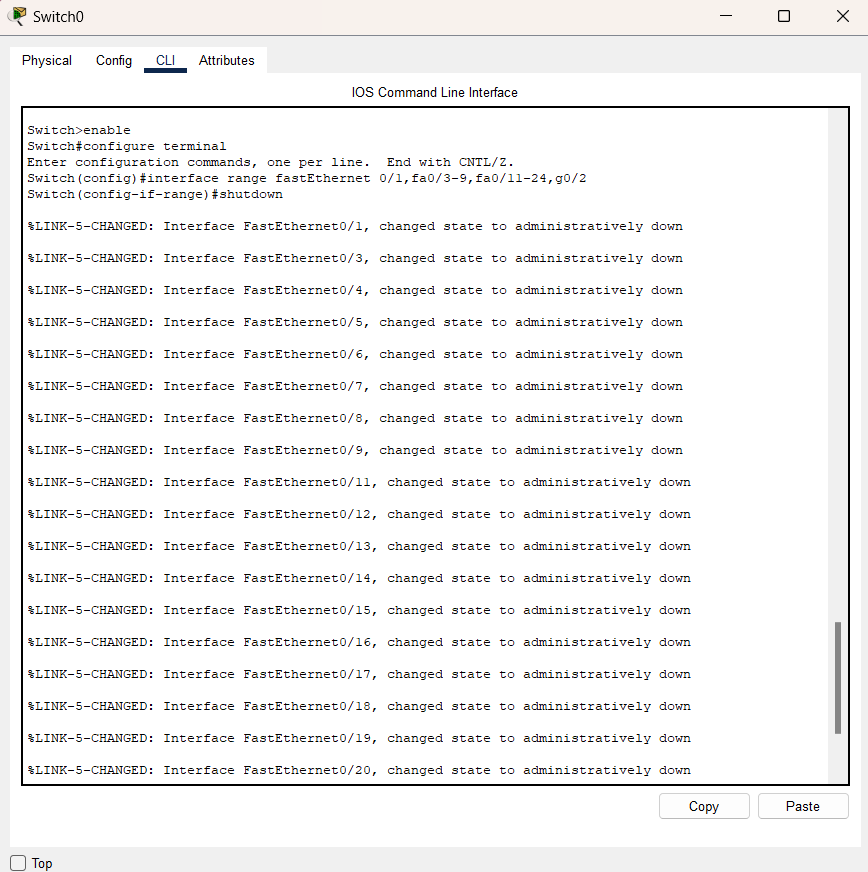
* Ensuring that console and VTY sessions close after 7 minutes exactly
* A strong encrypted ten-character password is created for the privileged EXEC mode.
* A MOTD banner that warns about unauthorized access to the devices is created.
* Password encryption for all the passwords
* Assigning username and encrypted password
* Enabling SSH and using security.com as domain name and using a modulus of 1024
* The VTY lines should then use SSH for incoming connections.
* The VTY lines should use the username and password that were configured to authenticate the logins.
* Impede brute force login attempts by using a command that blocks login attempts for 45 seconds .if someone fails three attempts within 100 seconds.

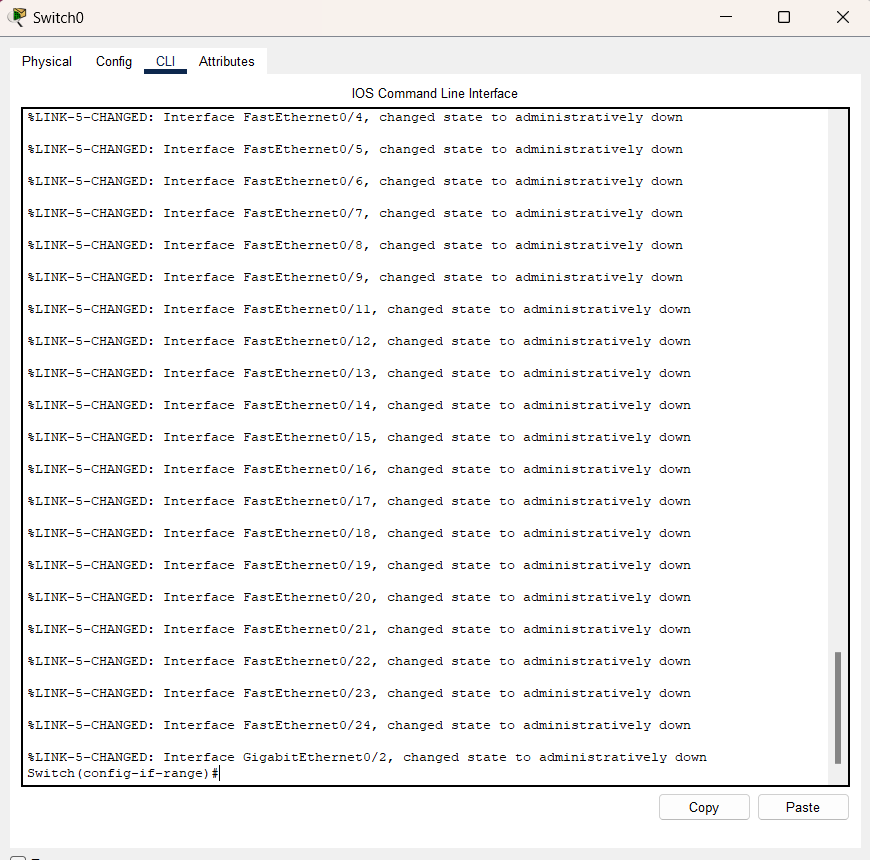
****

**Step 3: Switch Configuration:**

We are configuring only switch 0.

* Ensuring all the unused switch ports are administratively down.

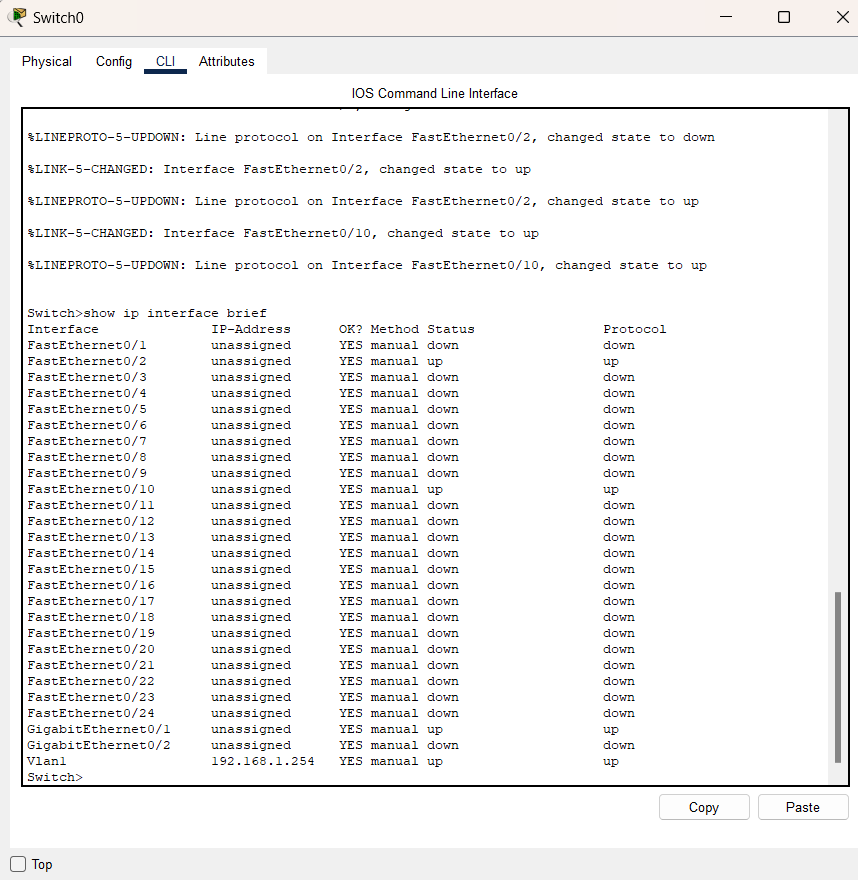
****

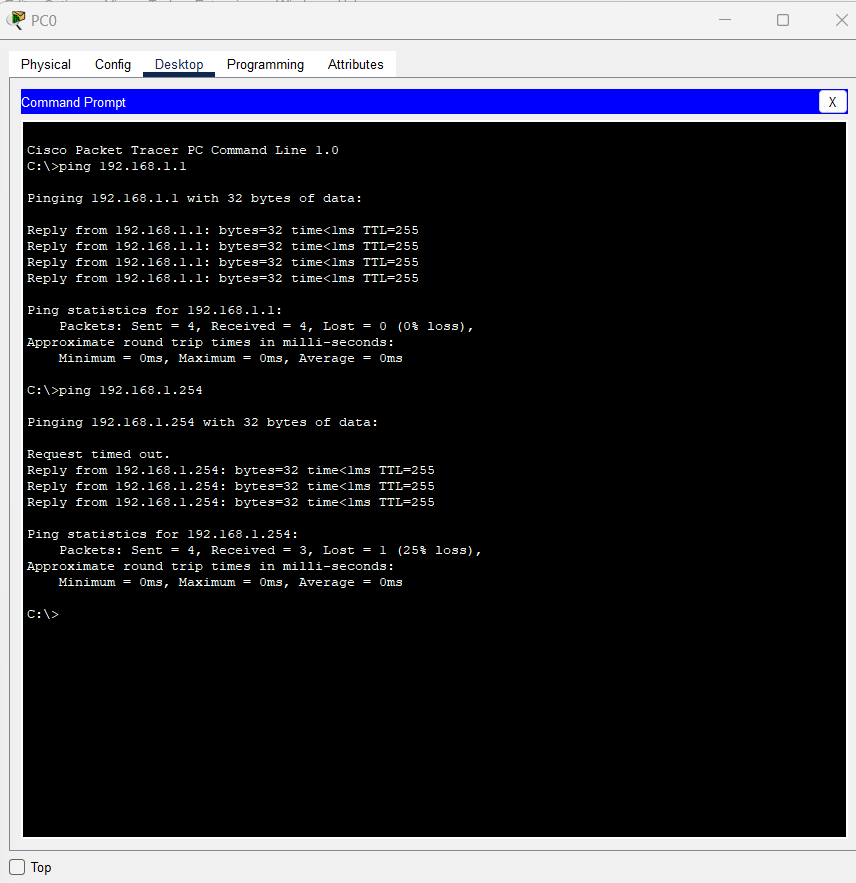
****

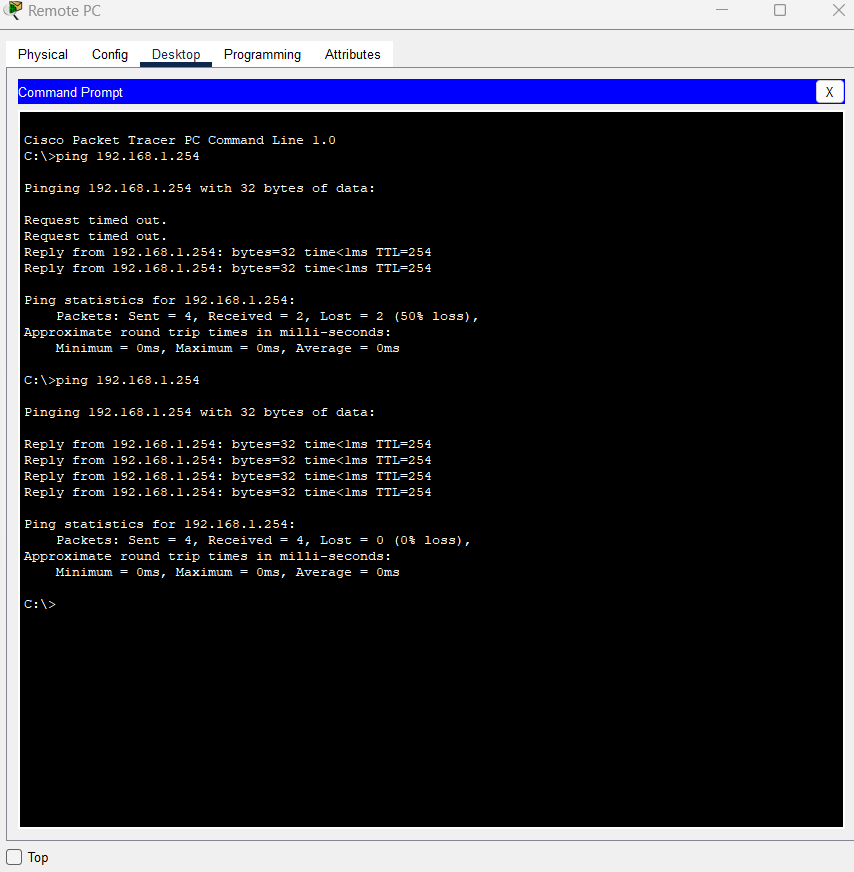
* The switch 0 default management interface should accept connections over the network. The switch should be reachable from the remote networks.
* We are creating a VLAN inside switch 0 and assigning it an IP address of 192.168.1.254 and assigning it its default gateway.
* Using aimen@1234! As password for the privileged EXEC mode.
* Configuring SSH using the same method as did in router.
* Creating username and encrypted password.
* The VTY lines should now only accept connections over SSH.
* Also, the VTY lines should only allow the network administrator account to access the switch management interface.
* Hosts on both LANs should be able to ping the switch management interface.

A screenshot of a computer

Description automatically generated

****





**Network Outage Scenario 2: Default Gateway Issues**

For a device to communicate across multiple networks, it must be configured with an IP address, a subnet mask, and a default gateway. The default gateway is used when the host wants to send a packet to a device on another network. The default gateway address is generally the address of the router interface, which is attached to the local network that the host is connected to.

**Problem:**

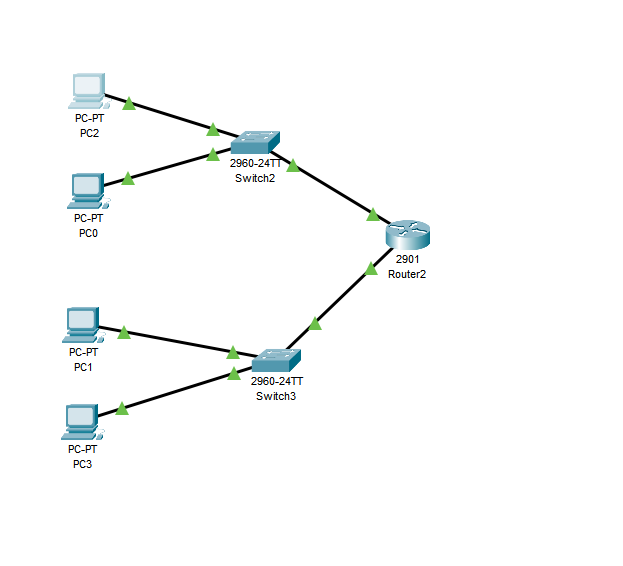
Troubleshooting due to an issue in the default gateway.

**Tools:**

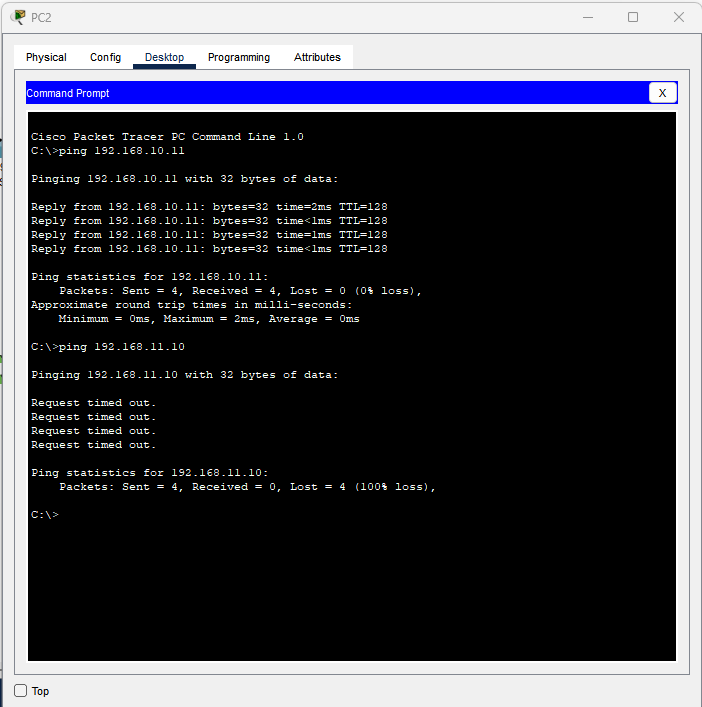
The tool we are using is **cisco packet tracer**. Using this tool, we can generate many scenarios related to the problem we are facing and can explain our understanding in a better way. This will help us to figure out a better solution to our problem.

**Solution:**

**We are using packet tracer to create the scenario as shown below:**



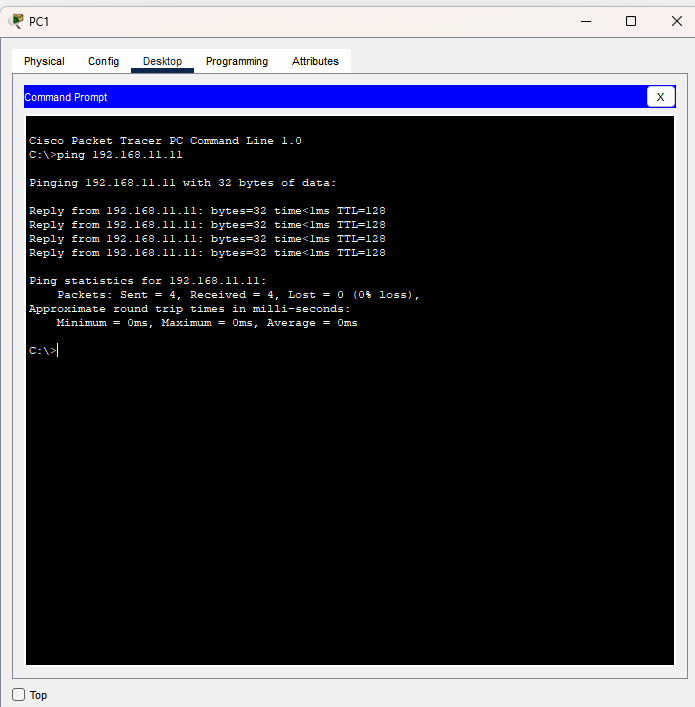
We will see if all the PCs are connected to one another and can communicate easily. For this, we will be using the ping command. If the result is timed out that means there is an issue in the connection between the PCs. if all the PCs are communicating with each other in a subnet then we will ping them with the switch, if that is working fine then we will ping it with the router connecting the subnets.

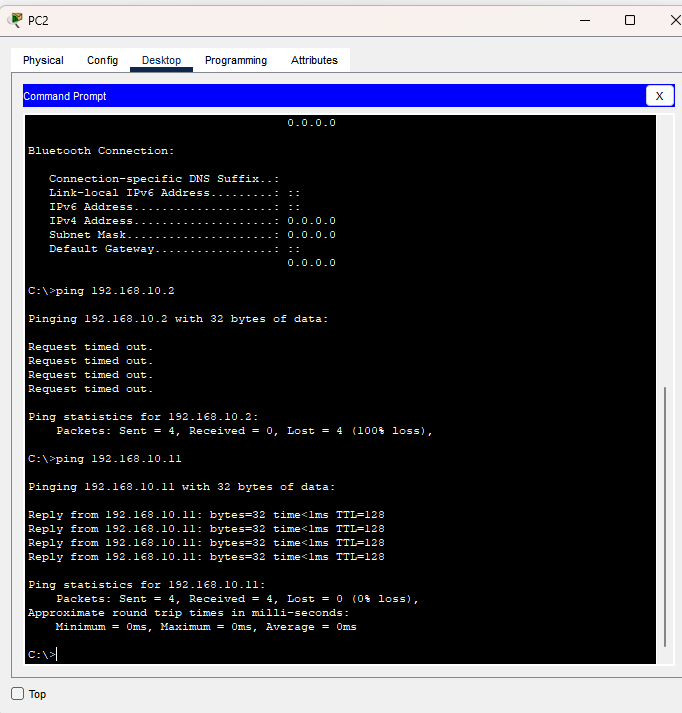


**Steps:**

* We will check the ip address of the PC. After this step we can easily see if our default gateway is correct or not. If not then we will take necessary steps.
* If the pcs ip addresses are not correctly configured then we will change them by going into the ip configure bar in the PCs. then from there we can change the ip addresses according to our requirement.
* If the default gateway is not configured correctly, then we will correct them as well.
* We will check the ip configuration of the switches as well if they have been assigned ips.
* If the ips have not been assigned to the switches, then we will go to the terminal of the switches and give them the ip addresses. We will use interface command for this purpose.

After all of these steps we will ping the PCs and the switches as well as the router to check if we have succeeded in figuring out the problem and solving it.





**Deliverables:**

Provide all available simulation/coding scrips.