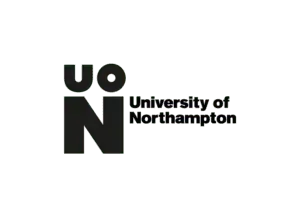


****

**Networking**

Assignment

Report

**Submitted By**

Name: Serena Yonjan

Uno.id : 20251095

Submission date:10/30/2025

**Question 1:**

**Scenario**

**Suppose a small Research Center of ABC university has two Computer Labs. First lab,**

**PC\_LAB\_1 which consists of three computers and one server connected with each other**

**through a switch which is further connected to a router. Similarly , Second lab, PC\_LAB\_2**

**which consists of four computers and one server connected with each other through a**

**switch which is further connected to a router. Both the routers of PC\_LAB\_1 and PC\_LAB\_2,**

**are further connected with each other to create a network based on routing information**

**protocol RIPv2.**

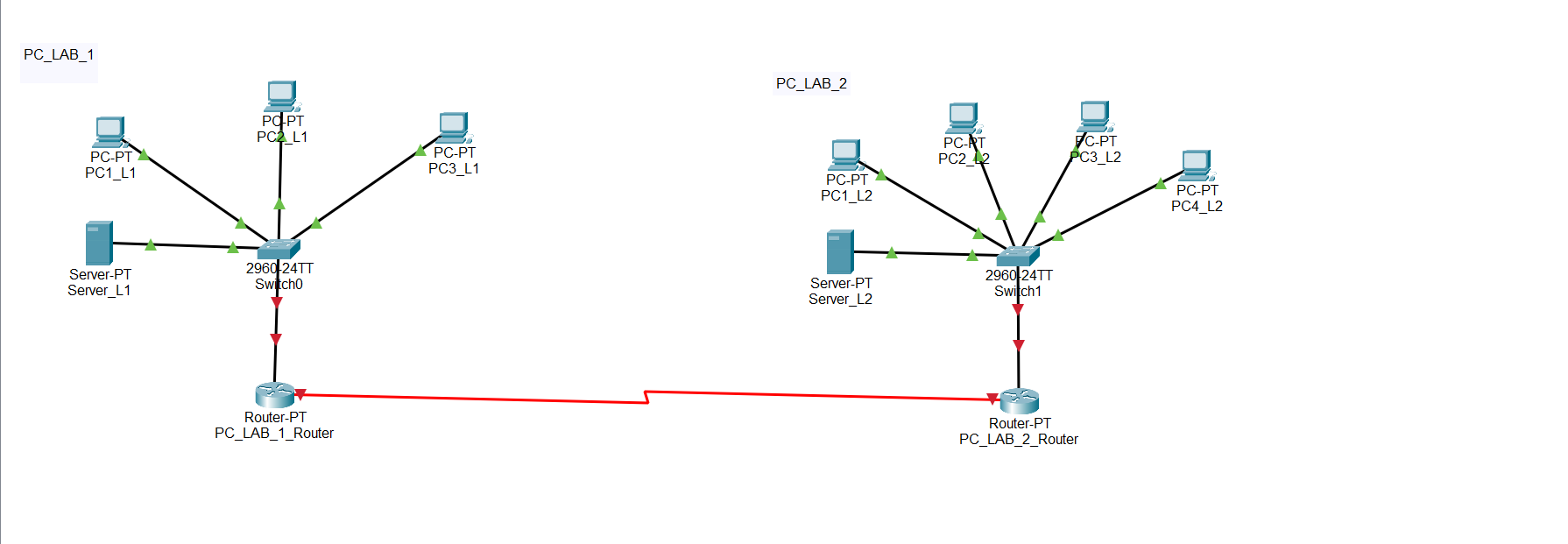
**Considering yourself as the Network Administrator of the University Research Center, you**

**are required to perform following tasks using the Packet Tracer Tool.**

**Take screenshot after completing each activity /task and paste in the MS Word File after**

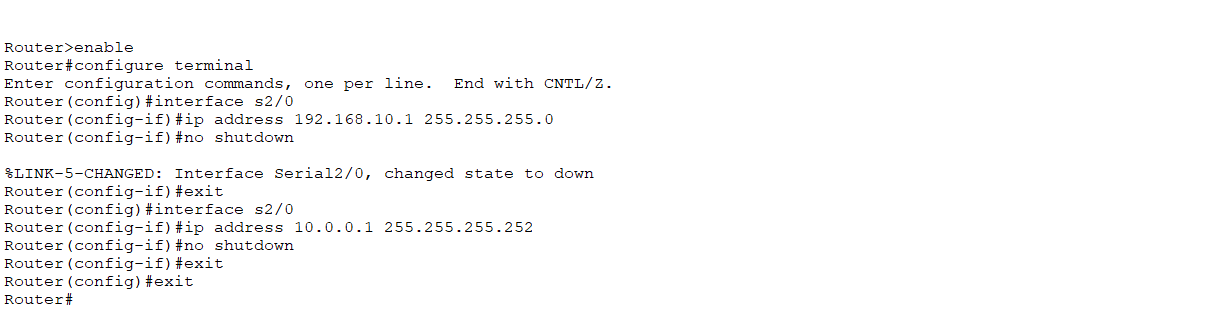
**completing the tasks:**

**Task1:**

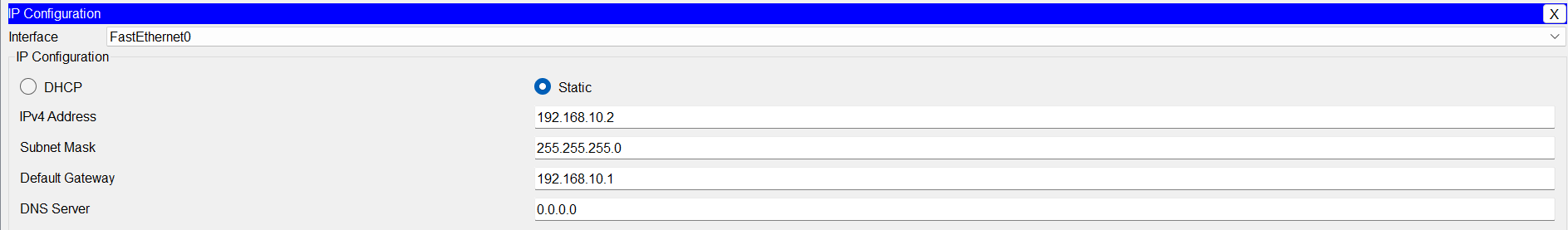


**Task 2:**

**LAB1\_Router Configuration**



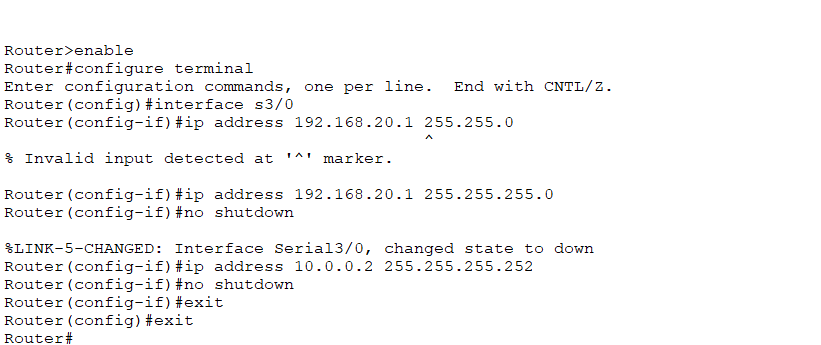
**PC1\_LAB1 Configure:**



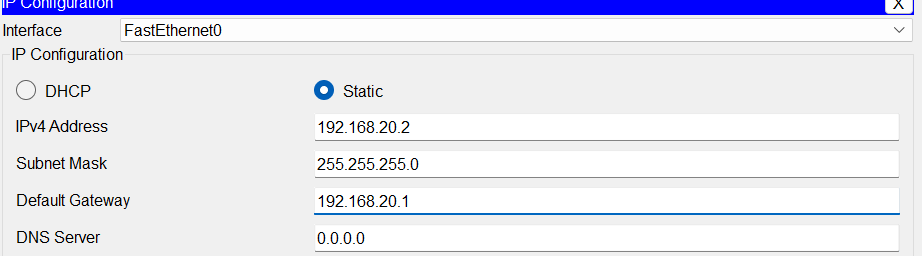
LAB1\_Server Configure:



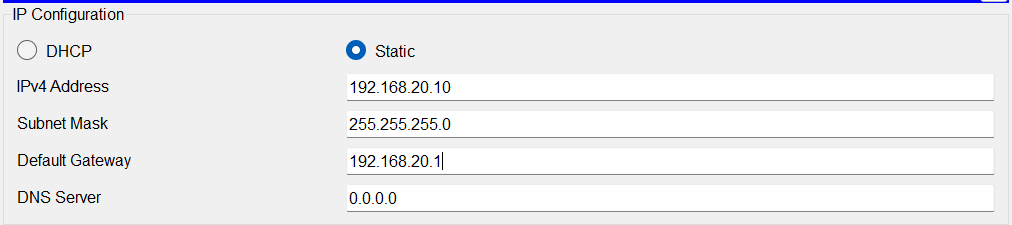
**LAB2\_Router Configuration:**



**PC1\_LAB2 Configure:**

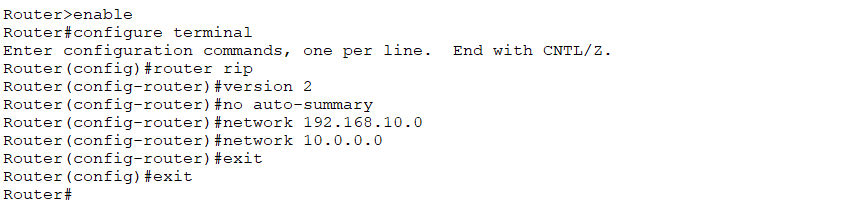


LAB2\_Server Configure:

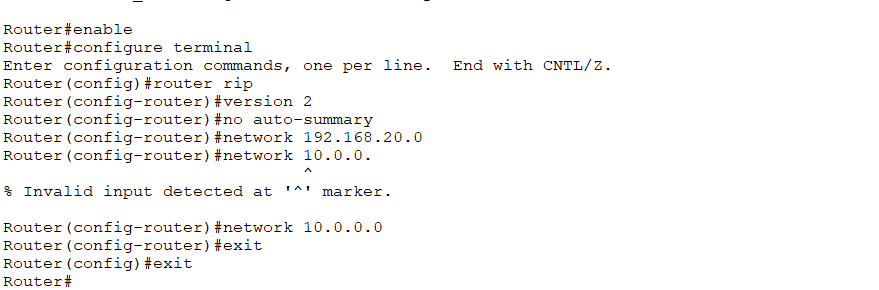


**Task 3:**

**RIPv2 Configuration – LAB1\_Router:**



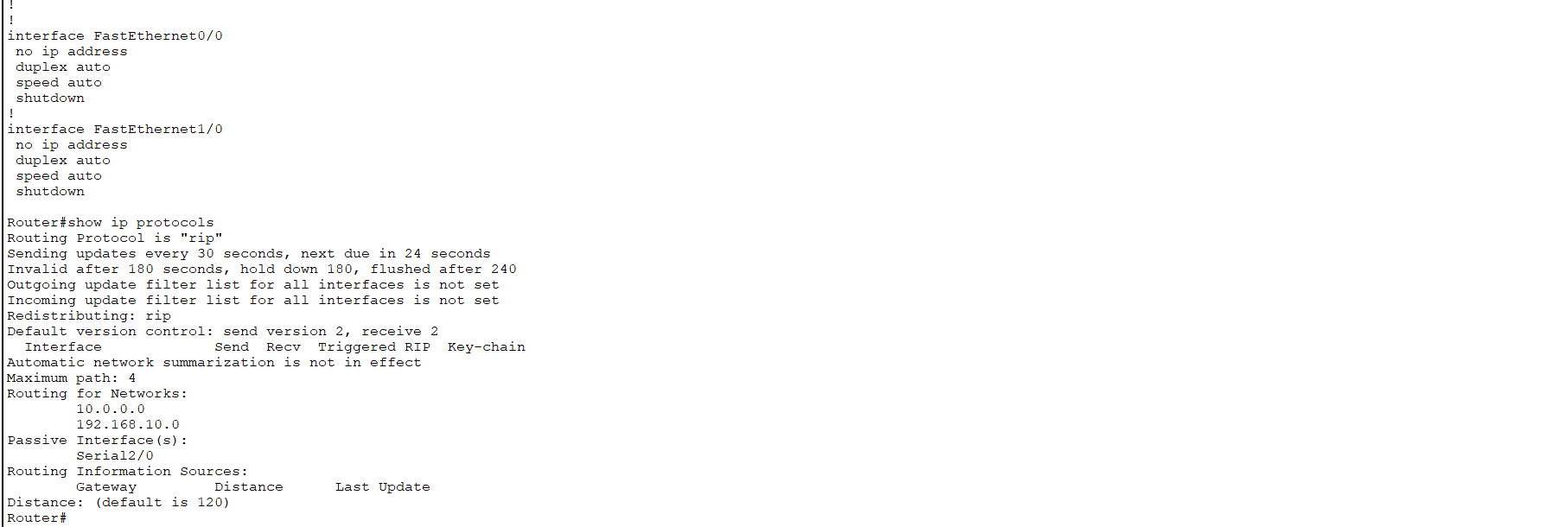
**RIPv2 Configuration – LAB2\_Router**:



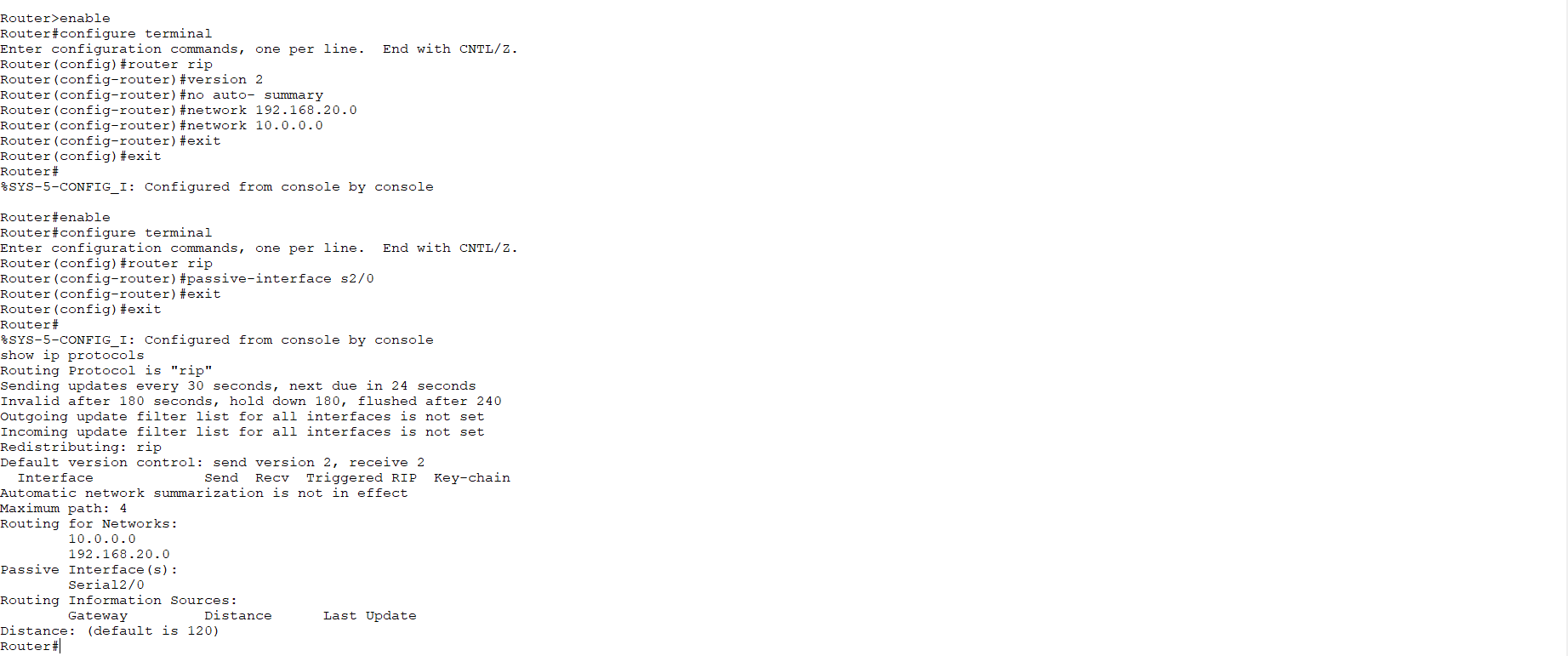
**Task 4:**

**Passive Interface – LAB1\_Router:**





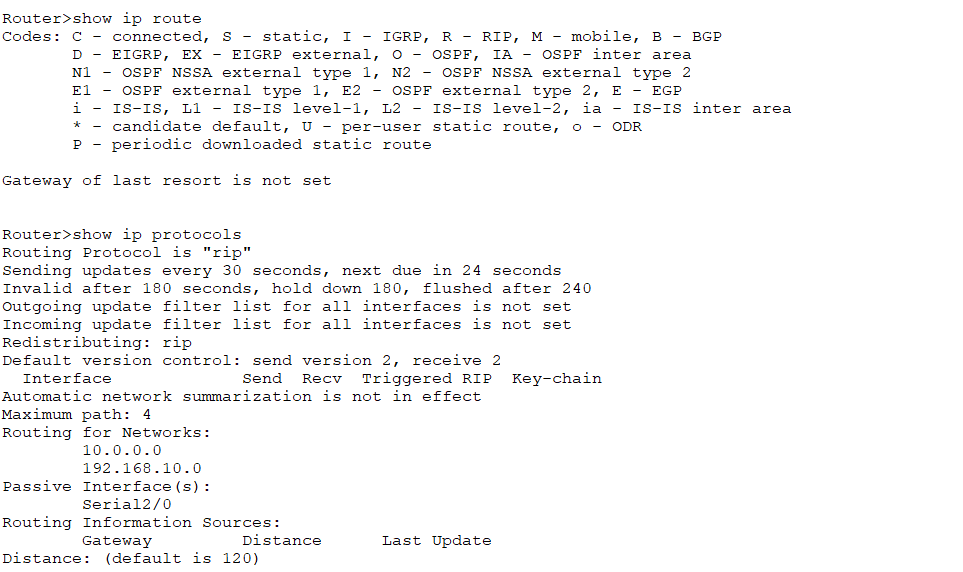
**Passive Interface – LAB2\_Router:**



**Task 5:**

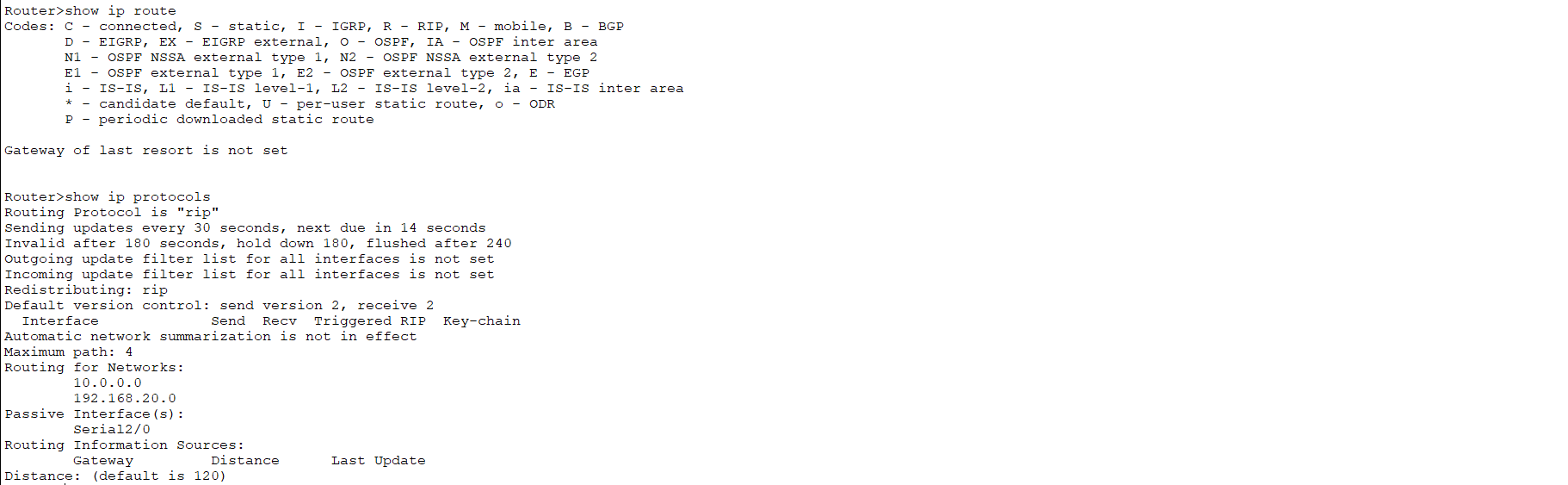
**LAB1\_Router:**

**Show Ip route and Ip protocols:**

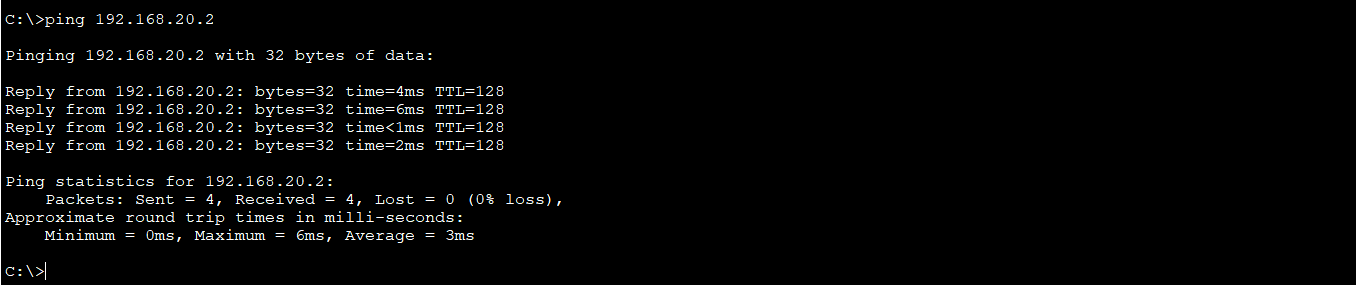


**LAB2\_Router:**

**Show Ip route and protocols:**



**Task 6:**



**Question 2:**

**Introduction :**

**Router can learn of remote networks via static or dynamic routing. This activity focuses on how**

**remote networks are added to the routing table using static routes. This is one of two ways that**

**a remote network can be added to the routing table. Static routes are configured by the**

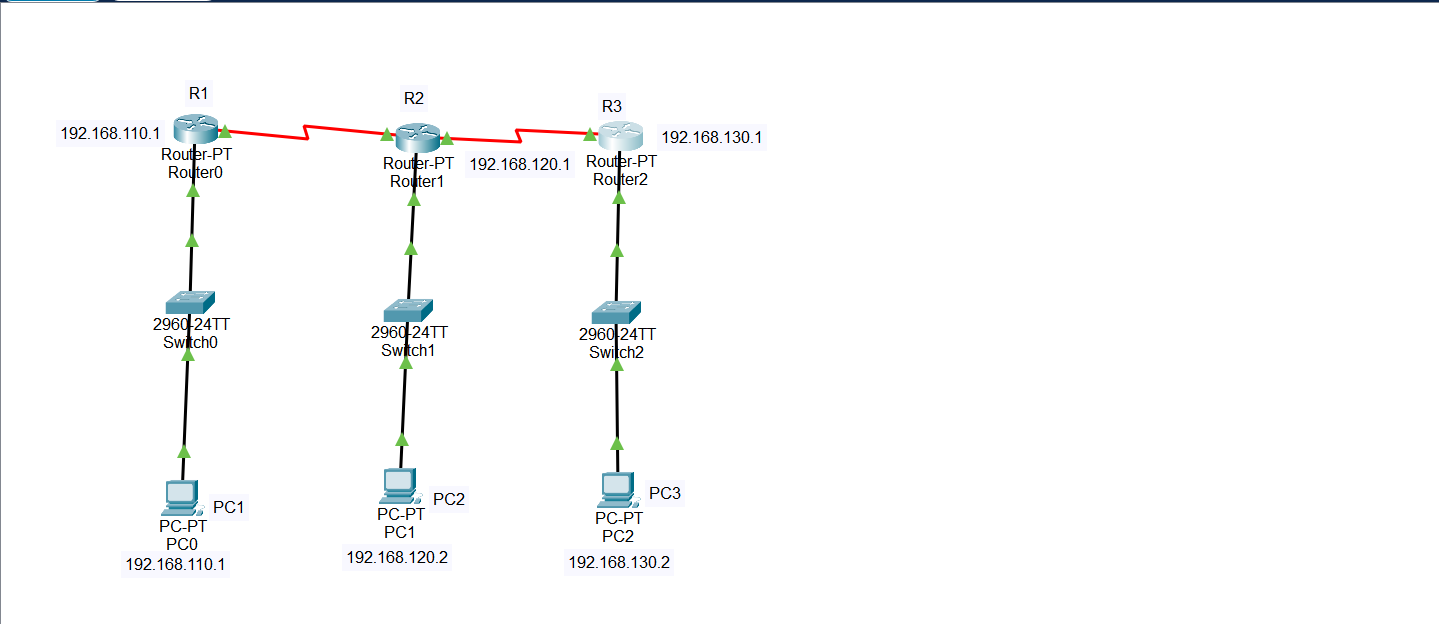
**networks administrator and include the network address and subnet mask of the remote**

**network, along with the IP address of the Next-hop router or the exit interface of the local**

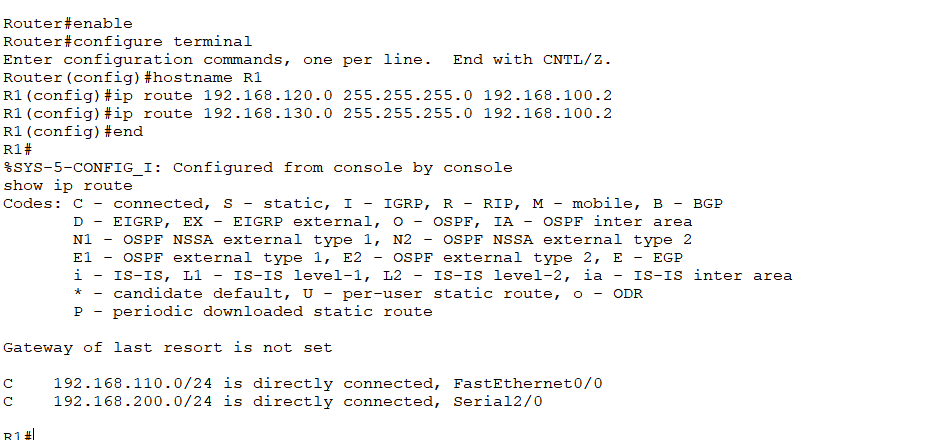
**router.**

**Configure static Routing**

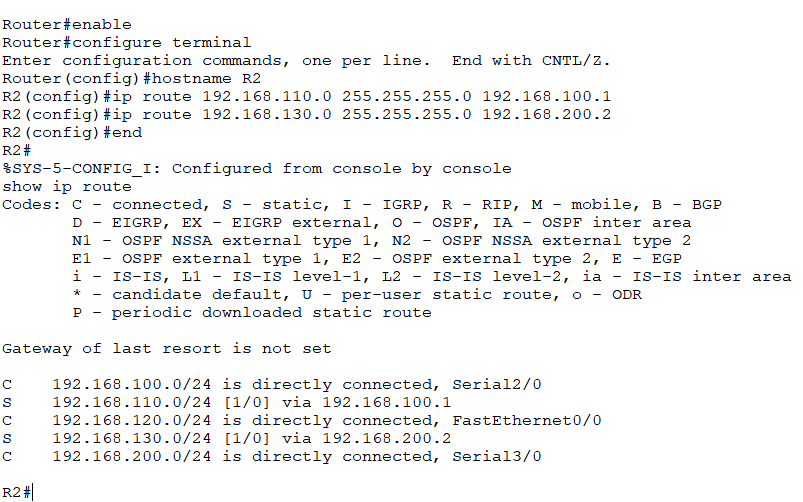
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | Ip address | Subnet mask | Gateway |
| R1 | F0/0 | 192.168.100.1 | 255.255.255.0 | - |
|  | S0/0/0 | 192.168.110.1 | 255.255.255.0 | - |
| R2 | S0/0/0 | 192.168.100.2 | 255.255.255.0 | - |
|  | S0/0/1 | 192.168.200.1 | 255.255.255.0 | - |
|  | F0/0 | 192.168.120.1 | 255.255.255.0 | - |
| R3 | S0/0/0 | 192.168.200.2 | 255.255.255.0 | - |
|  | F0/0 | 192.168.130.1 | 255.255.255.0 | - |
| PC1 | NIC | 192.168.110.2 | 255.255.255.0 | 192.168.110.1 |
| PC2 | NIC | 192.168.120.2 | 255.255.255.0 | 192.168.120.1 |
| PC3 | NIC | 192.168.130.2 | 255.255.255.0 | 192.168.130.1 |



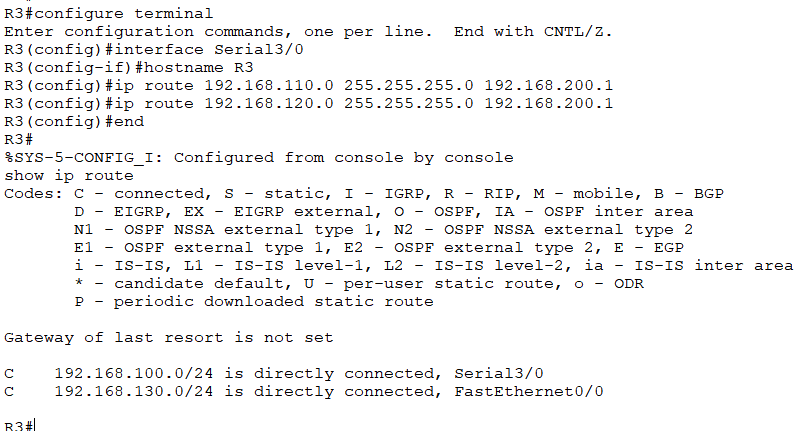
**Task 1: Configure static route on R1**



**Task 2: Configure static route on R2**

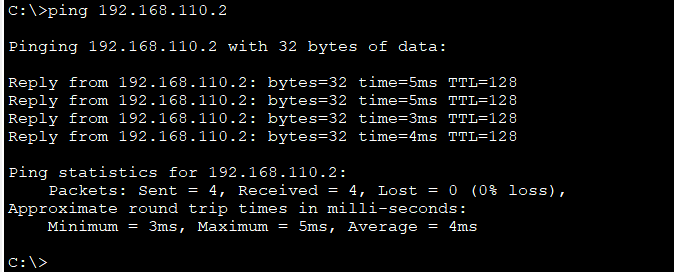


Task 3: Configure static route on R3

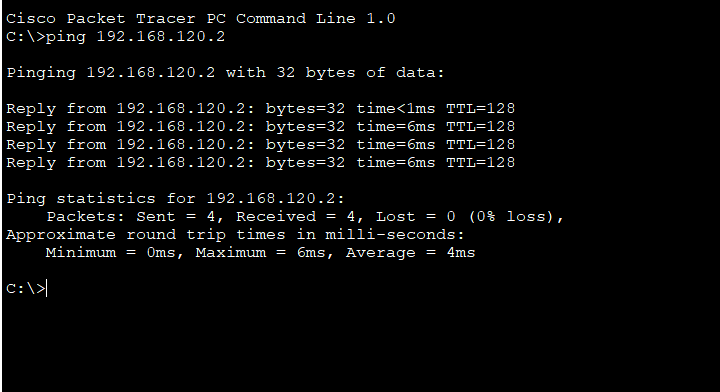


Task 4 : Check the connectivity

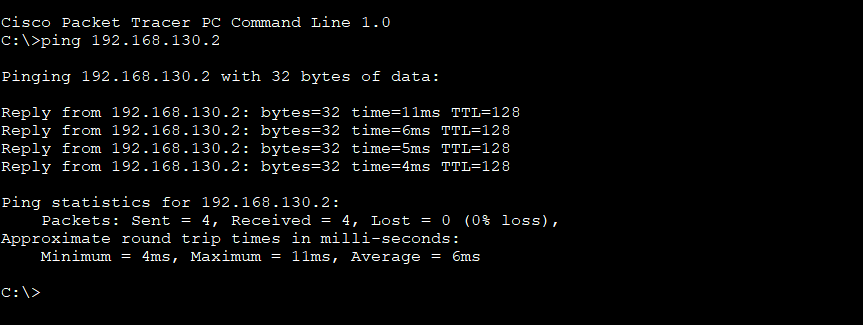
Ping from PC1



Ping from PC2



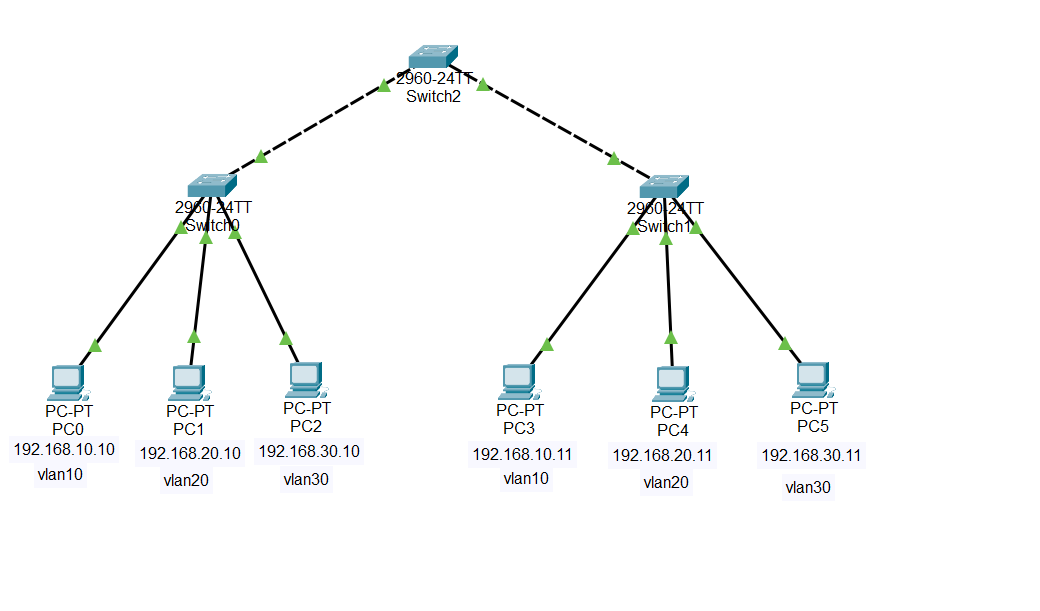
Ping from PC3



**Question 3:**

**Configuring VLANs and Trunks.**

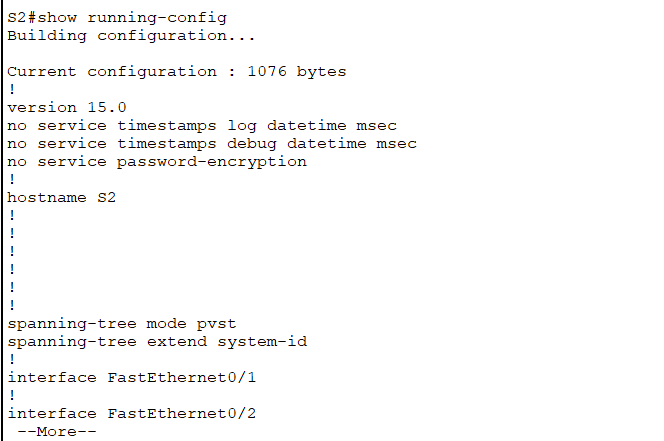
**Topology Diagram**



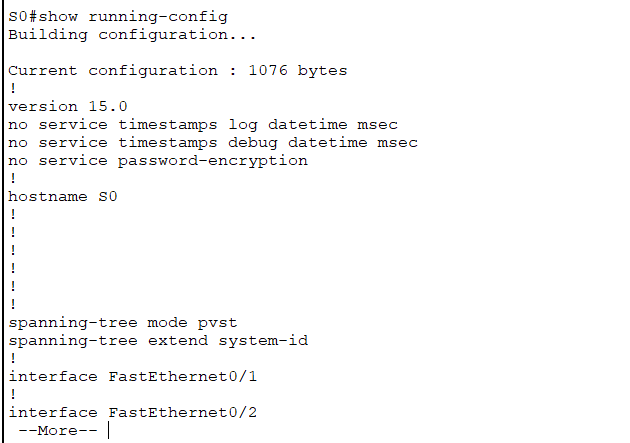
**Task 1: View the Default VLAN Configuration**

**a. Verify the current running configuration on the switches.**

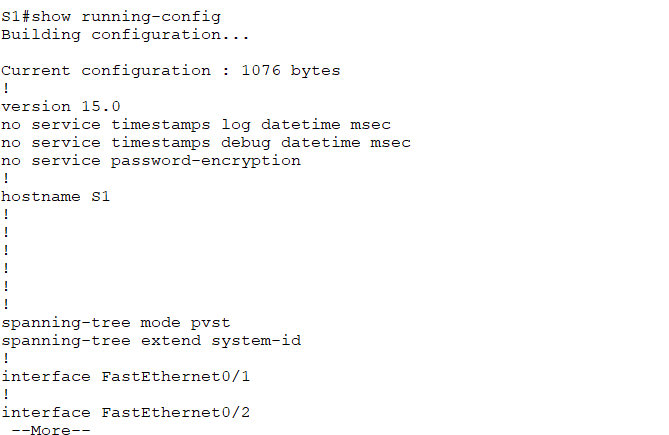
**Switch 2:**



**Switch 0:**

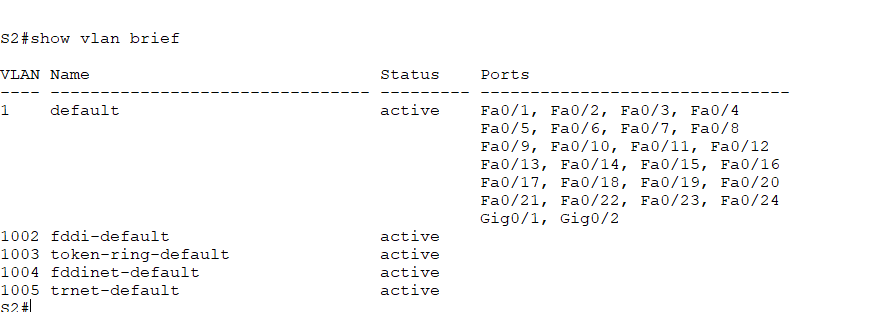
****

**Switch 1:**

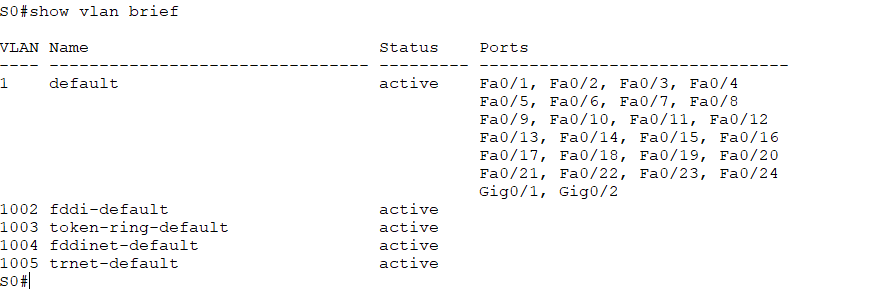
****

**b. Display the current VLANs.**

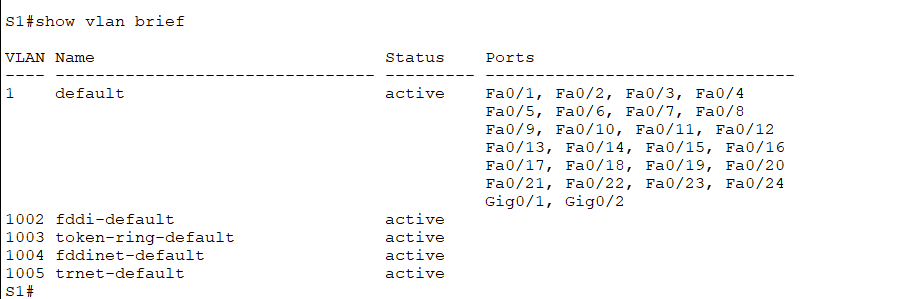
**Switch 2:**



**Switch 0:**

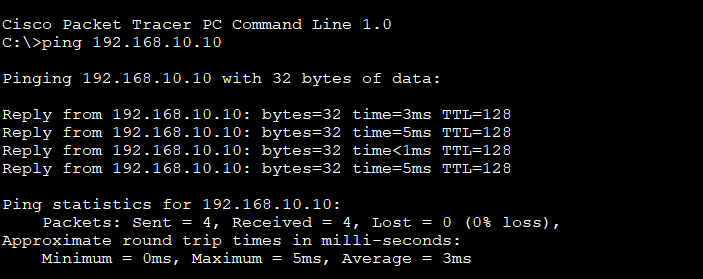


**Switch 3:**

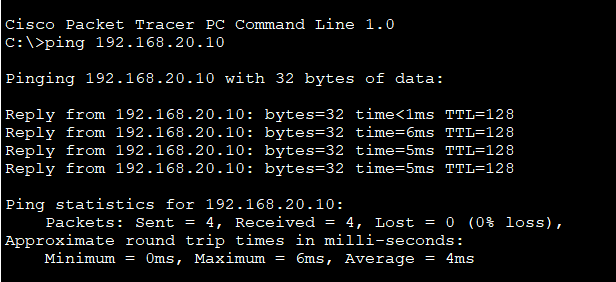


**c. Verify connectivity between PCs on the same network.**

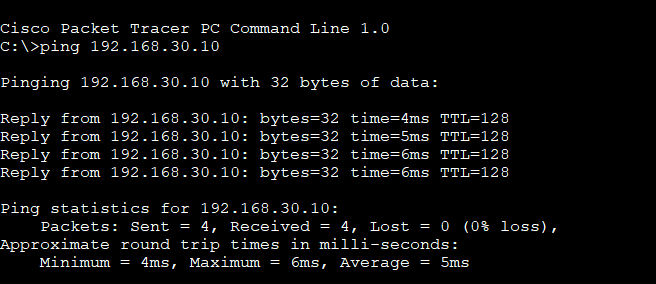
**PC0-PC3**



**PC1-PC4**

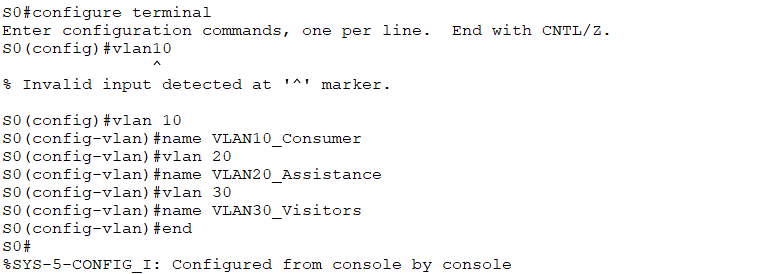


**PC2-PC5**

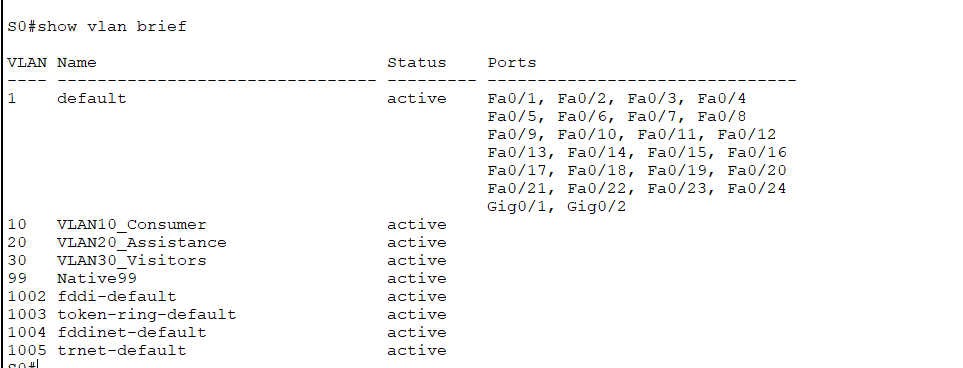


**Task 2: Configure VLANs**

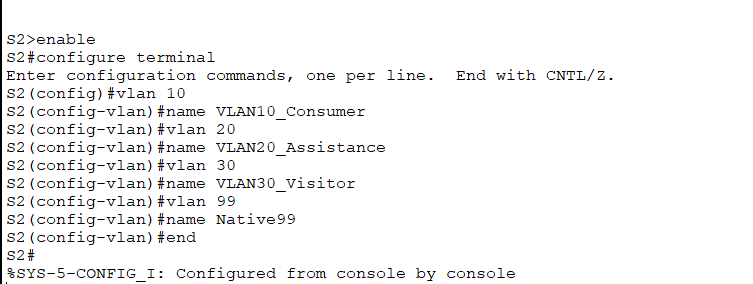
**a. Create VLANs on S0**

****

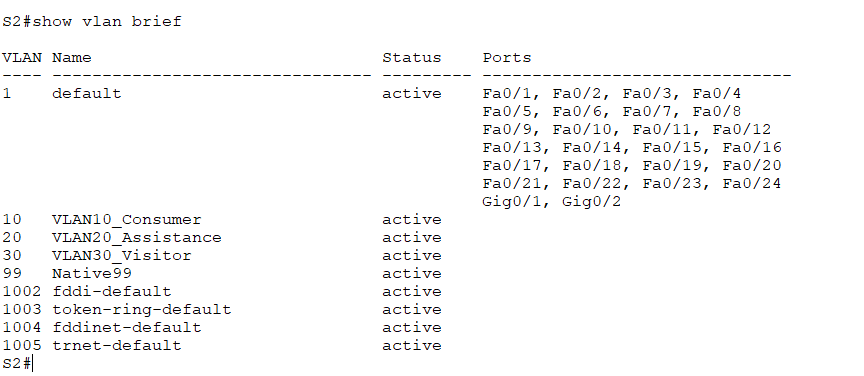
**b. Verify the VLAN Configuration**

****

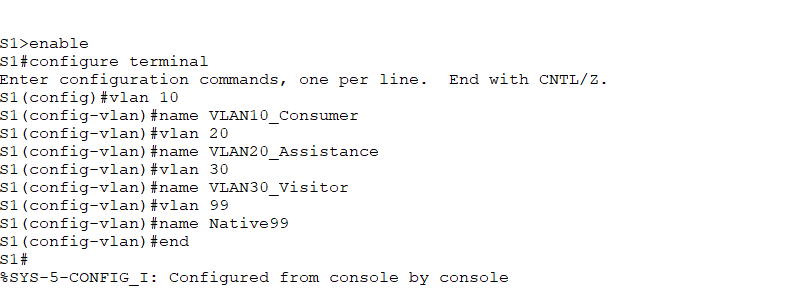
**Create VLANs on S2**

****

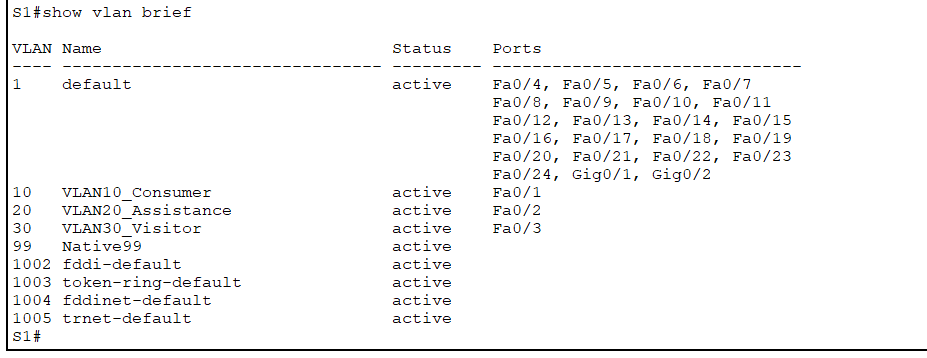
**Verify the VLAN Configuration**



**Create VLANs on S1**

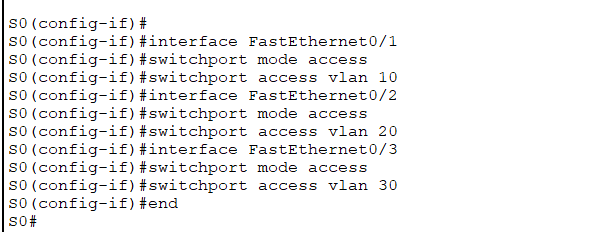


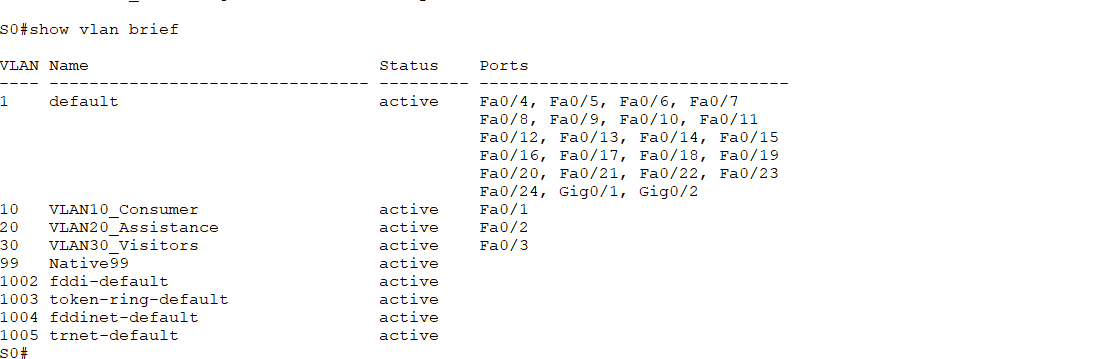
**Verify the VLAN Configuration**



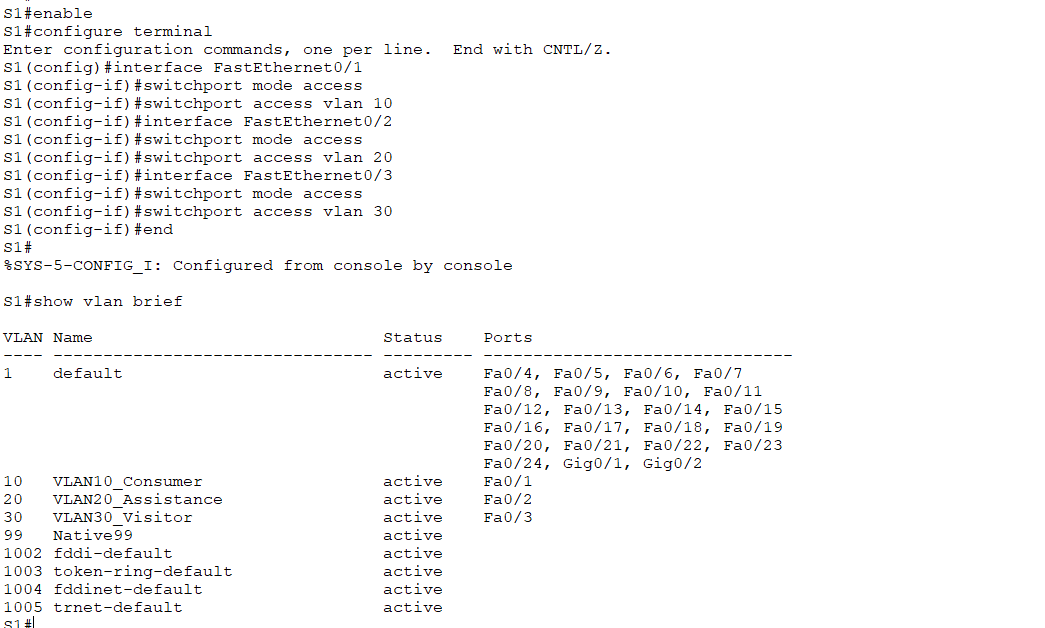
Task 3: Assign VLANs to Ports

a. Assign VLANs to the active ports on S0

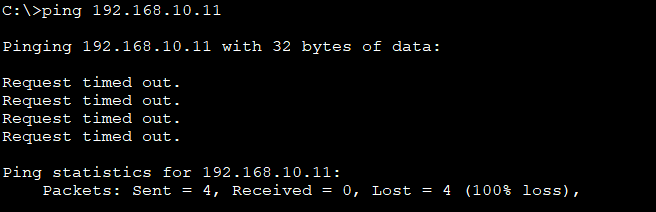




b. Assign VLANs to the active ports on S1



c. Verify loss of connectivity

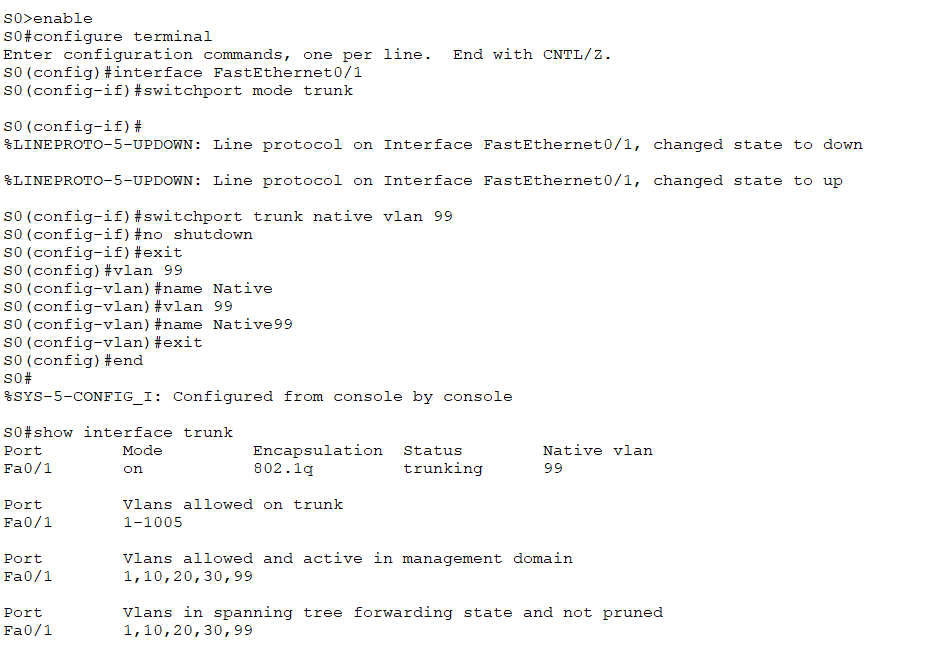


So we notice, PC0 is unable to ping PC3. PC0 and PC3 may not be able to ping each other when ports are moved to particular VLANs. Reason: Because there is no Layer-3 routing across VLANs by default and access ports place hosts into different VLAN broadcast domains, frames for those VLANs may not transit between switches if linking between switches isn’t configured.

Task 4: Configure Trunking

Configure S1 Fa0/1 and Fa0/3 for trunking and to use VLAN 99 as the native

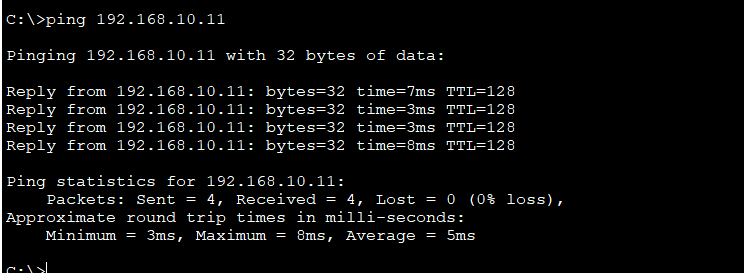
VLAN



b. Verify connectivity between devices on the same VLAN.

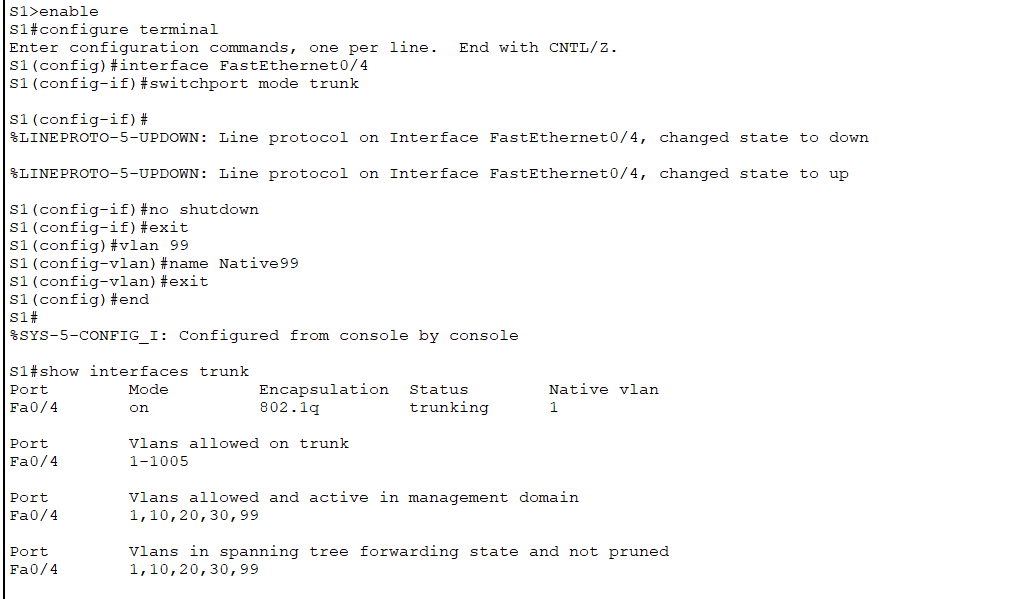
Although there is currently a native VLAN mismatch, pings between PCs on the same VLAN are

now successful. Why?

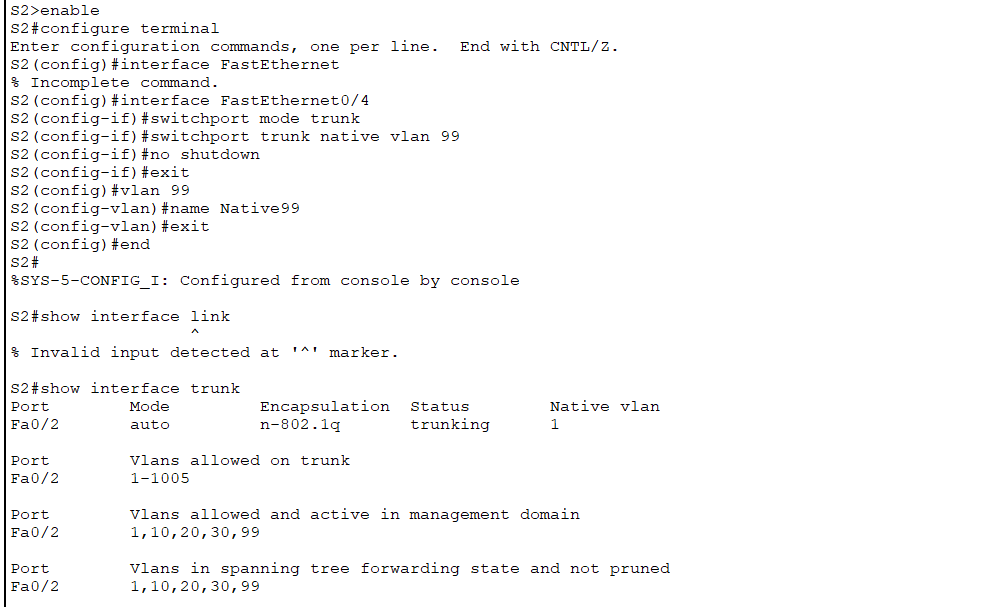


Devices on VLAN ping are visible. Pings between PCs on the same VLAN are successful despite the current native VLAN mismatch because VLAN data traffic is tagged. Only in tagged frames are impacted by the mismatch. Successful communication is made possible by accurately identifying and forwarding tagged VLAN traffic, such as that from PCs in VLAN 10, over the trunk link.

d. Verify trunking is enabled on S1 and configure VLAN 99 as the native VLAN.



Verify trunking is enabled on S2 and configure VLAN 99 as the native VLAN.



**Question 4:**

SSH should replace Telnet for management connections. Telnet uses insecure plain text

communication. SSH provides security for remote connections by providing strong encryption of

all transmitted data between devices. In this activity. You will secure a remote switch with

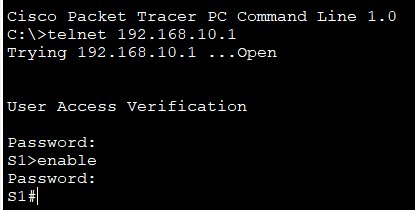
password encryption and SSH.

Instructions

**Task 1: Secure passwords**

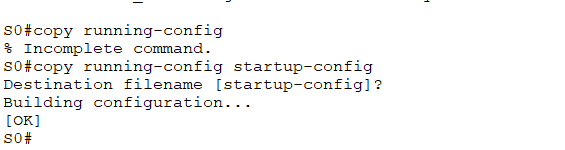
Using command prompt on PC1. Telnet to S1. The user EXEC and privileged EXEC

password is Naami



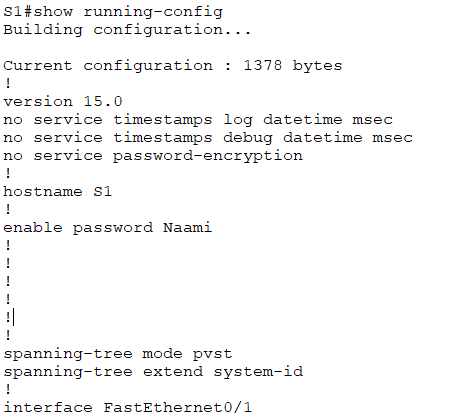
• Save the current configuration so that any mistakes you might make can be reversed by

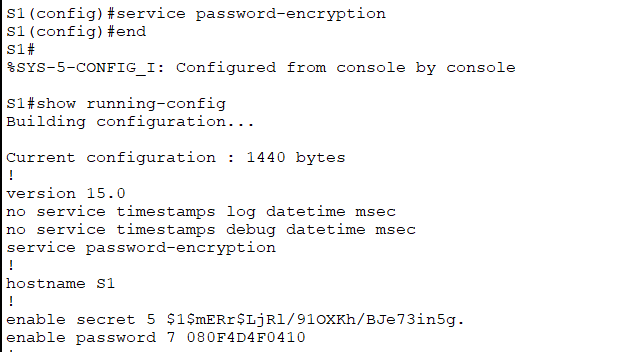
toggling the power for S1.



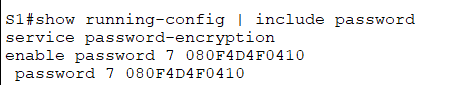
• Show the current configuration and note that the passwords are in plain text. Enter the

command that encrypts plain text passwords.





• Verify that the passwords are encrypted.



Task 2: Encrypt Communications

a. Set the IP domain name and generate secure keys.

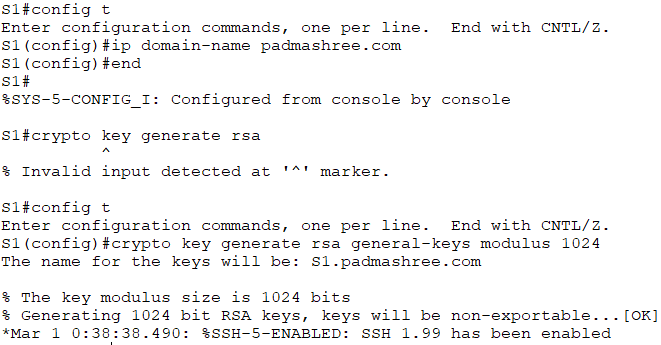
• It is generally not safe to use Telnet. Because data is transferred in plain text.

Therefore, use SSH whenever it is available.

• Configure the domain name to be padmashree.com

• Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024

length.

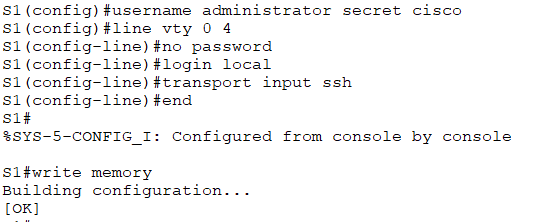


b. Create an SSH user and reconfigure the VTY lines for SSH only access.

• Create an administrator user with cisco as the secret password.

• Configure the VTY lines to check the local username database for login credentials

and to only allow SSH for remote access. Remove the existing vty line password.

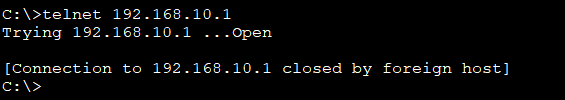




Task 3: Verify SSH Implementation

• Exit the telnet session and attempt to log back in using telnet. The attempt should fail.





• Attempt to log in using SSH command.

