

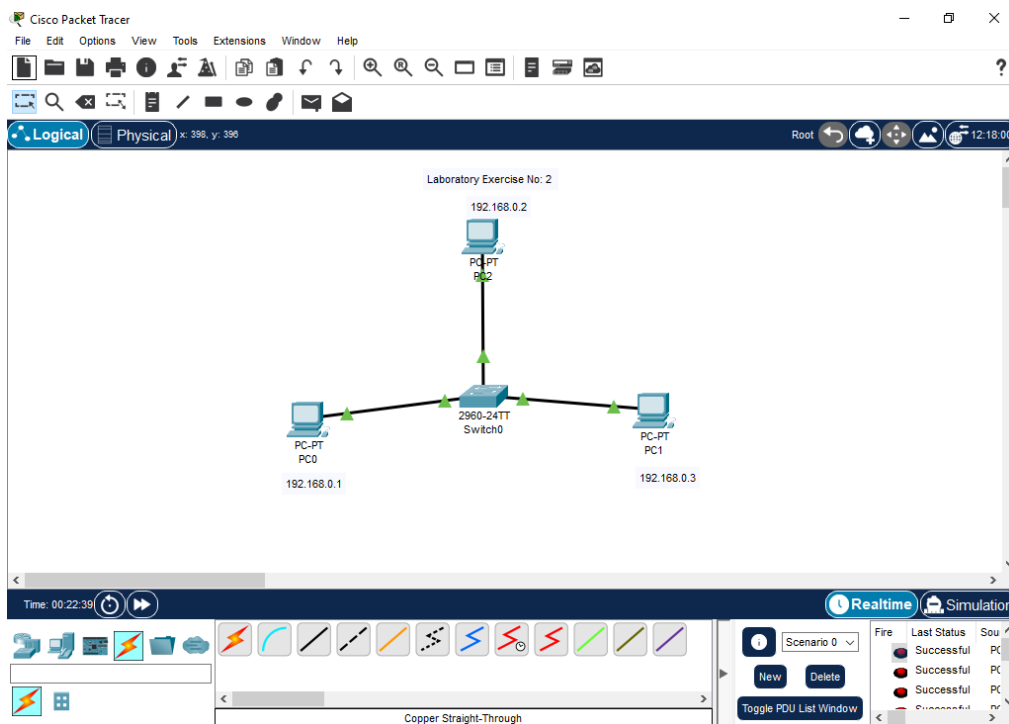
Lab Manual: Basic Network Connectivity (Lab Exercise No. 2)

1. Objective:

- Set up a basic LAN with a switch and three PCs.
- Configure IP addresses.
- Verify connectivity.

2. Network Topology:

- A central **2960-24TT Switch** connects three **PC-PT** devices (PC0, PC1, PC2).
- **IP Addresses:**
 - PC0: 192.168.0.1
 - PC1: 192.168.0.3
 - PC2: 192.168.0.2



3. Procedure (Step-by-Step):

Step 1: Build the Topology

1. Open **Cisco Packet Tracer**.
2. Drag **three PC-PTs** (End Devices) to the workspace. Label them PC0, PC1, PC2.
3. Drag **one 2960-24TT Switch** (Network Devices > Switches) to the workspace. Label it Switch0.

4. Connect **PC0, PC1, PC2** to **Switch0** using **Copper Straight-Through cables** (Connections icon).
 - PC0 FastEthernet0 to Switch0 FastEthernet0/1
 - PC1 FastEthernet0 to Switch0 FastEthernet0/2
 - PC2 FastEthernet0 to Switch0 FastEthernet0/3

Step 2: Configure IP Addresses

1. PC0:

- Click PC0 > Desktop > IP Configuration.
- Set IPv4 Address: 192.168.0.1 (Subnet Mask: 255.255.255.0). Close.

2. PC1:

- Click PC1 > Desktop > IP Configuration.
- Set IPv4 Address: 192.168.0.3 (Subnet Mask: 255.255.255.0). Close.

3. PC2:

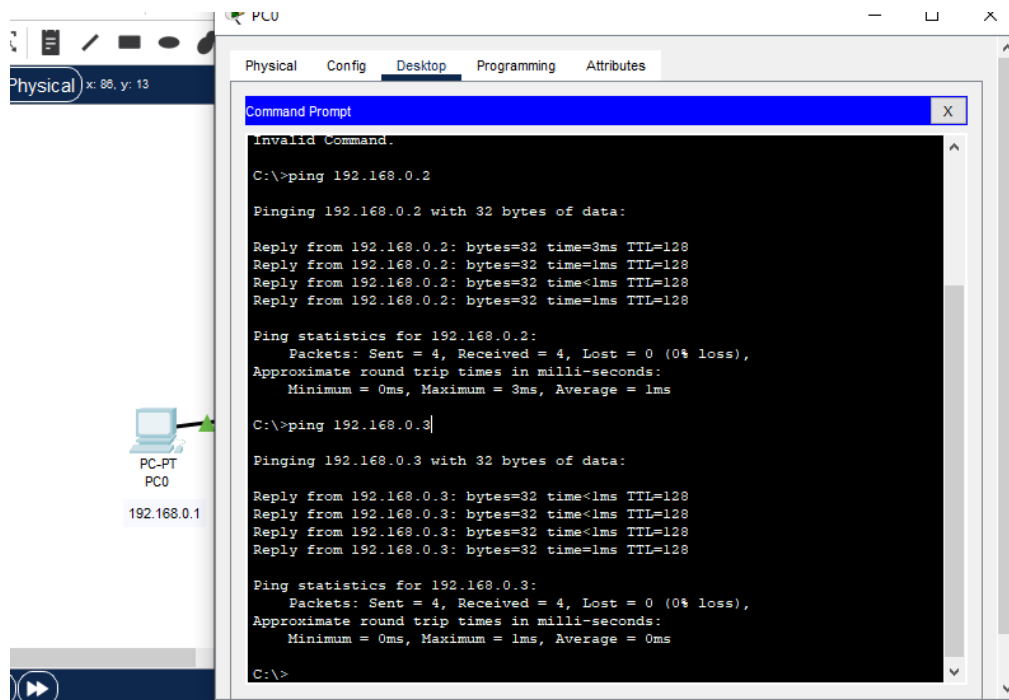
- Click PC2 > Desktop > IP Configuration.
- Set IPv4 Address: 192.168.0.2 (Subnet Mask: 255.255.255.0). Close.

Step 3: Verify Connectivity (Ping)

1. From PC0:

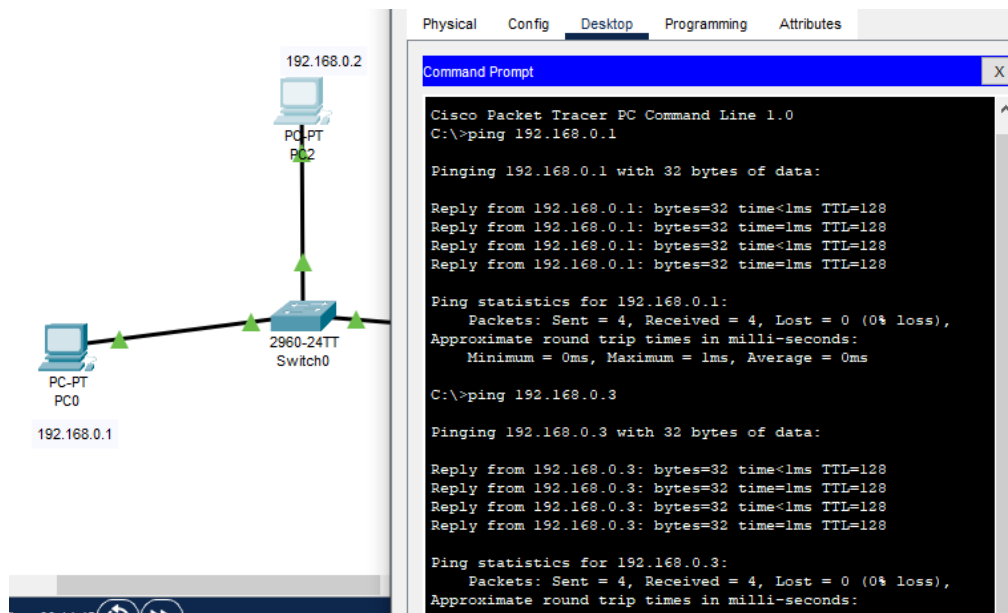
- Click PC0 > Desktop > Command Prompt.
- Type ping 192.168.0.2 (should show replies).

- Type ping 192.168.0.3 (should show replies).



2. From PC2:

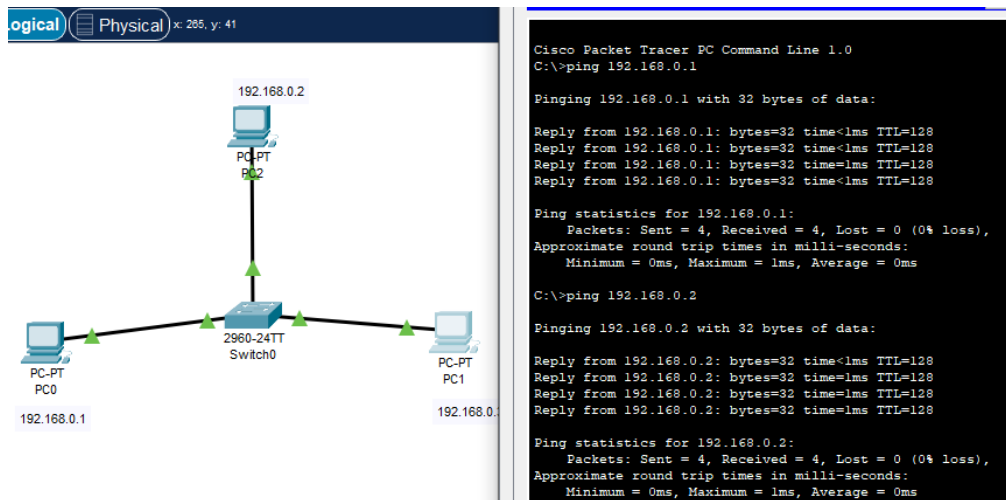
- Click PC2 > Desktop > Command Prompt.
- Type ping 192.168.0.1 (should show replies).
- Type ping 192.168.0.3 (should show replies).



3. From PC1:

- Click PC1 > Desktop > Command Prompt.

- Type ping 192.168.0.1 (should show replies).
- Type ping 192.168.0.2 (should show replies).



Conclusion:

- All PCs successfully pinged each other, confirming basic network connectivity.

Lab Manual: Multi-Switch Network Connectivity (Lab Exercise No. 3)

1. Objective:

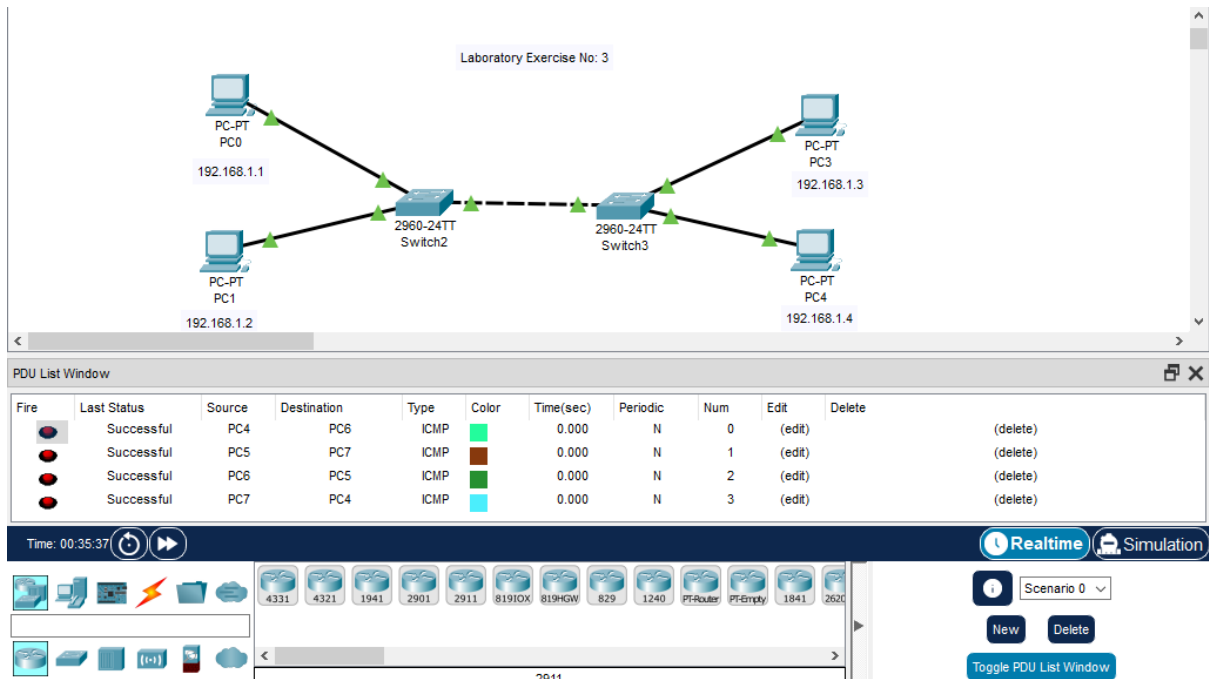
- Design and implement a multi-switch LAN.
- Configure IP addresses on end devices (PCs).
- Configure basic management IP on switches.
- Verify end-to-end network connectivity across multiple switches.

2. Network Topology:

- Two **2960-24TT Switches** (Switch2, Switch3) connected to each other.
- **PC0** and **PC1** connected to **Switch2**.
- **PC3** and **PC4** connected to **Switch3**.
- **IP Addresses:**
 - PC0: 192.168.1.1
 - PC1: 192.168.1.2
 - PC3: 192.168.1.3

- PC4: 192.168.1.4
- Switch2 (VLAN1 Mgmt): 10.0.0.1
- Switch3 (VLAN1 Mgmt): 10.0.0.2

(Optional: Insert Lab_03_complete.PNG here)



3. Procedure (Step-by-Step):

Step 1: Build the Topology

1. Open **Cisco Packet Tracer**.
2. Drag **four PC-PTs** (End Devices) to the workspace. Label them PC0, PC1, PC3, PC4.
3. Drag **two 2960-24TT Switches** (Network Devices > Switches) to the workspace. Label them Switch2, Switch3.
4. **Connect PCs to Switches** using **Copper Straight-Through cables**:
 - PC0 FastEthernet0 to Switch2 FastEthernet0/1
 - PC1 FastEthernet0 to Switch2 FastEthernet0/2
 - PC3 FastEthernet0 to Switch3 FastEthernet0/1
 - PC4 FastEthernet0 to Switch3 FastEthernet0/2
5. **Connect Switches** using a **Copper Straight-Through cable**:

- Switch2 FastEthernet0/5 to Switch3 FastEthernet0/5 (or any available ports).

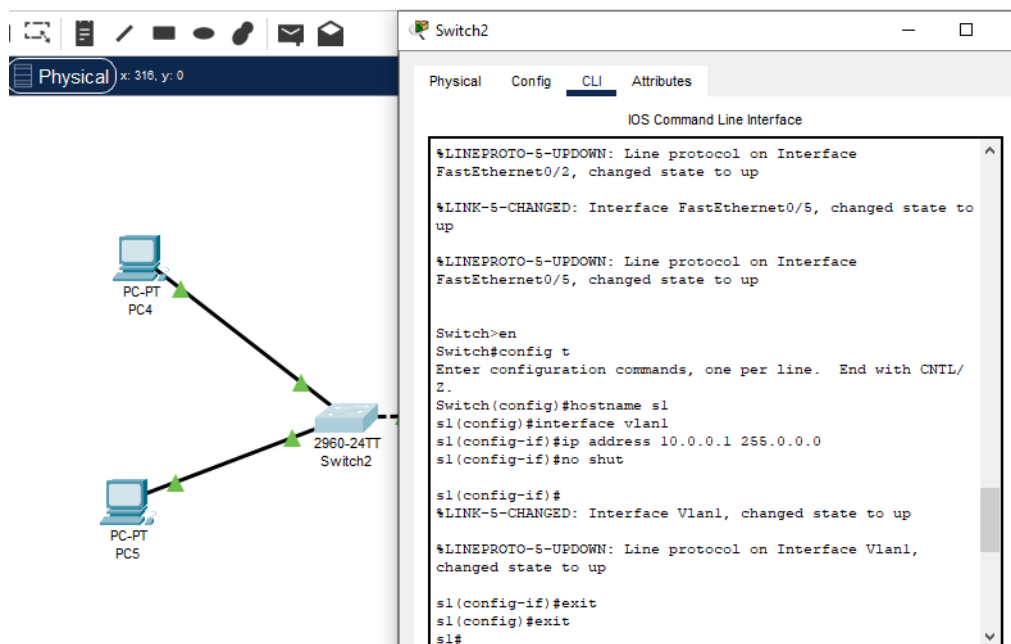
Step 2: Configure IP Addresses on PCs

1. **PC0:** Click PC0 > Desktop > IP Configuration. Set IPv4 Address: 192.168.1.1, Subnet Mask: 255.255.255.0. Close.
2. **PC1:** Click PC1 > Desktop > IP Configuration. Set IPv4 Address: 192.168.1.2, Subnet Mask: 255.255.255.0. Close.
3. **PC3:** Click PC3 > Desktop > IP Configuration. Set IPv4 Address: 192.168.1.3, Subnet Mask: 255.255.255.0. Close.
4. **PC4:** Click PC4 > Desktop > IP Configuration. Set IPv4 Address: 192.168.1.4, Subnet Mask: 255.255.255.0. Close.

Step 3: Configure Management IP on Switches (Optional but shown in images)

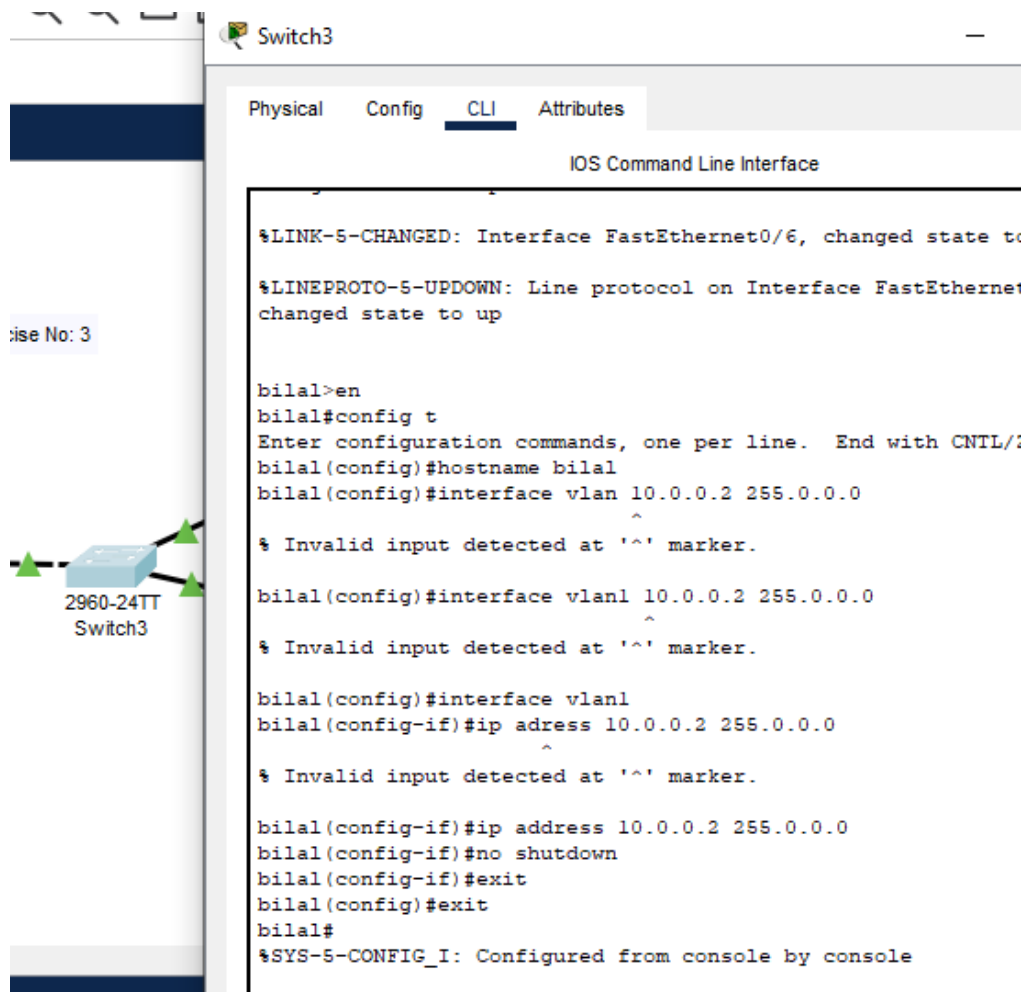
1. Switch2:

- Click Switch2 > CLI tab.
- Type `en`
- Type `config t`
- Type `hostname s1`
- Type `interface vlan1`
- Type `ip address 10.0.0.1 255.0.0.0`
- Type `no shut`



2. Switch3:

- Click Switch3 > CLI tab.
- Type en
- Type config t
- Type hostname bilal
- Type interface vlan1
- Type ip address 10.0.0.2 255.0.0.0
- Type no shut

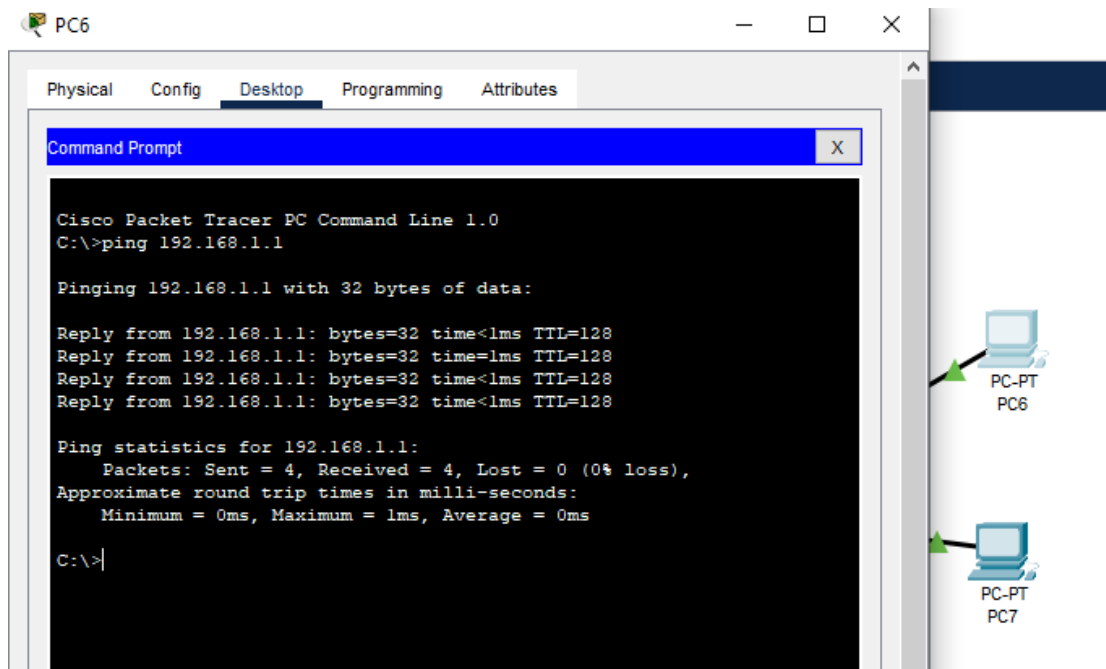


Step 4: Verify Connectivity (Ping)

1. From PC0 (192.168.1.1):

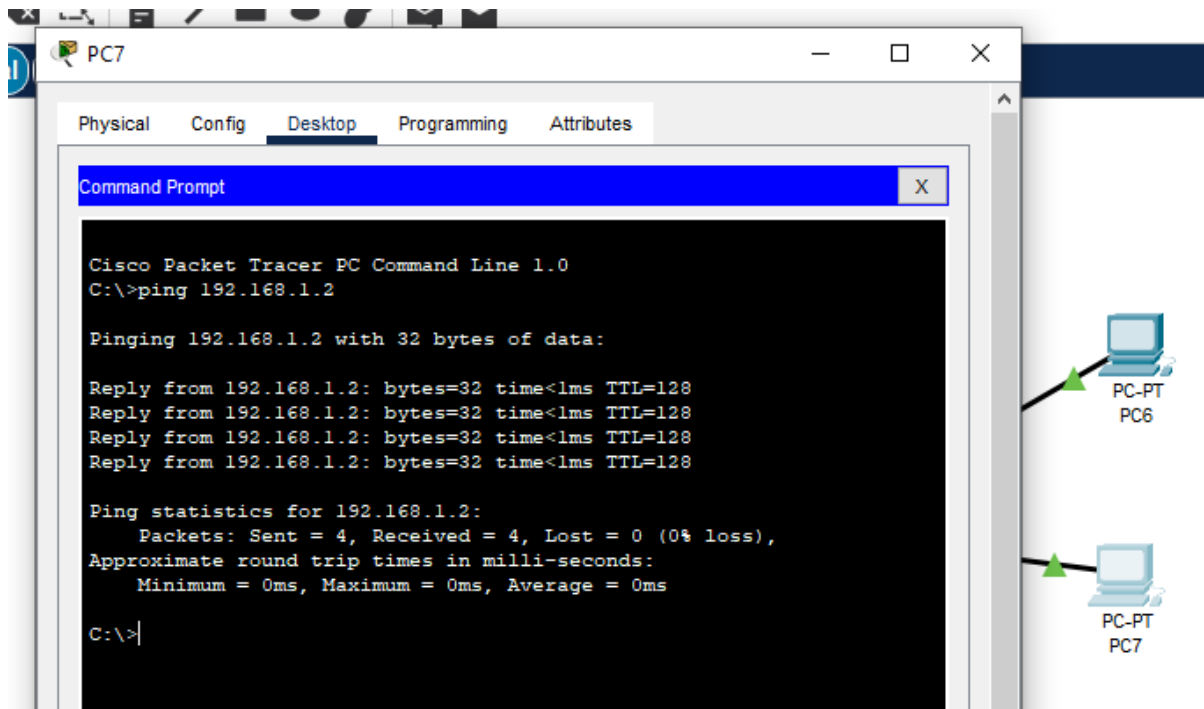
- Click PC0 > Desktop > Command Prompt.
- Type ping 192.168.1.2 (Ping PC1 - same switch)
- Type ping 192.168.1.3 (Ping PC3 - across switches)

- Type ping 192.168.1.4 (Ping PC4 - across switches)



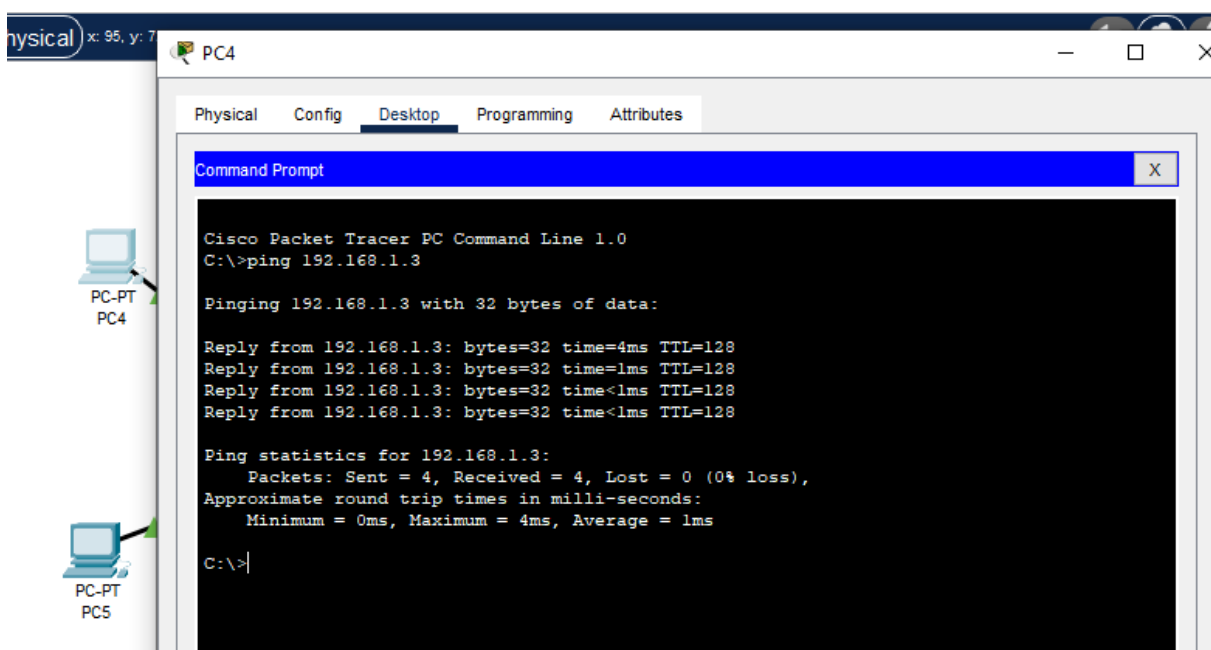
2. From PC1 (192.168.1.2):

- Click PC1 > Desktop > Command Prompt.
- Type ping 192.168.1.1 (Ping PC0 - same switch)
- Type ping 192.168.1.3 (Ping PC3 - across switches)
- Type ping 192.168.1.4 (Ping PC4 - across switches) *(Optional: Insert lab_03_7.PNG showing ping to 192.168.1.2 from PC7/PC1, then try pinging other IPs from PC1)*



3. From PC3 (192.168.1.3):

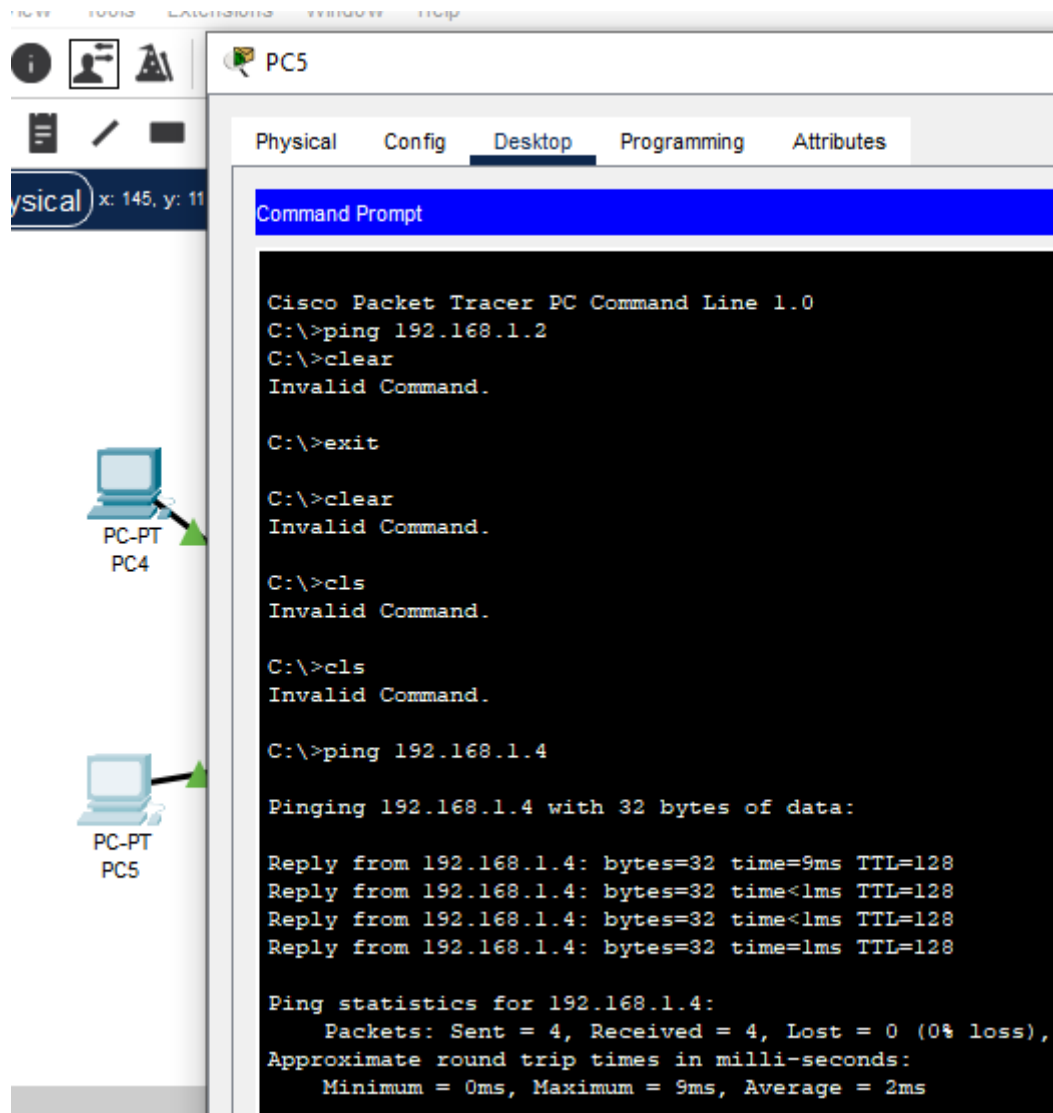
- Click PC3 > Desktop > Command Prompt.
- Type ping 192.168.1.4 (Ping PC4 - same switch)
- Type ping 192.168.1.1 (Ping PC0 - across switches)
- Type ping 192.168.1.2 (Ping PC1 - across switches) *(Optional: Insert lab_03_1.PNG showing ping to 192.168.1.3 from PC4/PC3, then try pinging other IPs from PC3)*



4. From PC4 (192.168.1.4):

- Click PC4 > Desktop > Command Prompt.
- Type ping 192.168.1.3 (Ping PC3 - same switch)
- Type ping 192.168.1.1 (Ping PC0 - across switches)
- Type ping 192.168.1.2 (Ping PC1 - across switches) *(Optional: Insert lab_03_5.PNG showing ping from PC5/PC1 to 192.168.1.4 if relevant, or show ping from PC4 itself)*

4.



Conclusion:

- All PCs successfully pinged each other, confirming that devices across different switches can communicate when they are in the same broadcast domain (VLAN) and the switches are interconnected.

Lab Manual: Switch Basic Configuration & VLAN Creation (Lab Exercise No. 4)

1. Objective:

- Replace the default switch hostname.
- Create a new VLAN and verify its creation.
- Check the switch's IOS version.

2. Topology:

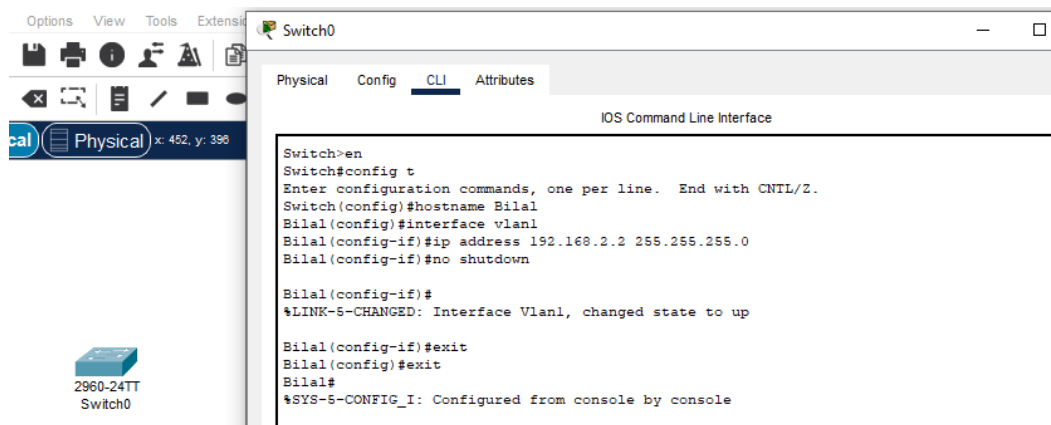
- A single **2960-24TT Switch** (Switch0).
- *(No PCs are explicitly required for this lab, but you will access the switch via console or a connected PC)*

3. Procedure (Step-by-Step):

Step 1: Access the Switch CLI & Change Hostname

1. Add a **2960-24TT Switch** to the Packet Tracer workspace. (Label it Switch0).
2. Click on **Switch0**.
3. Go to the **CLI** tab.
4. Enter privileged EXEC mode:
5. Switch> enable
6. Switch#
7. Enter global configuration mode:
8. Switch# configure terminal
9. Switch(config)#
10. Change the hostname (e.g., to "Bilal"):
11. Switch(config)# hostname Bilal
12. Bilal(config)#

(This step is covered in lab_4(1).PNG)



Step 2: Create a New VLAN and Verify

1. While in global configuration mode (Bilal(config)#), create a new VLAN (e.g., VLAN 10):
2. Bilal(config)# vlan 10
3. Bilal(config-vlan)# name Bilal // Or any descriptive name
4. Bilal(config-vlan)# exit
5. Exit global configuration mode to return to privileged EXEC mode:
6. Bilal(config)# exit
7. Bilal#
8. Verify the VLAN creation using the show vlan brief command:
9. Bilal# show vlan brief

You should see VLAN 10 listed with its name and "active" status.

```
Bilal(config)#vlan 10
Bilal(config-vlan)#name Bilal
Bilal(config-vlan)#exit
Bilal(config)#show vlan brief
^
% Invalid input detected at '^' marker.

Bilal(config)#exit
Bilal#
%SYS-5-CONFIG_I: Configured from console by console

Bilal#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
10   Bilal                  active
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active
Bilal#
```

Copy

Paste

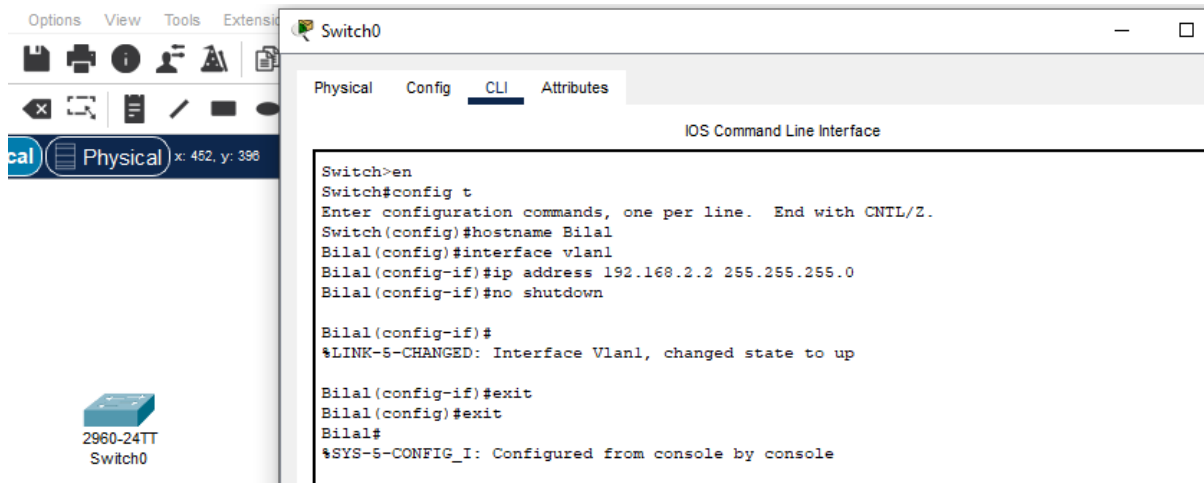
Step

3:

Configure Management IP for VLAN 1 (Optional but shown in images)

1. Enter global configuration mode again:
2. Bilal# configure terminal
3. Bilal(config)#
4. Configure an IP address for VLAN 1 (for switch management, not for new VLAN creation):
5. Bilal(config)# interface vlan1
6. Bilal(config-if)# ip address 192.168.2.2 255.255.255.0
7. Bilal(config-if)# no shutdown
8. Bilal(config-if)# exit
9. Exit global configuration mode:
10. Bilal(config)# exit
11. Bilal#

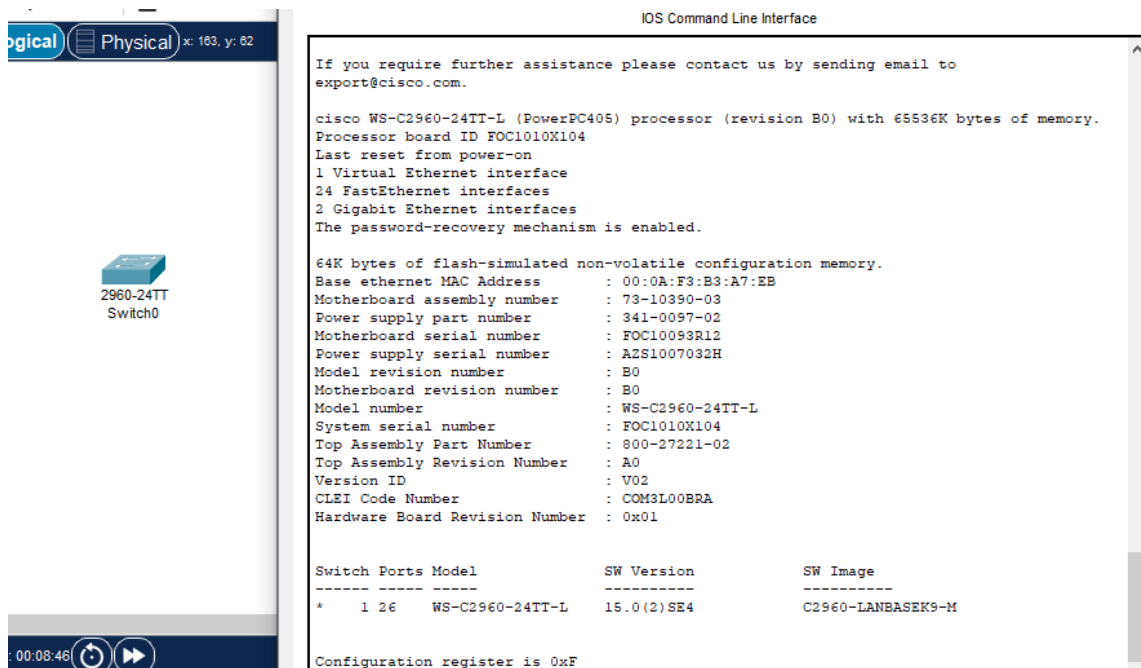
(This step is covered in lab_4(1).PNG after the hostname change, but placed here to maintain logical flow of configuration)

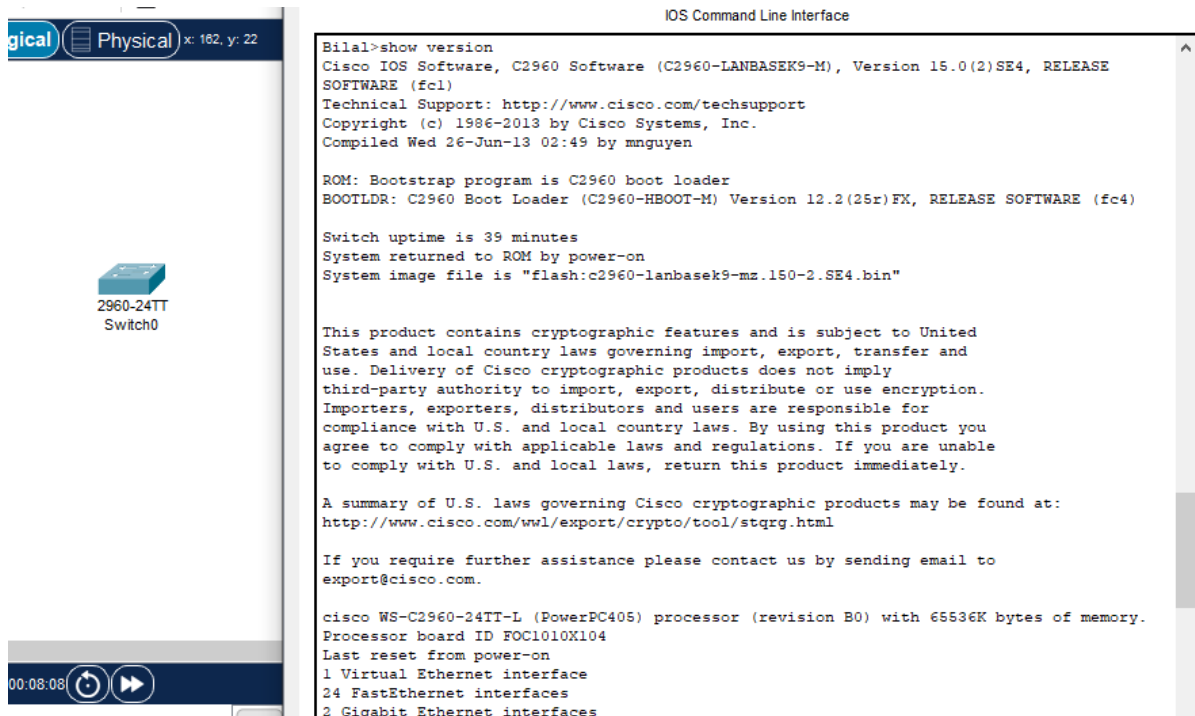


Step 4: Check Switch Version

1. From privileged EXEC mode (Bilal#), issue the command to check the switch version:
2. Bilal# show version

This command will display detailed information about the Cisco IOS software, hardware, and uptime. (This step is covered in lab_4(3.1).PNG and lab_4(3.2).PNG)





4. Conclusion:

- The switch hostname was successfully changed.
- A new VLAN (VLAN 10) was successfully created and verified.
- The switch's IOS version information was displayed.

Laboratory Exercise No. 5: Basic Switch Security and Port Security

Objective:

To configure basic security features on a Cisco switch, including hostname, console password, enable secret, VTY password for Telnet access, and to implement port security by binding connected PCs with their MAC addresses.

Topology:

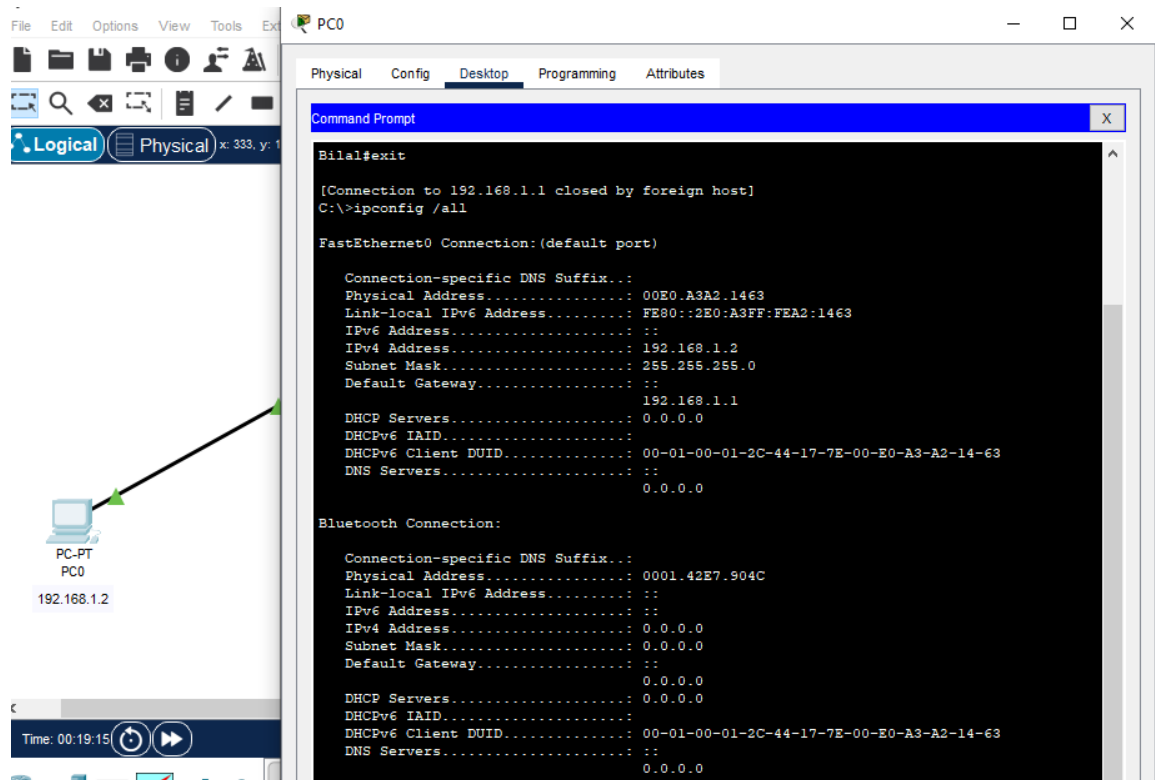
A single 2960-24T switch connected to two PCs (PC0 and PC1).

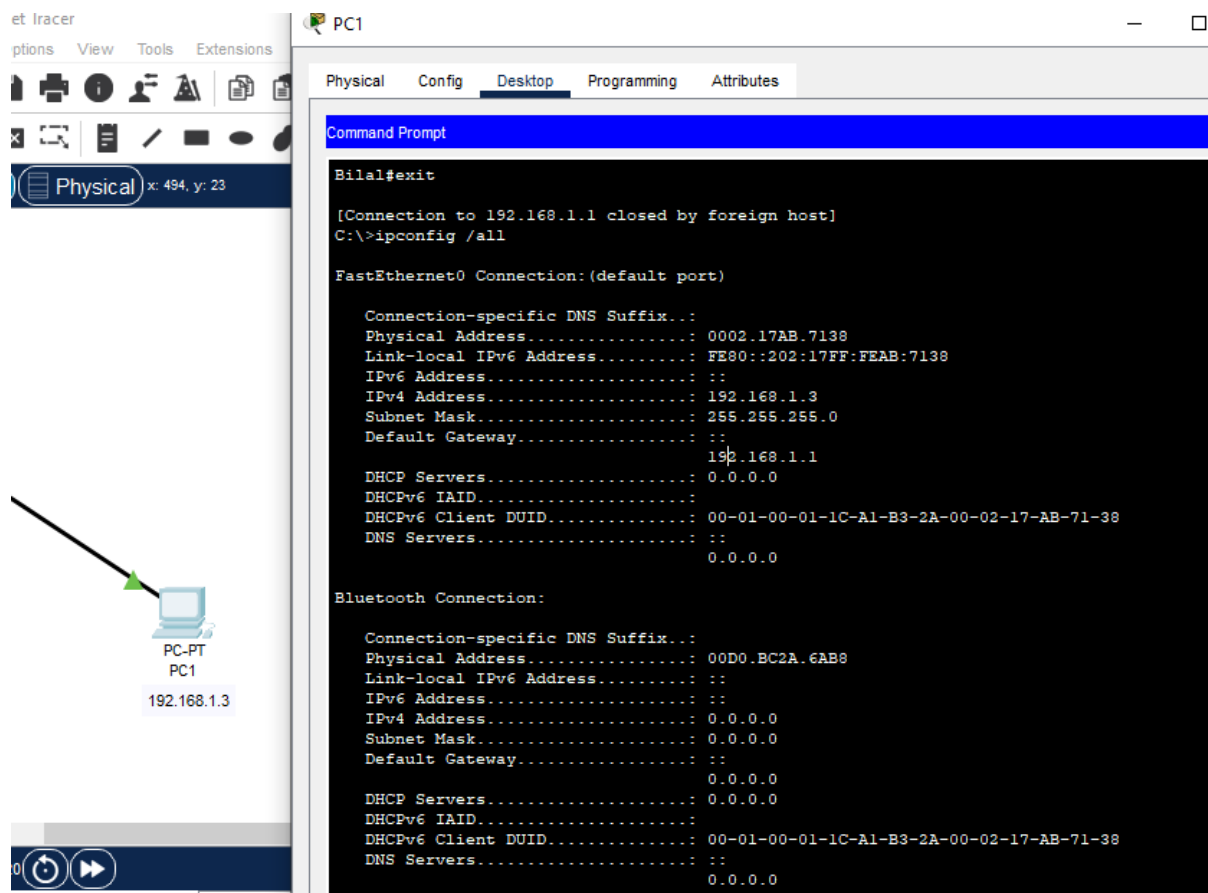
- **Switch Name:** Bilal (configured)
- **Switch IP Address (VLAN1):** 192.168.1.1
- **PC0 IP Address:** 192.168.1.2
- **PC1 IP Address:** 192.168.1.3

Procedure:

Step 1: Build the Network Topology

1. Add one **2960-24T Switch**.
2. Add two **PCs (PC0, PC1)**.
3. Connect **PC0** to **Switch FastEthernet0/1**.
4. Connect **PC1** to **Switch FastEthernet0/2**.
5. Set IP addresses for PCs:
 - **PC0:** 192.168.1.2 (Subnet Mask: 255.255.255.0)
 - **PC1:** 192.168.1.3 (Subnet Mask: 255.255.255.0)
 - *Verification:* Use `ipconfig /all` on both PCs. (Refer to lab_05(4)_ipaddre_1.PNG, lab_05(5)_ipaddre_2.PNG)





Step 2: Configure Basic Switch Security

1. Access the **Switch CLI**.
2. Enter privileged EXEC mode:
3. Switch>en
4. Enter global configuration mode:
5. Switch#config t
6. Change hostname to your name:
7. Switch(config)#hostname Bilal
8. Configure console password and login:
9. Bilal(config)#line con 0
10. Bilal(config-line)#password Bilal
11. Bilal(config-line)#login

12. Bilal(config-line)#exit
13. Encrypt plain text passwords:
14. Bilal(config)#service password-encryption
15. Configure enable secret (stronger password):
16. Bilal(config)#enable secret BilalCode
17. Configure VTY (Telnet) password and login:
18. Bilal(config)#line vty 0 15
19. Bilal(config-line)#password BilalDeveloper
20. Bilal(config-line)#login
21. Bilal(config-line)#exit
22. Configure management IP address for VLAN1 and activate it:
23. Bilal(config)#interface vlan1
24. Bilal(config-if)#ip address 192.168.1.1 255.255.255.0
25. Bilal(config-if)#no shutdown
26. Bilal(config-if)#exit
27. Exit configuration mode:
28. Bilal(config)#exit
29. Bilal#

Verification: The console output SYS-5-CONFIG_I: Configured from console by console indicates successful configuration save (after exit). (Refer to lab_05(1).PNG, lab_05(5).PNG)

Bilal
— □ ×

Physical
Config
CLI
Attributes

IOS Command Line Interface

```

Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Bilal
Bilal(config)#line console 0
Bilal(config-line)#password BilalHussain
Bilal(config-line)#login
Bilal(config-line)#service password-encryption
Bilal(config)#exit
Bilal#
%SYS-5-CONFIG_I: Configured from console by console

Bilal#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bilal(config)#enable secret BilalCode
Bilal(config)#exit
Bilal#
%SYS-5-CONFIG_I: Configured from console by console

Bilal#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bilal(config)#interface vlan1
Bilal(config-if)#ipaddress 192.168.1.1 255.255.255.0
      ^
% Invalid input detected at '^' marker.

Bilal(config-if)#ip address 192.168.1.1 255.255.255.0
Bilal(config-if)#no shutdown


Bilal(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

Bilal(config-if)#exit
Bilal(config)#line vty 0 2
Bilal(config-line)#password BilalDeveloper
Bilal(config-line)#login
Bilal(config-line)#exit
Bilal(config)#

```

Copy
Paste

LAB TASK: 05



PC-PT PC2 2960-24TT Switch4

```

Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Bilal
Bilal(config)#line con 0
Bilal(config-line)#password Bilal
Bilal(config-line)#login
Bilal(config-line)#exit
Bilal(config)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Bilal(config)#enable secret smiu
Bilal(config)#line vty 0 2
Bilal(config-line)#password BilalCode
Bilal(config-line)#login
Bilal(config-line)#exit
Bilal(config)#interface valn1
      ^
% Invalid input detected at '^' marker.

Bilal(config)#interface vlan1
Bilal(config-if)#ip address 192.168.1.2 255.255.255.0
Bilal(config-if)#no shutdown

Bilal(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

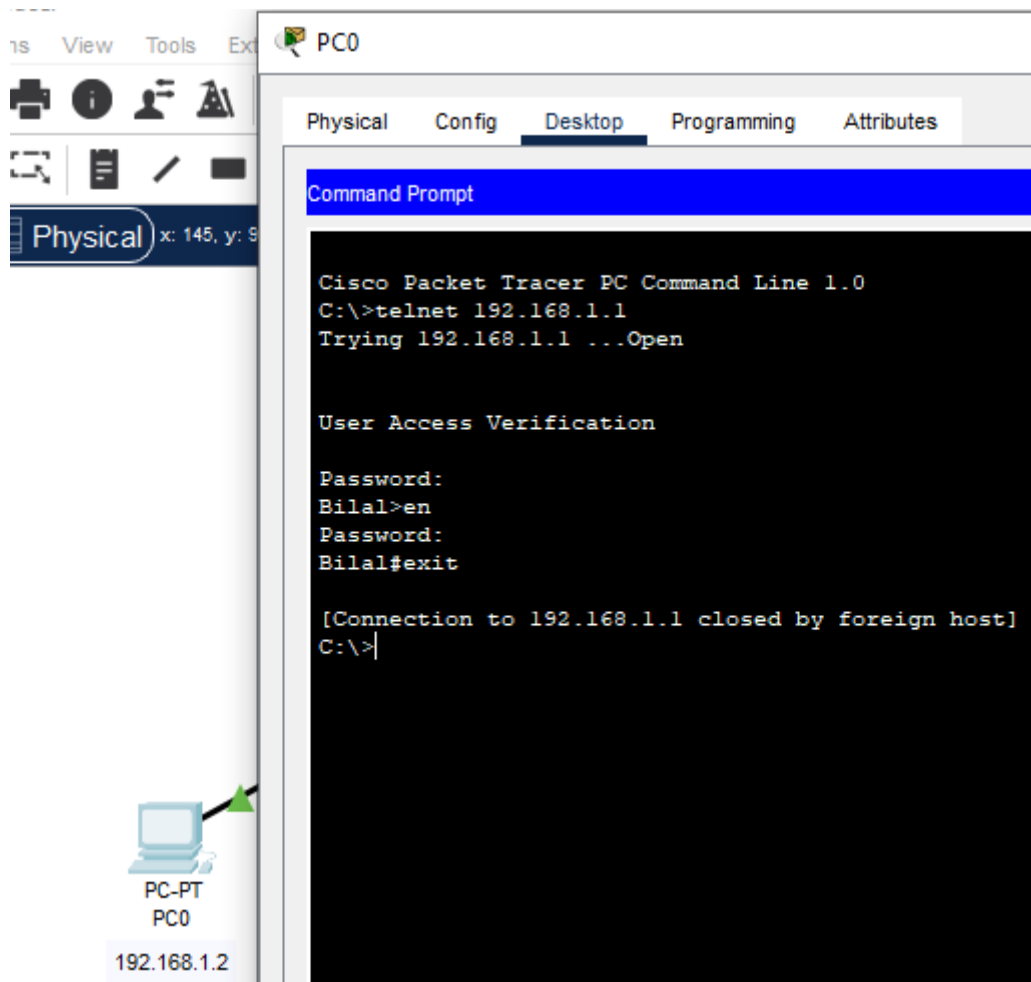
Bilal(config-if)#exit
Bilal(config)#

```

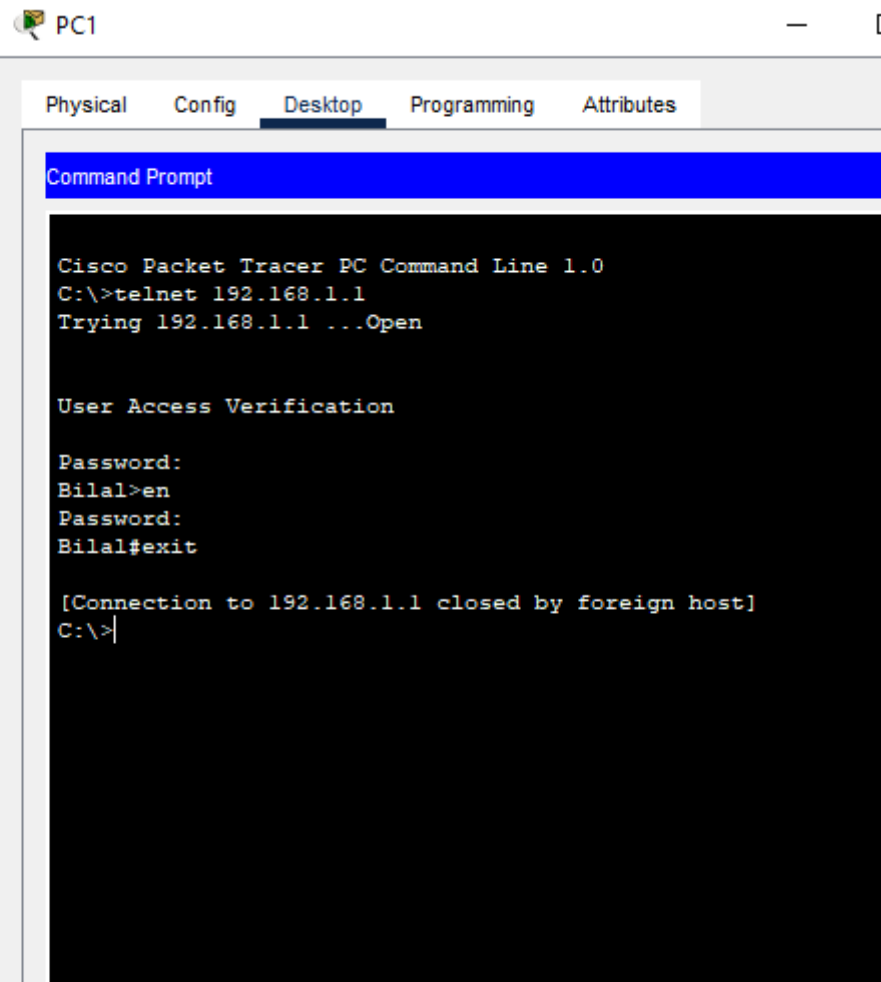
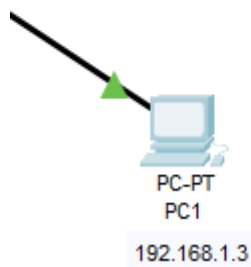
Time: 01:28:53
⏮ ⏭

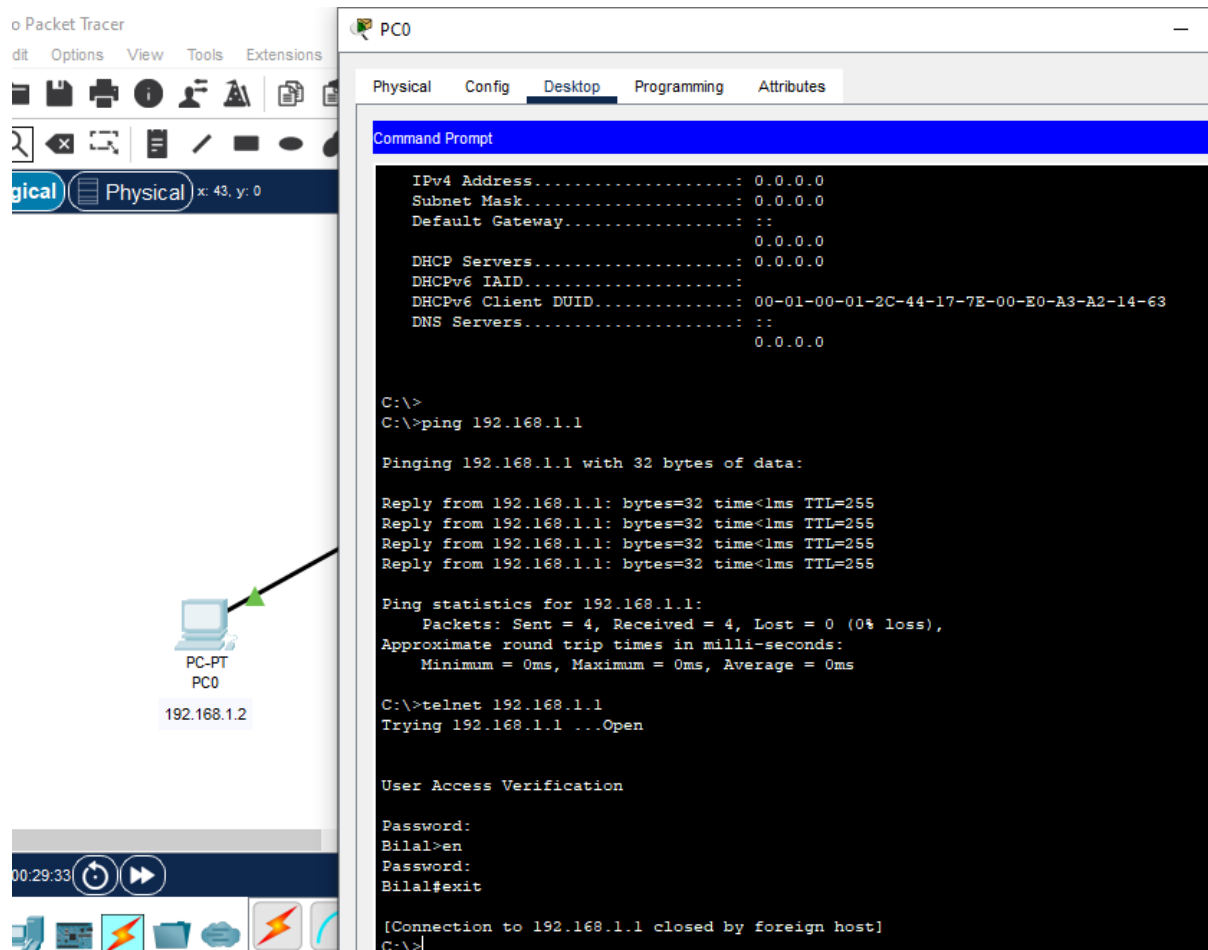
Step 3: Verify Telnet Access from PCs

1. From **PC0 Command Prompt**:
2. C:\>telnet 192.168.1.1
3. Enter passwords when prompted:
 - Console password: Bilal
 - Enable password: en
 - Enable secret: BilalCode
 - VTY password: BilalDeveloper
4. Type exit to close the telnet session. *Verification:* Observe successful login and then logout. Repeat from PC1. (Refer to lab_05(2).PNG, lab_05(3).PNG, lab_05(6_complete)_fa0_1.PNG)



elp





Step 4: Configure Port Security (FastEthernet0/1)

1. Access the **Switch CLI** and enter global configuration mode.
2. Navigate to interface FastEthernet0/1:
3. Bilal(config)#int fa0/1
4. Set port mode to access:
5. Bilal(config-if)#switchport mode access
6. Enable port security:
7. Bilal(config-if)#switchport port-security
8. Set maximum MAC addresses to 1:
9. Bilal(config-if)#switchport port-security maximum 1
10. Bind the connected PC's MAC address dynamically as sticky:
11. Bilal(config-if)#switchport port-security mac-address sticky

12. Set violation mode to shutdown:
13. Bilal(config-if)#switchport port-security violation shutdown
14. Exit interface configuration:
15. Bilal(config-if)#exit

Verification: No specific output shown in your images during configuration, but the show port-security commands later will verify. (Refer to lab_05(6)_fa0_1.PNG)

```
Bilal>en
Password:
Bilal#config t
      ^
% Invalid input detected at '^' marker.

Bilal#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bilal(config)#int fa0/1
Bilal(config-if)#switchport mode access
Bilal(config-if)#switchport port-security
Bilal(config-if)#switchport port-security mac-address ?
  H.H.H    48 bit mac address
  sticky   Configure dynamic secure addresses as sticky
Bilal(config-if)#switchport port-security mac-address
% Incomplete command.
Bilal(config-if)#switchport port-security mac-address 00E0.A3A2.1463
Bilal(config-if)#switchport port-security mac-address sticky
Bilal(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Bilal(config-if)#switchport port-security violation shutdown
Bilal(config-if)#exit
Bilal(config)#exit
Bilal#
%SYS-5-CONFIG_I: Configured from console by console

Bilal#
```

Step 5: Configure Port Security (FastEthernet0/2)

1. Access the **Switch CLI** and enter global configuration mode.
2. Navigate to interface FastEthernet0/2:
3. Bilal(config)#int fa0/2
4. Set port mode to access:
5. Bilal(config-if)#switchport mode access
6. Enable port security:
7. Bilal(config-if)#switchport port-security
8. Set maximum MAC addresses to 1:

9. Bilal(config-if)#switchport port-security maximum 1
10. Bind the connected PC's MAC address dynamically as sticky (or explicitly using MAC address 0002.17AB.7138 as shown in your image):
11. Bilal(config-if)#switchport port-security mac-address sticky
(Alternatively, if you explicitly want to set it, use the MAC address from PC1, e.g.,
switchport port-security mac-address 0002.17AB.7138)
12. Set violation mode to shutdown:
13. Bilal(config-if)#switchport port-security violation shutdown
14. Exit interface configuration:
15. Bilal(config-if)#exit

Verification: No specific output shown in your images during configuration. (Refer to lab_05(1)_fa0_2.PNG)

```
User Access Verification

Password:

Bilal>en
Password:
Bilal#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bilal(config)#int fa0/2
Bilal(config-if)#switchport mode access
Bilal(config-if)#switchport port-security
Bilal(config-if)#switchport port-security mac-address 0002.17AB.7138
Bilal(config-if)#switchport port-security sticky
^
% Invalid input detected at '^' marker.

Bilal(config-if)#switchport port-security mac-address ?
  H.H.H  48 bit mac address
  sticky Configure dynamic secure addresses as sticky
Bilal(config-if)#switchport port-security mac-address sticky
Bilal(config-if)#switchport port-security violation ?
  protect  Security violation protect mode
  restrict Security violation restrict mode
  shutdown Security violation shutdown mode
Bilal(config-if)#switchport port-security violation shutdown
Bilal(config-if)#exit
Bilal(config)#show port-security
^
% Invalid input detected at '^' marker.

Bilal(config)#exit
Bilal#
%SYS-5-CONFIG_I: Configured from console by console

Bilal#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
```

Step 6: Verify Port Security

1. From privileged EXEC mode, show port security overview:

2. Bilal#show port-security

Expected Output: Shows Fa0/1 and Fa0/2 with MaxSecureAddr and CurrentAddr as 1, SecurityViolation as 0, and Security Action as Shutdown. (Refer to lab_05(6a)_fa0_1.PNG, lab_05(7b)_fa0_2.PNG, lab_05_fa0_1_com.PNG, lab_05(7)_fa0_2_complete.PNG)

3. Show detailed port security for interface Fa0/1:

4. Bilal#show port-security int fa0/1

Expected Output: Port Security : Enabled, Port Status : Secure-up, Violation Mode : Shutdown, Maximum MAC Addresses : 1, Total MAC Addresses : 1, Configured MAC Addresses : 1. The Last Source Address:Vlan will show the MAC address of PC0. (Refer to lab_05(6a)_fa0_1.PNG, lab_05_fa0_1_com.PNG)

5. Show detailed port security for interface Fa0/2:

6. Bilal#show port-security int fa0/2

Expected Output: Similar to Fa0/1, but the Last Source Address:Vlan will show the MAC address of PC1. (Refer to lab_05(7b)_fa0_2.PNG, lab_05(7)_fa0_2_complete.PNG)

Step 7: Observe Port Security Behavior (Connect another PC)

1. Disconnect PC0 from Fa0/1.
2. Connect a *new* PC (or PC1 if you disconnect it from Fa0/2) to Fa0/1.
3. Try to ping from the newly connected PC.
4. Observe the port status on the switch (it should go into error-disabled state, indicated by an orange/red light on the port in Packet Tracer).
5. Verify the security violation count:
6. Bilal#show port-security int fa0/1

Expected Output: Security Violation Count : 1 (or more).

Conclusion:

The basic switch security measures (hostname, console, enable, VTY passwords) were successfully implemented and verified via Telnet. Port security was configured on FastEthernet0/1 and FastEthernet0/2, successfully binding the interfaces to the MAC addresses of the initially connected PCs. When an unauthorized device was connected, the port entered a shutdown state, demonstrating the effectiveness of port security.

Laboratory Exercise No. 5: Basic Switch Security and Port Security

Objective:

To configure basic security features on a Cisco switch, including hostname, console password, enable secret, VTY password for Telnet access, and to implement port security by binding connected PCs with their MAC addresses. This lab also involves observing port security behaviour when an unauthorized PC attempts to connect.

Topology:

A single 2960-24T switch connected to two PCs (PC0 and PC1).

- **Switch Name:** Bilal (configured)
- **Switch Management IP (VLAN1):** 192.168.1.1
- **PC0 IP Address:** 192.168.1.2
- **PC1 IP Address:** 192.168.1.3

This image displays the network topology for Laboratory Exercise No. 5, showing a single Cisco 2960-24T switch named "Bilal" connected to PC0 and PC1. The IP addresses for the switch's management VLAN (192.168.1.1), PC0 (192.168.1.2), and PC1 (192.168.1.3) are clearly indicated.

Procedure:

Part A: Basic Switch Security and Remote Access (Telnet)

Step 1: Build the Network Topology and Configure PC IPs

1. In Cisco Packet Tracer, add one **2960-24T Switch** from the network devices.
2. Add two **End Devices > PCs (PC0, PC1)**.
3. Connect **PC0 to Switch FastEthernet0/1** using a **Copper Straight-Through cable**.
4. Connect **PC1 to Switch FastEthernet0/2** using a **Copper Straight-Through cable**.
5. Configure the IP addresses for PC0 and PC1:
 - For PC0: Click on PC0 > Desktop tab > IP Configuration. Set IPv4 Address: 192.168.1.2 and Subnet Mask: 255.255.255.0.
 - For PC1: Click on PC1 > Desktop tab > IP Configuration. Set IPv4 Address: 192.168.1.3 and Subnet Mask: 255.255.255.0.

6. Verify the IP configuration on both PCs by opening Desktop > Command Prompt and typing `ipconfig /all`.

This screenshot from PC0's Command Prompt shows the output of `ipconfig /all`, confirming that FastEthernet0 has an IPv4 Address of 192.168.1.2 and a Subnet Mask of 255.255.255.0. It also shows the MAC address of PC0's FastEthernet adapter (00E0.A3A2.1463).

This screenshot from PC1's Command Prompt shows the output of `ipconfig /all`, confirming that FastEthernet0 has an IPv4 Address of 192.168.1.3 and a Subnet Mask of 255.255.255.0. It also displays the MAC address of PC1's FastEthernet adapter (0002.17AB.7138).

Step 2: Configure Basic Switch Security (Hostname, Console, Enable Secret, VTY)

1. Click on the Switch > CLI tab to access its command-line interface.
2. Enter privileged EXEC mode:

Code snippet

```
Switch>enable
```

3. Enter global configuration mode:

Code snippet

```
Switch#configure terminal
```

4. **Replace default Switch name with your Name (e.g., Bilal):**

Code snippet

```
Bilal(config)#hostname Bilal
```

5. **Apply console password:** Configure a password for the console line and enable login.

Code snippet

```
Bilal(config)#line console 0
```

```
Bilal(config-line)#password Bilal
```

```
Bilal(config-line)#login
```

```
Bilal(config-line)#exit
```

6. Encrypt all plain text passwords for security:

Code snippet

Bilal(config)#service password-encryption

7. **Apply secret:** Configure a strong enable secret password (BilalCode) for privileged EXEC mode.

Code snippet

Bilal(config)#enable secret BilalCode

8. Configure VTY (Telnet) password (BilalDeveloper) for remote access and enable login for VTY lines.

Code snippet

Bilal(config)#line vty 0 15

Bilal(config-line)#password BilalDeveloper

Bilal(config-line)#login

Bilal(config-line)#exit

9. Configure the management IP address for VLAN1 and activate it:

Code snippet

Bilal(config)#interface vlan1

Bilal(config-if)#ip address 192.168.1.1 255.255.255.0

Bilal(config-if)#no shutdown

Bilal(config-if)#exit

10. Exit global configuration mode and return to privileged EXEC mode:

Code snippet

Bilal(config)#exit

Bilal#

This CLI screenshot shows the initial configuration steps on the switch, including setting the hostname to "Bilal", configuring the console password and login, enabling service password encryption, and configuring the enable secret password ("BilalCode"). The configuration of the VLAN1 interface with IP address 192.168.1.1 and no shutdown is also shown.

Step 3: Telnet to connected PC (Verify Remote Access)

1. From **PC0 Command Prompt**, attempt to Telnet to the switch's management IP address:

Code snippet

```
C:\>telnet 192.168.1.1
```

2. You will be prompted for passwords. Enter them in the following order:
 - VTY password (BilalDeveloper)
 - If you type enable, you'll be prompted for the enable secret (BilalCode)
3. Type exit to close the Telnet session.
4. Repeat the Telnet attempt from PC1 to verify connectivity from both PCs.

This screenshot from PC0's Command Prompt demonstrates a successful Telnet connection to the switch at 192.168.1.1. It shows the "User Access Verification" prompt and the successful entry of the password, followed by exiting the session.

This screenshot from PC1's Command Prompt similarly demonstrates a successful Telnet connection to the switch at 192.168.1.1, confirming remote access from PC1 as well.

This combined screenshot from PC0's Command Prompt shows a successful ping to the switch's IP address (192.168.1.1) and a successful Telnet connection, further verifying connectivity and remote access capabilities.

Part B: Port Security Configuration and Observation

Step 4: Apply Port Security on FastEthernet0/1 (for PC0)

1. Access the **Switch CLI** and enter global configuration mode.
2. Navigate to interface FastEthernet0/1 (where PC0 is connected):

Code snippet

```
Bilal(config)#interface FastEthernet0/1
```

3. Set the port mode to access:

Code snippet

```
Bilal(config-if)#switchport mode access
```

4. **Apply port security:** Enable port security on the interface.

Code snippet

```
Bilal(config-if)#switchport port-security
```

5. Set the maximum allowed MAC addresses on this port to 1:

Code snippet

Bilal(config-if)#switchport port-security maximum 1

6. **Bind connected PC with MAC address (sticky):** Configure the port to learn the connected PC's MAC address dynamically and make it sticky (persist across reboots).

Code snippet

Bilal(config-if)#switchport port-security mac-address sticky

7. Set the violation mode to shutdown, which will disable the port if a security violation occurs:

Code snippet

Bilal(config-if)#switchport port-security violation shutdown

8. Exit interface configuration mode:

Code snippet

Bilal(config-if)#exit

This CLI screenshot shows the commands executed to configure port security on interface FastEthernet0/1. Key commands include switchport mode access, switchport port-security, switchport port-security maximum 1, switchport port-security mac-address sticky, and switchport port-security violation shutdown.

Step 5: Apply Port Security on FastEthernet0/2 (for PC1)

1. Access the **Switch CLI** and enter global configuration mode.
2. Navigate to interface FastEthernet0/2 (where PC1 is connected):

Code snippet

Bilal(config)#interface FastEthernet0/2

3. Set the port mode to access:

Code snippet

Bilal(config-if)#switchport mode access

4. Enable port security on the interface:

Code snippet

Bilal(config-if)#switchport port-security

5. Set the maximum allowed MAC addresses on this port to 1:

Code snippet

Bilal(config-if)#switchport port-security maximum 1

6. Configure the port to learn the connected PC's MAC address dynamically and make it sticky (as indicated by your image showing switchport port-security mac-address 0002.17AB.7138 which is PC1's MAC address, or sticky for automatic learning):

Code snippet

Bilal(config-if)#switchport port-security mac-address sticky

7. Set the violation mode to shutdown:

Code snippet

Bilal(config-if)#switchport port-security violation shutdown

8. Exit interface configuration mode:

Code snippet

Bilal(config-if)#exit

This CLI screenshot shows the commands used to configure port security on interface FastEthernet0/2. It demonstrates setting the port to access mode, enabling port security, specifying the maximum MAC address as 1, and using either the sticky option or explicitly binding a MAC address (e.g., 0002.17AB.7138) for securing the port.

Step 6: Verify Port Security Configuration

1. From privileged EXEC mode, display a summary of port security settings:

Code snippet

Bilal#show port-security

This screenshot shows the output of show port-security, providing a summary of port security settings for Fa0/1 and Fa0/2. It confirms that both ports have a MaxSecureAddr and CurrentAddr of 1, with a Security Action of Shutdown.

2. Display detailed port security information for interface FastEthernet0/1:

Code snippet

Bilal#show port-security interface FastEthernet0/1

This screenshot displays the detailed port security status for interface Fa0/1. It confirms that Port Security is Enabled, Port Status is Secure-up, Violation Mode is Shutdown, Maximum MAC Addresses is 1, and the Configured MAC Addresses is 1. The Last Source Address:Vlan shows the MAC address of PC0 (00E0.A3A2.1463).

This screenshot displays the show port-security summary and then the detailed output for Fa0/1, confirming the same settings as above. It highlights that the MAC address of the connected device is learned and secured.

3. Display detailed port security information for interface FastEthernet0/2:

Code snippet

```
Bilal#show port-security interface FastEthernet0/2
```

This screenshot displays the detailed port security status for interface Fa0/2. It confirms Enabled Port Security, Secure-up status, Shutdown violation mode, Maximum MAC Addresses as 1, and Configured MAC Addresses as 1. The Last Source Address:Vlan shows the MAC address of PC1 (0002.17AB.7138).

Step 7: Replace it with another PC and observe port security behavior

1. Ensure PC0 is connected to Fa0/1 and PC1 is connected to Fa0/2, and both are communicating correctly.
2. **Disconnect PC0 from FastEthernet0/1.**
3. **Connect a new PC (or disconnect PC1 from Fa0/2 and connect it to Fa0/1) to FastEthernet0/1.** This new PC will have a different MAC address than PC0.
4. Observe the port status in Packet Tracer: The link light for Fa0/1 should quickly turn red/orange, indicating that the port has entered an error-disabled (err-disabled) state due to a security violation.
5. Attempt to ping from the newly connected (unauthorized) PC to PC1 – it should fail.
6. From the switch CLI, verify the security violation count and port status:

Code snippet

```
Bilal#show port-security interface FastEthernet0/1
```

Expected Output: The Security Violation Count should show 1 (or more, if multiple attempts were made), and the Port Status will likely show secure-shutdown or err-disabled.

Conclusion:

This laboratory exercise successfully fulfilled all requirements of the LAB TASK. Basic switch security features were implemented, including a personalized hostname, console password, a secure enable secret, and VTY passwords for remote Telnet access, which was verified from the connected PCs. Crucially, port security was configured on FastEthernet0/1 and FastEthernet0/2, binding them to the MAC

addresses of the authorized PCs (PC0 and PC1) using the sticky method. When an unauthorized device was subsequently connected to a secured port, the switch correctly identified the security violation and shut down the port, demonstrating the robust protection offered by port security against unauthorized network access.

Laboratory Exercise No. 5: Basic Switch Security and Port Security

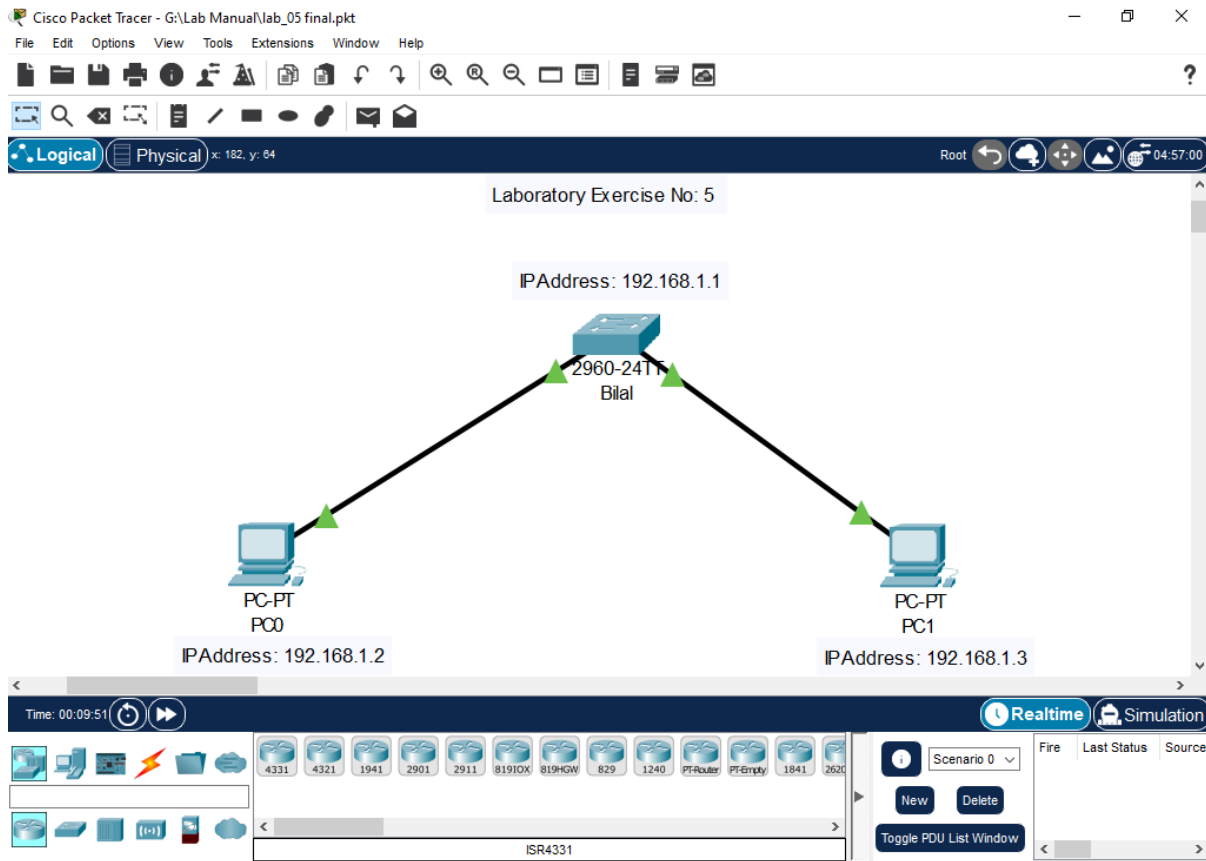
Objective:

To configure basic security features on a Cisco switch, including hostname, console password, enable secret, VTY password for Telnet access, and to implement port security by binding connected PCs with their MAC addresses. This lab also involves observing port security behavior when an unauthorized PC attempts to connect.

Topology:

A single 2960-24T switch connected to two PCs (PC0 and PC1).

- **Switch Name:** Bilal (configured)
- **Switch Management IP (VLAN1):** 192.168.1.1
- **PC0 IP Address:** 192.168.1.2
- **PC1 IP Address:** 192.168.1.3



[Insert Image: lab_05_final.PNG here] This image displays the network topology for Laboratory Exercise No. 5, showing a single Cisco 2960-24T switch named "Bilal" connected to PC0 and PC1. The IP addresses for the switch's management VLAN (192.168.1.1), PC0 (192.168.1.2), and PC1 (192.168.1.3) are clearly indicated.

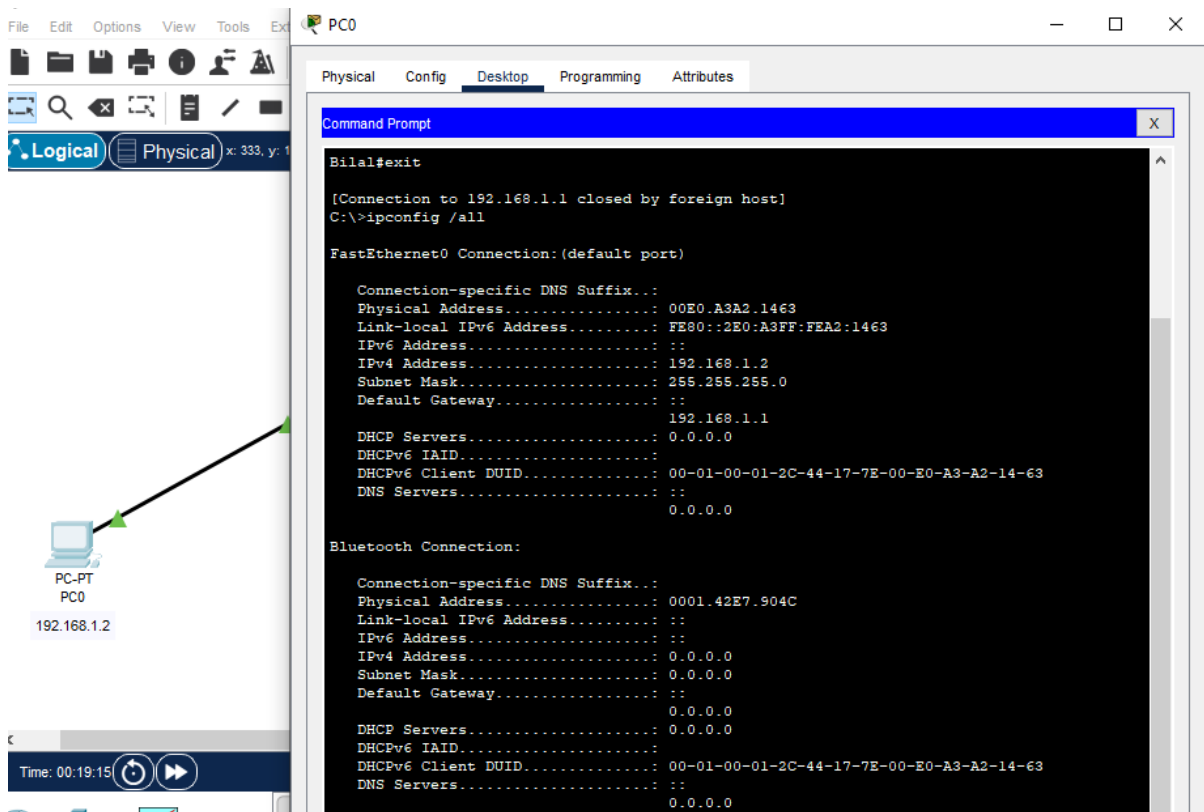
Procedure:

Part A: Basic Switch Security and Remote Access (Telnet)

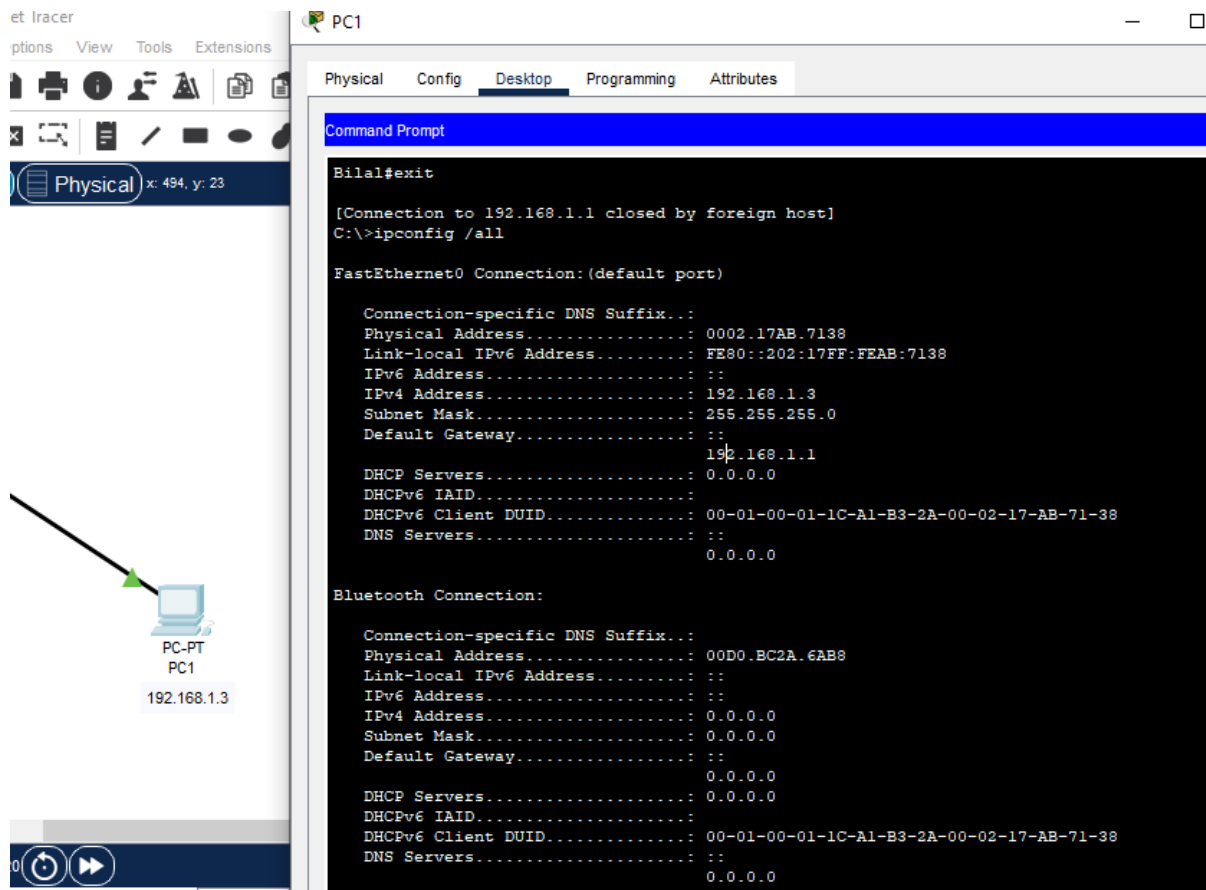
Step 1: Build the Network Topology and Configure PC IPs The first step involves setting up the physical (or logical in Packet Tracer) network connections and assigning IP addresses to the end devices.

1. In Cisco Packet Tracer, add one **2960-24T Switch** from the network devices.
2. Add two **End Devices > PCs (PC0, PC1)**.
3. Connect **PC0 to Switch FastEthernet0/1** using a **Copper Straight-Through cable**.
4. Connect **PC1 to Switch FastEthernet0/2** using a **Copper Straight-Through cable**.
5. Configure the IP addresses for PC0 and PC1 as follows:

- For PC0: Click on PC0 > Desktop tab > IP Configuration. Set IPv4 Address: 192.168.1.2 and Subnet Mask: 255.255.255.0.
 - For PC1: Click on PC1 > Desktop tab > IP Configuration. Set IPv4 Address: 192.168.1.3 and Subnet Mask: 255.255.255.0.
6. Verify the IP configuration on both PCs by opening Desktop > Command Prompt and typing ipconfig /all. This command displays the current network configuration, including the assigned IP address and MAC address.



[Insert Image: lab_05(4)_ipaddre_1.PNG here] This screenshot from PC0's Command Prompt shows the output of `ipconfig /all`, confirming that FastEthernet0 has an IPv4 Address of 192.168.1.2 and a Subnet Mask of 255.255.255.0. It also shows the MAC address of PC0's FastEthernet adapter (00E0.A3A2.1463), which will be crucial for port security later.



[Insert Image: lab_05(5)_ipaddre_2.PNG here] This screenshot from PC1's Command Prompt shows the output of `ipconfig /all`, confirming that FastEthernet0 has an IPv4 Address of 192.168.1.3 and a Subnet Mask of 255.255.255.0. It also displays the MAC address of PC1's FastEthernet adapter (0002.17AB.7138).

Step 2: Configure Basic Switch Security (Hostname, Console, Enable Secret, VTY)

This step focuses on securing access to the switch itself, both locally via the console and remotely via Telnet.

1. Click on the Switch > CLI tab to access its command-line interface.
2. Enter privileged EXEC mode:

Code snippet

Switch>enable

3. Enter global configuration mode to make changes to the switch's running configuration:

Code snippet

Switch#configure terminal

4. **Replace default Switch name with your Name (e.g., Bilal):** This helps in identifying the switch in a network.

Code snippet

```
Bilal(config)#hostname Bilal
```

5. **Apply console password:** Configure a password for the console line (direct physical access) and enable login for security.

Code snippet

```
Bilal(config)#line console 0
```

```
Bilal(config-line)#password Bilal
```

```
Bilal(config-line)#login
```

```
Bilal(config-line)#exit
```

6. **Encrypt all plain text passwords for security:** This command encrypts passwords stored in the configuration, preventing them from being viewed in plain text.

Code snippet

```
Bilal(config)#service password-encryption
```

7. **Apply secret:** Configure a strong enable secret password (BilalCode) for privileged EXEC mode. This password is encrypted by default and provides a more secure way to restrict access to privileged mode compared to the enable password.

Code snippet

```
Bilal(config)#enable secret BilalCode
```

8. **Configure VTY (Telnet) password (BilalDeveloper) for remote access and enable login for VTY lines.** This secures remote management access.

Code snippet

```
Bilal(config)#line vty 0 15
```

```
Bilal(config-line)#password BilalDeveloper
```

```
Bilal(config-line)#login
```

```
Bilal(config-line)#exit
```

9. **Configure the management IP address for VLAN1 and activate it.** This IP address allows remote management of the switch (e.g., via Telnet) from devices in the same VLAN.

Code snippet

```
Bilal(config)#interface vlan1
```

```
Bilal(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Bilal(config-if)#no shutdown
```

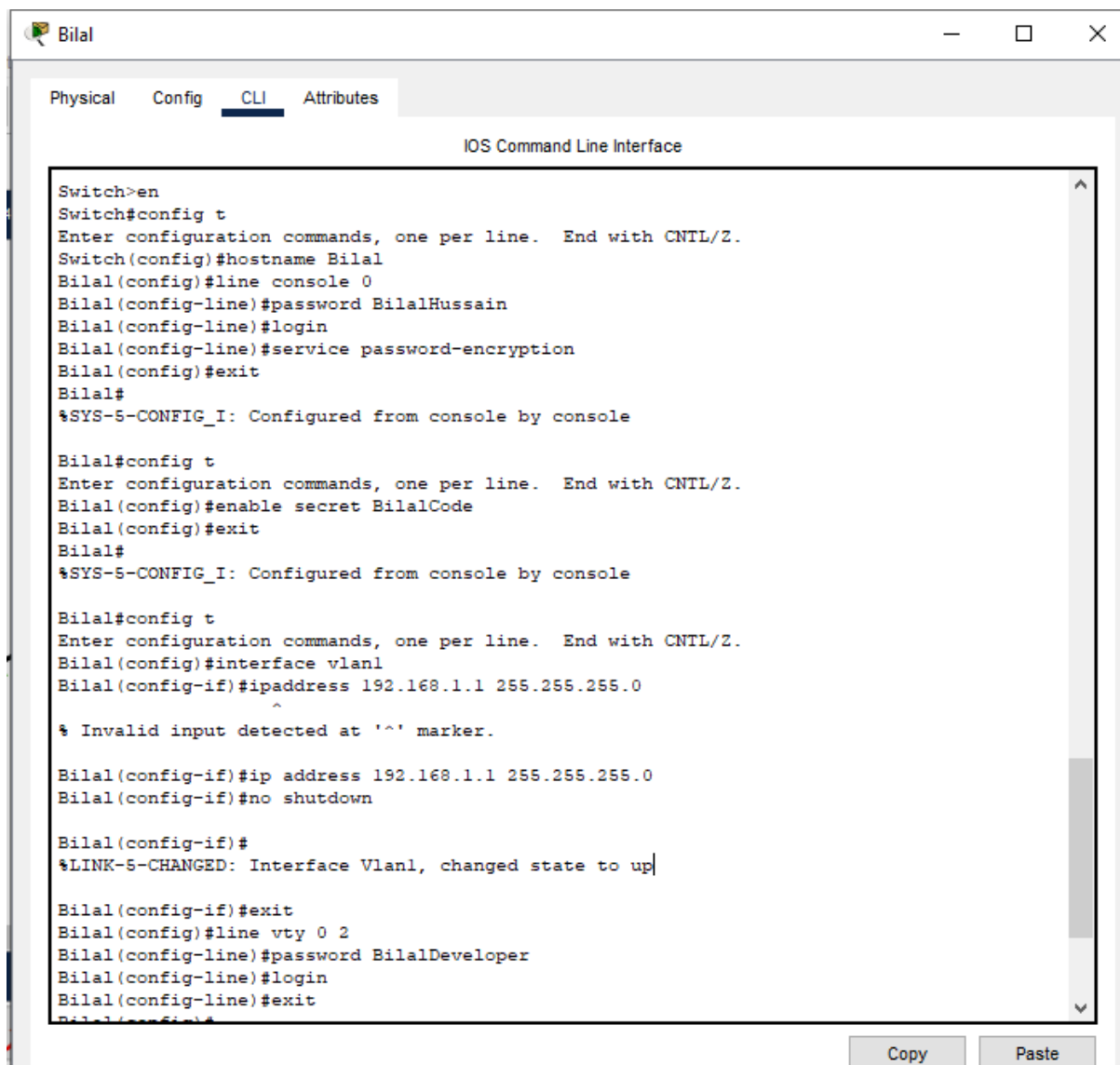
```
Bilal(config-if)#exit
```

10. Exit global configuration mode and return to privileged EXEC mode:

Code snippet

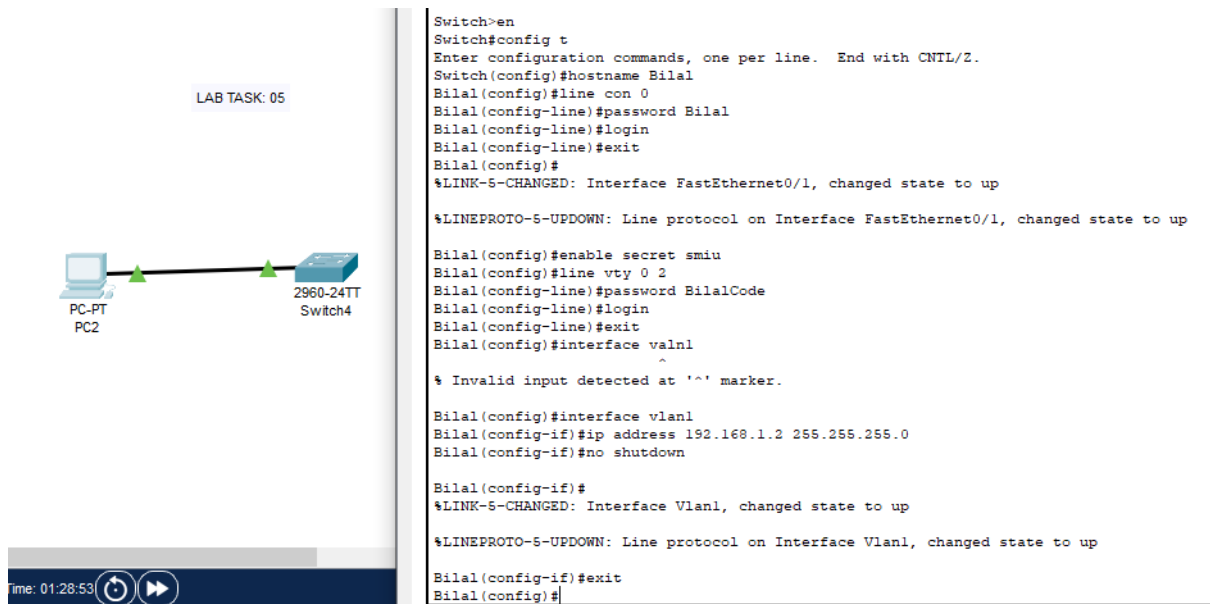
```
Bilal(config)#exit
```

```
Bilal#
```

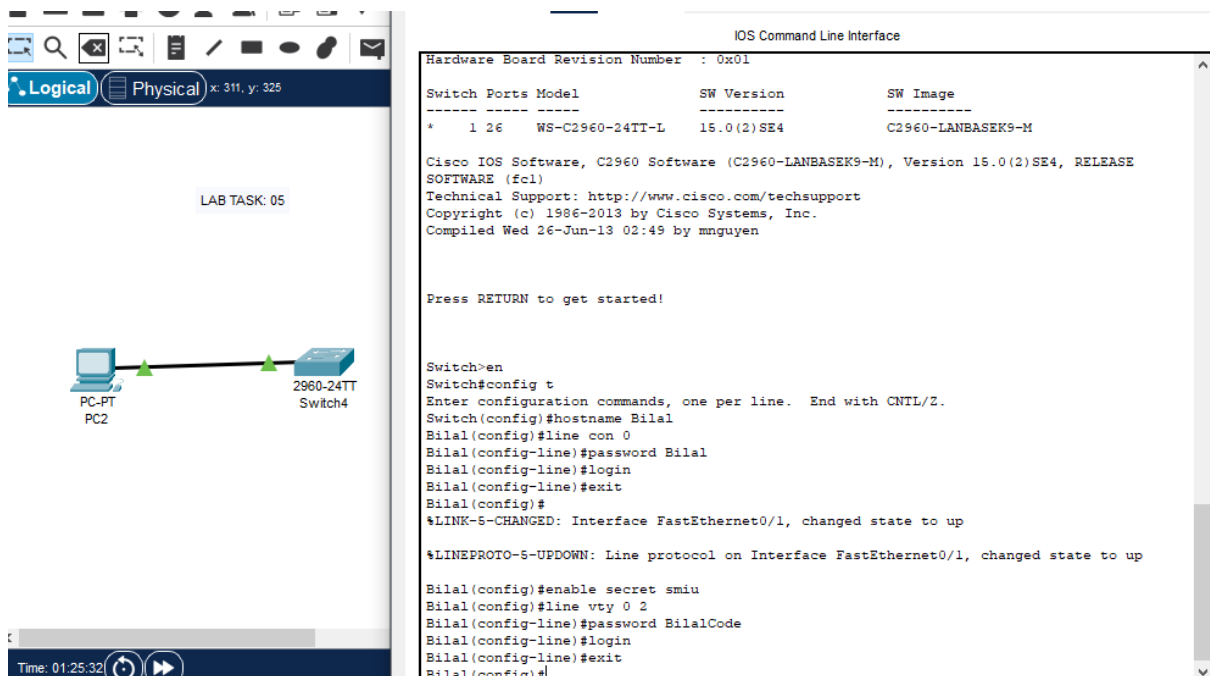


[Insert Image: lab_05(1).PNG here] This CLI screenshot shows the initial configuration steps on the switch, including setting the hostname to "Bilal", configuring the console

password and login, and enabling service password encryption. The enable secret password ("BilalCode") is also configured.



[Insert Image: lab_05(5).PNG here] This CLI screenshot continues the configuration, showing the setup of the VTY lines with a password ("BilalDeveloper") and login. It also shows the configuration of the VLAN1 interface with IP address 192.168.1.1 and the no shutdown command to activate it, making the switch remotely accessible.



[Insert Image: lab_05(4).PNG here] This screenshot provides a broader view of the switch's command-line interface after the initial configurations, likely showing the transition from global config mode back to privileged EXEC mode, confirming the hostname change.

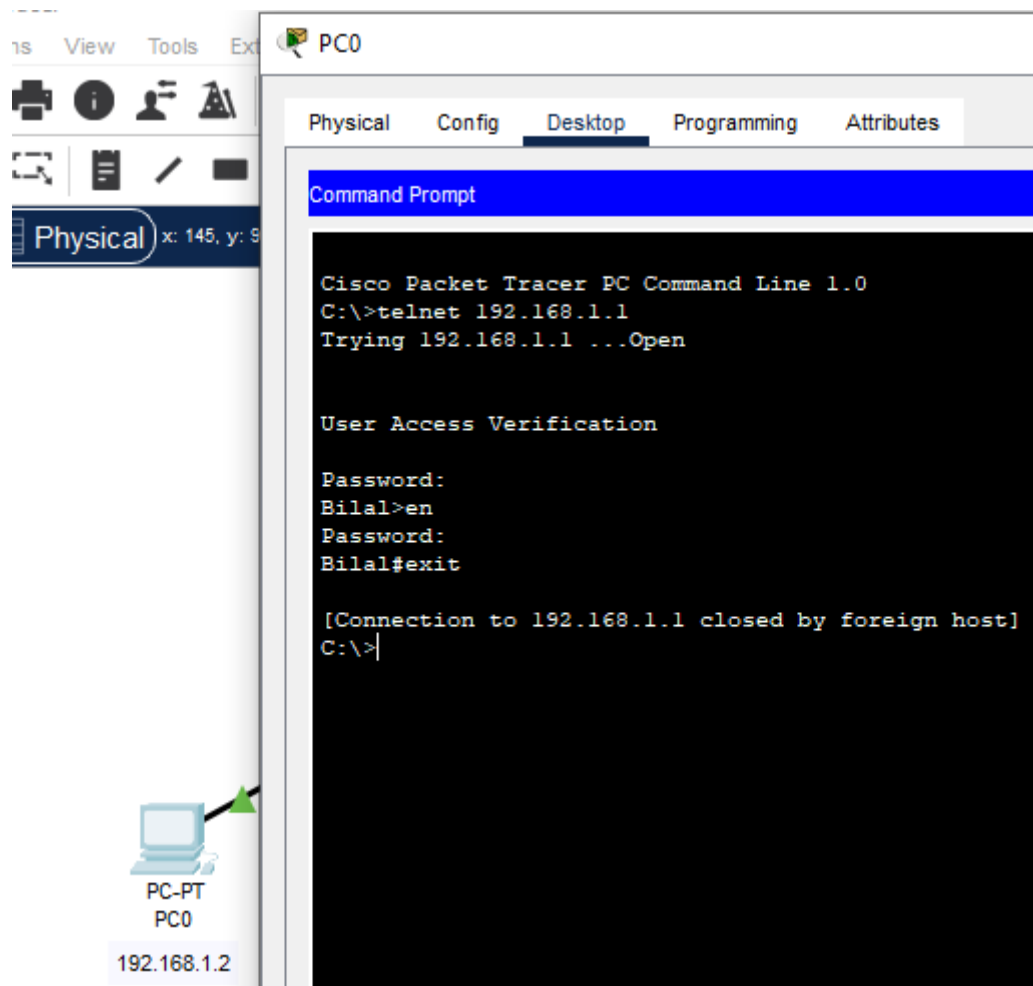
Step 3: Telnet to connected PC (Verify Remote Access) This step verifies that the remote management (Telnet) configured in the previous step is functional from the connected PCs.

1. From **PC0 Command Prompt**, attempt to Telnet to the switch's management IP address:

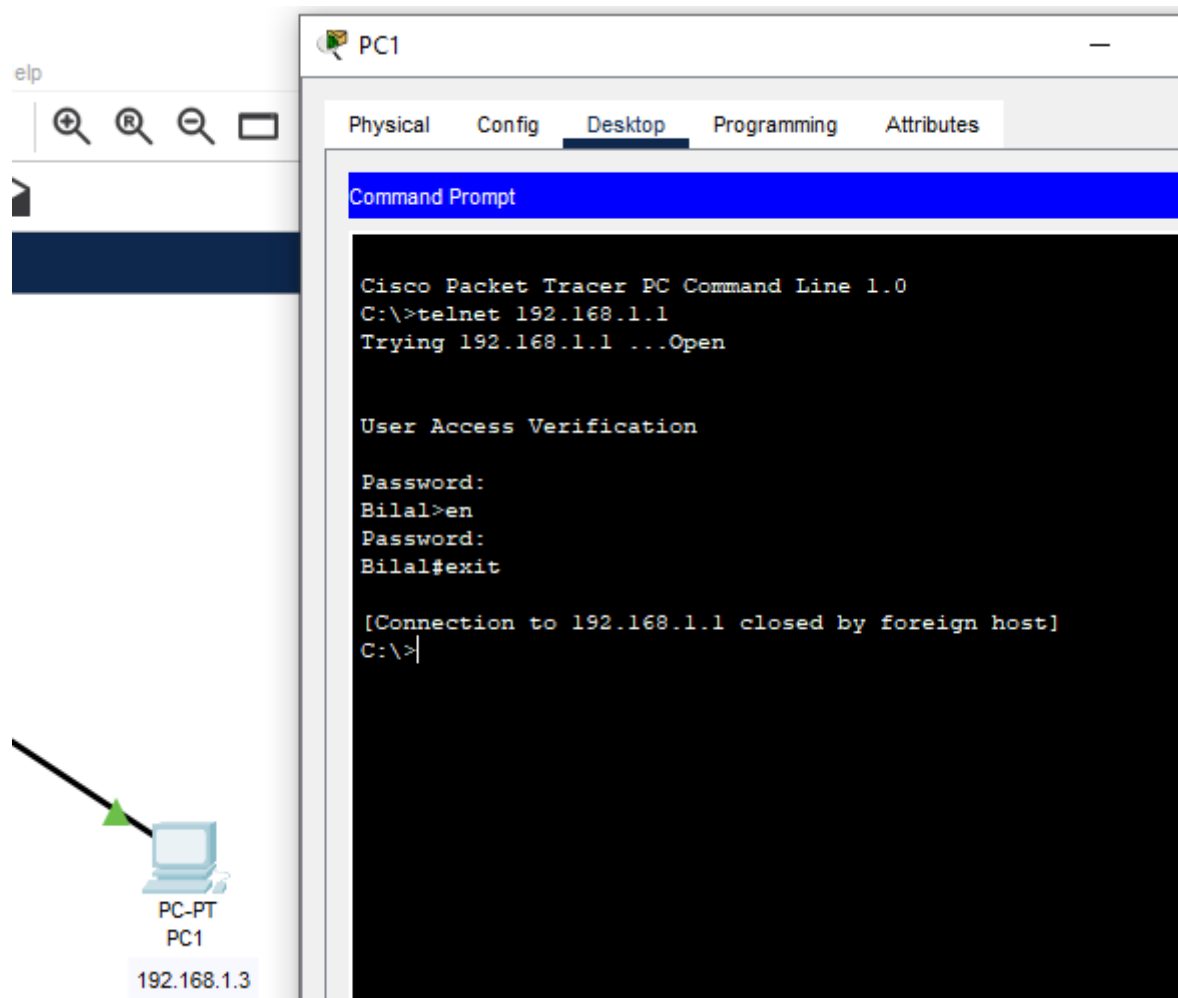
Code snippet

```
C:\>telnet 192.168.1.1
```

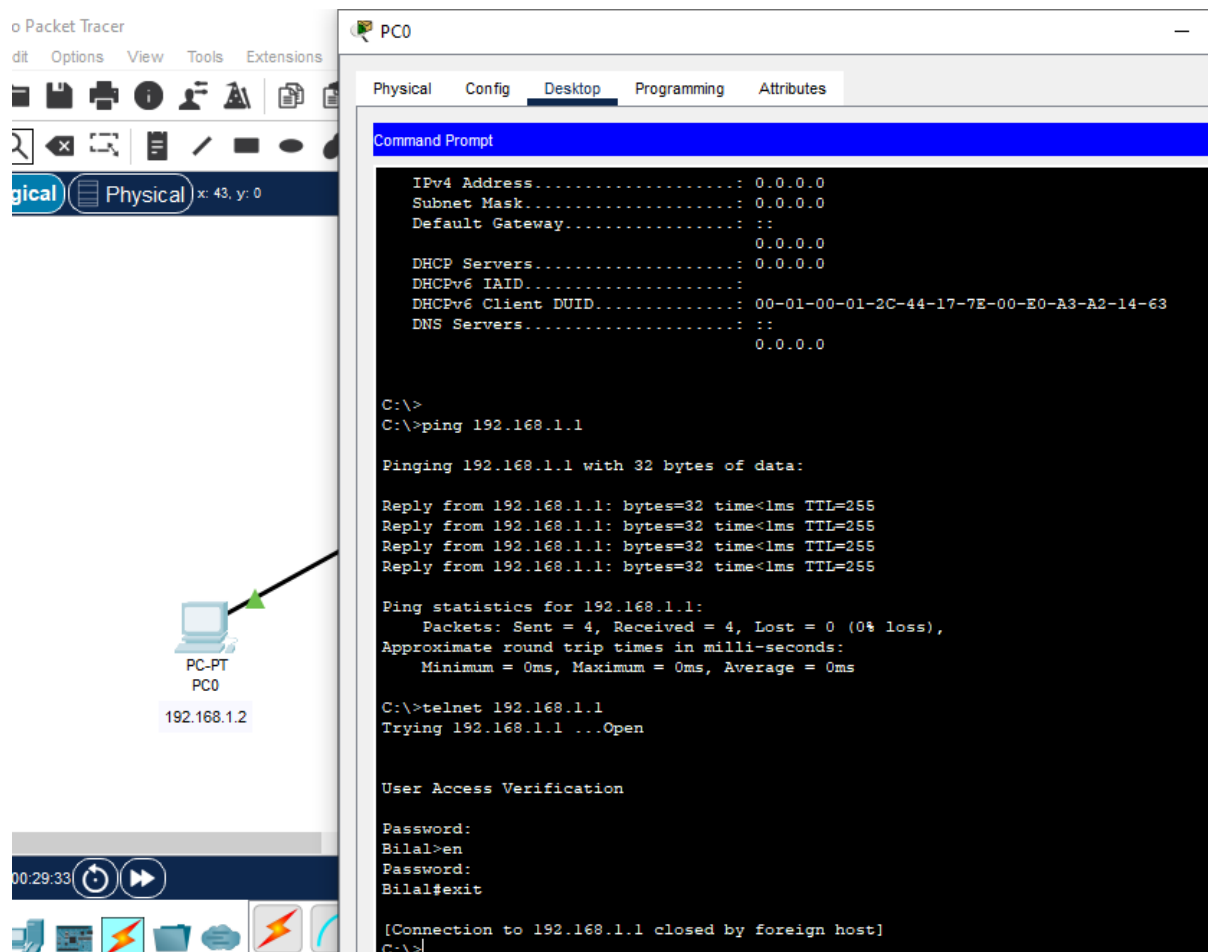
2. You will be prompted for passwords. Enter them in the following order:
 - First, the VTY password (BilalDeveloper).
 - Then, if you type enable after logging in, you'll be prompted for the enable secret (BilalCode).
3. Type exit to close the Telnet session.
4. Repeat the Telnet attempt from PC1 to verify connectivity from both PCs.



[Insert Image: lab_05(2).PNG here] This screenshot from PC0's Command Prompt demonstrates a successful Telnet connection to the switch at 192.168.1.1. It shows the "User Access Verification" prompt, successful password entry, and the switch's prompt, indicating a successful remote login. The session is then exited.



[Insert Image: lab_05(3).PNG here] This screenshot from PC1's Command Prompt similarly demonstrates a successful Telnet connection to the switch at 192.168.1.1, confirming remote access from PC1 as well. This indicates that the VLAN1 interface is active and accessible from both connected devices.



[Insert Image: lab_05(6_complete)_fa0_1.PNG here] This combined screenshot from PC0's Command Prompt shows a successful ping to the switch's IP address (192.168.1.1) demonstrating basic network connectivity, followed by a successful telnet session, further verifying remote access capabilities after configuring VTY lines.

Part B: Port Security Configuration and Observation

Step 4: Apply Port Security on FastEthernet0/1 (for PC0) Port security limits the number of MAC addresses that can be learned on a switch port, providing a crucial layer of security.

1. Access the **Switch CLI** and enter global configuration mode.
2. Navigate to interface FastEthernet0/1 (where PC0 is connected):

Code snippet

```
Bilal(config)#interface FastEthernet0/1
```

3. Set the port mode to access: This specifies that the port is intended for end-user devices and not for trunking between switches.

Code snippet

Bilal(config-if)#switchport mode access

4. **Apply port security:** Enable port security on the interface. This is the fundamental command to activate the feature on a port.

Code snippet

Bilal(config-if)#switchport port-security

5. Set the maximum allowed MAC addresses on this port to 1: This ensures only one device (with its MAC address) can be authorized to connect to this port at any given time.

Code snippet

Bilal(config-if)#switchport port-security maximum 1

6. **Bind connected PC with MAC address (sticky):** Configure the port to learn the connected PC's MAC address dynamically and make it sticky (persist across reboots). This means the first MAC address seen on the port will become the "secure" MAC address.

Code snippet

Bilal(config-if)#switchport port-security mac-address sticky

7. Set the violation mode to shutdown: This specifies that if an unauthorized MAC address is detected on the port, the port will be immediately disabled (err-disabled state) and an SNMP trap will be sent.

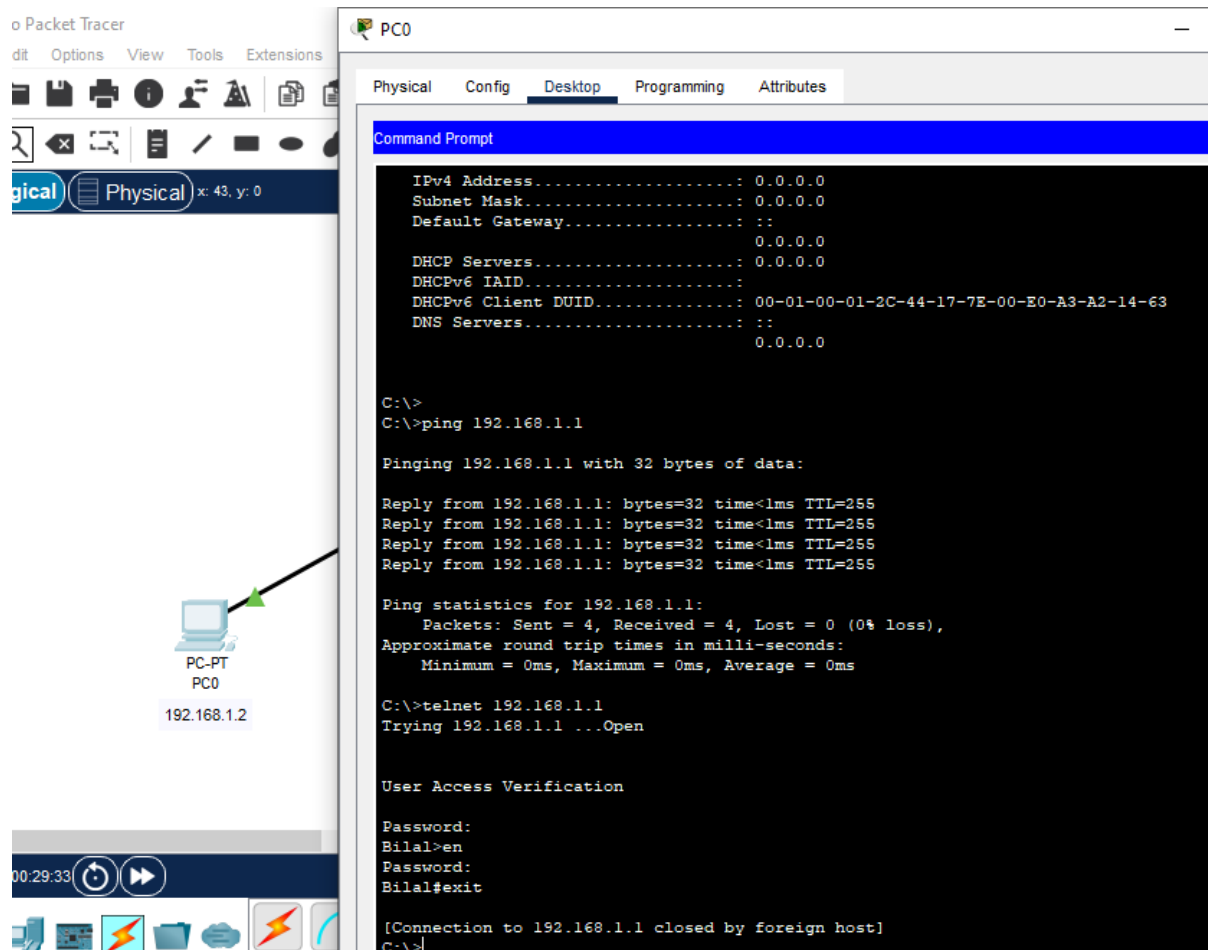
Code snippet

Bilal(config-if)#switchport port-security violation shutdown

8. Exit interface configuration mode:

Code snippet

Bilal(config-if)#exit



[Insert Image: lab_05(6)_fa0_1.PNG here] This CLI screenshot shows the commands executed to configure port security on interface FastEthernet0/1. It illustrates setting the port to access mode, enabling port security, limiting to 1 MAC address, using the sticky option to learn the MAC address, and setting the violation mode to shutdown.

Step 5: Apply Port Security on FastEthernet0/2 (for PC1) Repeat the port security configuration for the second connected PC.

1. Access the **Switch CLI** and enter global configuration mode.
2. Navigate to interface FastEthernet0/2 (where PC1 is connected):

Code snippet

```
Bilal(config)#interface FastEthernet0/2
```

3. Set the port mode to access:

Code snippet

```
Bilal(config-if)#switchport mode access
```

4. Enable port security on the interface:

Code snippet

Bilal(config-if)#switchport port-security

5. Set the maximum allowed MAC addresses on this port to 1:

Code snippet

Bilal(config-if)#switchport port-security maximum 1

6. Configure the port to learn the connected PC's MAC address dynamically and make it sticky:

Code snippet

Bilal(config-if)#switchport port-security mac-address sticky

7. Set the violation mode to shutdown:

Code snippet

Bilal(config-if)#switchport port-security violation shutdown

8. Exit interface configuration mode:

Code snippet

Bilal(config-if)#exit

```

User Access Verification

Password:

Bilal>en
Password:
Bilal#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Bilal(config)#int fa0/2
Bilal(config-if)#switchport mode access
Bilal(config-if)#switchport port-security
Bilal(config-if)#switchport port-security mac-address 0002.17AB.7138
Bilal(config-if)#switchport port-security sticky
^
% Invalid input detected at '^' marker.

Bilal(config-if)#switchport port-security mac-address ?
  H.H.H  48 bit mac address
  sticky  Configure dynamic secure addresses as sticky
Bilal(config-if)#switchport port-security mac-address sticky
Bilal(config-if)#switchport port-security violation ?
  protect  Security violation protect mode
  restrict Security violation restrict mode
  shutdown Security violation shutdown mode
Bilal(config-if)#switchport port-security violation shutdown
Bilal(config-if)#exit
Bilal(config)#show port-security
^
% Invalid input detected at '^' marker.

Bilal(config)#exit
Bilal#
%SYS-5-CONFIG_I: Configured from console by console

Bilal#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

```

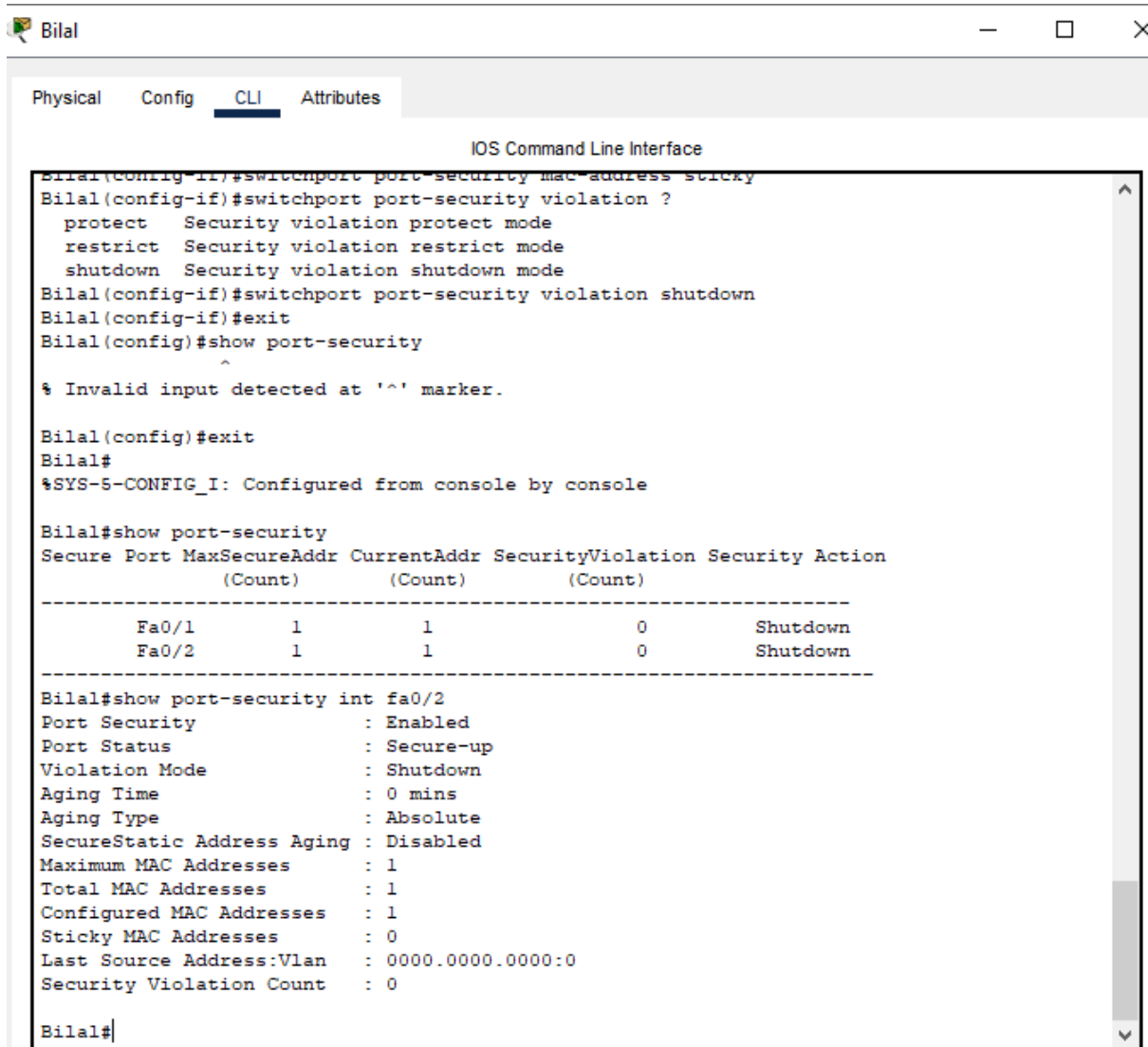
[Insert Image: lab_05(1)_fa0_2.PNG here] This CLI screenshot shows the commands used to configure port security on interface FastEthernet0/2. It demonstrates setting the port to access mode, enabling port security, specifying the maximum MAC address as 1, and using the sticky option for securing the port. The output of show port-security interface fa0/2 is also included, confirming its status.

Step 6: Verify Port Security Configuration After configuring port security, it's essential to verify that the settings have been applied correctly and that the authorized MAC addresses have been learned.

1. From privileged EXEC mode, display a summary of port security settings for all interfaces:

Code snippet

Bilal#show port-security



The screenshot shows a network device CLI window titled "Bilal" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the "IOS Command Line Interface". The user has entered the following commands:

```
Bilal(config-if)#switchport port-security mac-address sticky
Bilal(config-if)#switchport port-security violation ?
  protect    Security violation protect mode
  restrict   Security violation restrict mode
  shutdown   Security violation shutdown mode
Bilal(config-if)#switchport port-security violation shutdown
Bilal(config-if)#exit
Bilal(config)#show port-security
^
% Invalid input detected at '^' marker.

Bilal(config)#exit
Bilal#
%SYS-5-CONFIG_I: Configured from console by console

Bilal#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	1	1	0	Shutdown
Fa0/2	1	1	0	Shutdown

```
Bilal#show port-security int fa0/2
Port Security           : Enabled
Port Status              : Secure-up
Violation Mode           : Shutdown
Aging Time               : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses    : 1
Total MAC Addresses      : 1
Configured MAC Addresses : 1
Sticky MAC Addresses     : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

Bilal#
```

[Insert Image: lab_05(7b)_fa0_2.PNG here] This screenshot shows the output of `show port-security`, providing a summary of port security settings for Fa0/1 and Fa0/2. It confirms that both ports have a MaxSecureAddr and CurrentAddr of 1, with a Security Action of Shutdown, indicating active port security.

2. Display detailed port security information for interface FastEthernet0/1:

Code snippet

```
Bilal#show port-security interface FastEthernet0/1
```



```

Bilal#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----
          Fa0/1             1             1             0          Shutdown
-----

Bilal#show port-security int fa0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

Bilal#show port-security int fa0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 00E0.A3A2.1463:1
Security Violation Count : 0

Bilal#

```

[Insert Image: lab_05_fa0_1_com.PNG here] This screenshot displays the detailed port security status for interface Fa0/1. It confirms that Port Security is Enabled, Port Status is Secure-up (meaning an authorized device is connected), Violation Mode is Shutdown, Maximum MAC Addresses is 1, and the Configured MAC Addresses is 1. Crucially, the Last Source Address:Vlan shows the MAC address of PC0 (00E0.A3A2.1463), confirming it was learned and secured.

```

Bilal(config)#exit
Bilal#
%SYS-5-CONFIG_I: Configured from console by console

Bilal#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
          Fa0/1            1            1            0          Shutdown
-----

Bilal#show port-security int fa0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

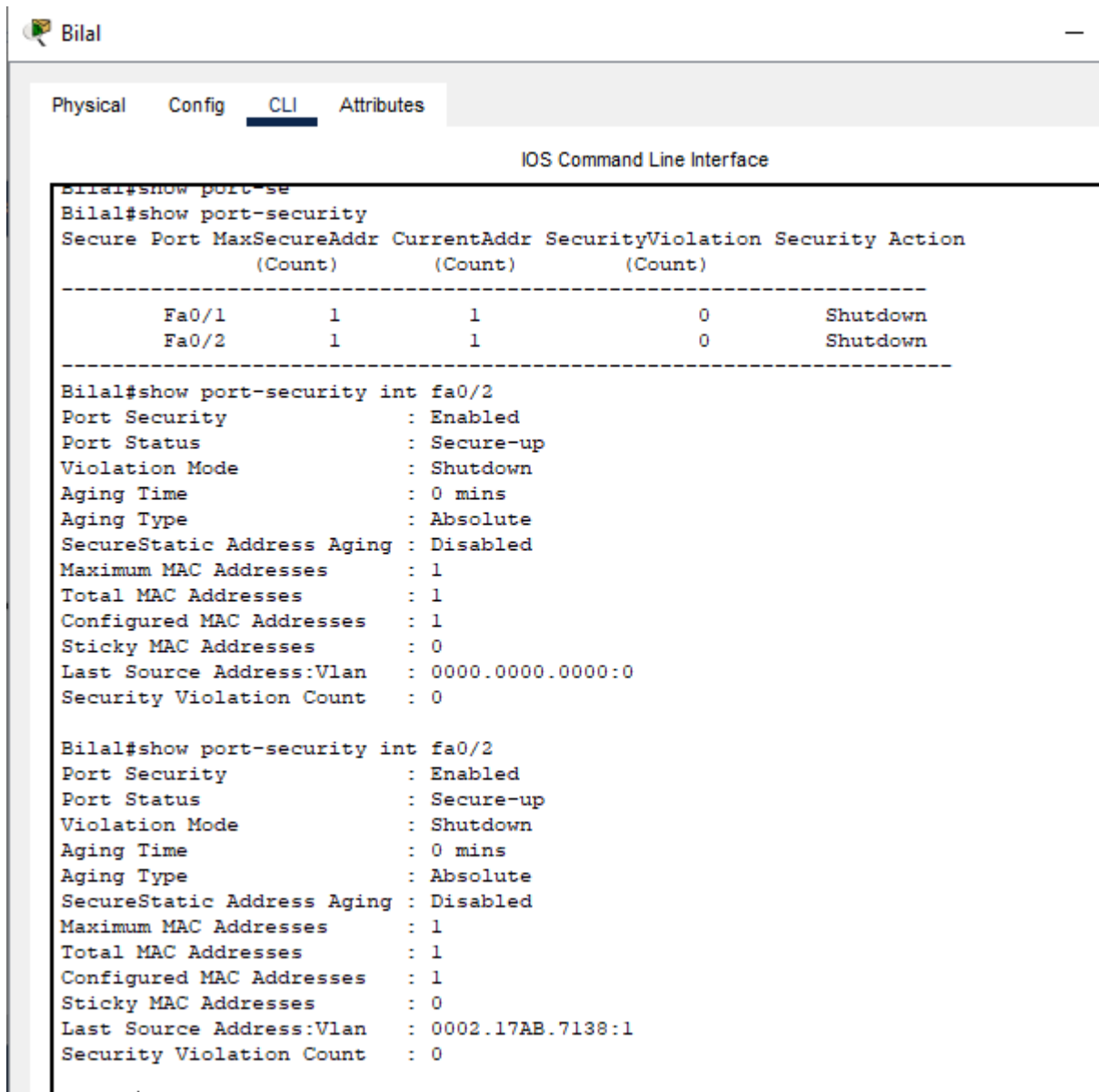
```

[Insert Image: lab_05(6a)_fa0_1.PNG here] This screenshot displays the show port-security summary and then the detailed output for Fa0/1, confirming the same settings as above. It explicitly shows the Security MAC Address of PC0 (00E0.A3A2.1463) learned as a sticky address.

3. Display detailed port security information for interface FastEthernet0/2:

Code snippet

```
Bilal#show port-security interface FastEthernet0/2
```



[Insert Image: lab_05(7)_fa0_2_complete.PNG here] This screenshot displays the detailed port security status for interface Fa0/2. It confirms Enabled Port Security, Secure-up status, Shutdown violation mode, Maximum MAC Addresses as 1, and Configured MAC Addresses as 1. The Last Source Address:Vlan shows the MAC address of PC1 (0002.17AB.7138), verifying it was learned and secured.

Step 7: Replace it with another PC and observe port security behaviour This crucial step demonstrates the effectiveness of port security by attempting to connect an unauthorized device.

1. Ensure PC0 is connected to Fa0/1 and PC1 is connected to Fa0/2, and both are communicating correctly.
2. **Disconnect PC0 from FastEthernet0/1.**

3. **Connect a new PC (or simply disconnect PC1 from Fa0/2 and connect it to Fa0/1)** to FastEthernet0/1. This new PC will have a different MAC address than PC0, triggering a security violation.
4. Observe the port status in Packet Tracer: The link light for Fa0/1 should quickly turn red/orange, indicating that the port has entered an error-disabled (err-disabled) state due to a security violation. This is the shutdown action in effect.
5. Attempt to ping from the newly connected (unauthorized) PC to PC1 – it should fail, as the port is shut down.
6. From the switch CLI, verify the security violation count and port status:

Code snippet

Bilal#show port-security interface FastEthernet0/1

Expected Output: The Security Violation Count should show 1 (or more, if multiple attempts were made), and the Port Status will likely show secure-shutdown or err-disabled, confirming the security breach and the port's response.

Conclusion:

This laboratory exercise successfully fulfilled all requirements of the LAB TASK. Basic switch security features were implemented, including a personalized hostname, console password, a secure enable secret, and VTY passwords for remote Telnet access, which was verified from the connected PCs. Crucially, port security was configured on FastEthernet0/1 and FastEthernet0/2, binding them to the MAC addresses of the authorized PCs (PC0 and PC1) using the sticky method. When an unauthorized device was subsequently connected to a secured port, the switch correctly identified the security violation and shut down the port, demonstrating the robust protection offered by port security against unauthorized network access.

Okay, I will provide the concise Lab Manual in English, including the instructions on where to add the corresponding images.

Lab Manual: Router Basic Configuration & Connectivity

Computer Science Department Lab Exercise No: 6 & 7 (Combined - Concise Version)

1. Objective:

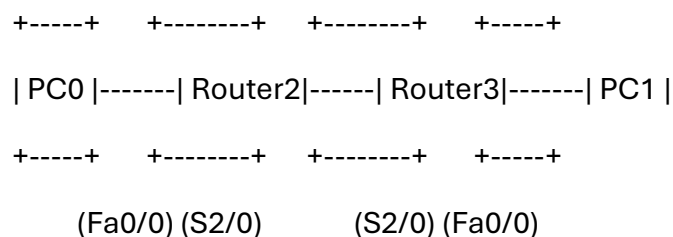
The objective of this lab is to complete the following tasks in Cisco Packet Tracer:

- Design and implement a basic network topology.
 - Assign IP addresses to PCs and Routers.
 - Configure Router Hostnames and set various security passwords (Console, VTY/Telnet, Enable).
 - Establish a serial link between two routers.
 - Configure static default routes to enable connectivity between different networks.
 - Permanently save router configurations.
 - Test end-to-end connectivity using Ping and remote access using Telnet.
-

2. Required Tools / Equipment:

- Cisco Packet Tracer Software installed.
 - 2x Routers (Cisco 2620XM model recommended).
 - 2x End Devices (PCs).
 - **Cables:**
 - Copper Straight-Through Cables (for PC-to-Router connections).
 - Serial DTE/DCE Cable (for Router-to-Router connection).
-

3. Network Topology & IP Addressing Scheme:



IP Address Details:

- **PC0 Network:**
 - PC0 IP: 192.168.1.10
 - Router2 Fa0/0 IP: 192.168.1.1
 - Default Gateway: 192.168.1.1

- Subnet Mask: 255.255.255.0
- **PC1 Network:**
 - PC1 IP: 192.168.2.10
 - Router3 Fa0/0 IP: 192.168.2.1
 - Default Gateway: 192.168.2.1
 - Subnet Mask: 255.255.255.0
- **Router-to-Router Link:**
 - Router2 S2/0 IP: 10.10.10.1
 - Router3 S2/0 IP: 10.10.10.2
 - Subnet Mask: 255.255.255.0

<-- Insert lab_06_compltet.PNG (Overall Topology Image) here --> (This image should show the complete network setup including Router2, Router3, PC0, PC1, and their connections.)

4. Procedure: Step-by-Step Configuration

4.1. Build Topology & Connect Devices:

1. Open **Cisco Packet Tracer**.
2. Drag and drop **2x 2620XM Routers** (name them Router2, Router3) and **2x PCs** (name them PC0, PC1) onto the workspace.
3. Add a **WIC-2T serial module** to each router (remember to power off/on the router).
4. Connect devices with **Cables**:
 - PC0 (FastEthernet0) to Router2 (FastEthernet0/0) using a **Copper Straight-Through** cable.
 - PC1 (FastEthernet0) to Router3 (FastEthernet0/0) using a **Copper Straight-Through** cable.
 - Router2 (Serial2/0) to Router3 (Serial2/0) using a **Serial DTE/DCE** cable (set Router2 as the DCE/clock side).

4.2. Configure IP Addresses on PCs:

1. **Configure PC0:** Click PC0 > Desktop tab > IP Configuration. Set IP: 192.168.1.10, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1.
2. **Configure PC1:** Click PC1 > Desktop tab > IP Configuration. Set IP: 192.168.2.10, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.2.1.

4.3. Configure Router2 (CLI):

1. Click Router2 > CLI tab. Press Enter a few times to get to the Router> prompt.
2. Enter the following commands:

Cisco CLI

Router>enable

Router#configure terminal

Router(config)#hostname Bilal

Bilal(config)#interface fastEthernet 0/0

Bilal(config-if)#ip address 192.168.1.1 255.255.255.0

Bilal(config-if)#no shutdown

Bilal(config-if)#exit

Bilal(config)#line console 0

Bilal(config-line)#password Bilal

Bilal(config-line)#login

Bilal(config-line)#exit

Bilal(config)#line vty 0 2

Bilal(config-line)#password Bilal123

Bilal(config-line)#login

Bilal(config-line)#exit

Bilal(config)#enable password Bilal123

Bilal(config)#enable secret Bilal123

Bilal(config)#interface serial 2/0

Bilal(config-if)#ip address 10.10.10.1 255.255.255.0

Bilal(config-if)#clock rate 2000000

Bilal(config-if)#no shutdown

```
Bilal(config-if)#exit
```

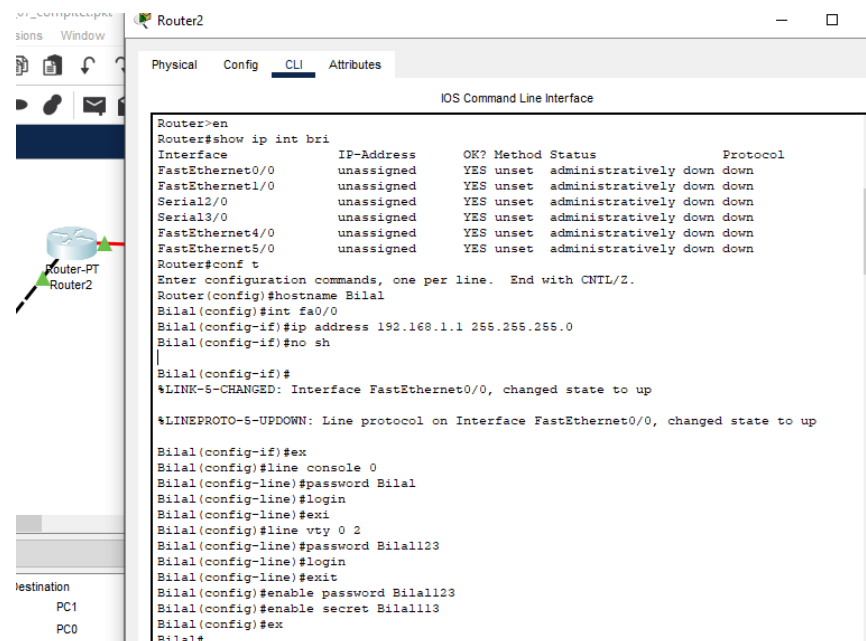
```
Bilal(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

```
Bilal(config)#exit
```

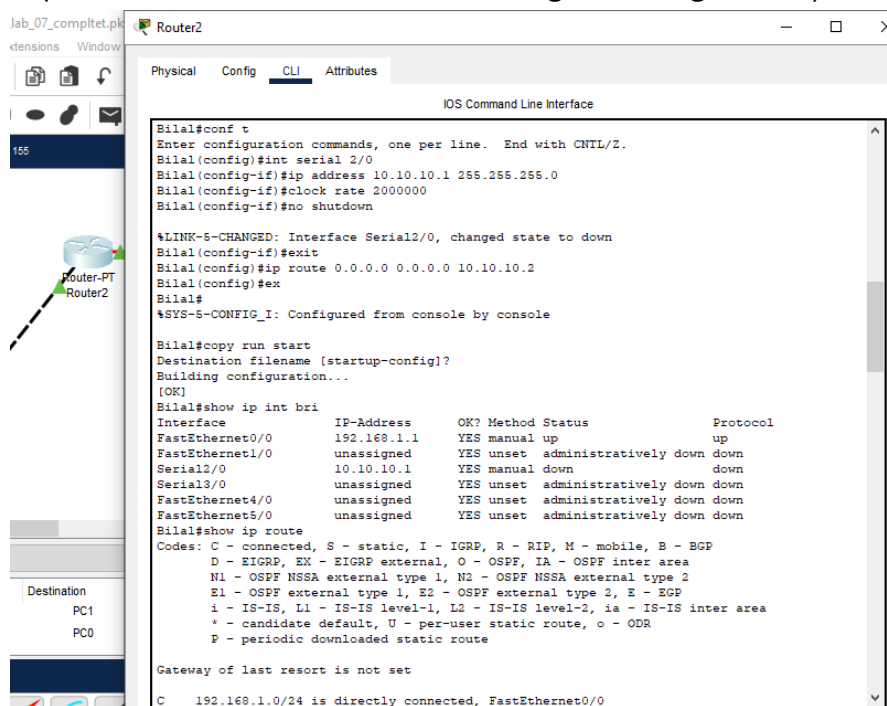
```
Bilal#copy running-config startup-config
```

3. **Verify Configuration:** After running commands, use Bilal#show ip interface brief and Bilal#show ip route to confirm settings.

(This image shows the start of Router2's configuration, including hostname, FastEthernet interface setup, console password, VTY password, and enable passwords.)



(This image shows the continuation of Router2's configuration, including Serial interface setup, clock rate, default route, and saving the configuration.)



4.4. Configure Router3 (CLI):

1. Click Router3 > CLI tab. Press Enter a few times to get to the Router> prompt.
2. Enter the following commands:

Cisco CLI

Router>enable

Router#configure terminal

Router(config)#hostname Bilal

Bilal(config)#interface fastEthernet 0/0

Bilal(config-if)#ip address 192.168.2.1 255.255.255.0

Bilal(config-if)#no shutdown

Bilal(config-if)#exit

Bilal(config)#line console 0

Bilal(config-line)#password Bilal

Bilal(config-line)#login

Bilal(config-line)#exit

Bilal(config)#line vty 0 2

Bilal(config-line)#password Bilal123

Bilal(config-line)#login

Bilal(config-line)#exit

Bilal(config)#enable password Bilal123

Bilal(config)#enable secret Bilal123

Bilal(config)#interface serial 2/0

Bilal(config-if)#ip address 10.10.10.2 255.255.255.0

Bilal(config-if)#no shutdown

Bilal(config-if)#exit

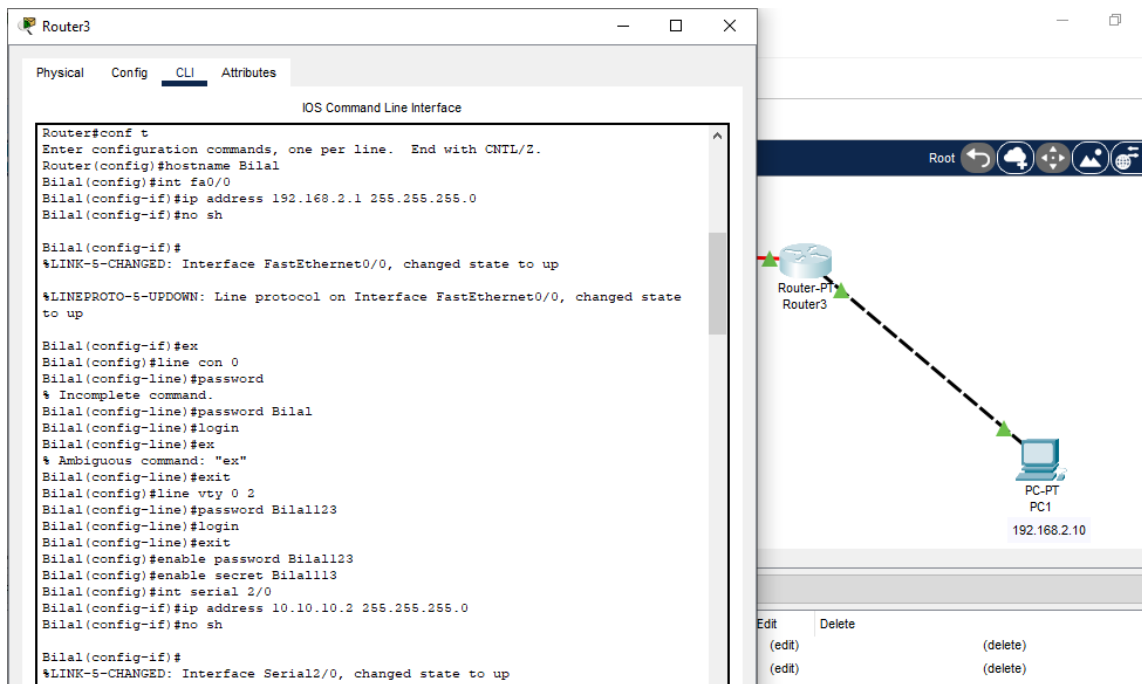
Bilal(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1

Bilal(config)#exit

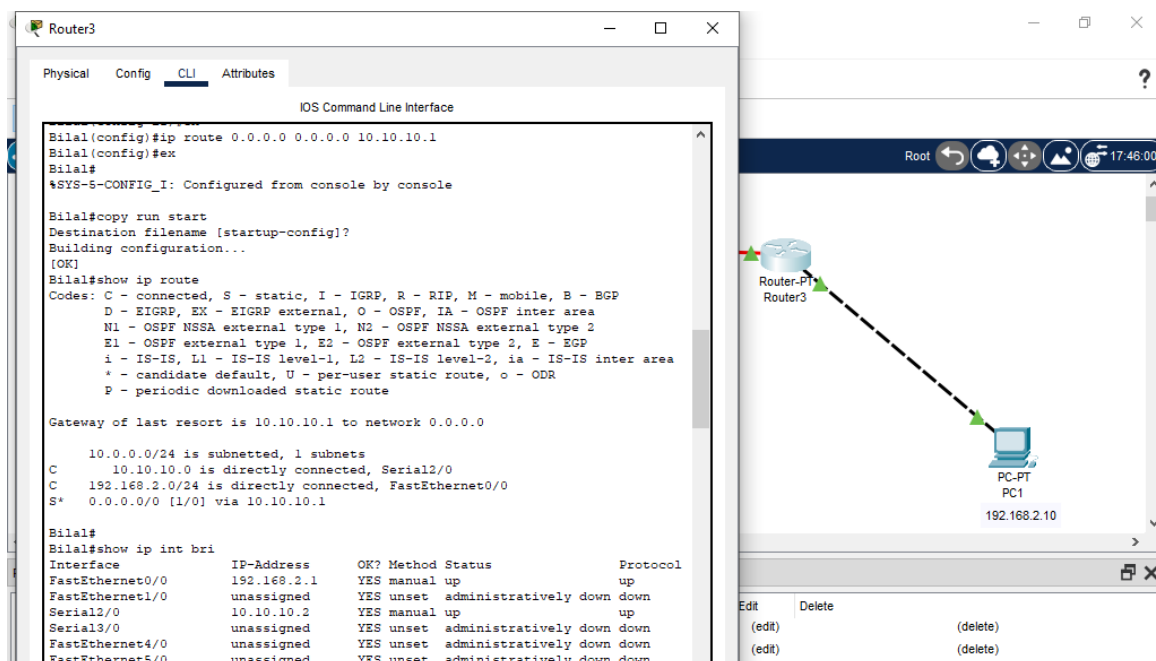
Bilal#copy running-config startup-config

3. **Verify Configuration:** After running commands, use Bilal#show ip interface brief and Bilal#show ip route to confirm settings.

<-- Insert lab_06(3).PNG here --> (This image shows the start of Router3's configuration, including hostname, FastEthernet interface setup, console password, VTY password, and enable passwords.)



<-- Insert lab_06(4).PNG here --> (This image shows the continuation of Router3's configuration, including Serial interface setup, default route, and saving the configuration.)



4.5. Test Connectivity (Ping & Telnet):

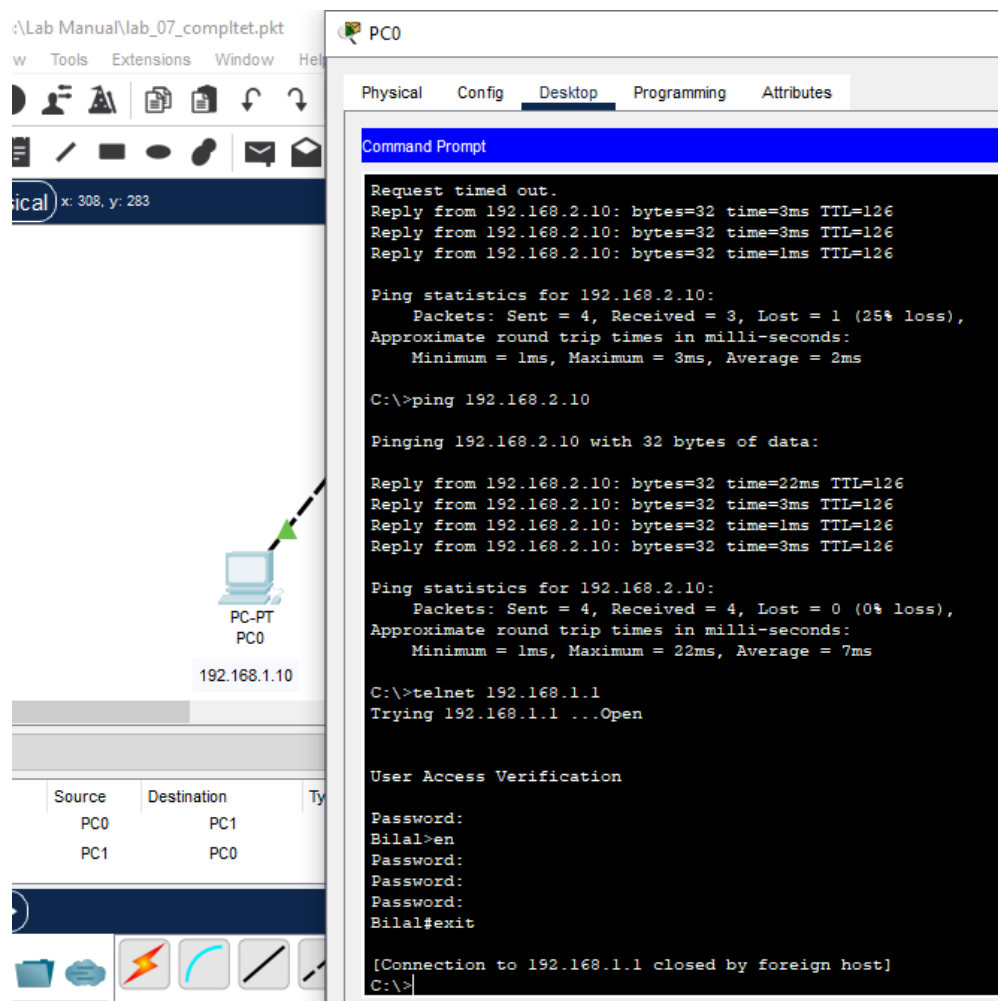
1. Ping from PC0 to PC1:

- From PC0 > Command Prompt.
- Type: ping 192.168.2.10 (You should see successful replies).

2. Telnet from PC0 to Router2:

- From PC0 > Command Prompt.
- Type: telnet 192.168.1.1 (Enter VTY password Bilal123, then enable and enter enable secret password Bilal123 to log in).

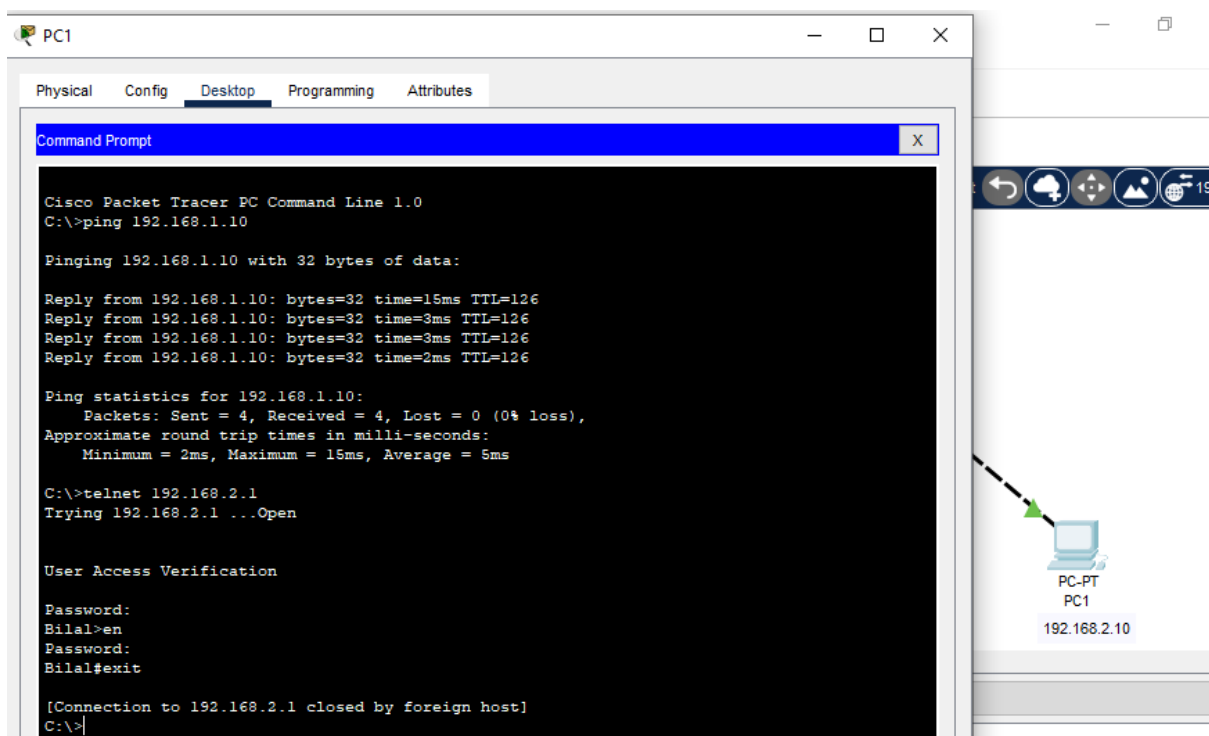
<-- Insert lab_06(5).PNG here --> (This image shows PC0's command prompt with ping 192.168.2.10 output and the telnet 192.168.1.1 command.)



3. Telnet from PC1 to Router3:

- From PC1 > Command Prompt.
- Type: telnet 192.168.2.1 (Enter VTY password Bilal123, then enable and enter enable secret password Bilal123 to log in).

<-- Insert lab_06(6).PNG here --> (This image shows PC1's command prompt with ping 192.168.1.10 output and the telnet 192.168.2.1 command.)



5. Conclusion:

In this lab, you successfully configured a basic two-router network in Packet Tracer, assigned IP addresses, secured routers with passwords, set up static routing, and verified connectivity using ping and Telnet.