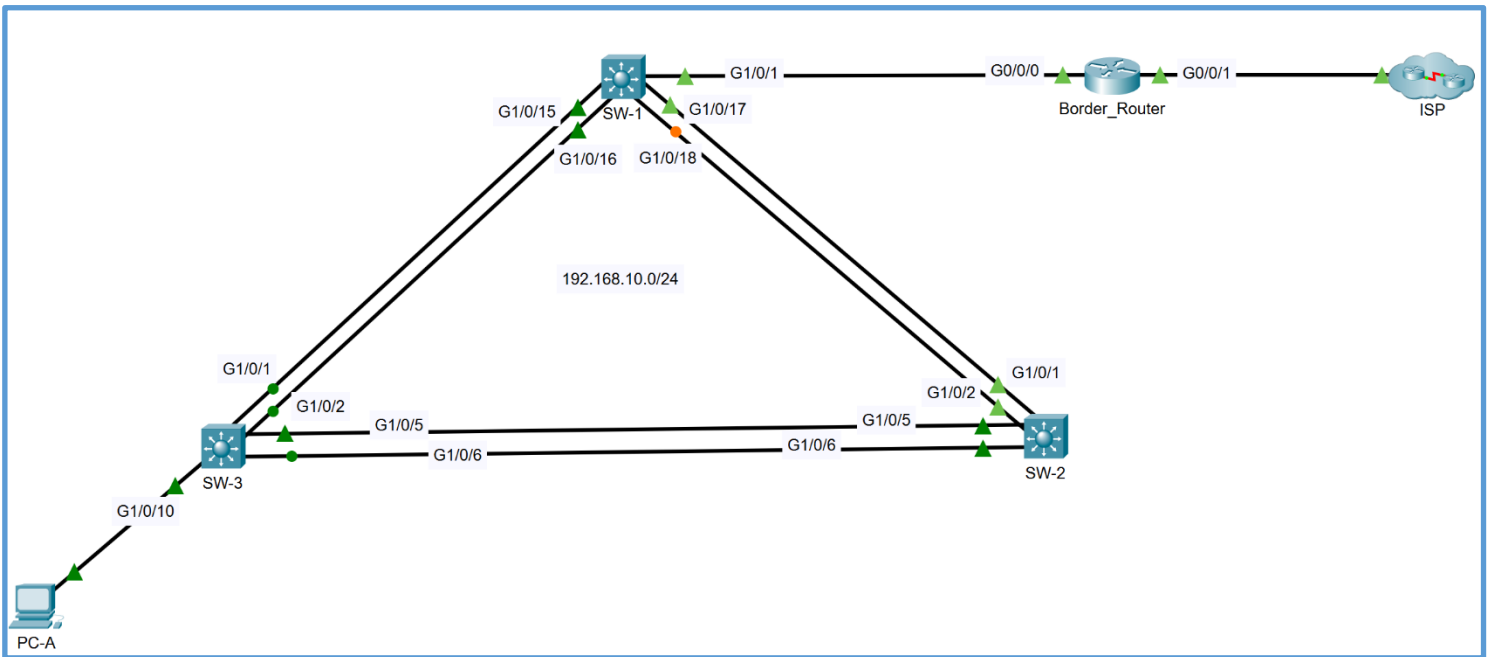


## PART – 1

### Lab Activity – IP Services:

- There is only one LAN in the topology below. Please develop the following topology on the physical pod/rack in the lab room.



### Required Resources:

- Three Layer-3/Multilayer Switches (Cisco Catalyst 1000 Series with Cisco IOS Release 15.1+ image)
- One router (Cisco 4221 with Cisco IOS Release 17.6+ image)
- One PC (Windows with Terminal Emulation Program)
- Cables:
  - Console cables to configure the Cisco IOS devices through the console port.
  - Ethernet and serial cables as shown in the topology.

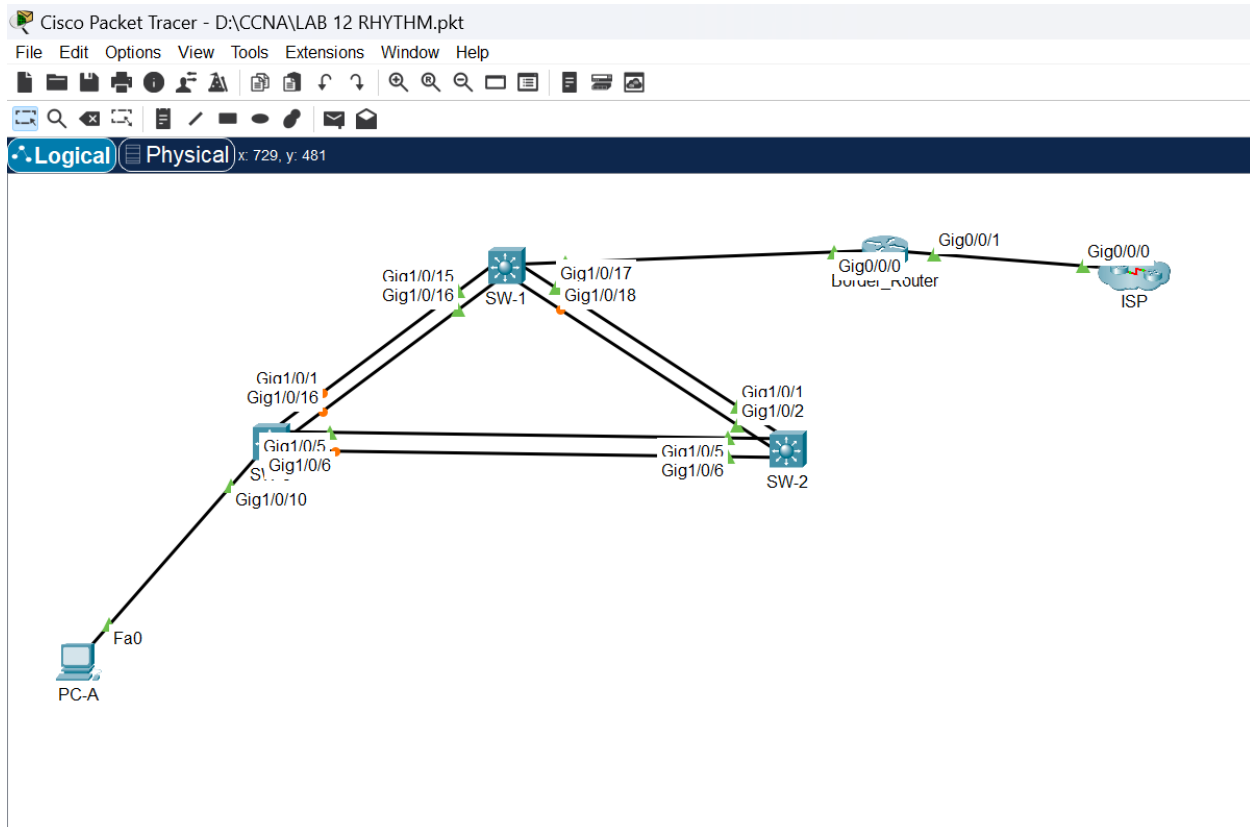
### Lab Description:

- In this lab, please build one LAN based simple network.
  - LAN with three switches, one router, and one host.

### Instructions:

Step 1: Set up the network topology.

- Develop the topology by using all the devices mentioned above and then cable them all together:
  - Turn on the devices.
  - Connect the switch with the default gateway.
  - Connect the PCs and server with their respective switch.
  - Make sure all the lights between switches, PC, and border\_router are green/active.



Step 2: For this lab consideration, copy the following instructions (without bullet points) into each switch and then the router:

**Note:** Prior to copying the below instructions, check the configuration for any obvious errors/typos.

SW-1	SW-2	SW-3
------	------	------

<ul style="list-style-type: none"> <li>• enable</li> <li>• config terminal</li> <li>• no ip domain-lookup</li> <li>• hostname SW-1</li> <li>• enable secret trios</li> <li>• int vlan 1</li> <li>• ip address 192.168.10.1 255.255.255.0</li> <li>• no shutdown</li> <li>• exit</li> <li>• ip default-gateway 192.168.10.10</li> <li>• username admin password cisco123</li> <li>• ip domain-name trios.com</li> <li>• line console 0</li> <li>• password cisco</li> <li>• login local</li> <li>• exit</li> <li>• line vty 0 15</li> <li>• password cisco</li> <li>• transport input ssh</li> <li>• login local</li> <li>• exit</li> <li>• crypto key generate rsa 1024</li> <li>• exit</li> <li>• copy running startup</li> </ul>	<ul style="list-style-type: none"> <li>• enable</li> <li>• config terminal</li> <li>• no ip domain-lookup</li> <li>• hostname SW-2</li> <li>• enable secret trios</li> <li>• int vlan 1</li> <li>• ip address 192.168.10.2 255.255.255.0</li> <li>• no shutdown</li> <li>• exit</li> <li>• ip default-gateway 192.168.10.10</li> <li>• username admin password cisco123</li> <li>• ip domain-name trios.com</li> <li>• line console 0</li> <li>• password cisco</li> <li>• login local</li> <li>• exit</li> <li>• line vty 0 15</li> <li>• password cisco</li> <li>• transport input ssh</li> <li>• login local</li> <li>• exit</li> <li>• crypto key generate rsa 1024</li> <li>• exit</li> <li>• copy running startup</li> </ul>	<ul style="list-style-type: none"> <li>• enable</li> <li>• config terminal</li> <li>• no ip domain-lookup</li> <li>• hostname SW-3</li> <li>• enable secret trios</li> <li>• int vlan 1</li> <li>• ip address 192.168.10.3 255.255.255.0</li> <li>• no shutdown</li> <li>• exit</li> <li>• ip default-gateway 192.168.10.10</li> <li>• username admin password cisco123</li> <li>• ip domain-name trios.com</li> <li>• line console 0</li> <li>• password cisco</li> <li>• login local</li> <li>• exit</li> <li>• line vty 0 15</li> <li>• password cisco</li> <li>• transport input ssh</li> <li>• login local</li> <li>• exit</li> <li>• crypto key generate rsa 1024</li> <li>• exit</li> <li>• copy running startup</li> </ul>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Switches

The image displays the Cisco Packet Tracer interface with three switch configuration windows (SW-1, SW-2, SW-3) and a network diagram. The switches are configured with the following commands:

```

Switch>enable
Switch>config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname SW-1
SW-1(config)#enable secret trios
SW-1(config)#int vlan 1
SW-1(config-if)#ip address 192.168.10.1 255.255.255.0
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#ip default-gateway 192.168.10.10
SW-1(config)#username admin password cisco123
SW-1(config)#ip domain-name trios.com
SW-1(config)#line console 0
SW-1(config-line)#password cisco
SW-1(config-line)#login local
SW-1(config-line)#exit
SW-1(config)#line vty 0 15
SW-1(config-line)#password cisco
SW-1(config-line)#transport input ssh
SW-1(config-line)#login local
SW-1(config-line)#exit
SW-1(config)#crypto key generate rsa
The name for the keys will be: SW-1.trios.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
SW-1(config)#exit
*Mar 1 0:18:5.917: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-1#copy running startup
Destination filename [startup-config]?
Building configuration...
[OK]
SW-1#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
  
```

The network diagram shows three switches (SW-1, SW-2, SW-3) connected in a triangle topology. SW-1 is connected to SW-2 and SW-3. SW-2 is connected to SW-3. A PC is connected to SW-1. The switches are configured with the following commands:

```

Switch>enable
Switch>config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname SW-2
SW-2(config)#enable secret trios
SW-2(config)#int vlan 1
SW-2(config-if)#ip address 192.168.10.2 255.255.255.0
SW-2(config-if)#no shutdown
SW-2(config-if)#exit
SW-2(config)#ip default-gateway 192.168.10.10
SW-2(config)#username admin password cisco123
SW-2(config)#ip domain-name trios.com
SW-2(config)#line console 0
SW-2(config-line)#password cisco
SW-2(config-line)#login local
SW-2(config-line)#exit
SW-2(config)#line vty 0 15
SW-2(config-line)#password cisco
SW-2(config-line)#transport input ssh
SW-2(config-line)#login local
SW-2(config-line)#exit
SW-2(config)#crypto key generate rsa
The name for the keys will be: SW-2.trios.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
SW-2(config)#exit
*Mar 1 0:18:54.767: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-2#copy running startup
Destination filename [startup-config]?
Building configuration...
[OK]
SW-2#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
  
```

```

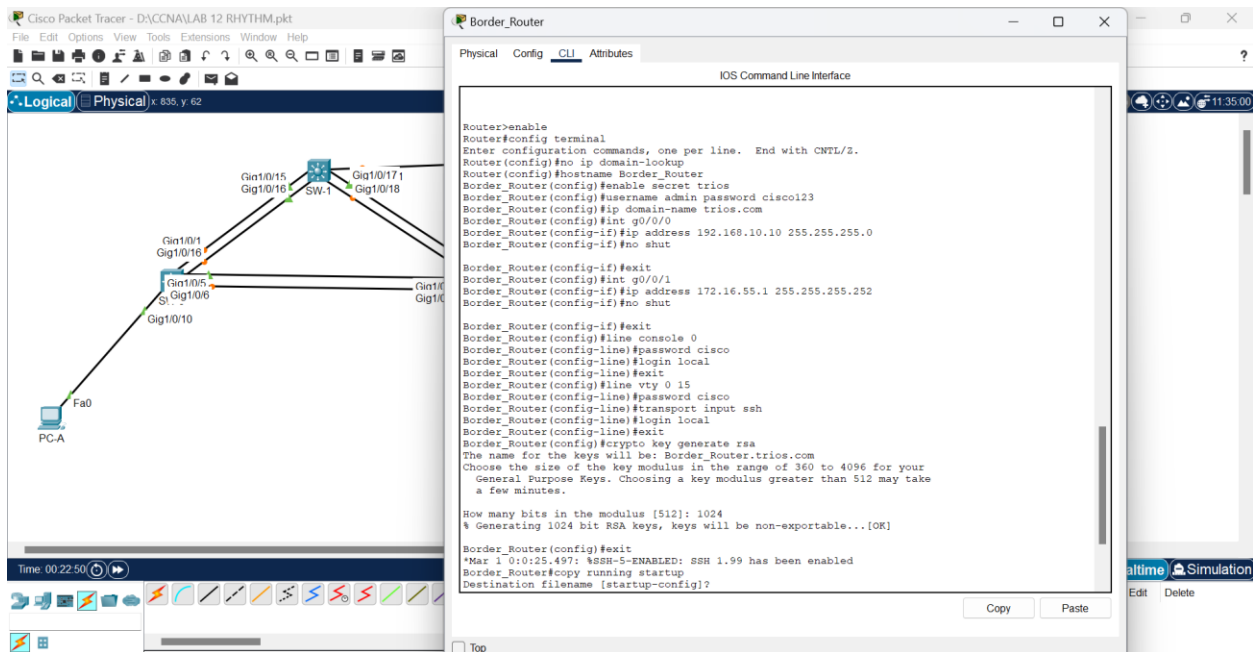
Switch>enable
Switch>config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname SW-3
SW-3(config)#enable secret trios
SW-3(config)#int vlan 1
SW-3(config-if)#ip address 192.168.10.3 255.255.255.0
SW-3(config-if)#no shutdown
SW-3(config-if)#exit
SW-3(config)#ip default-gateway 192.168.10.10
SW-3(config)#username admin password cisco123
SW-3(config)#ip domain-name trios.com
SW-3(config)#line console 0
SW-3(config-line)#password cisco
SW-3(config-line)#login local
SW-3(config-line)#exit
SW-3(config)#line vty 0 15
SW-3(config-line)#password cisco
SW-3(config-line)#transport input ssh
SW-3(config-line)#login local
SW-3(config-line)#exit
SW-3(config)#crypto key generate rsa
The name for the keys will be: SW-3.trios.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
SW-3(config)#exit
*Mar 1 0:19:40.770: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-3#copy running startup
Destination filename [startup-config]?
Building configuration...
[OK]
SW-3#
SW-3#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
  
```

## Border\_Router

- enable
- config terminal
- no ip domain-lookup
- hostname Border\_Router
- enable secret trios
- username admin password cisco123
- ip domain-name trios.com
- int g0/0/0

```
ip address 192.168.10.10 255.255.255.0
no shut
exit
• int g0/0/1
  ip address 172.16.55.1 255.255.255.252
  no shut
  exit
• line console 0
  password cisco
  login local
  exit
• line vty 0 15
  password cisco
  transport input ssh
  login local
  exit
• crypto key generate rsa
  1024
• exit
• copy running startup
```

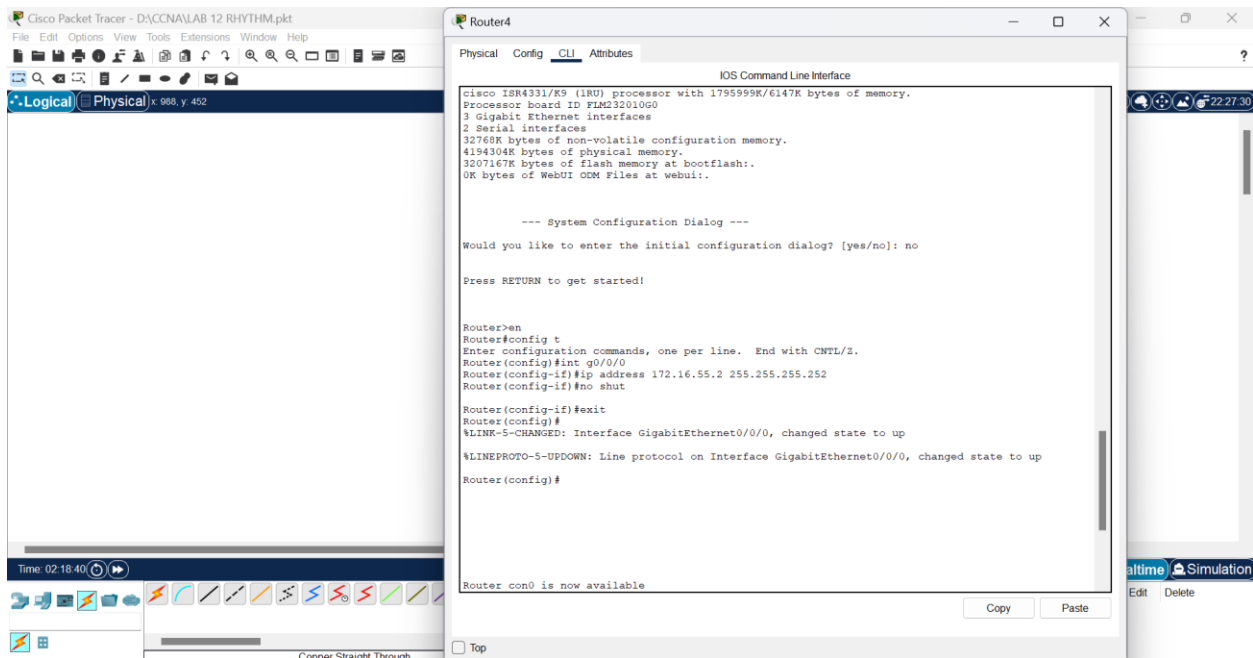
## Border Router



The image shows a Cisco Packet Tracer network diagram and the configuration window for a Border Router. The network diagram on the left shows a PC-A connected to a switch (SW-1) via a Fa0 interface. The switch is connected to a Border Router via GigabitEthernet0/0/15 and GigabitEthernet0/0/16. The Border Router is also connected to a switch (SW-2) via GigabitEthernet0/0/17 and GigabitEthernet0/0/18. The Border Router configuration window on the right shows the following commands:

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname Border_Router
Border_Router(config)#enable secret cisco123
Border_Router(config)#username admin password cisco123
Border_Router(config)#ip domain-name trios.com
Border_Router(config)#int g0/0/0
Border_Router(config-if)#ip address 192.168.10.10 255.255.255.0
Border_Router(config-if)#no shut
Border_Router(config-if)#exit
Border_Router(config)#int g0/0/1
Border_Router(config-if)#ip address 172.16.55.1 255.255.255.252
Border_Router(config-if)#no shut
Border_Router(config-if)#exit
Border_Router(config)#line console 0
Border_Router(config-line)#password cisco
Border_Router(config-line)#login local
Border_Router(config-line)#exit
Border_Router(config)#line vty 0 15
Border_Router(config-line)#password cisco
Border_Router(config-line)#transport input ssh
Border_Router(config-line)#login local
Border_Router(config-line)#exit
Border_Router(config)#crypto key generate rsa
The name for the keys will be: Border_Router.trios.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Border_Router(config)#exit
*Mar 1 01:02:54.497: %SSH-5-ENABLED: SSH 1.99 has been enabled
Border_Router#copy running startup
Destination filename [startup-config]?
Copy Paste
```

## ISP Router 4

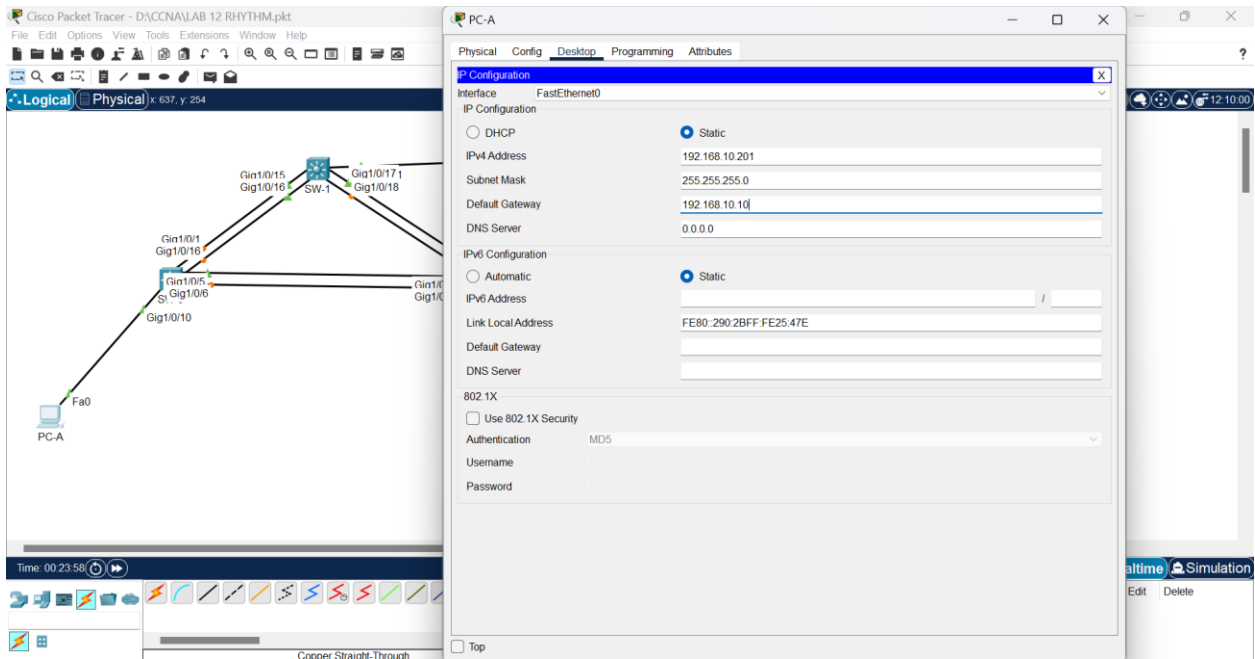


The image shows a Cisco Packet Tracer network diagram and the configuration window for Router4. The network diagram on the left shows a PC-A connected to a switch (SW-1) via a Fa0 interface. The switch is connected to a Border Router via GigabitEthernet0/0/15 and GigabitEthernet0/0/16. The Border Router is also connected to a switch (SW-2) via GigabitEthernet0/0/17 and GigabitEthernet0/0/18. The Router4 configuration window on the right shows the following commands:

```
Router4>enable
Router4#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router4(config)#int g0/0/0
Router4(config-if)#ip address 172.16.55.2 255.255.255.252
Router4(config-if)#no shut
Router4(config-if)#exit
Router4(config)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
Router4(config)#
Router4 con0 is now available
Copy Paste
```

Step 3: Configure PC-A as below:

- IP address: 192.168.10.201
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.10.10



## IMPORTANT:

**Remove console cable(s) now so that PC-A can be connected using Secure Shell Protocol (SSH) to the intermediary devices and explore through CDP/LLDP.**

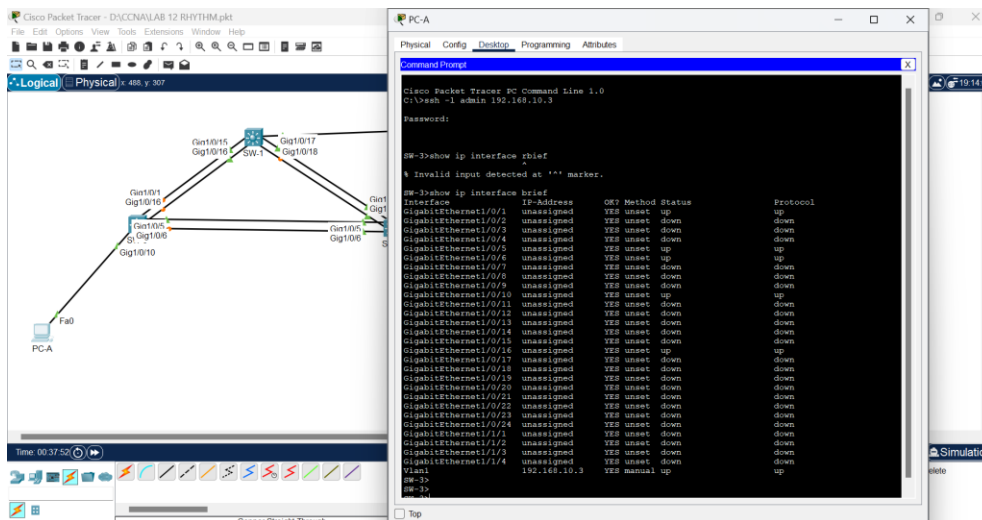
Step 4: Use SSH to remotely access network devices.

- Use the PC-A to remotely access the SW-3 switch. Next, from the SW-3 you will SSH into the SW-2 switch.
  - On the PC-A, open a command prompt.
  - SSH into the SW-3 at **192.168.10.3** using the username **admin** and the password **cisco123**.

PC-A> **ssh -l admin 192.168.10.3**

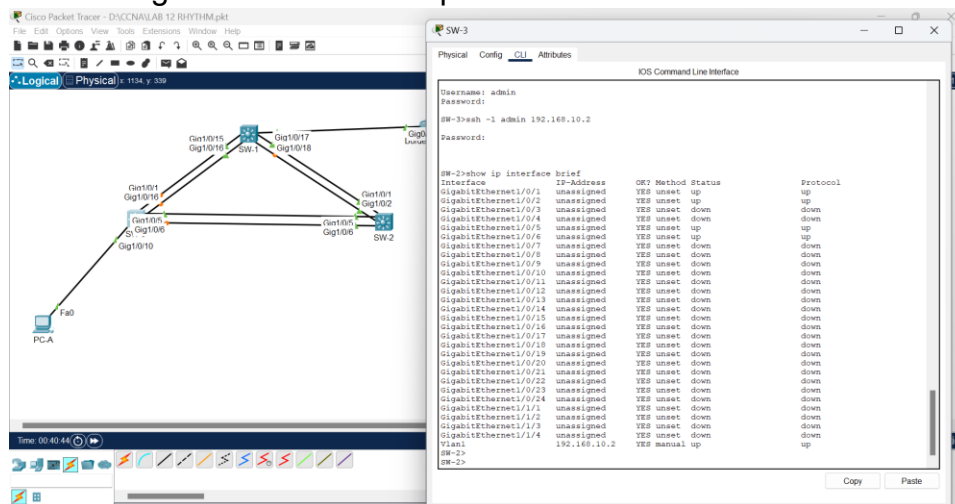
Open

Password:



**SW-3>**

- Use the **show ip interface brief** command to document the SW-3 switch's virtual interfaces, IP addresses, subnet mask, and other required information in the Addressing Table below to map the network.





### Step 5: Use CDP to Discover Neighbouring Devices:

- Security best practice recommends only running CDP when needed, so it may need to be turned on. Use the **show cdp** command to display CDP status.
- If CDP is disabled, run the following command on the global configuration mode for the SW-3 switch to enable CDP:
  - SW-3# **configure terminal**
  - SW-3 (Config) # **cdp run**

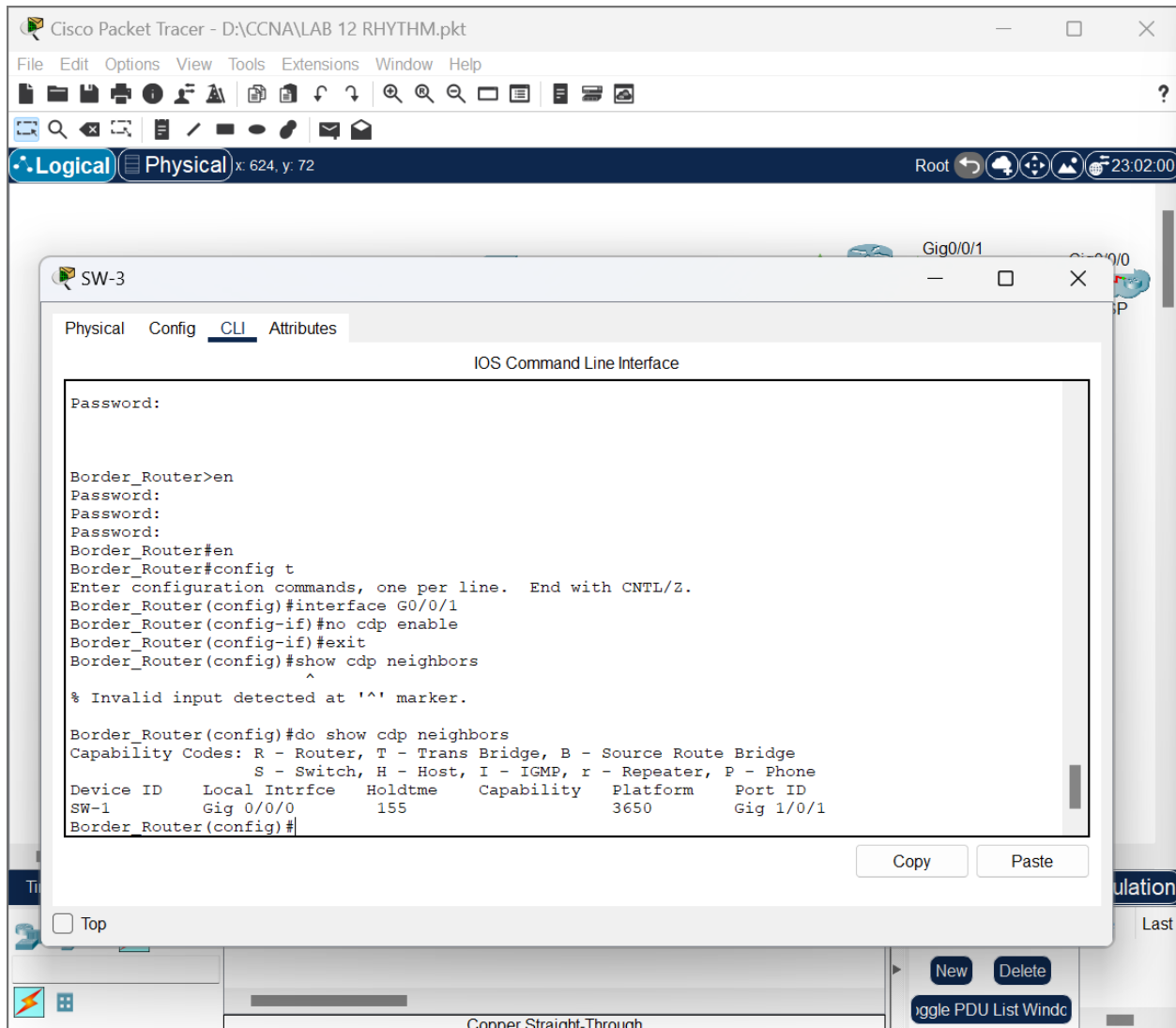
The image shows the Cisco Packet Tracer interface. The main window displays a network diagram with several devices: SW-1, SW-2, SW-3, a Buried\_router, and an ISP. Connections are shown between these devices. A terminal window for SW-3 is open, showing the following commands and output:

```
SW-3>
GigabitEthernet1/1/3 unassigned YES unset down down
GigabitEthernet1/1/4 unassigned YES unset down down
Vlan1 192.168.10.2 YES manual up up
SW-2>
SW-2>ex
[Connection to 192.168.10.2 closed by foreign host]
SW-3>config t
^
% Invalid input detected at '^' marker.

SW-3>en
Password:
Password:
SW-3#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-3(config)#cdp run
SW-3(config)#
```

The terminal window also has 'Copy' and 'Paste' buttons at the bottom right. The bottom of the interface shows a toolbar with various tools and a status bar indicating 'Conner Straight-Through'.

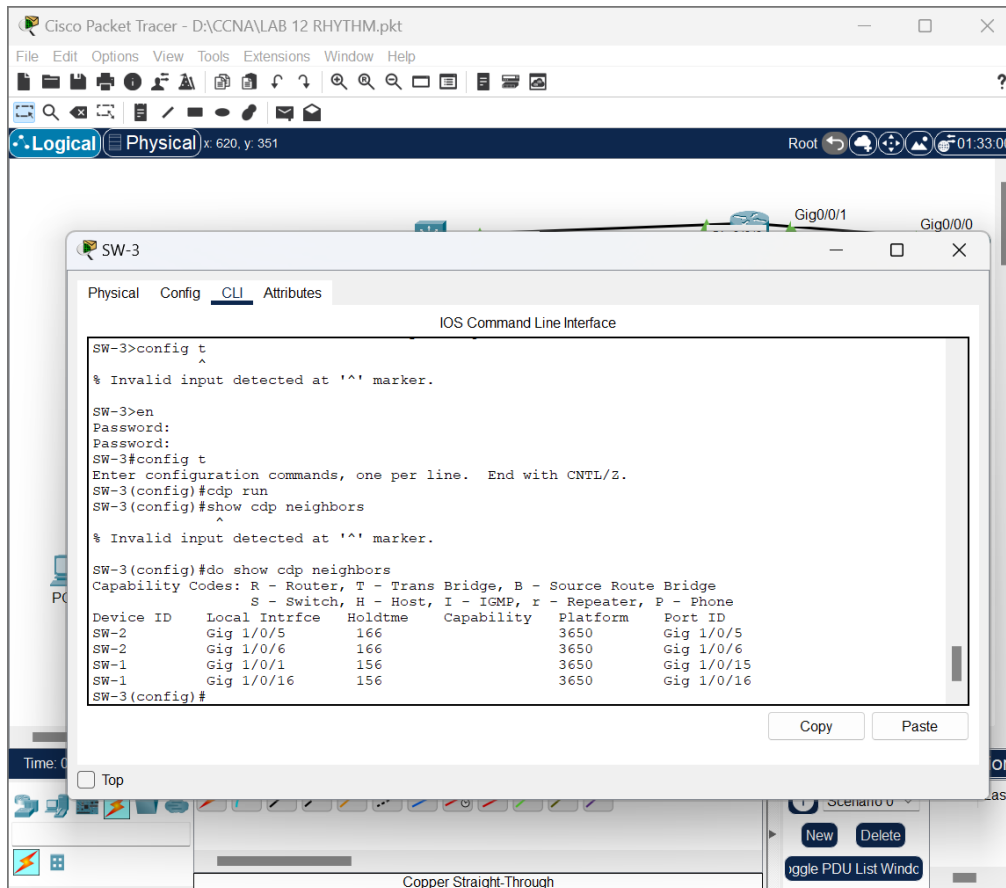
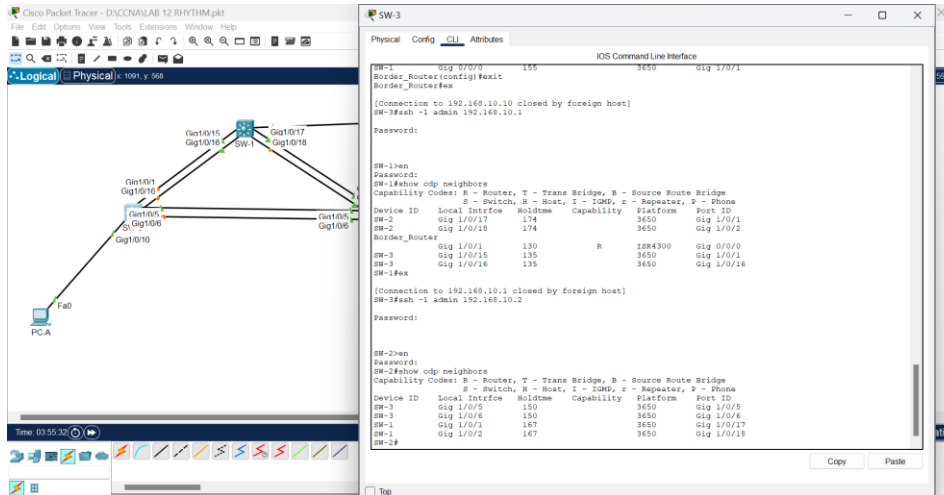
- You need to turn on CDP globally on all the three switches and Border\_Router if needed, but it is a good idea to only broadcast CDP information to internal network devices and not to external networks. To do this, after turning on the CDP protocol on all intermediary devices, disable CDP on the G0/0/1 interface of Border\_Router using the commands below:
  - Border\_Router (Config) # **cdp run**
  - Border\_Router (Config) # **interface G0/0/1**
  - Border\_Router (Config-if) # **no cdp enable**
  - Border\_Router (Config-if) # **exit**



- Issue a **show cdp neighbors** command at SW-3 to find any neighbouring network devices.

Note: CDP will only show connected Cisco devices that are also running CDP.

- SW-3# **show cdp neighbors**



Use CDP to complete the Addressing Table below:					
Device Hostname	Local Interface	IP Address	Subnet Mask	Interface	Connected Neighbour
Border_Router	Gig 0/0/0	192.168.10.10	255.255.255.0	Gig 0/0/1	SW-1
SW-1	Gig 1/0/17	192.168.10.1	255.255.255.0	Gig 1/0/1	SW-2
SW-1	Gig 1/0/18	192.168.10.1	255.255.255.0	Gig 1/0/2	SW-2
SW-1	Gig 1/0/1	192.168.10.1	255.255.255.0	Gig 0/0/0	Border_Router
SW-1	Gig 1/0/15	192.168.10.1	255.255.255.0	Gig 1/0/1	SW-3
SW-1	Gig 1/0/16	192.168.10.1	255.255.255.0	Gig 1/0/16	SW-3
SW-2	Gig 1/0/5	192.168.10.2	255.255.255.0	Gig 1/0/5	SW-3
SW-2	Gig 1/0/6	192.168.10.2	255.255.255.0	Gig 1/0/6	SW-3
SW-2	Gig 1/0/1	192.168.10.2	255.255.255.0	Gig 1/0/17	SW-1
SW-2	Gig 1/0/2	192.168.10.2	255.255.255.0	Gig 1/0/18	SW-1
SW-3	Gig 1/0/5	192.168.10.3	255.255.255.0	Gig 1/0/5	SW-2
SW-3	Gig 1/0/6	192.168.10.3	255.255.255.0	Gig 1/0/6	SW-2
SW-3	Gig 1/0/1	192.168.10.3	255.255.255.0	Gig 1/0/15	SW-1
SW-3	Gig 1/0/16	192.168.10.3	255.255.255.0	Gig 1/0/16	SW-1

Questions:

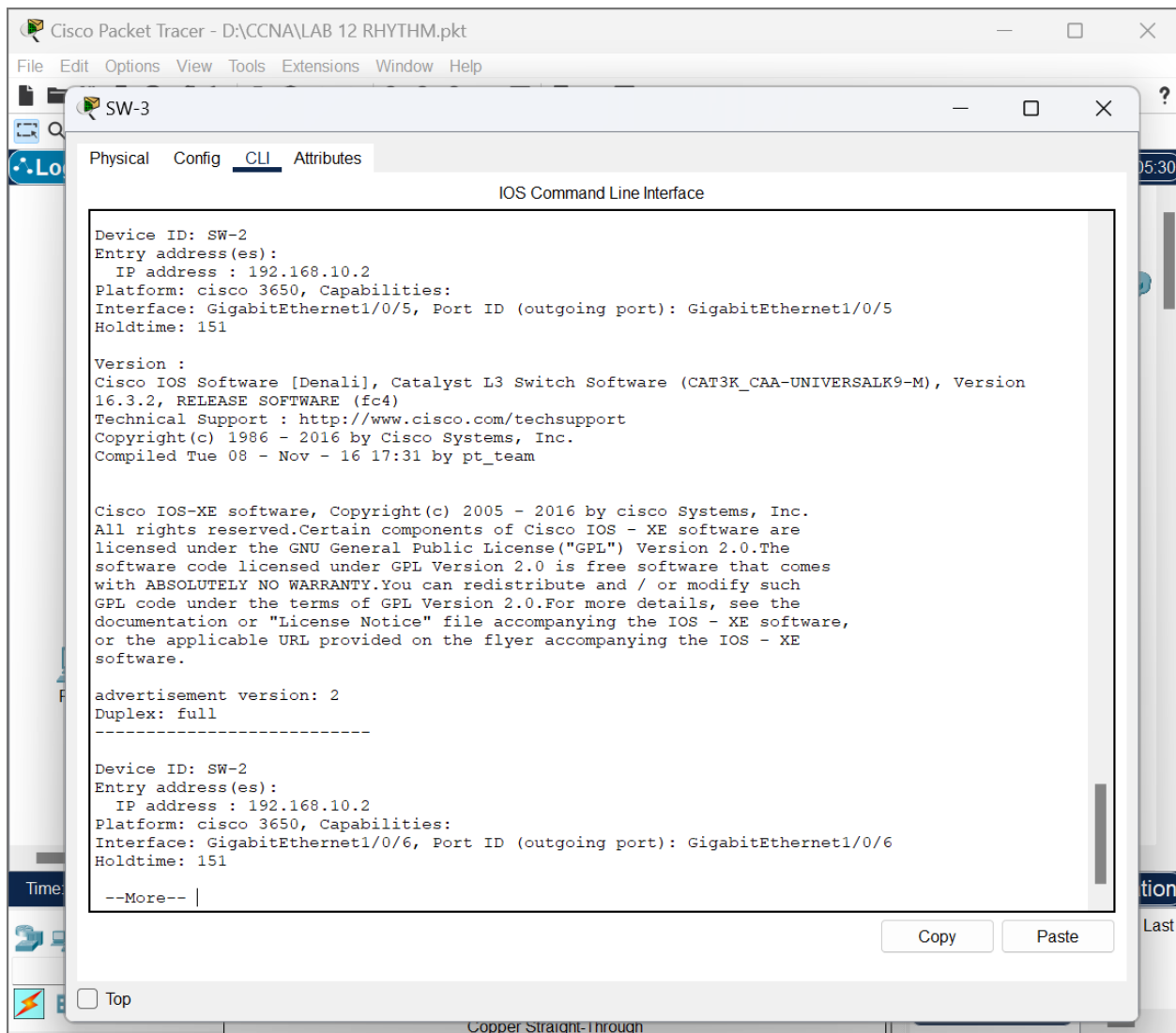
- Is there a neighbouring network device? YES
- What type of device is it? Switches and Router
- What is its name? SW-2, SW-1, SW-3 and Border\_Router
- On what interface is it connected? (In case of SW-3)
- Gig 1/0/5, Gig 1/0/6 to SW-2 and
- Gig 1/0/1, Gig 1/0/16 to SW-1

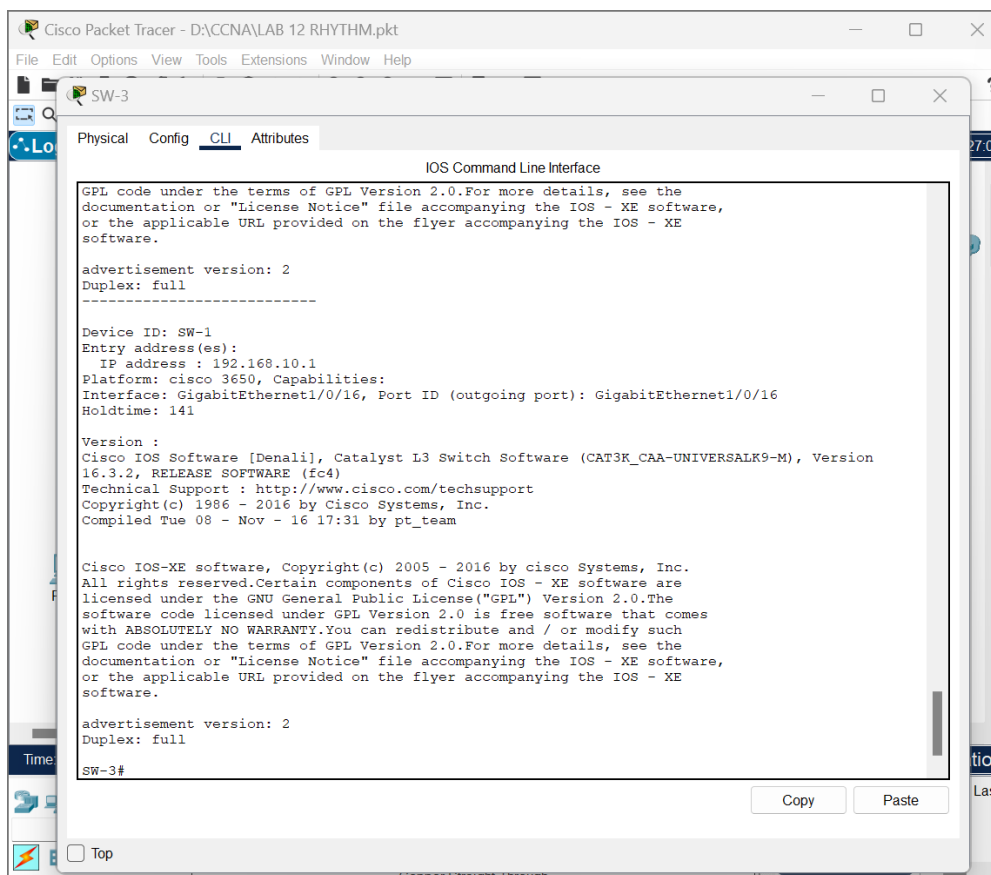
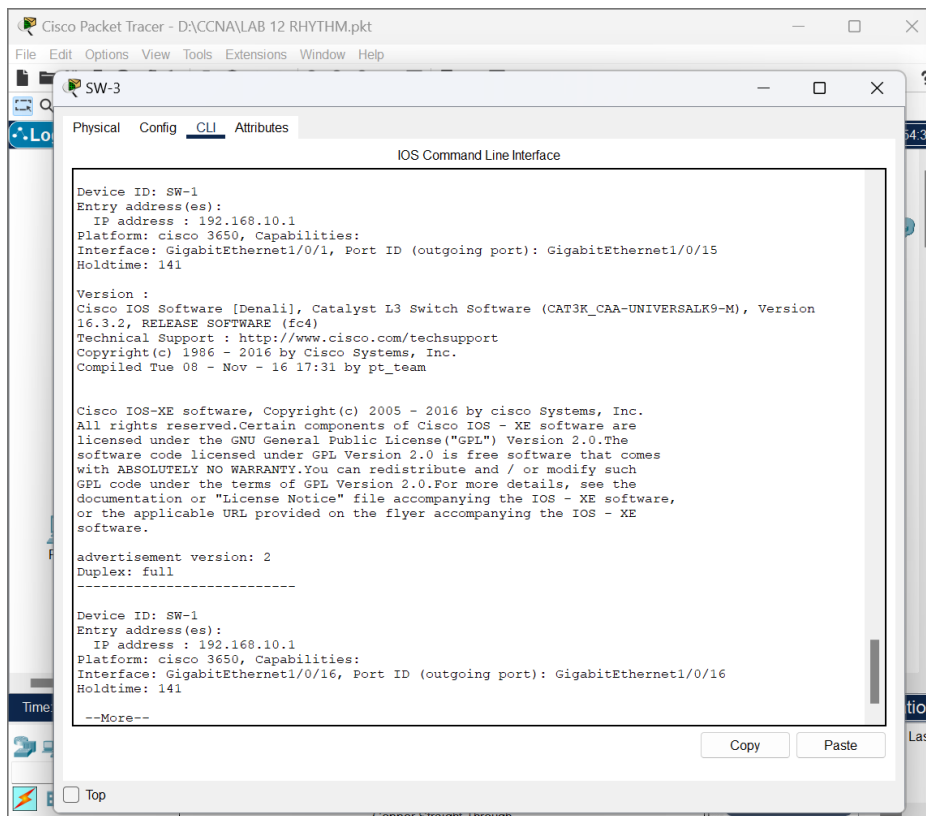
- Is the device's IP address listed? No

Record the information from the answers to these questions in the Addressing Table above.

Note: It may take some time for CDP updates to be received.

- To find the IP address of the neighbouring device, use the **show cdp neighbors detail** command and record the IP address:
- SW-3# **show cdp neighbors detail**





Question:

- Aside from the neighbouring device's IP address, what other piece of potentially sensitive information is listed?

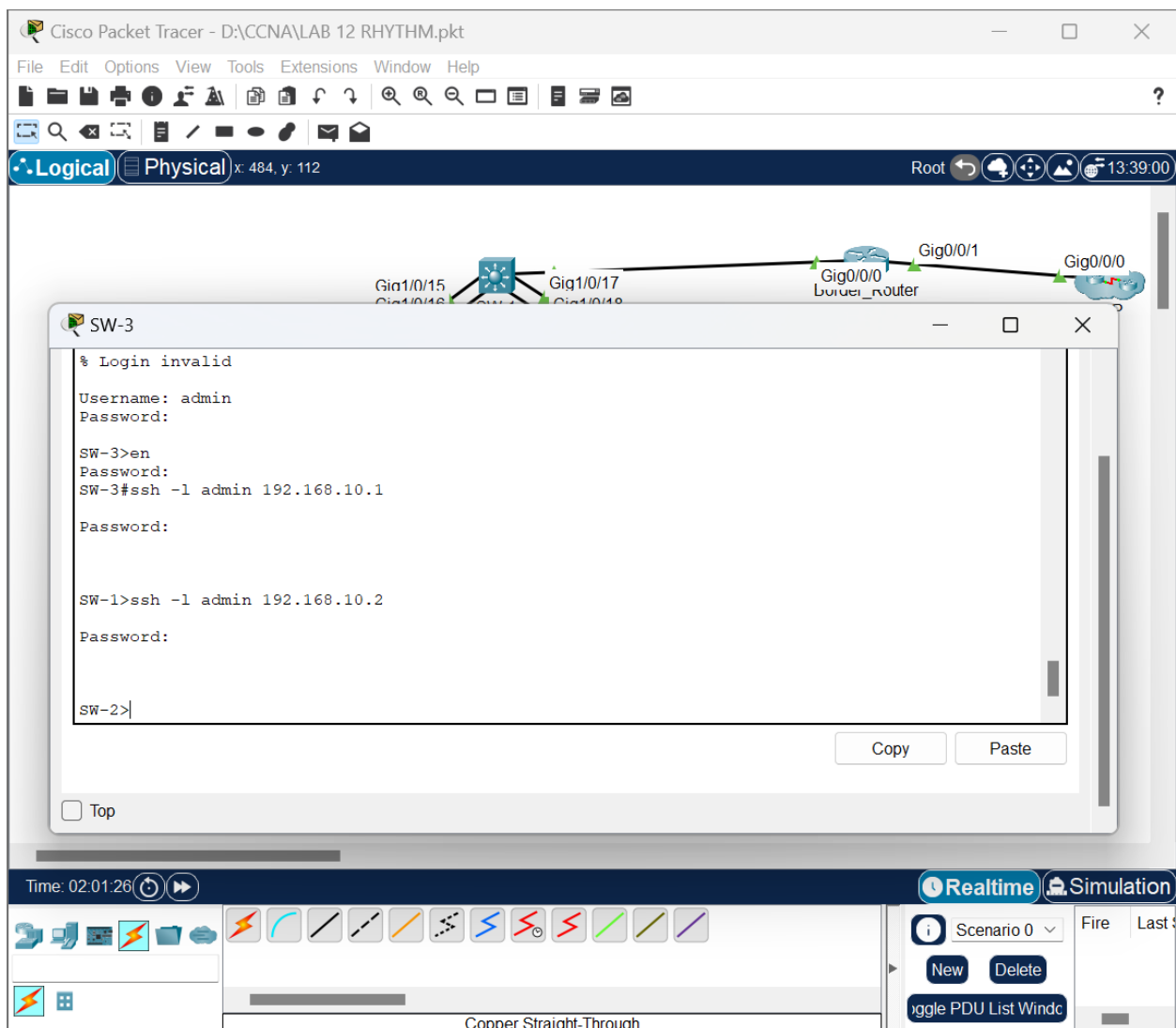
Answer: Version: Show neighboring device version

Platform: Model of the neighboring Device

Copy right Support

- Now that you know the IP address of the neighbour device, connect to it with the SSH to discover other devices that may be its neighbours.

Note: To connect with the SSH, use the same username **admin** and password **cisco123**.



As in picture I can easily Login into SW-1 and SW-2 using ssh

- After you are remotely connected to the next neighbour, use the **show cdp neighbors** command, and the **show cdp neighbors detail** command to discover other connected neighbour devices.

The first screenshot shows the network topology in Cisco Packet Tracer. A PC is connected to a switch (SW-1) via a Fa0/20 interface. The switch has several other interfaces connected to other devices, including a router (R1) and another switch (SW-2).

The second screenshot shows the output of the **show cdp neighbors** command on SW-1. The output lists the following information:

```

SW-1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, x - Repeater, P - Phone
Device ID Local Interface Holdtime Capability Platform Port ID
SW-1 Gig 1/0/1 157 3650 Gig 1/0/17
SW-2 Gig 1/0/2 157 3650 Gig 1/0/18
SW-3 Gig 1/0/5 161 3650 Gig 1/0/6
SW-1#show cdp neighbors detail

```

The third screenshot shows the output of the **show cdp neighbors detail** command on SW-1. The output provides detailed information about the discovered devices, including their IP addresses, platforms, and capabilities.

```

Device ID: SW-1
Entry addresses:
IP address: 192.168.10.1
Platform: cisco 3650, Capabilities:
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): GigabitEthernet1/0/17
Holdtime: 150

Version :
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.2, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986 - 2016 by Cisco Systems, Inc.
Compiled Tue 08 - Nov - 16 17:31 by pt_team

Cisco IOS-XE software, Copyright (c) 2005 - 2016 by Cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS - XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and / or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS - XE software,
or the applicable URL provided on the flyer accompanying the IOS - XE
software.

advertisement version: 2
Duplex: full

```



### Question:

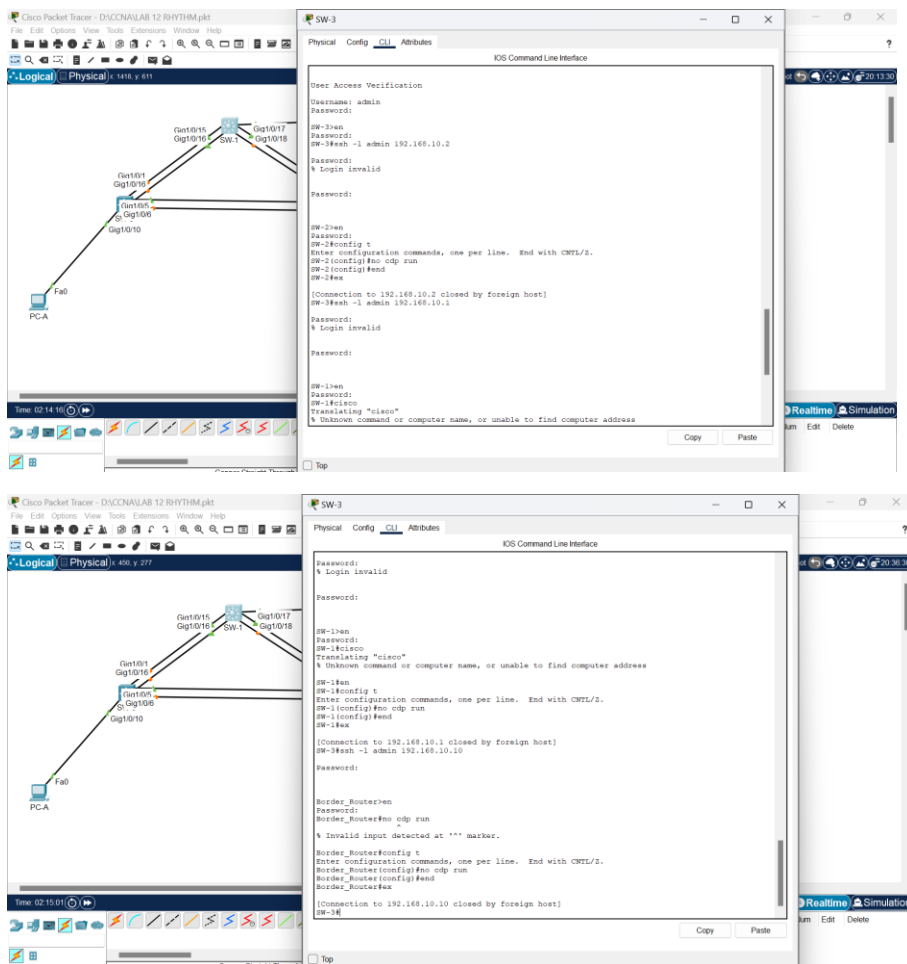
- What types of network devices neighbour this device? Switches SW1 and SW3

Record any newly discovered devices in the Addressing Table above. Include their hostname, interfaces, and IP addresses.

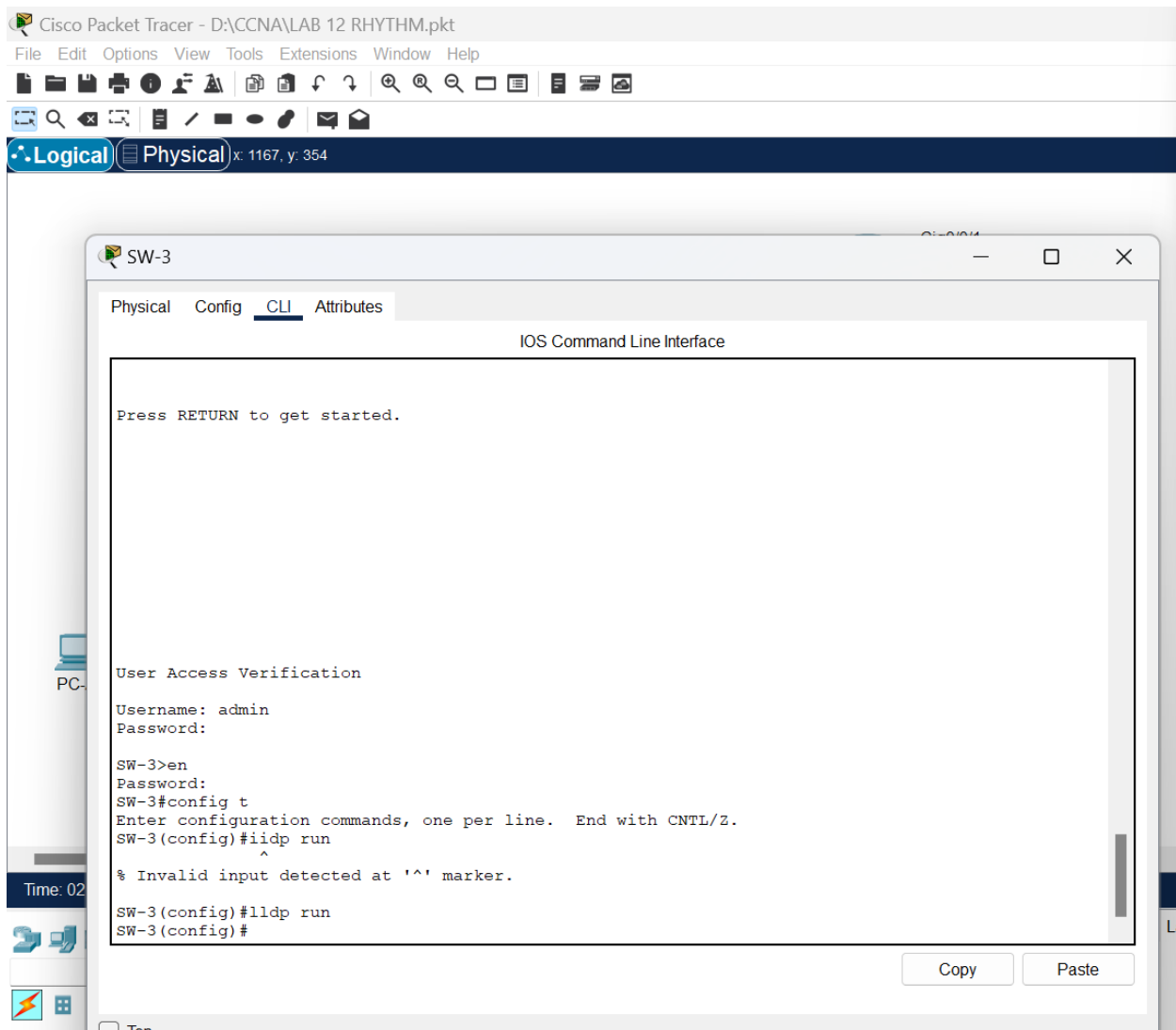
- Continue discovering new network devices using SSH and the show CDP commands. Eventually, you will reach the end of the network and there will be no more devices to discover. Yes

Step 6: Use LLDP to discover neighbouring devices:

- Repeat Step 5, but this time use LLDP instead of CDP to discover all the devices and the relevant information that is required to complete the Addressing Table below.
- The switches and router were previously configured to use CDP. Switch SW-3 has already been configured to use CDP. Issue the **show cdp** command to verify if CDP is currently active. Disable CDP by issuing the following command on all switches and Border\_Router:
  - SW-3(config)# **no cdp run**



- LLDP can be configured to both transmit and receive on a specific interface. Configure SW-3 so it receives LLDP messages from other devices.
  - SW-3 (config)# **lldp run**



- You need to turn on LLDP globally on all the three switches and Border\_Router using the command **lldp run**, but due to security concerns it is a good idea to only send LLDP information to internal network devices and not to external networks. Discover which interface is connected to the internet by issuing the command **show ip interface brief** on Border\_Router.

Cisco Packet Tracer - D:\CCNA\LAB 12 RHYTHM.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 453, y: 58

SW-3

Physical Config CLI Attributes

IOS Command Line Interface

```

User Access Verification
Username: admin
Password:

SW-3>ssh -l admin 192.168.10.10

Password:
% Login invalid

Password:

Border_Router>en
Border_Router#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0      192.168.10.10   YES manual up          up
GigabitEthernet0/0/1      172.16.55.1     YES manual up          up
GigabitEthernet0/0/2      unassigned      YES unset  administratively down down
Serial0/1/0               unassigned      YES unset  administratively down down
Serial0/1/1               unassigned      YES unset  administratively down down
Vlan1                     unassigned      YES unset  administratively down down
Border_Router#

```

Copy Paste

Top

Copper Straight Through

toggle PDU List Window

SW-3

Physical Config CLI Attributes

IOS Command Line Interface

```

Border_Router(config)#interface g0/0/1
Border_Router(config-if)#no lldp transmit
Border_Router(config-if)#no lldp receive
Border_Router(config-if)#exit
Border_Router(config)#exit
Border_Router#exit

[Connection to 192.168.10.10 closed by foreign host]
SW-3>ssh -l admin 192.168.10.2

Password:

SW-2>en
SW-2#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-2(config)#lldp run
SW-2(config)#end
SW-2#ex
% Ambiguous command: "e"
SW-2#ex

[Connection to 192.168.10.2 closed by foreign host]
SW-3>ssh -l 192.168.10.1
% Incomplete command.
SW-3>ssh -l admin 192.168.10.1

Password:

SW-1>en
SW-1#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-1(config)#lldp run
SW-1(config)#end
SW-1#ex

[Connection to 192.168.10.1 closed by foreign host]
SW-3>

```

Copy Paste

Top

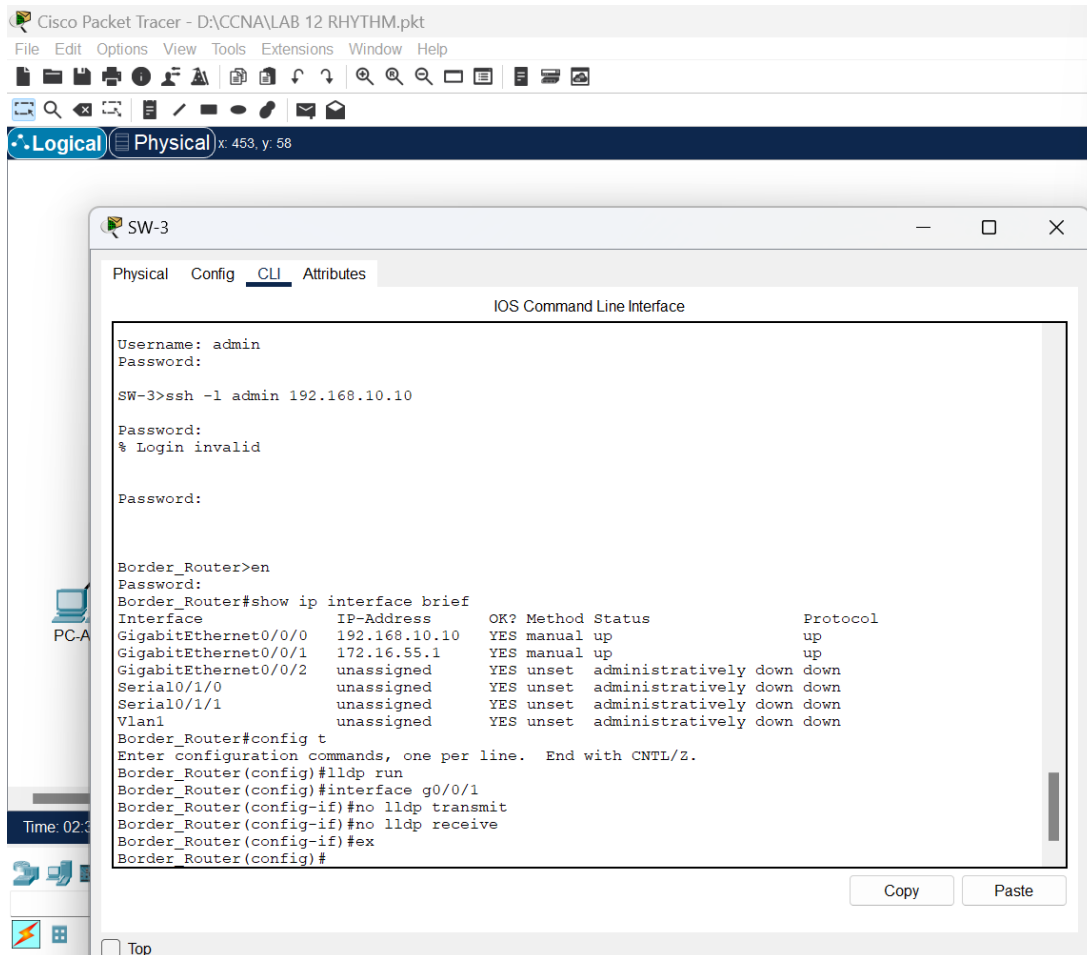
Time: 02:33:15

Copper Straight-Through

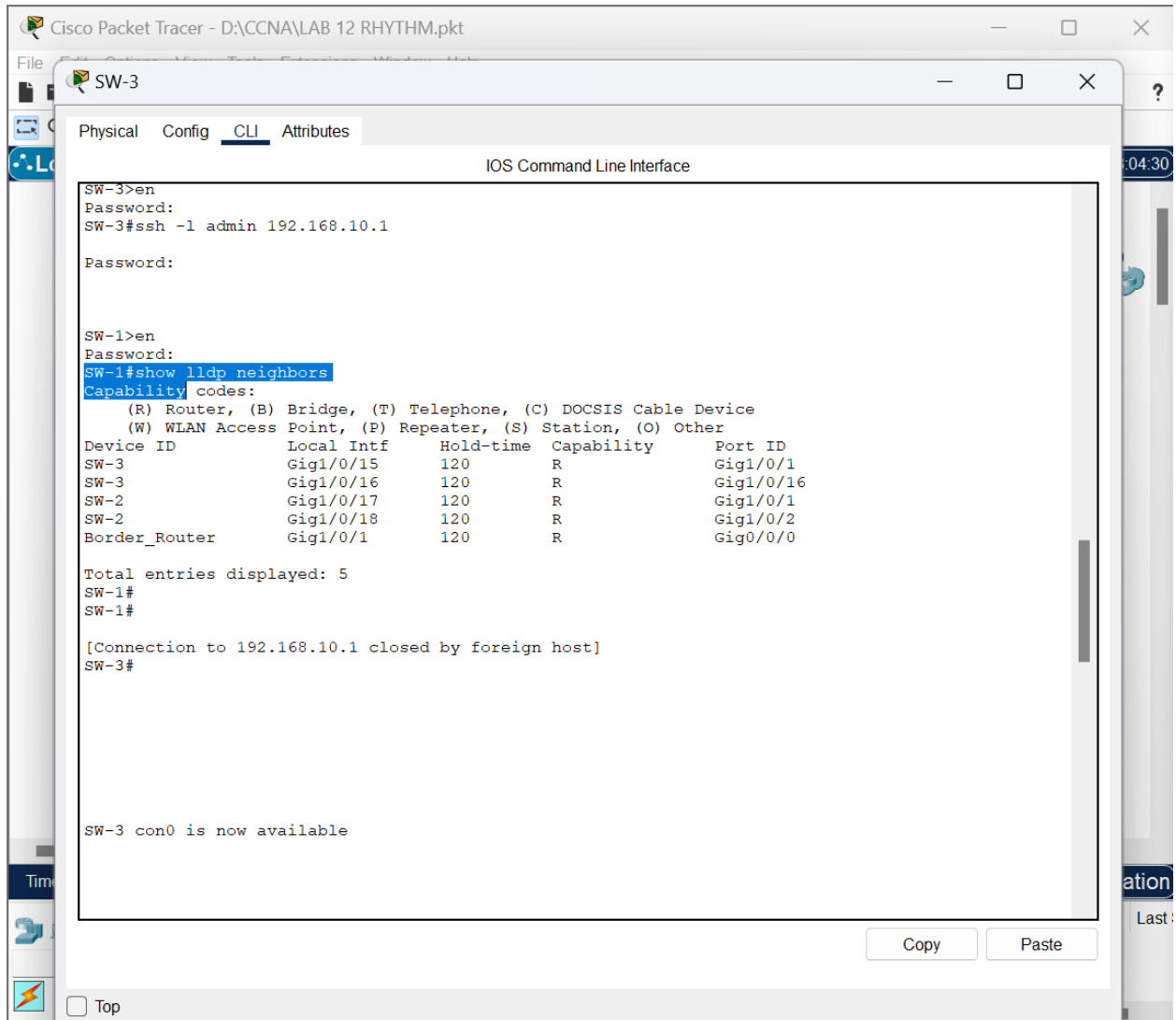
Simulation

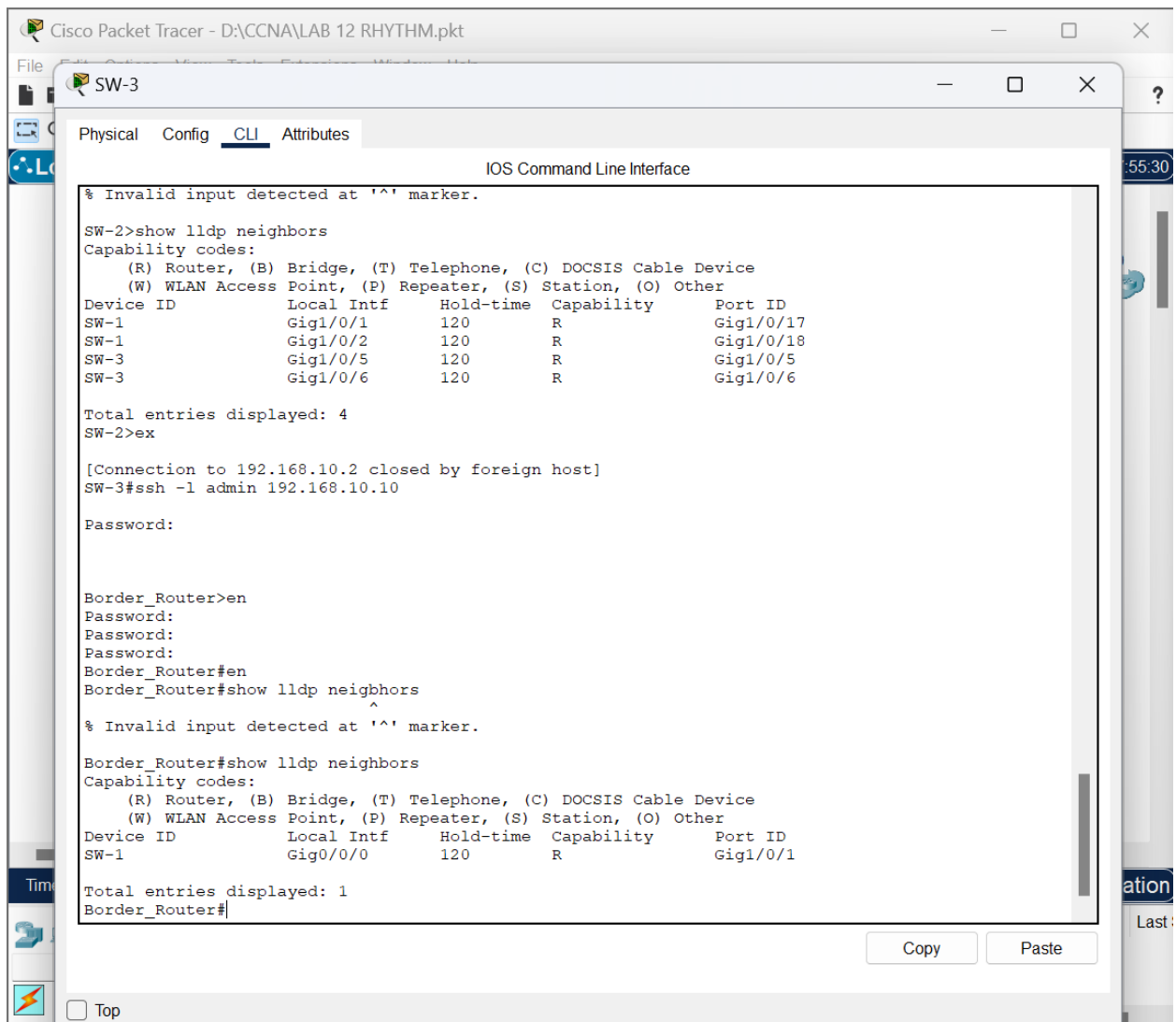
- Enable the LLDP protocol and completely disable LLDP on the interface that is connected to the internet.

- Border\_Router (Config) # **lldp run**
- Border\_Router (Config) # **interface G0/0/1**
- Border\_Router (Config-if) # **no lldp transmit**
- Border\_Router (Config-if) # **no lldp receive**
- Border\_Router (Config-if) # **exit**



- Use the **show lldp neighbors** command to verify that SW-3 is receiving messages from other neighbouring devices.





Cisco Packet Tracer - D:\CCNA\LAB 12 RHYTHM.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1112, y: 571

```
graph LR
    SW1[SW-1] ---|Gig1/0/15| SW2[SW-2]
    SW1 ---|Gig1/0/16| SW2
    SW1 ---|Gig1/0/17| BR[Border_router]
    SW1 ---|Gig1/0/18| BR
    BR ---|Gig0/0/1| ISP[ISP]
    BR ---|Gig0/0/0| ISP
```

SW-3

```
SW-1#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-1(config)#lldp run
SW-1(config)#end
SW-1#ex

[Connection to 192.168.10.1 closed by foreign host]
SW-3>
SW-3>en
Password:
SW-3#show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf    Hold-time    Capability    Port ID
SW-1           Gig1/0/1     120          R             Gig1/0/15
SW-1           Gig1/0/16    120          R             Gig1/0/16
SW-2           Gig1/0/5     120          R             Gig1/0/5
SW-2           Gig1/0/6     120          R             Gig1/0/6

Total entries displayed: 4
SW-3#
```

Copy Paste

Top

Conner Straight-Through

New Delete

Toggle PDU List Window

Note: You may add more rows in the table, if needed.

Use LLDP to complete this Addressing Table:					
Device Hostname	Interface	IP Address	Subnet Mask	Local Interface	Connected Neighbour
SW-1	Gig 1/0/15	192.168.10.1	255.255.255.0	Gig 1/0/1	SW-3
SW-1	Gig 1/0/16	192.168.10.1	255.255.255.0	Gig 1/0/16	SW-3
SW-1	Gig 1/0/17	192.168.10.1	255.255.255.0	Gig 1/0/1	SW-2
SW-1	Gig 1/0/18	192.168.10.1	255.255.255.0	Gig 1/0/2	SW-2
SW-1	Gig 1/0/1	192.168.10.1	255.255.255.0	Gig 0/0/0	Border_Router
SW-2	Gig 1/0/1	192.168.10.2	255.255.255.0	Gig 1/0/1	SW-1
SW-2	Gig 1/0/2	192.168.10.2	255.255.255.0	Gig 1/0/16	SW-1
SW-2	Gig 1/0/5	192.168.10.2	255.255.255.0	Gig 1/0/1	SW-3
SW-2	Gig 1/0/6	192.168.10.2	255.255.255.0	Gig 1/0/2	SW-3
Border_Router	Gig 0/0/0	192.168.10.10	255.255.255.0	Gig 1/0/1	SW-1
SW-3	Gig 1/0/1	192.168.10.3	255.255.255.0	Gig 1/0/15	SW-3
SW-3	Gig 1/0/16	192.168.10.3	255.255.255.0	Gig 1/0/16	SW-3
SW-3	Gig 1/0/5	192.168.10.3	255.255.255.0	Gig 1/0/5	SW-2
SW-3	Gig 1/0/6	192.168.10.3	255.255.255.0	Gig 1/0/6	SW-2