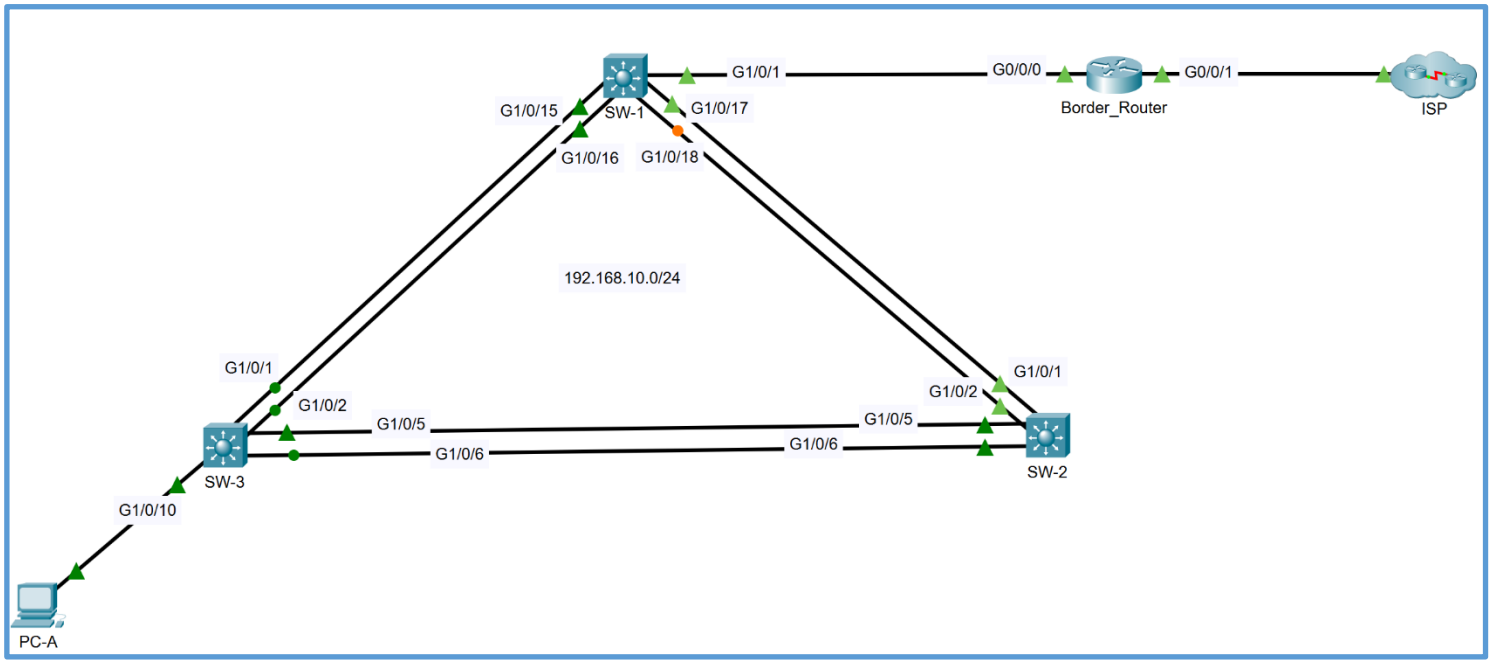
PART – 1

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.

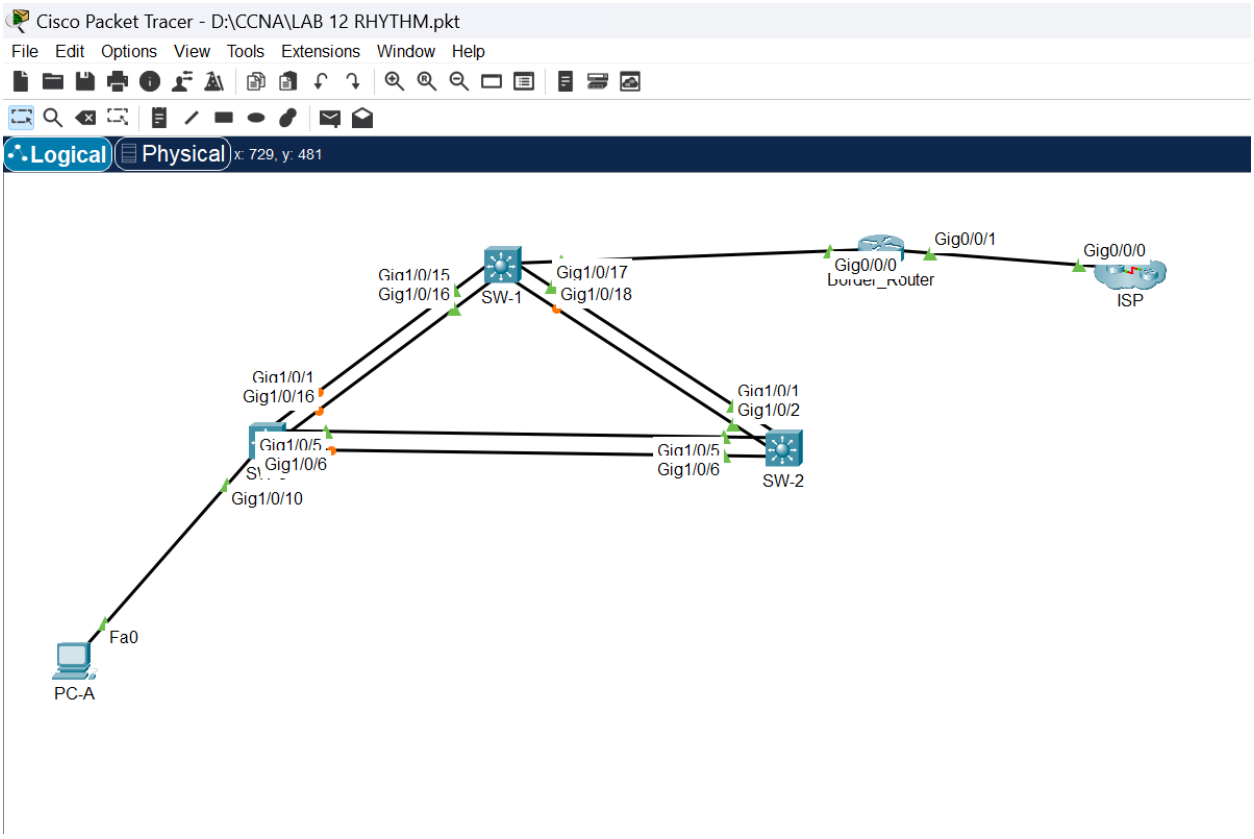
Lab Description:

- 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.



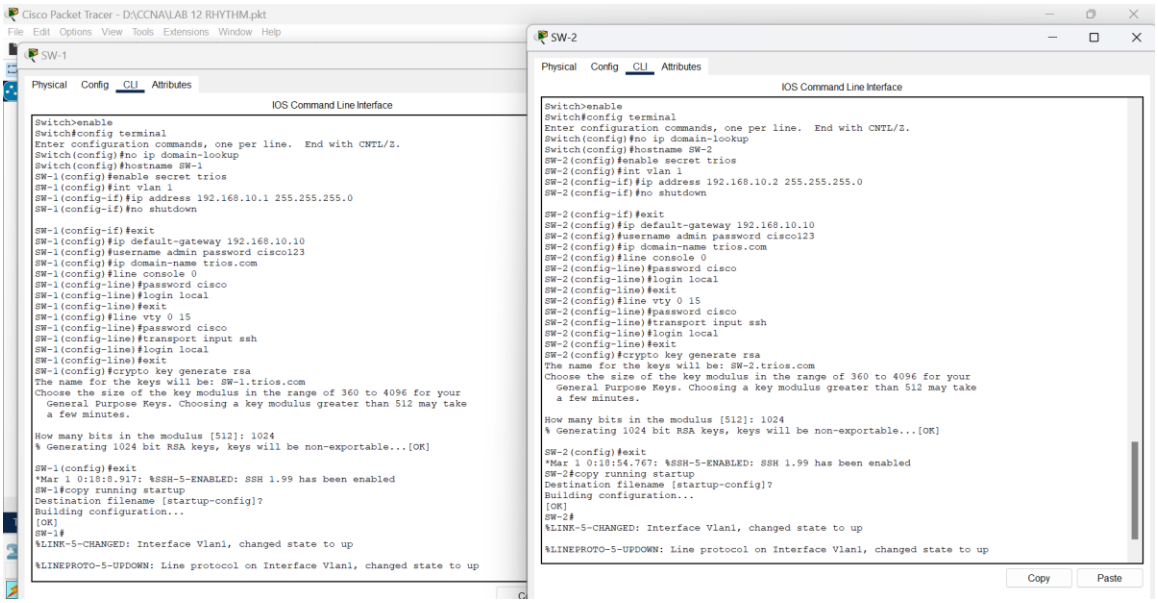
Step 2: For this lab consideration, copy the following instructions (without bullet points) into each switch and then the router:

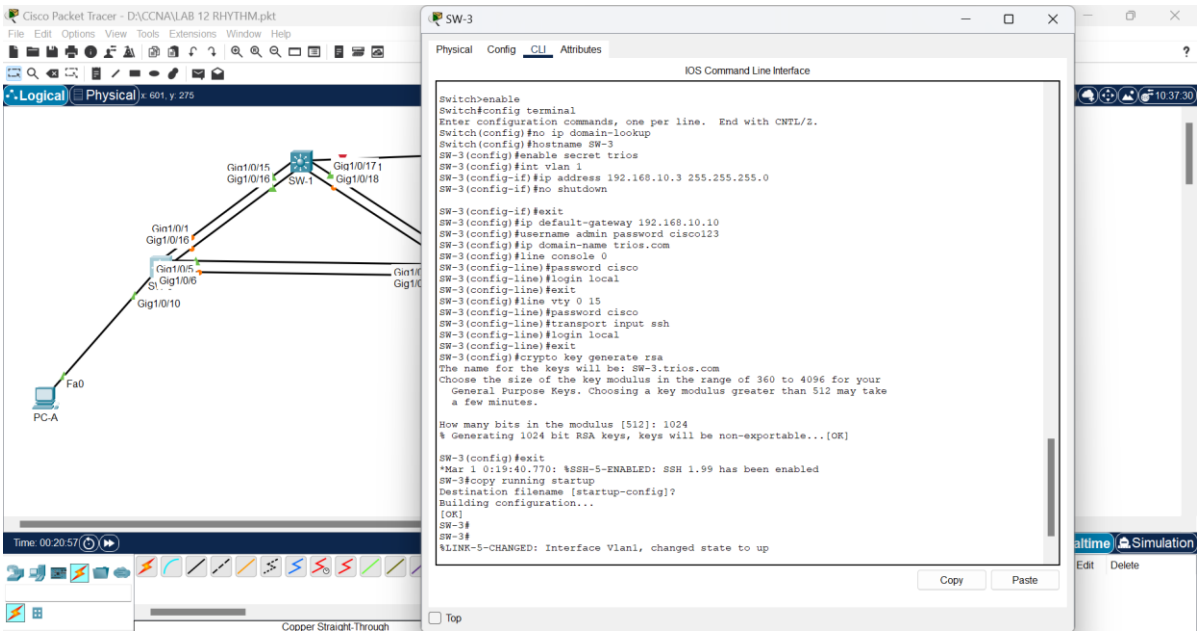
Note: Prior to copying the below instructions, check the configuration for any obvious errors/typos.

SW-1	SW-2	SW-3

• enable • config terminal • no ip domain-lookup • hostname SW-1 • enable secret trios • int vlan 1 • ip address 192.168.10.1 255.255.255.0 • no shutdown • exit • ip default-gateway 192.168.10.10 • username admin password cisco123 • ip domain-name trios.com • 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	• enable • config terminal • no ip domain-lookup • hostname SW-2 • enable secret trios • int vlan 1 • ip address 192.168.10.2 255.255.255.0 • no shutdown • exit • ip default-gateway 192.168.10.10 • username admin password cisco123 • ip domain-name trios.com • 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	• enable • config terminal • no ip domain-lookup • hostname SW-3 • enable secret trios • int vlan 1 • ip address 192.168.10.3 255.255.255.0 • no shutdown • exit • ip default-gateway 192.168.10.10 • username admin password cisco123 • ip domain-name trios.com • 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

Switches



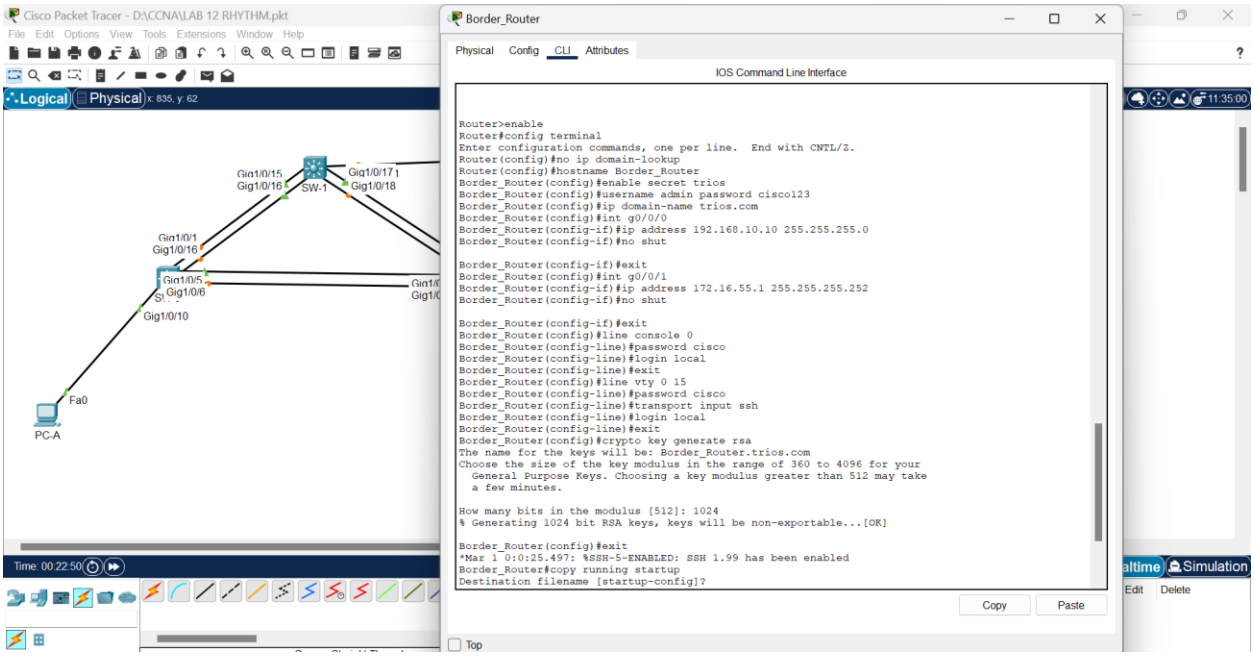


Border_Router
• enable • config terminal • no ip domain-lookup • hostname Border_Router • enable secret trios • username admin password cisco123 • ip domain-name trios.com • int g0/0/0

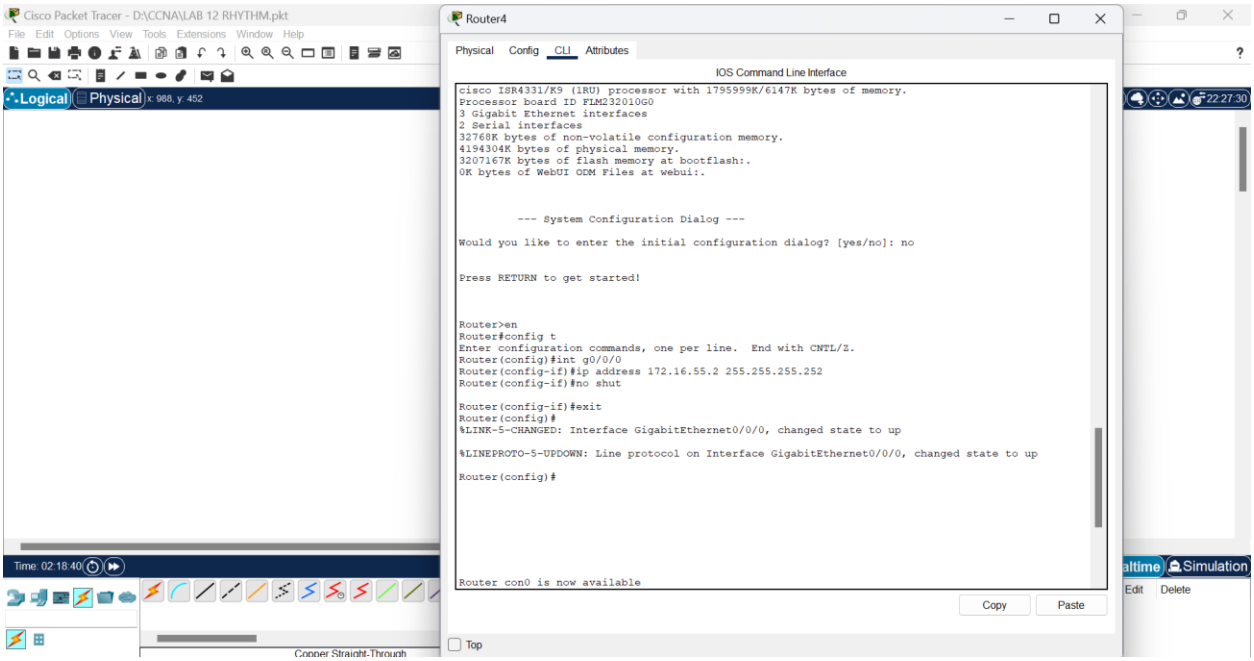
ip address 192.168.10.10 255.255.255.0
no shut
exit

- 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

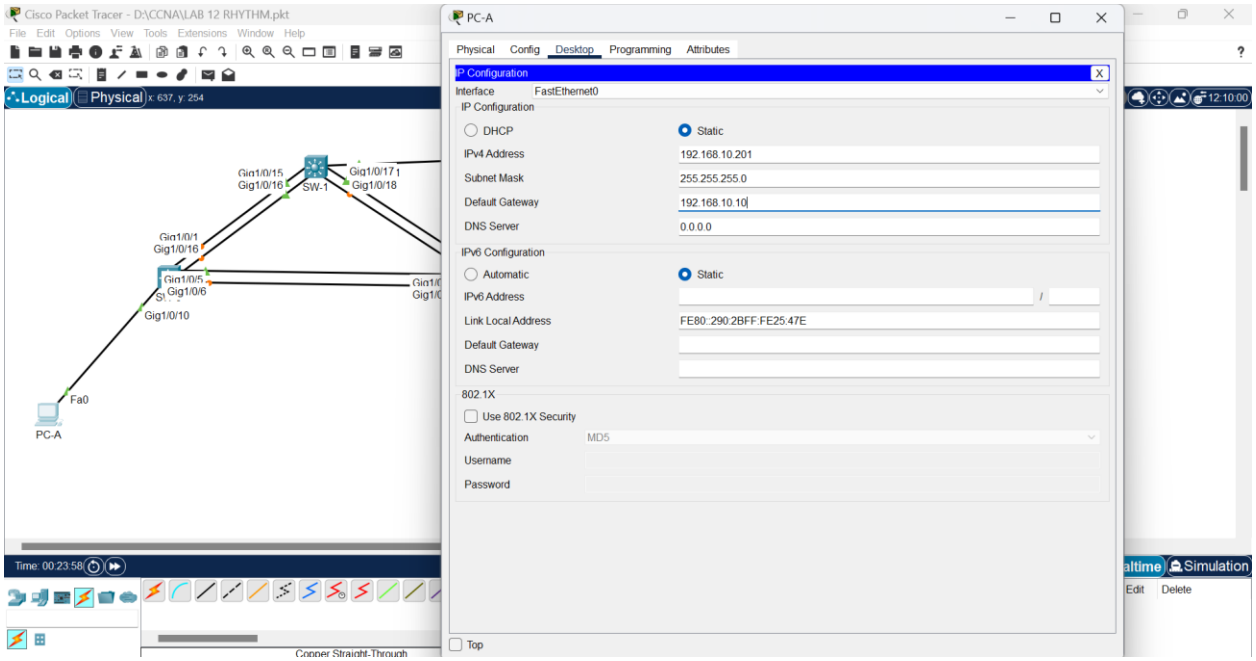


ISP Router 4



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

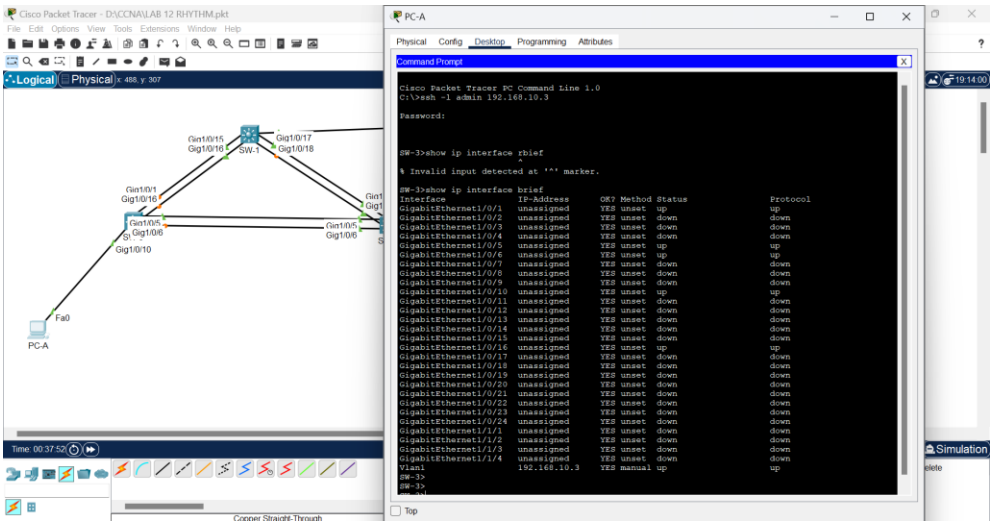


IMPORTANT:

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.

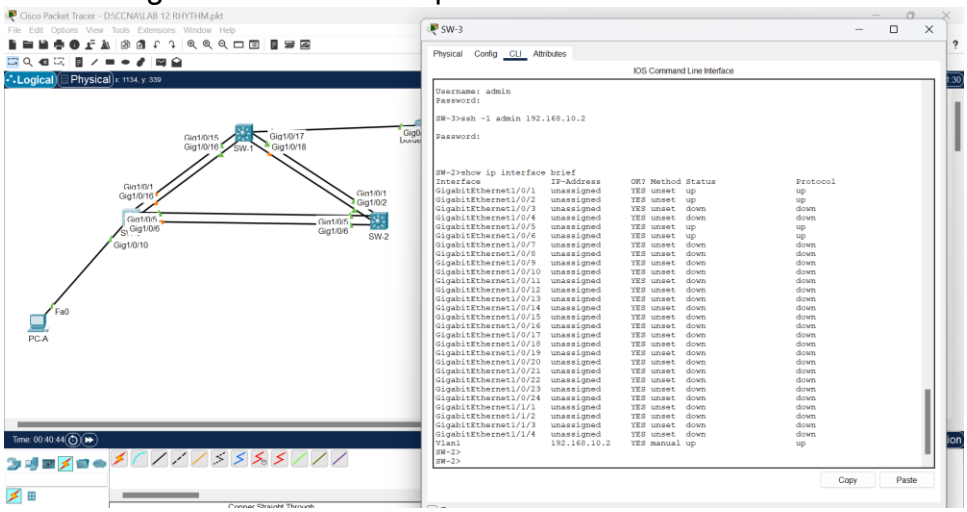
Step 4: Use SSH to remotely access network devices.

- Use the PC-A to remotely access the SW-3 switch. Next, from the SW-3 you will SSH into the SW-2 switch.
  a. On the PC-A, open a command prompt.
  b. 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:



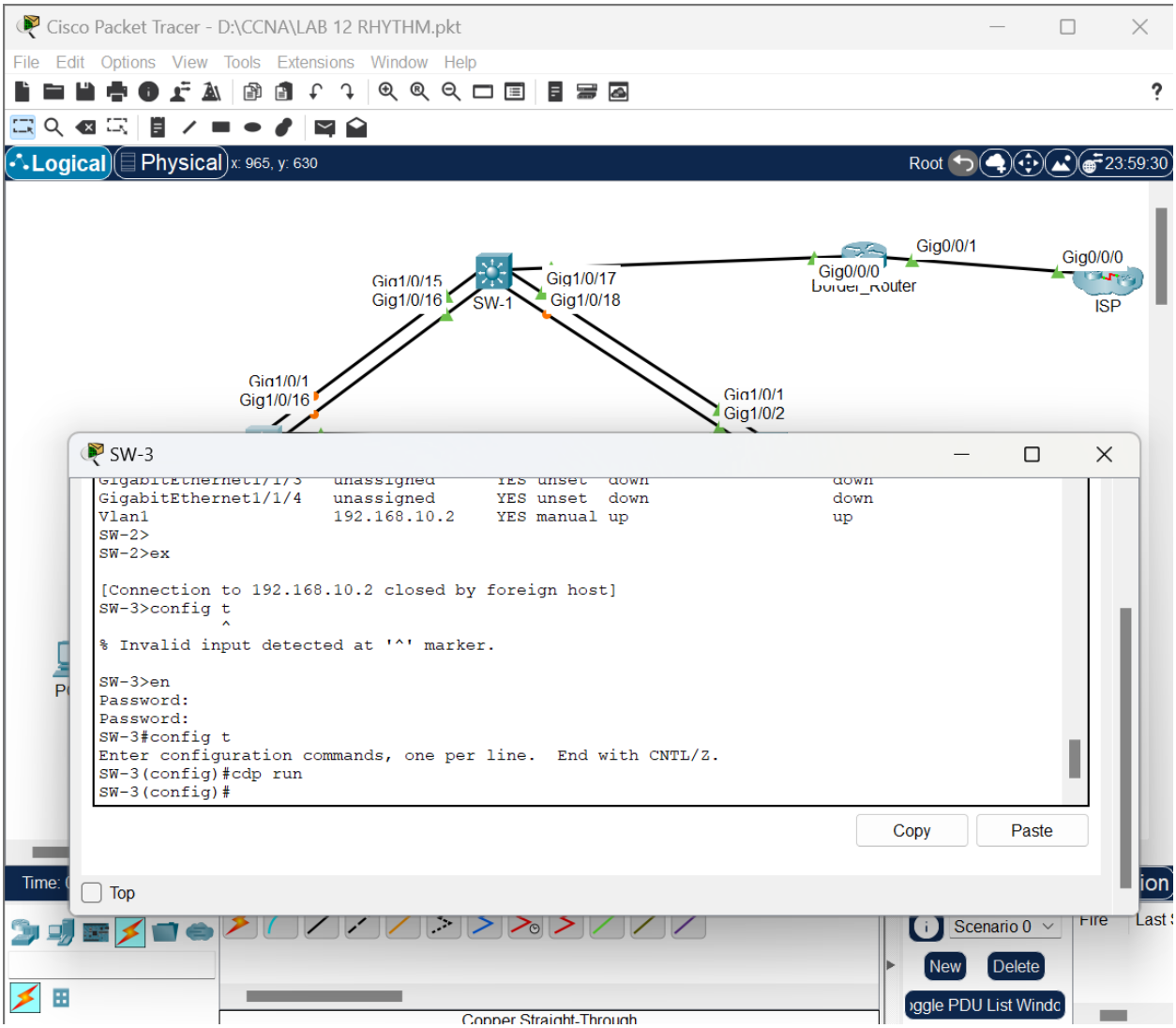
SW-3>

- 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.

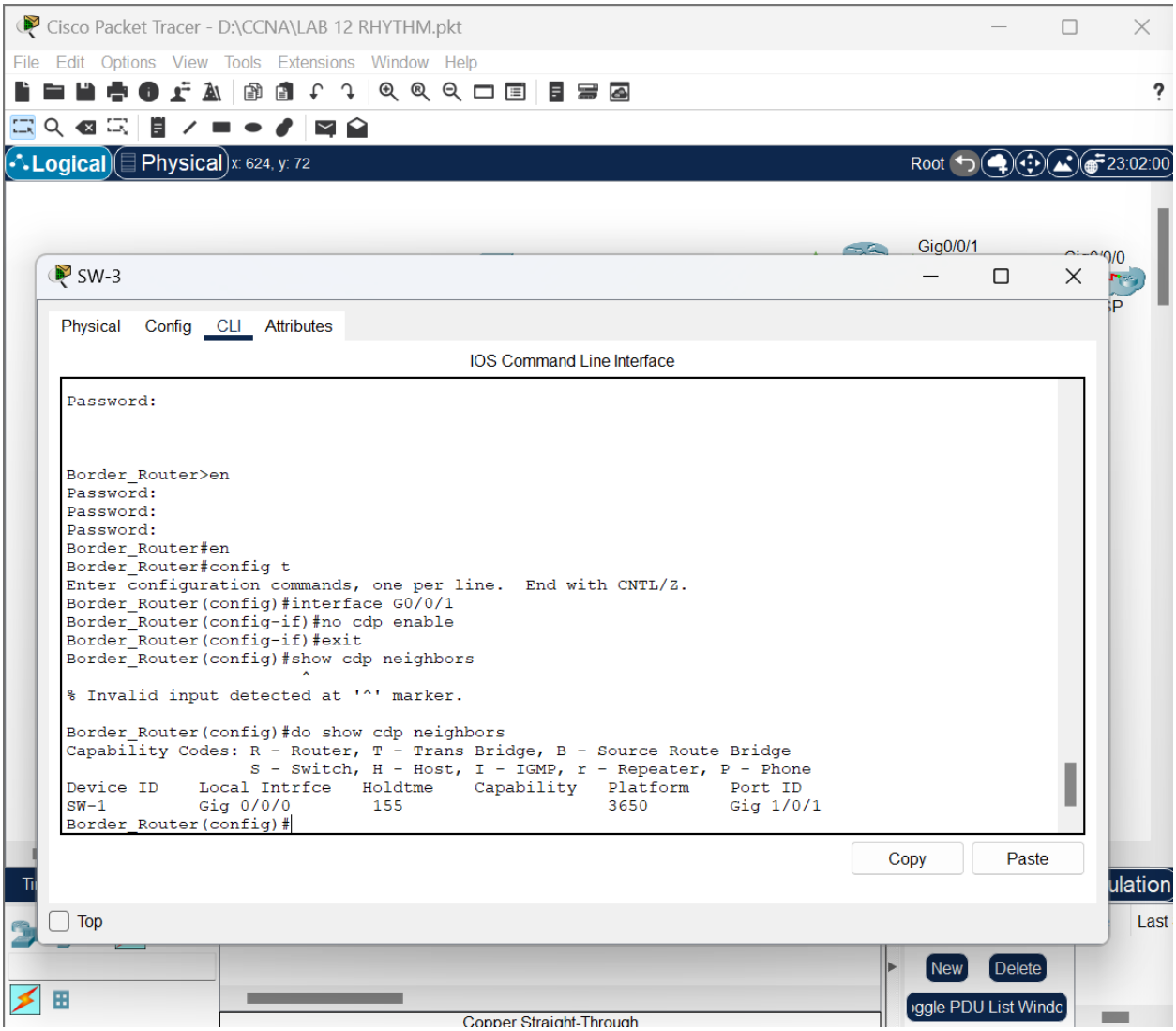


Step 5: Use CDP to Discover Neighbouring Devices:

- 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***



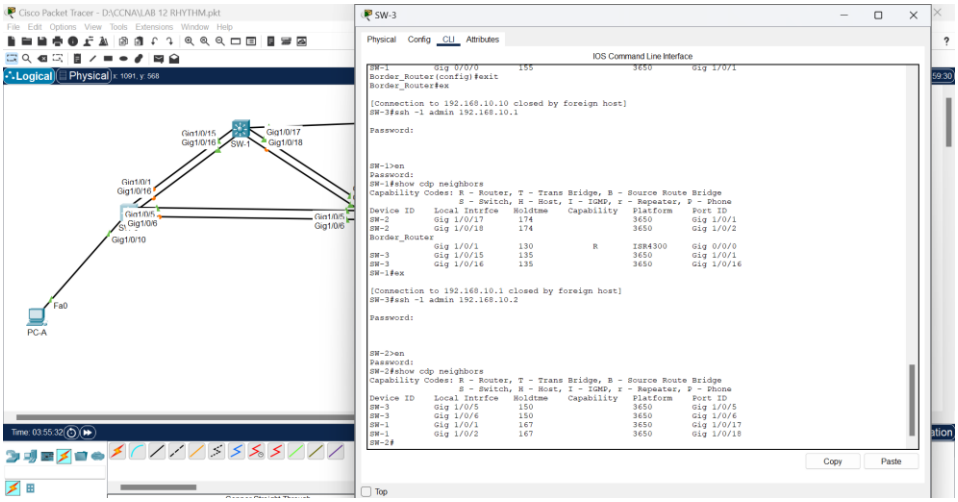
- You need to turn on CDP globally on all the three switches and Border_Router if needed, but it is a good idea to only broadcast CDP information to internal network devices and not to external networks. To do this, after turning on the CDP protocol on all intermediary devices, disable CDP on the G0/0/1 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***

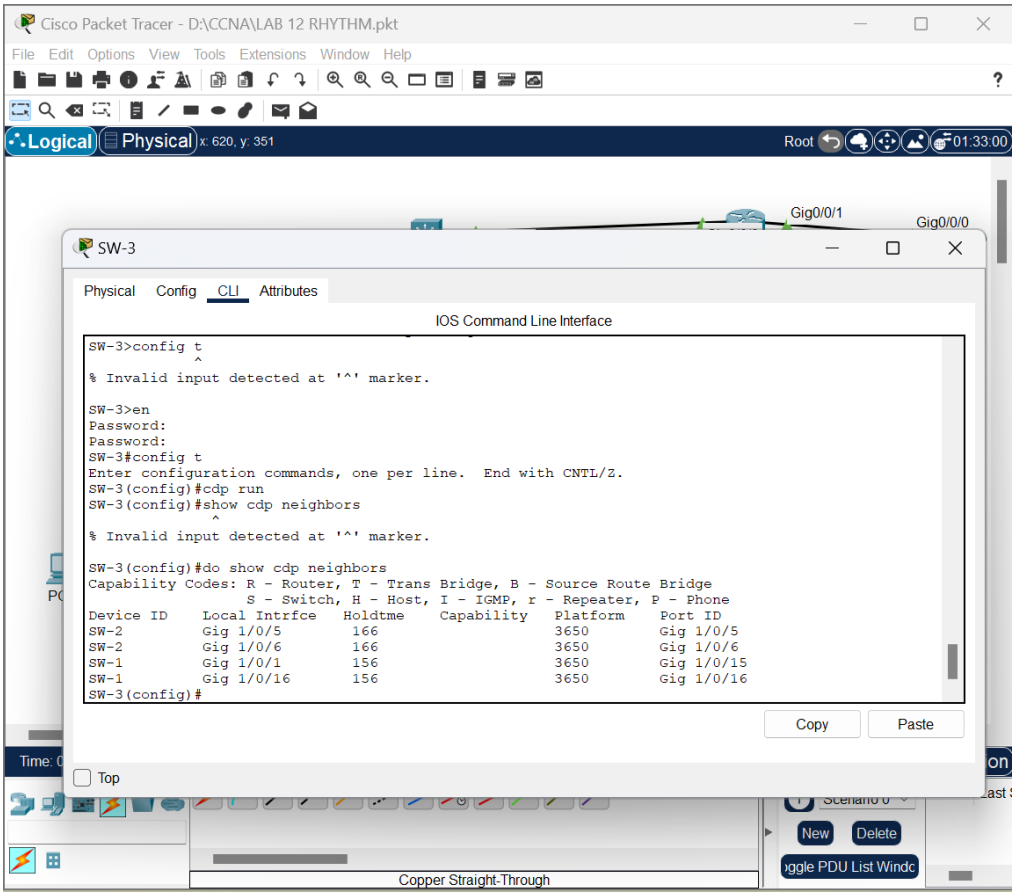


- Issue a **show cdp neighbors** command at SW-3 to find any neighbouring network devices.

  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:

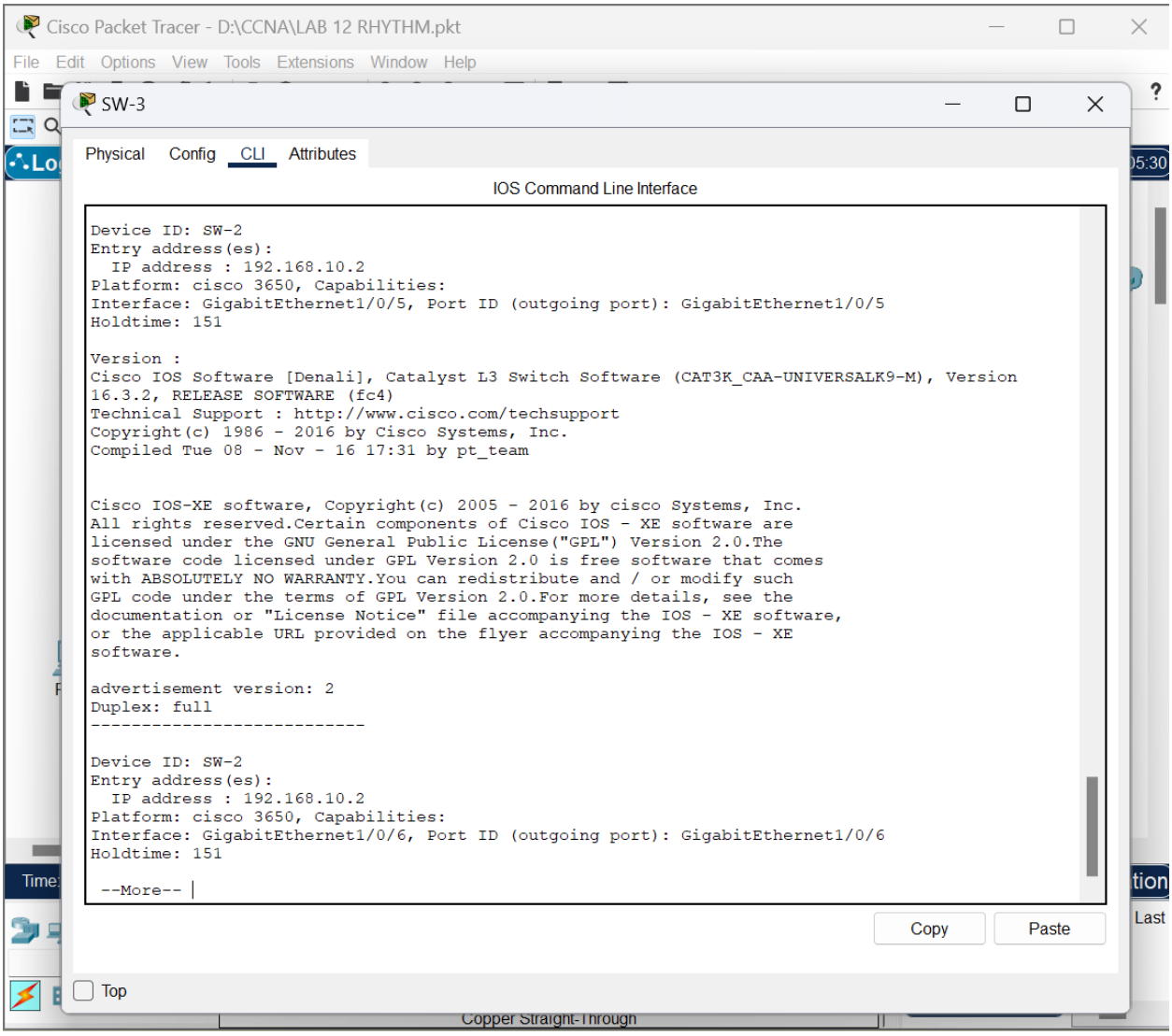
- Is there a neighbouring network device? YES
- What type of device is it? Switches and Router
- What is its name? SW-2, SW-1, SW-3 and Border_Router
- On what interface is it connected? (In case of SW-3)
- Gig 1/0/5, Gig 1/0/6 to SW-2 and
- Gig 1/0/1, Gig 1/0/16 to SW-1

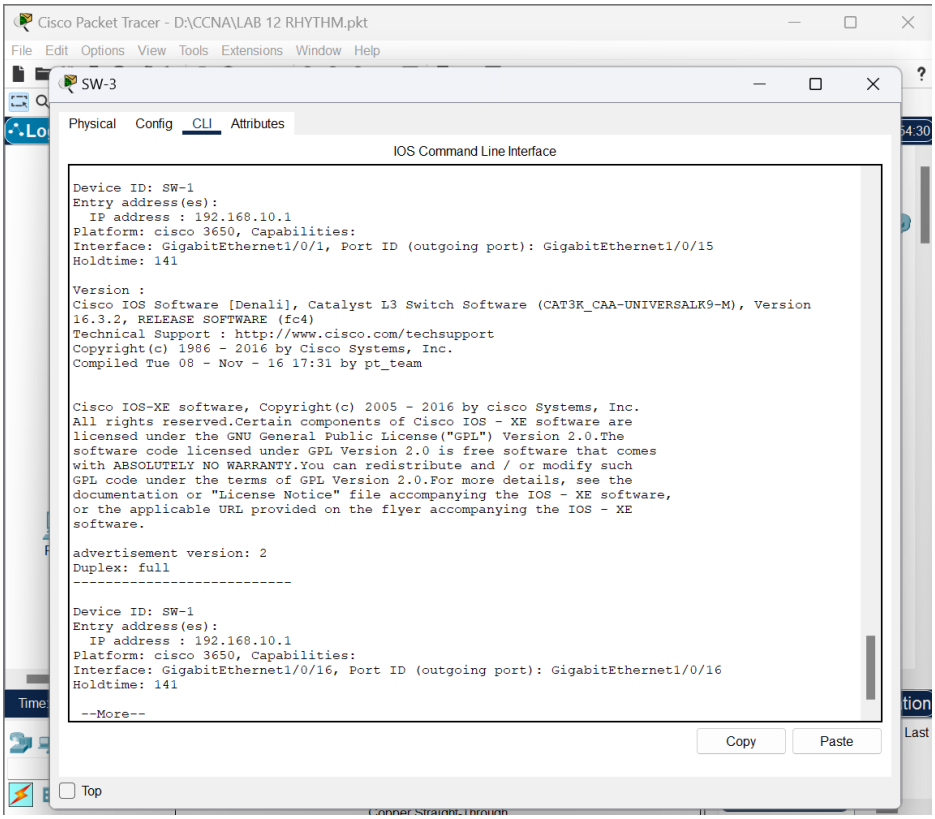
- Is the device's IP address listed? No

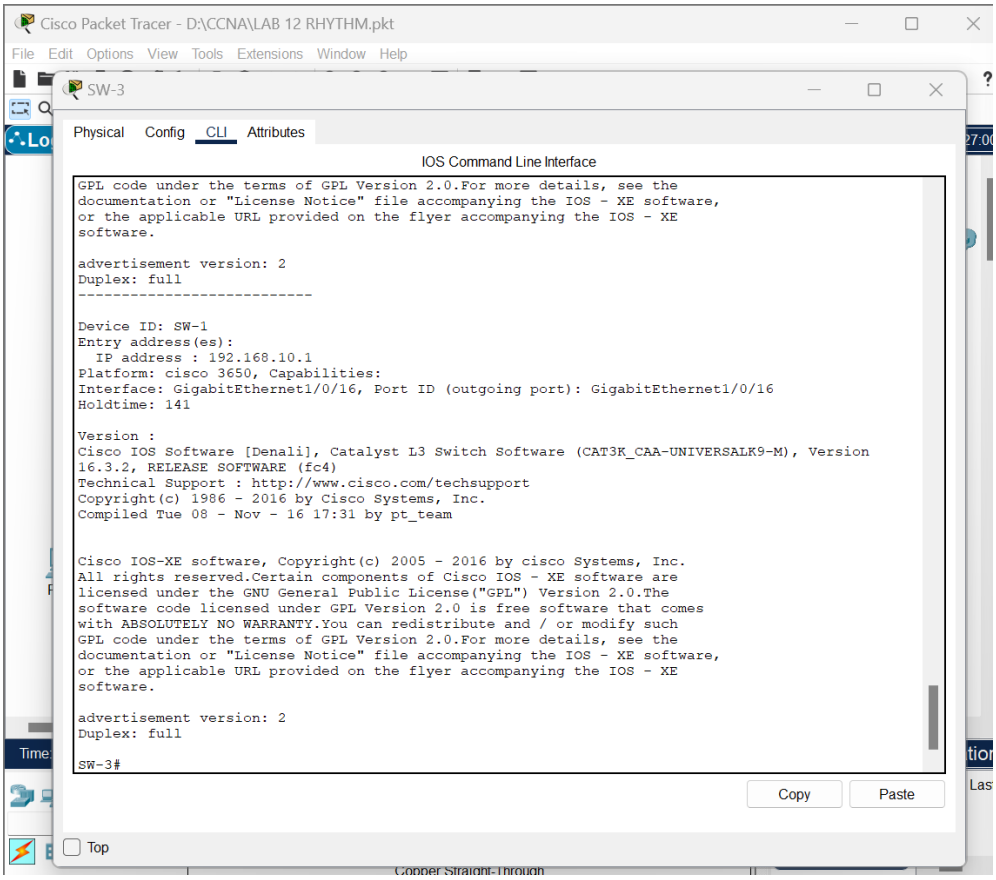
  Record the information from the answers to these questions in the Addressing Table above.

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***



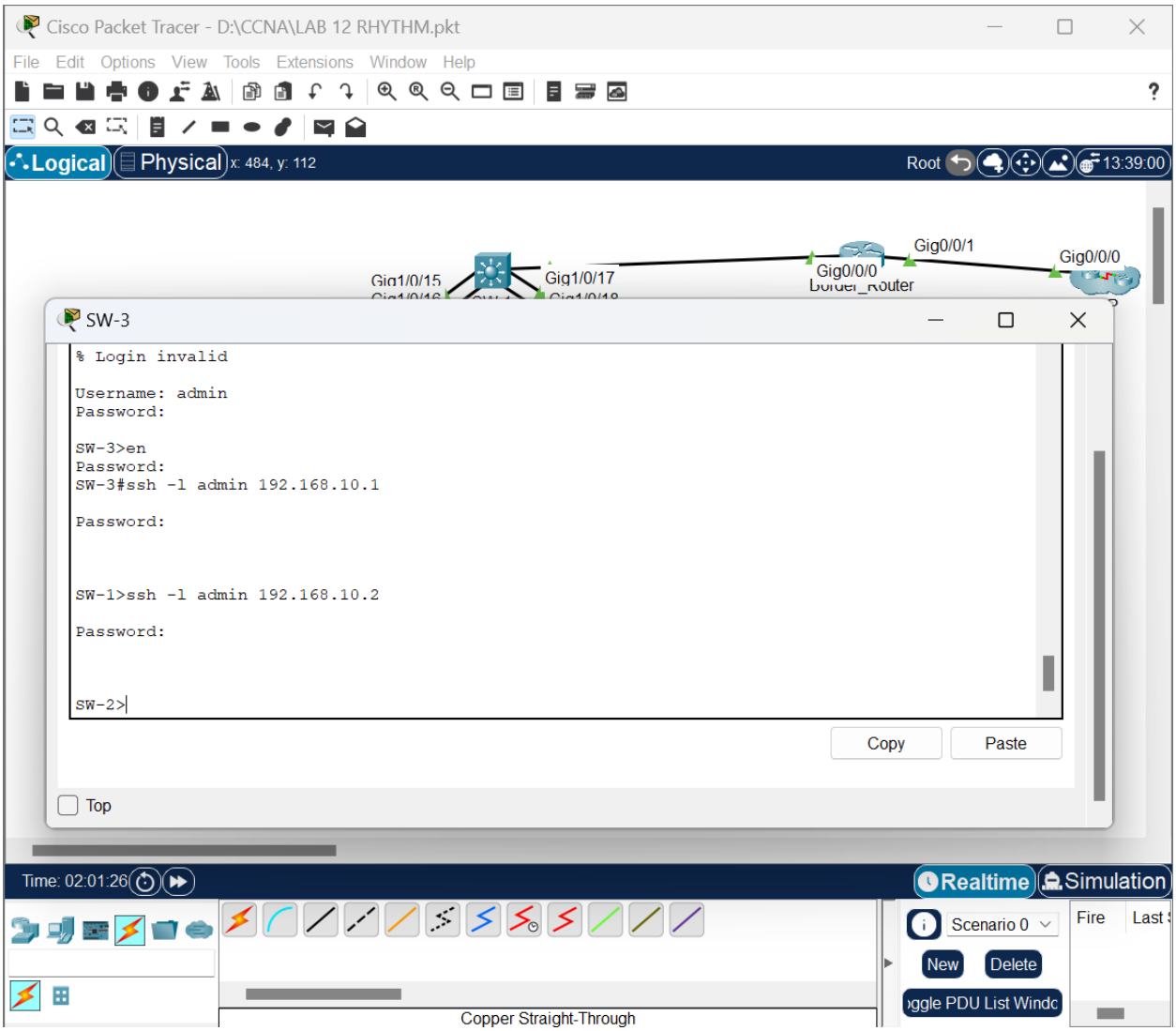

Cisco Packet Tracer - D:\CCNA\LAB 12 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
SW-3
Physical Config CLI Attributes
IOS Command Line Interface
Device ID: SW-1
Entry address(es):
IP address : 192.168.10.1
Platform: cisco 3650, Capabilities:
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): GigabitEthernet1/0/15
Holdtime: 141
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
Device ID: SW-1
Entry address(es):
IP address : 192.168.10.1
Platform: cisco 3650, Capabilities:
Interface: GigabitEthernet1/0/16, Port ID (outgoing port): GigabitEthernet1/0/16
Holdtime: 141
--More--
Copy
Paste
Top


Cisco Packet Tracer - D:\CCNA\LAB 12 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
SW-3
Physical Config CLI Attributes
IOS Command Line Interface
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
Device ID: SW-1
Entry address(es):
IP address : 192.168.10.1
Platform: cisco 3650, Capabilities:
Interface: GigabitEthernet1/0/16, Port ID (outgoing port): GigabitEthernet1/0/16
Holdtime: 141
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
SW-3#
Copy
Paste
Top

Question:

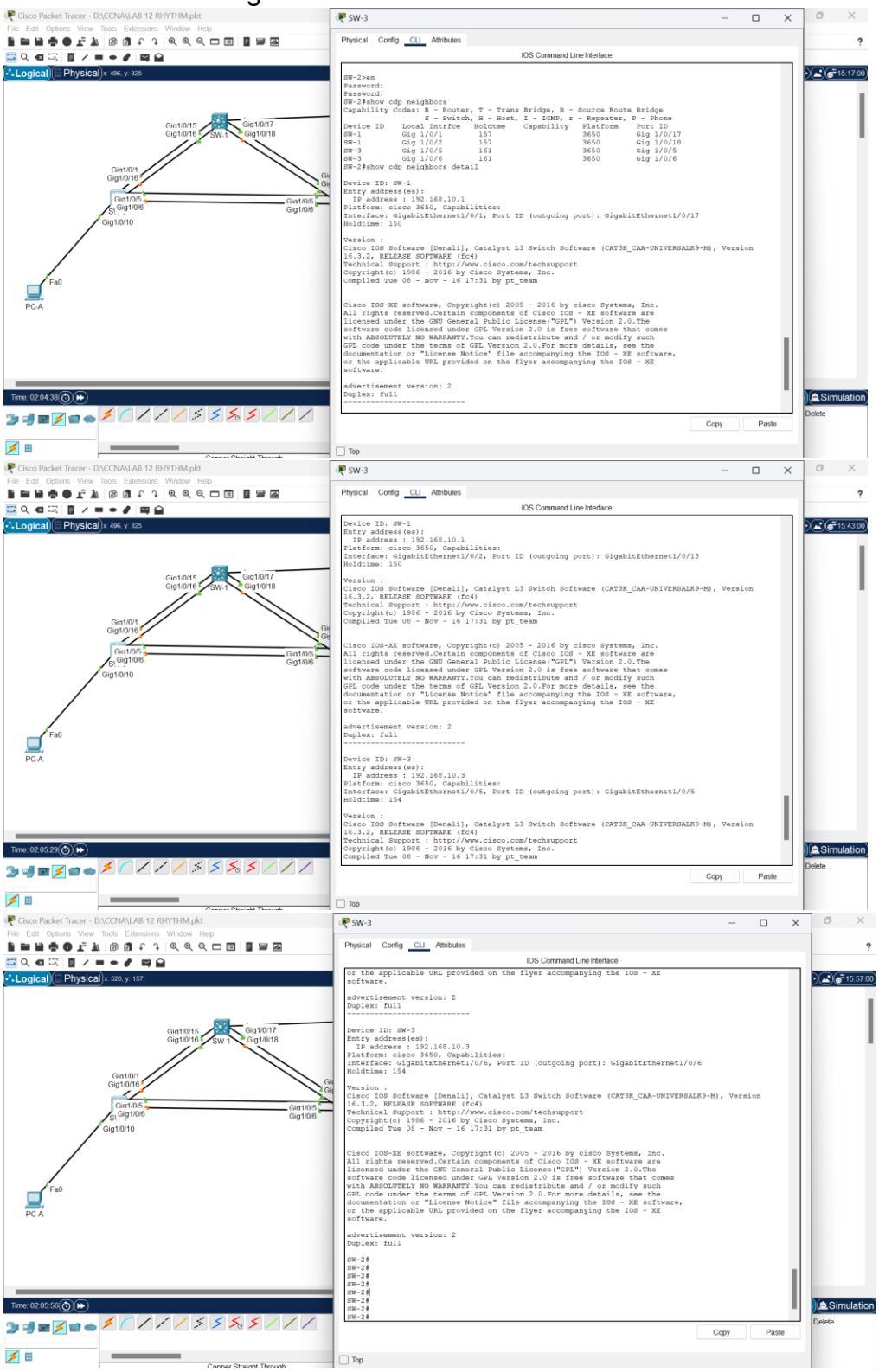
- Aside from the neighbouring device's IP address, what other piece of potentially sensitive information is listed?
  Answer: Version: Show neighboring device version
  Platform: Model of the neighboring Device
  Copy right Support
- Now that you know the IP address of the neighbour device, connect to 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.



Question:

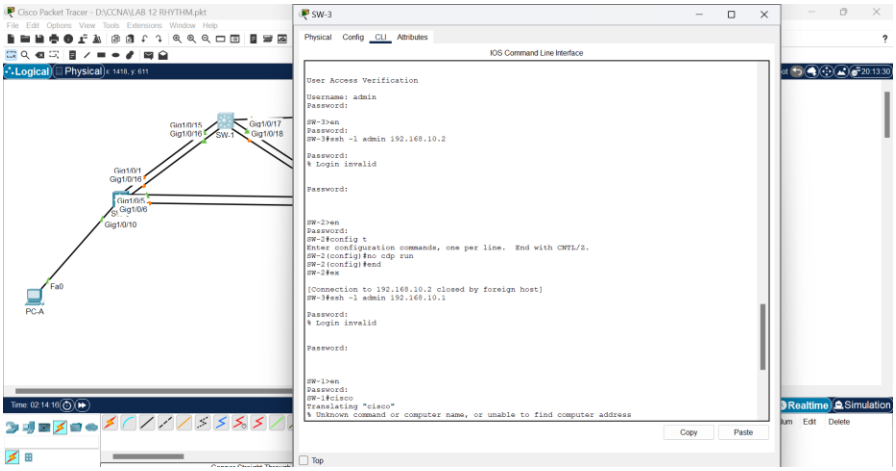
- What types of network devices neighbour this device? Switches SW1 and SW3

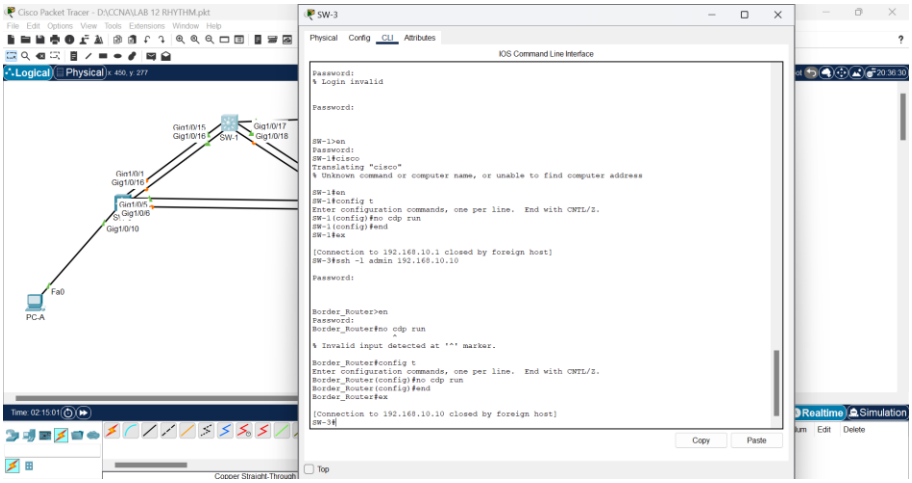
  Record any newly discovered devices in the Addressing Table above. Include their hostname, interfaces, and IP addresses.

- 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

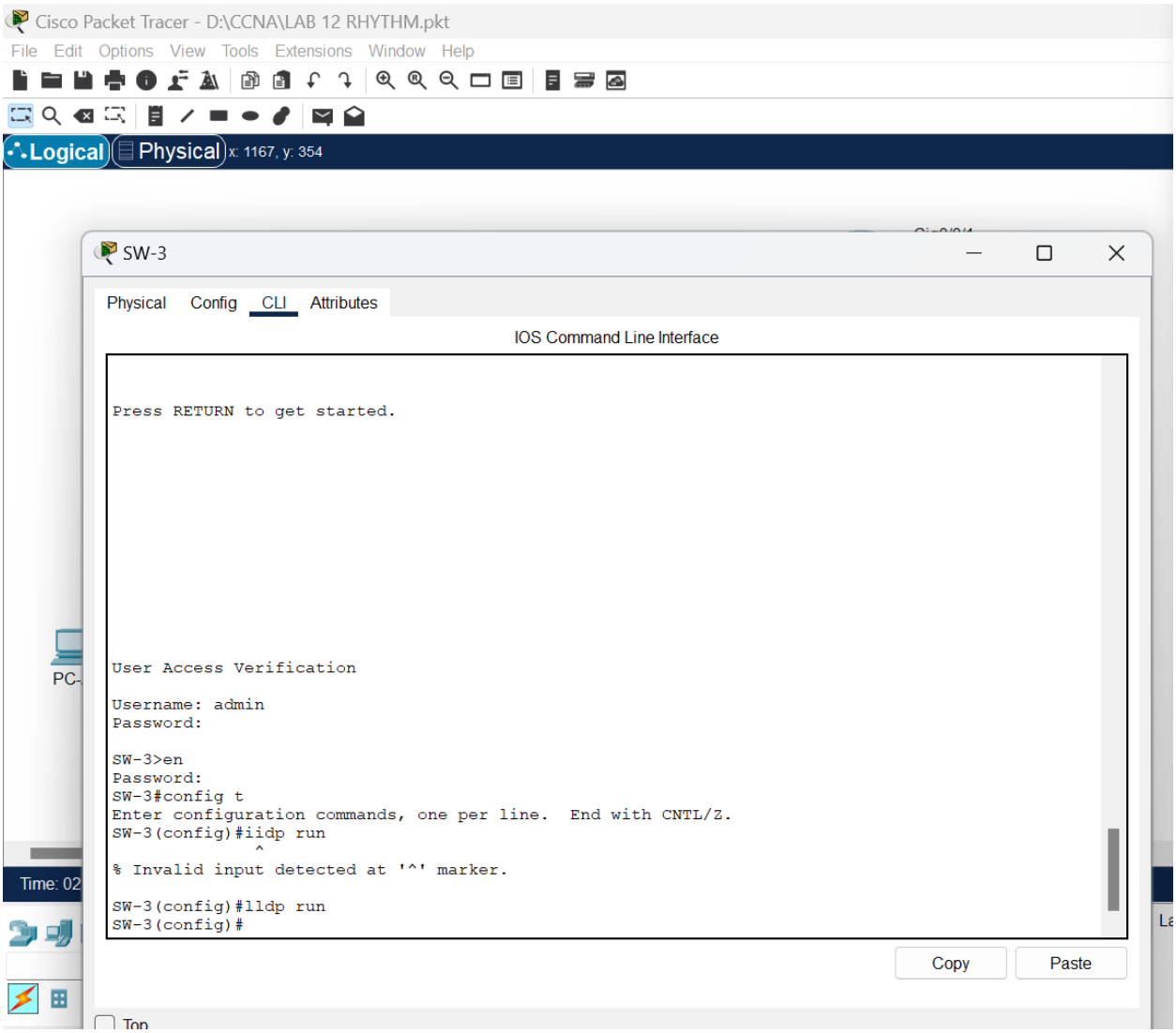
Step 6: Use LLDP to discover neighbouring devices:

- 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***

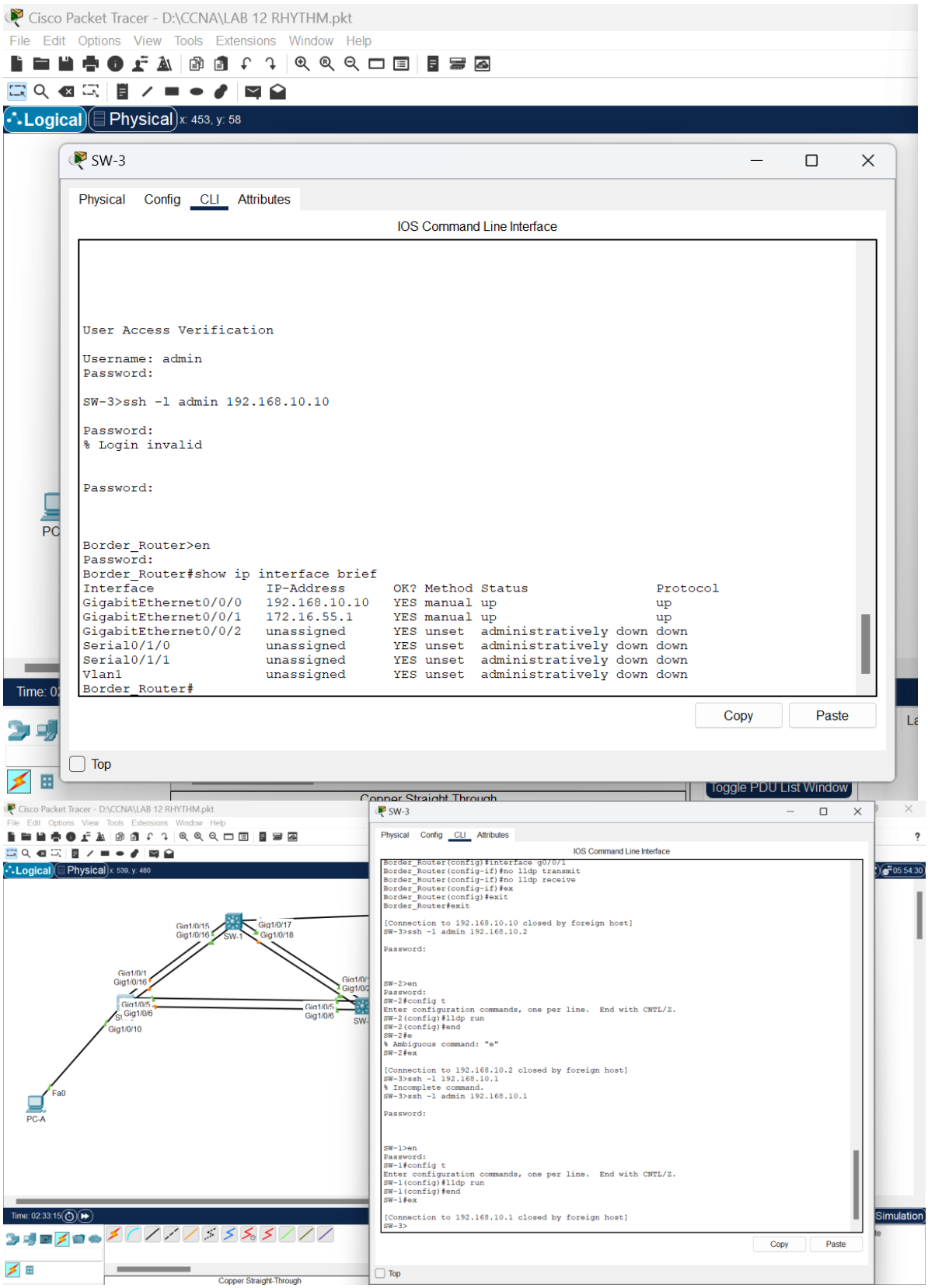




- LLDP can be configured to both transmit and receive on a specific interface. Configure SW-3 so it receives LLDP messages from other devices.
    - SW-3 (config)# ***lldp run***

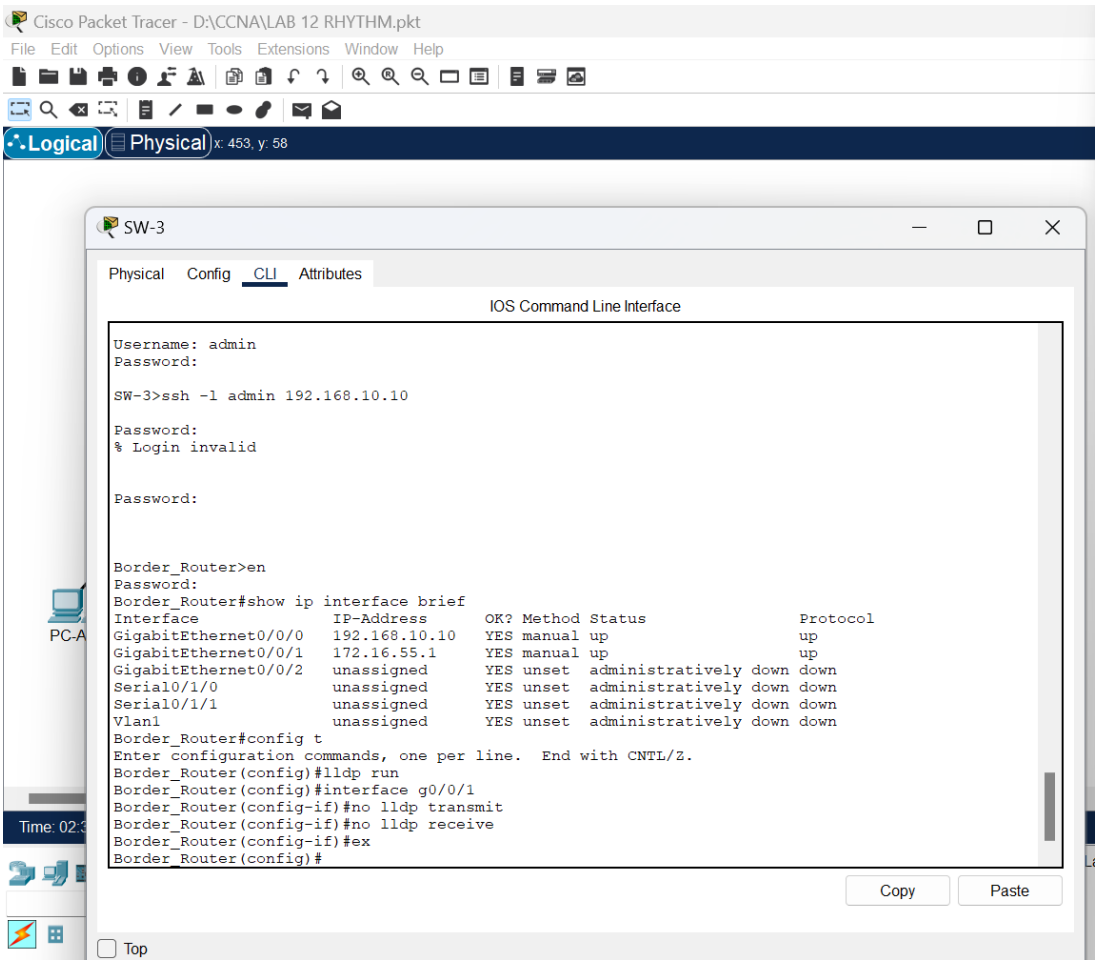


- You need to turn on LLDP globally on all the three switches and Border_Router using the command **lldp run**, but due to security concerns it is a good idea to only send LLDP information to internal network devices and not to external networks. Discover which interface is connected to the internet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

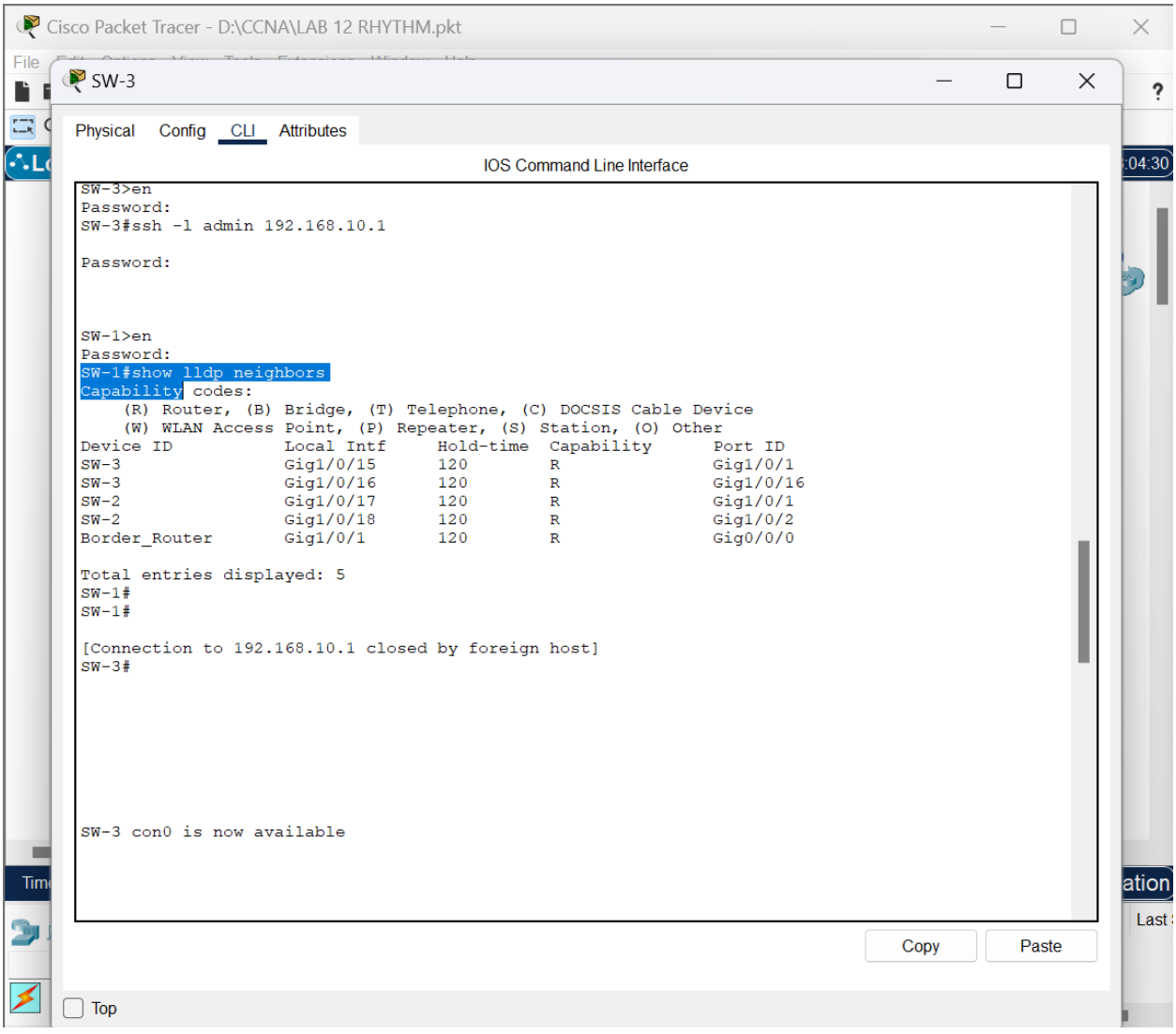


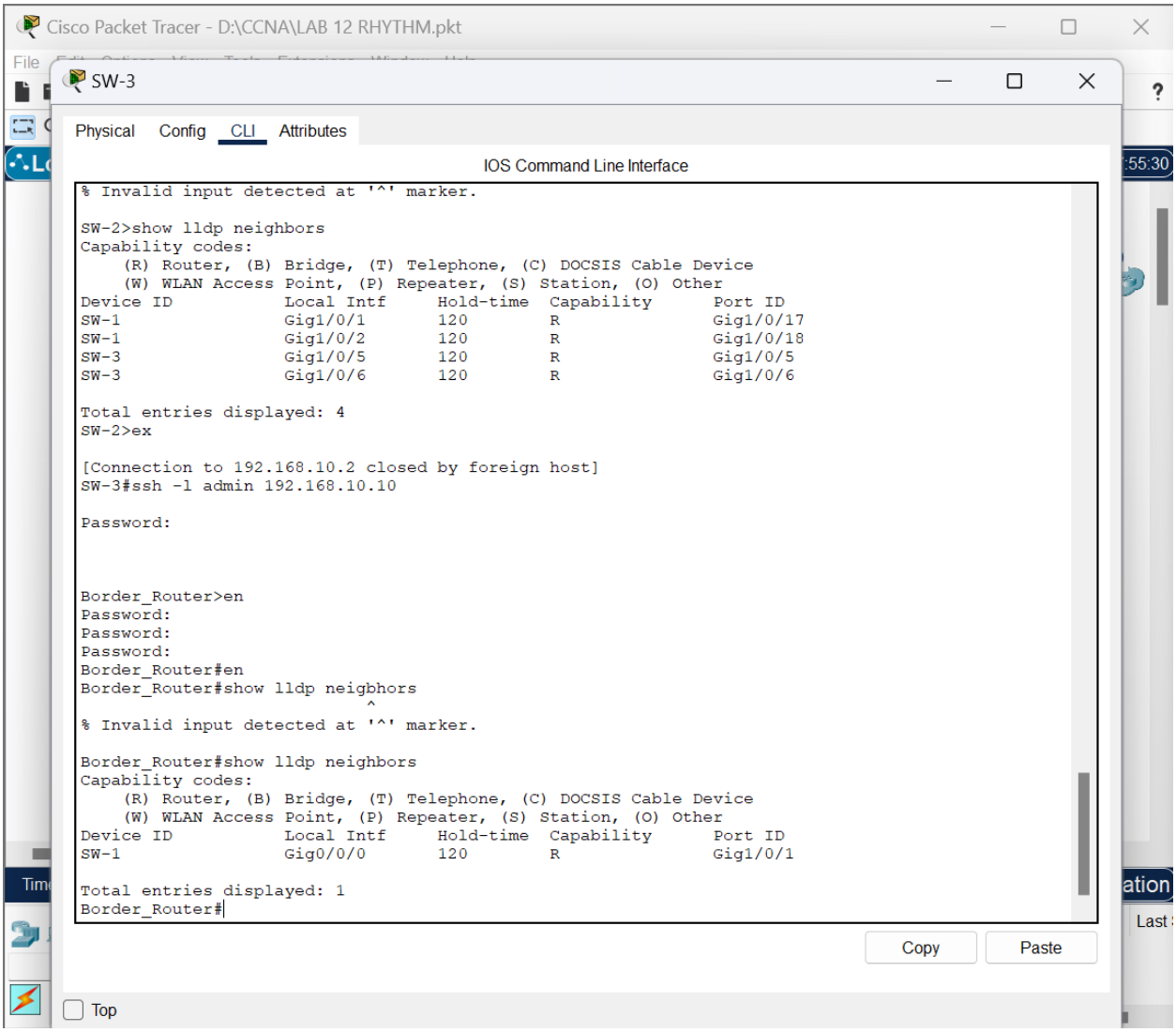
- Enable the LLDP protocol and completely disable LLDP on the interface that is connected to the internet.

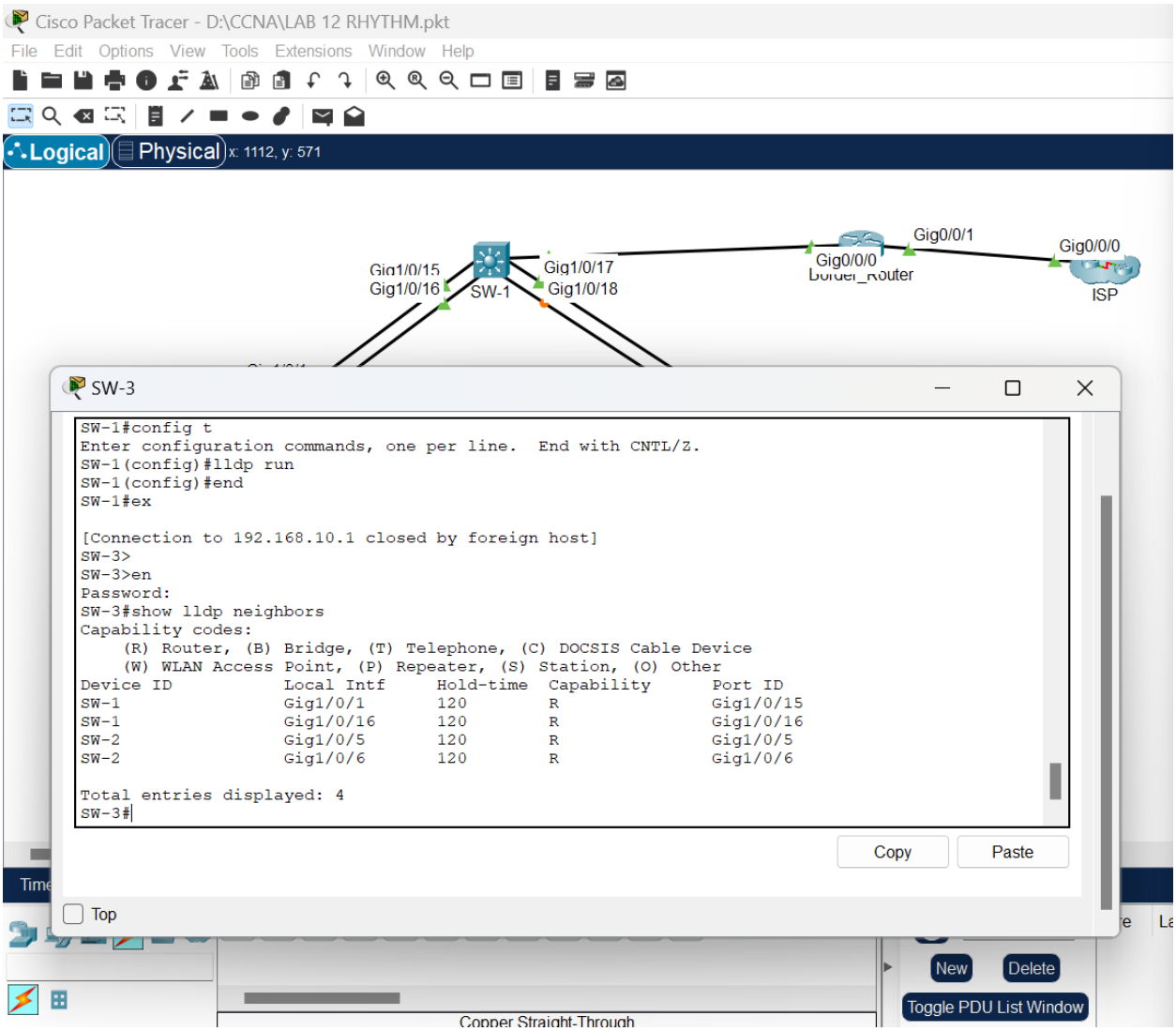
- Border_Router (Config) # ***lldp run***
- Border_Router (Config) # ***interface G0/0/1***
- Border_Router (Config-if) # ***no lldp transmit***
- Border_Router (Config-if) # ***no lldp receive***
- Border_Router (Config-if) # ***exit***



- 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
SW-3
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
SW-2>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 Gig1/0/17
SW-1 Gig1/0/2 120 R Gig1/0/18
SW-3 Gig1/0/5 120 R Gig1/0/5
SW-3 Gig1/0/6 120 R Gig1/0/6
Total entries displayed: 4
SW-2>ex
[Connection to 192.168.10.2 closed by foreign host]
SW-3#ssh -l admin 192.168.10.10
Password:
Border_Router>en
Password:
Password:
Password:
Border_Router#en
Border_Router#show lldp neigbhors
^
% Invalid input detected at '^' marker.
Border_Router#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 Gig0/0/0 120 R Gig1/0/1
Total entries displayed: 1
Border_Router#
Copy
Paste
Top


Cisco Packet Tracer - D:\CCNA\LAB 12 RHYTHM.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 1112, y: 571
Gig1/0/15
Gig1/0/16
SW-1
Gig1/0/17
Gig1/0/18
Gig0/0/1
Gig0/0/0
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
New
Delete
Toggle PDU List Window
Copper Straight-Through

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**