Lab Virtual Lab Build 1 - CML

Introduction

I designed and built a virtual network in Cisco Modeling Lab (CML) using one virtual firewall, one virtual network switch, and four virtual machines running Kali Linux, Windows 10, Windows 11, and Windows 7. The network was configured according to the specified requirements: all devices were interconnected, powered on, and verified as operational. I created a detailed network diagram in Microsoft Visio showing the layout of all components and their connections. Screenshots included in this document confirm that each device is active and communicating within the lab environment. Additionally, I documented a complete, step-by-step rebuild guide that outlines every action taken from launching CML to configuring each machine so the entire network can be replicated exactly as built. This submission contains all required deliverables: the network diagram, device status proof, and rebuild instructions, fully reflecting the work completed in this lab.

Device Status Proof

SW01

```
However, the shell is currently disabled. You can enable
it on this terminal by typing
   'term shell'
You can also enable it for all terminals by configuring the
   'shell processing full'
command. There is additional information in the man command.
For more information, enable shell, and then enter:
'man IOS.sh'
SW01>term shell
SW01>fetch

*Sep 12 22:38:27.209: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/1 TDR=0, TRC=0
% Bad IP address or host name% Unknown command or computer name, or unable to find compute
SW01>
SW01>
*Sep 12 22:38:57.236: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/1 TDR=0, TRC=0
SW01>
*Sep 12 22:39:27.271: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/1 TDR=0, TRC=0
SW01>
```

CPU	0.25%	MEMORY	30.29%

FW01

Cisco Modeling Labs | Workbench   FIRST LAB ▾
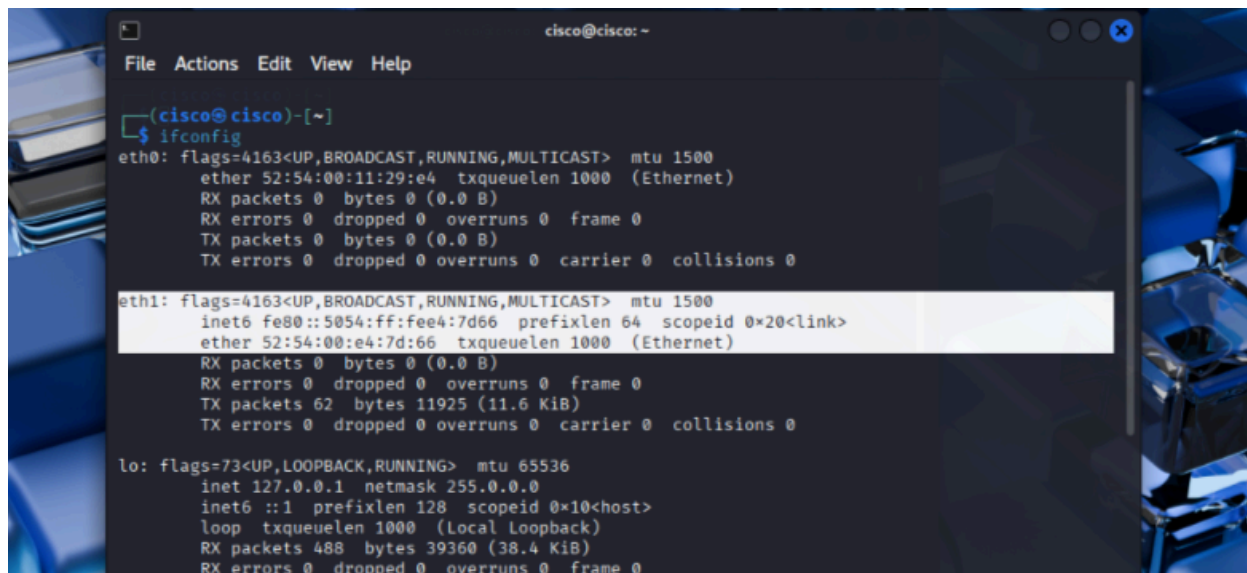
>_ SW01   >_ FW01
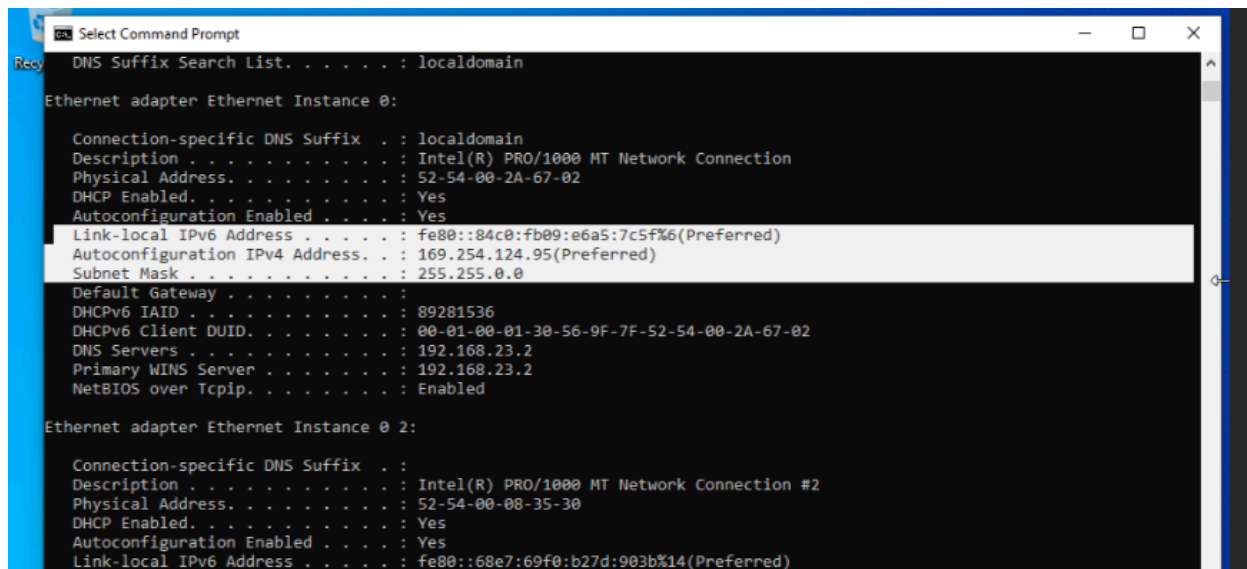
```
System is starting...
Starting system maintenance...

Scanning /dev/vda1... (0%)
Scanning /dev/vda1... (100%)

Scanning /dev/vda2... (0%)
Scanning /dev/vda2... (4%)
Scanning /dev/vda2... (12%)
Scanning /dev/vda2... (100%)
Serial number is FGVM01TM25002880


FW01 login:
```
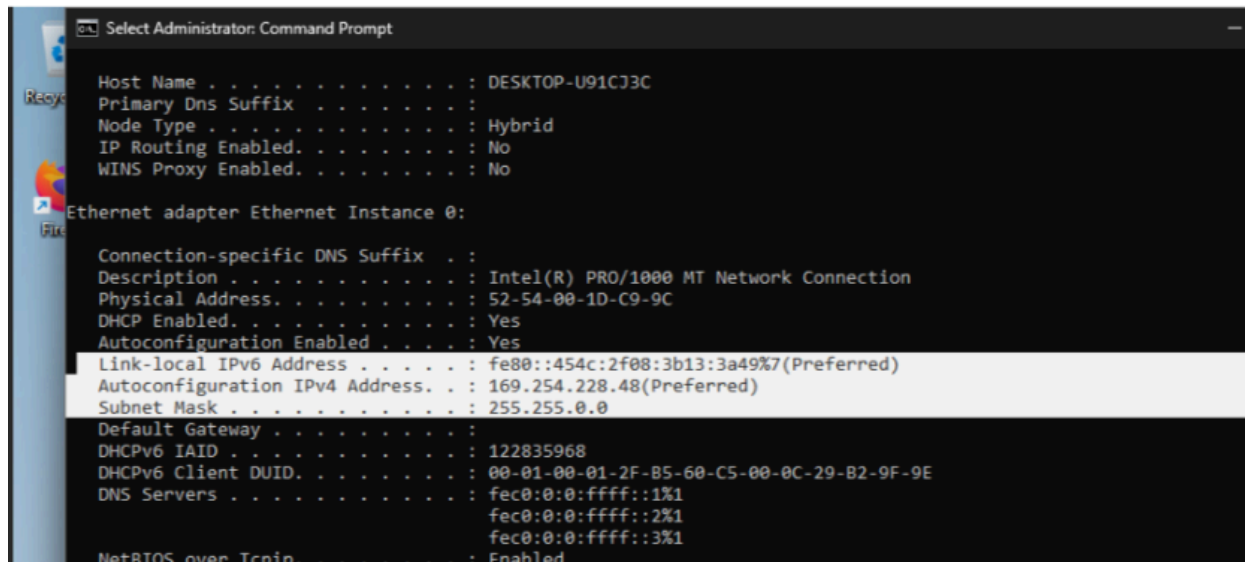
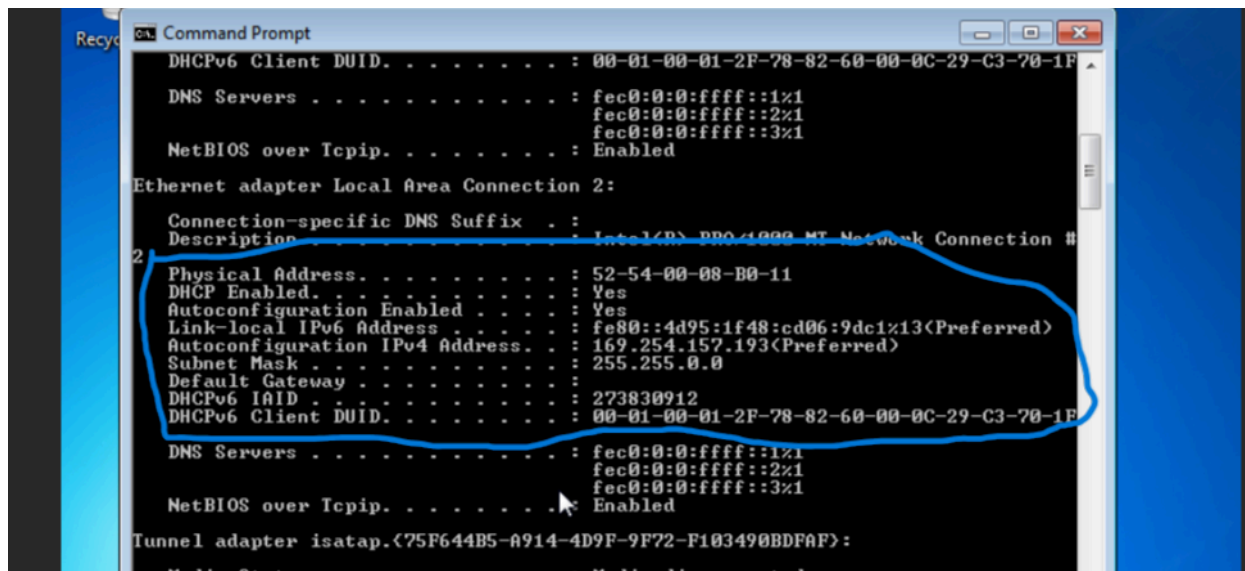## Kali

Windows10

Windows11


Windows7

Rebuild Guide

Step 1: Add the Internet Node

- Open Cisco Modeling Labs (CML).
- In the Device Library, search for "Internet" or "Cloud".
- Drag and drop it onto the workspace.
- Rename it to Internet.
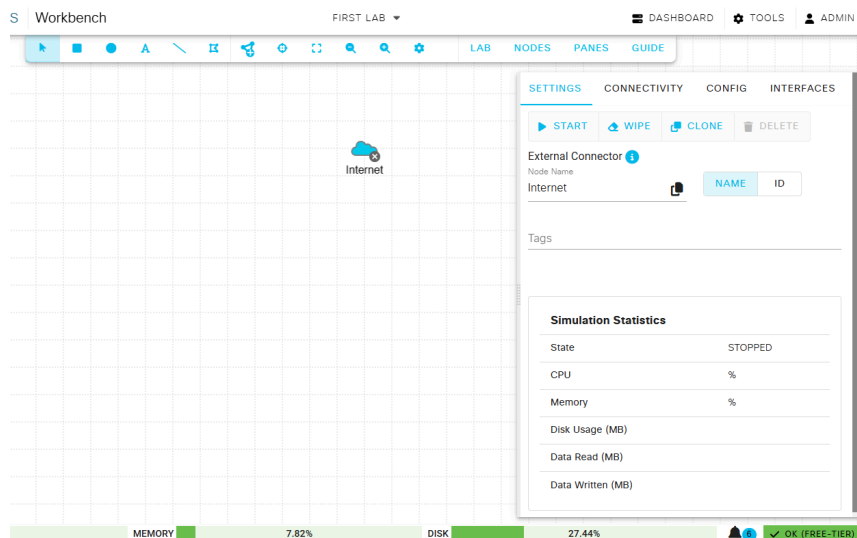
Step 2: Add the Firewall (FW01)

In the Device Library, search for "FortiGate" (as shown in your diagram).
Drag and drop it onto the workspace, placing it directly to the right of Internet.
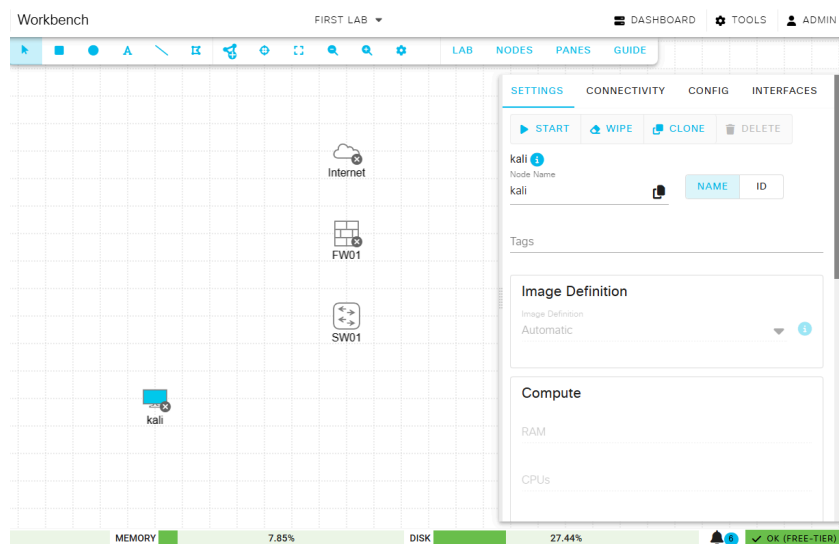Rename the device to FW01.
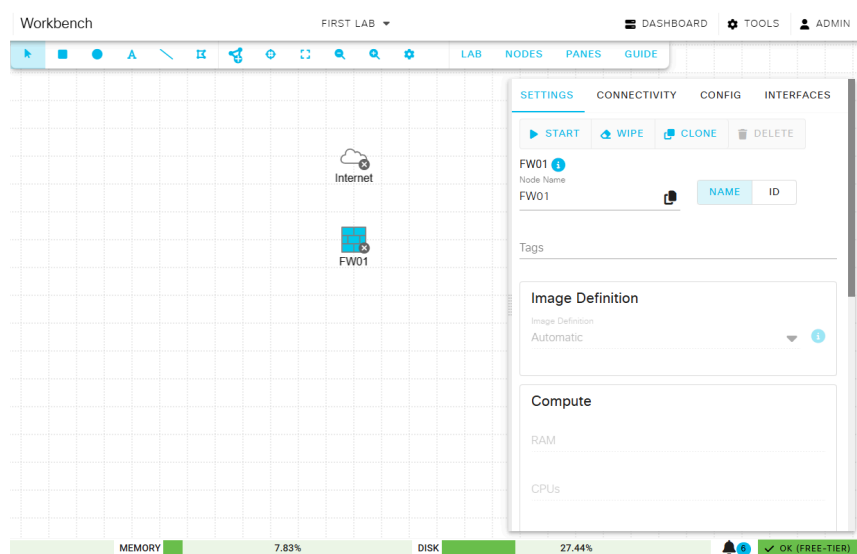
Step 3: Add the Switch (SW01)
- In the Device Library, search for "FW (Bricks)" (Layer 2 switch).
- Drag and drop it onto the workspace, placing it directly to the right of FW01.
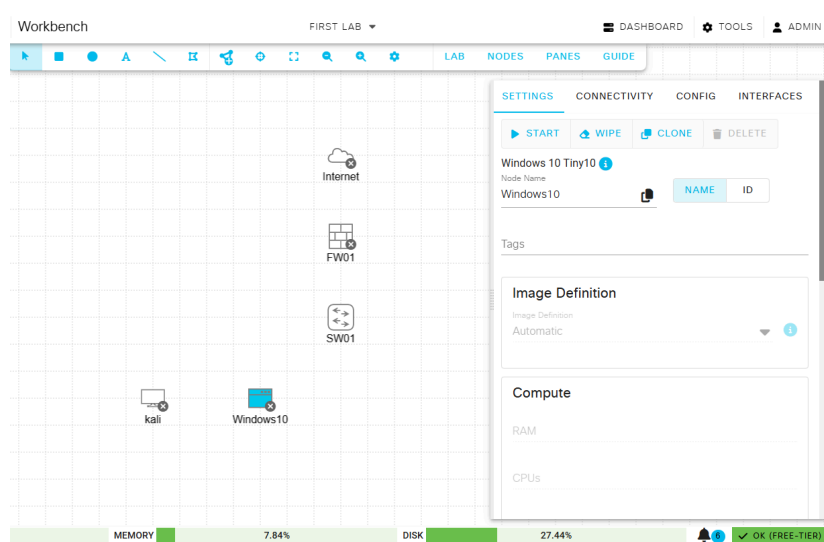- Rename the device to SW01.
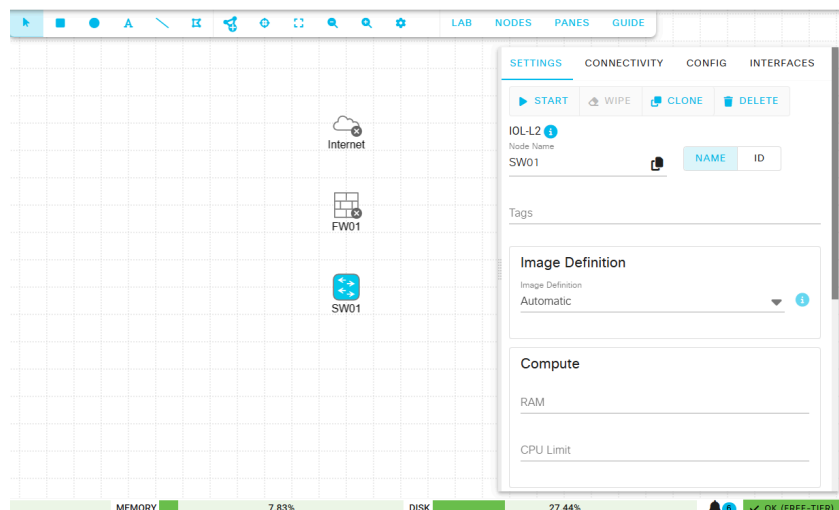
Step 4: Add Kali Linux VM
- In the Device Library, search for "Kali Linux".
- Drag and drop it onto the workspace, placing it below SW01 to the left.
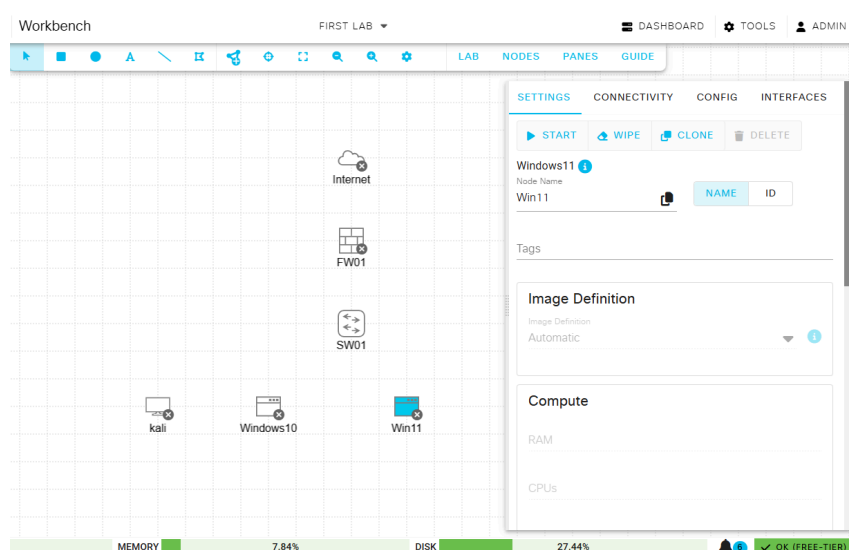- Rename the device to Kali.

Step 5: Add Windows 10 VM
- In the Device Library, search for "Tiny10 - Windows 10".
- Drag and drop it onto the workspace, placing it below SW01 and to the right of Kali.

● Rename the device to Windows10.

Step 6: Add Windows 11 VM

● In the Device Library, search for "Windows 11".
● Drag and drop it onto the workspace, placing it below SW01 and to the right of Windows 10.
● Rename the device to Windows11.

Step 7: Add Windows 7 VM

● In the Device Library, search for "Windows 7".
● Drag and drop it onto the workspace, placing it below SW01 and to the right of Windows 11.
● Rename the device to Windows7.
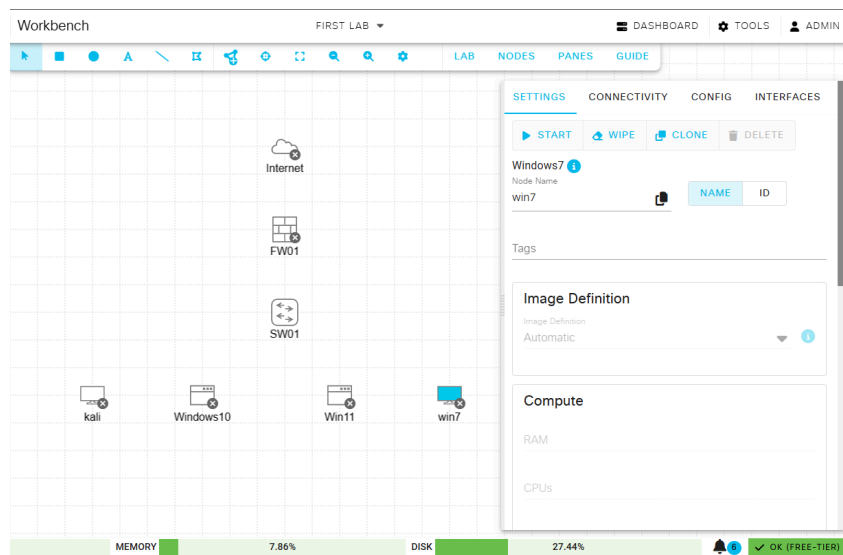
Step 8: Connect Internet to FW01

- Click the Connect tool (cable icon) at the top of CML.
- Click on Internet → select interface Ethernet0/0 (or default port).
- Click on FW01 → select Ethernet0/0 (as labeled in your diagram).
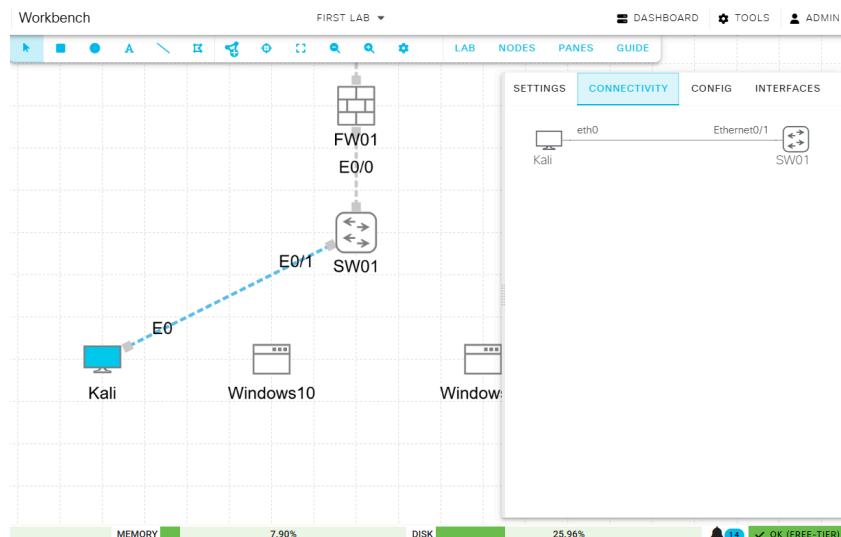- A link should appear.
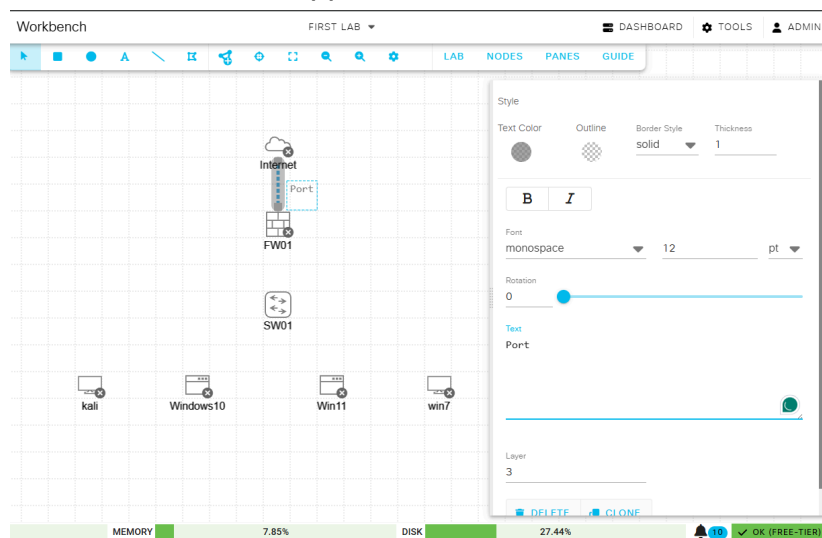
Step 9: Connect FW01 to SW01

- Use the Connect tool again.
- Click on FW01 → select Ethernet0/1 (as labeled in your diagram).
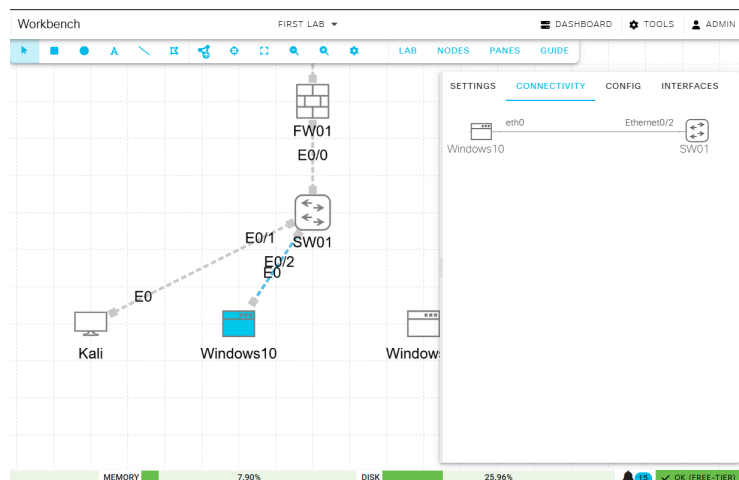- Click on SW01 → select any free port (e.g., GigabitEthernet0/0).
- A link should appear.
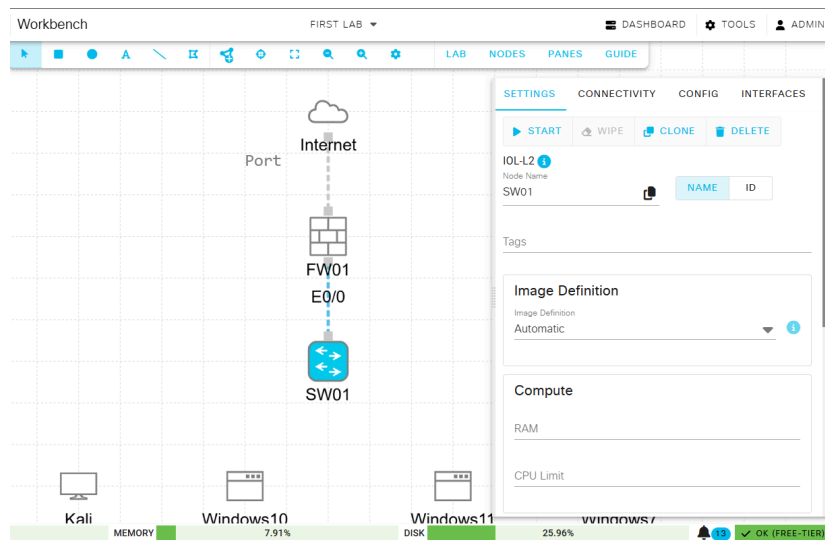
Step 10: Connect Kali to SW01

- Use the Connect tool.
- Click on Kali → select eth0.
- Click on SW01 → select next free port (e.g., GigabitEthernet0/1).
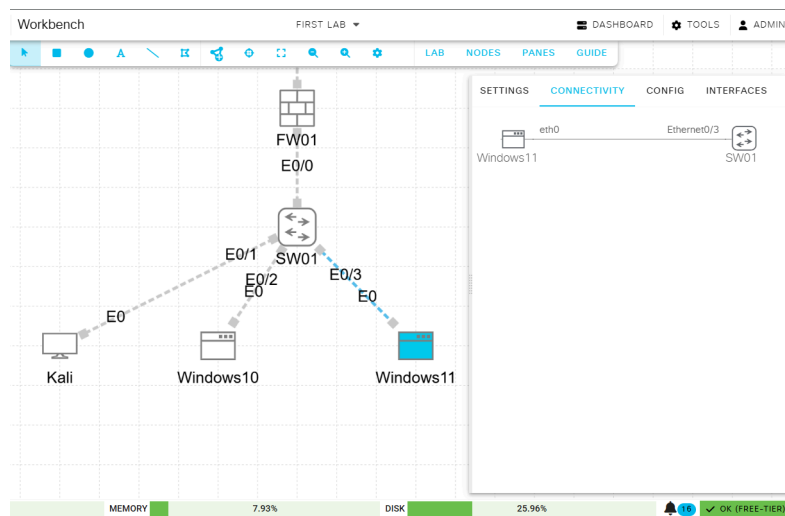- A link should appear.

Step 11: Connect Windows 10 to SW01

- Use the Connect tool.
- Click on Windows10 → select Ethernet0.
- Click on SW01 → select next free port (e.g., GigabitEthernet0/2).
- A link should appear.

Step 12: Connect Windows 11 to SW01
- Use the Connect tool.
- Click on Windows11 → select Ethernet0.
- Click on SW01 → select next free port (e.g., GigabitEthernet0/3).
- A link should appear.

Step 13: Connect Windows 7 to SW01
- Use the Connect tool.
- Click on Windows7 → select Ethernet0.
- Click on SW01 → select next free port (e.g., GigabitEthernet1/0).
- A link should appear.
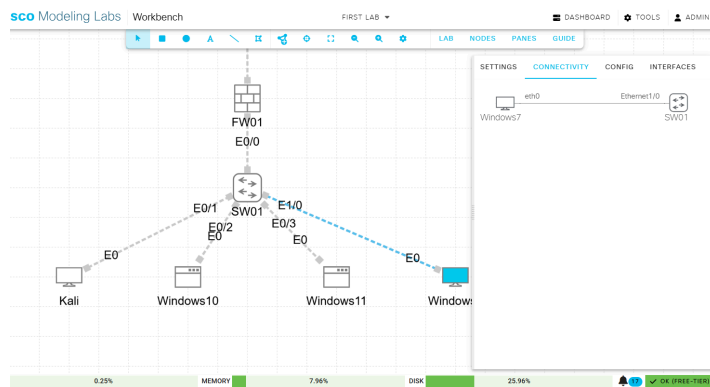
Step 14: Start the Internet Node
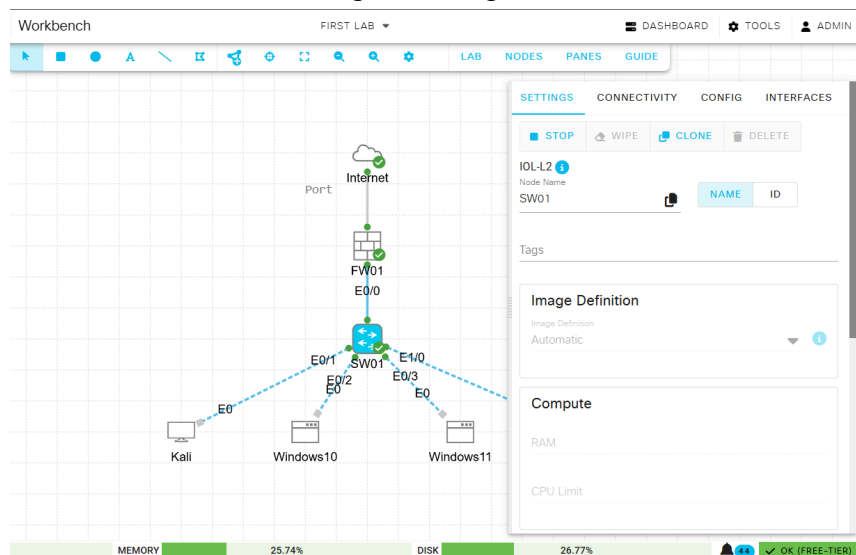- Right-click Internet → Select Start.
- Status light turns green immediately.
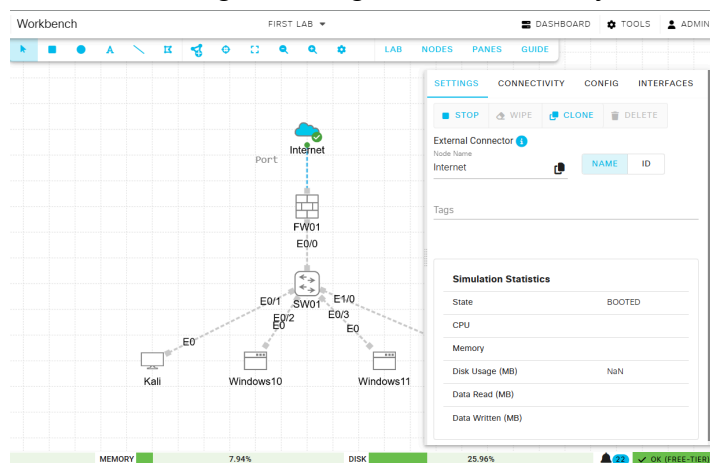
Step 15: Start the Firewall (FW01)
- Right-click FW01 → Select Start.
- Wait until status light turns green.
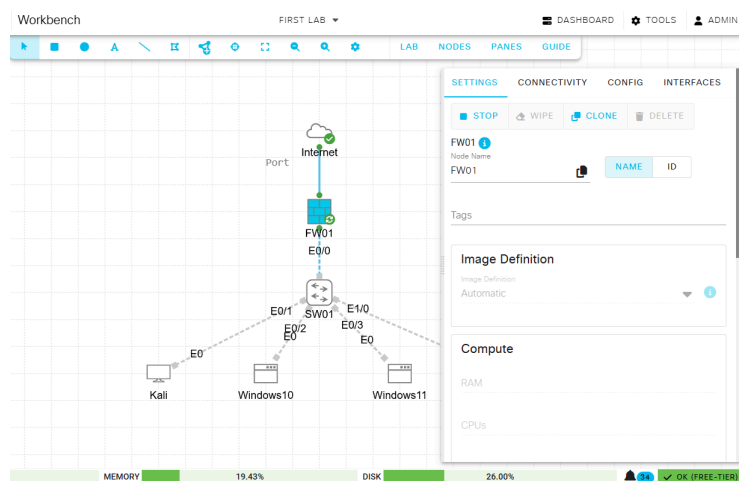
Step 16: Start the Switch (SW01)
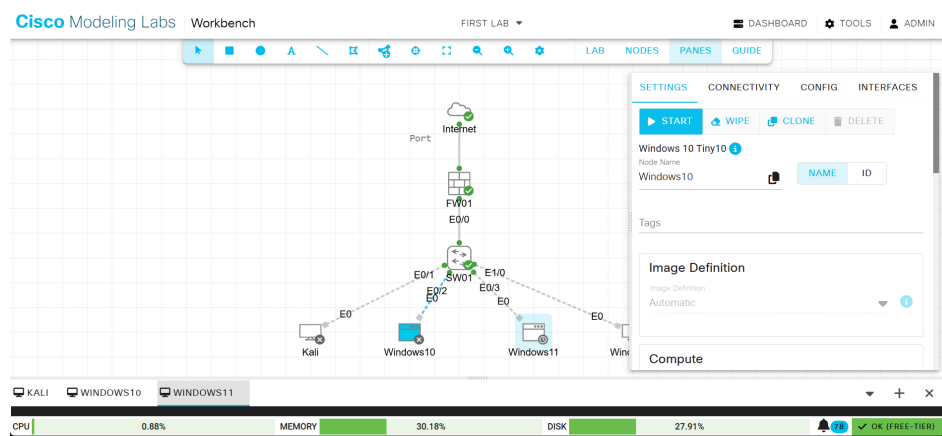- Right-click SW01 → Select Start.
- Wait until status light turns green.

Start VMs one at a time, so as not to use so much memory.

Step 17: Start Kali Linux VM
- Right-click Kali → Select Start.
- Wait for boot sequence to complete.
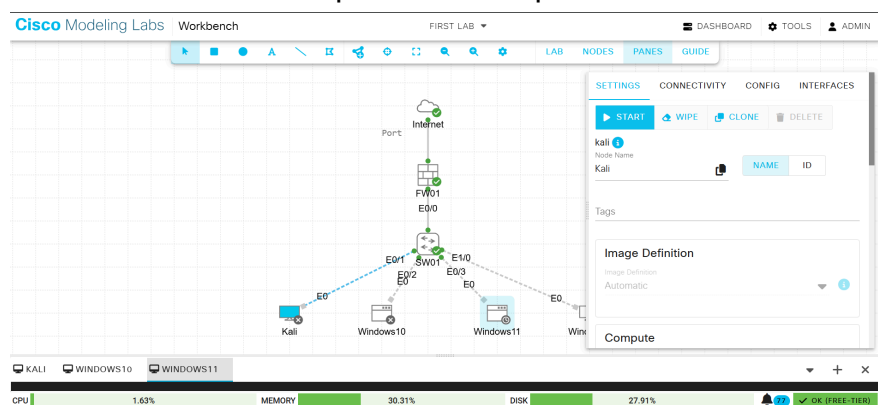
Step 18: Start Windows 10 VM
- Right-click Windows10 → Select Start.
- Wait for status light to turn green.

Step 19: Start Windows 11 VM

- Right-click Windows11 → Select Start.
- Wait for status light to turn green.
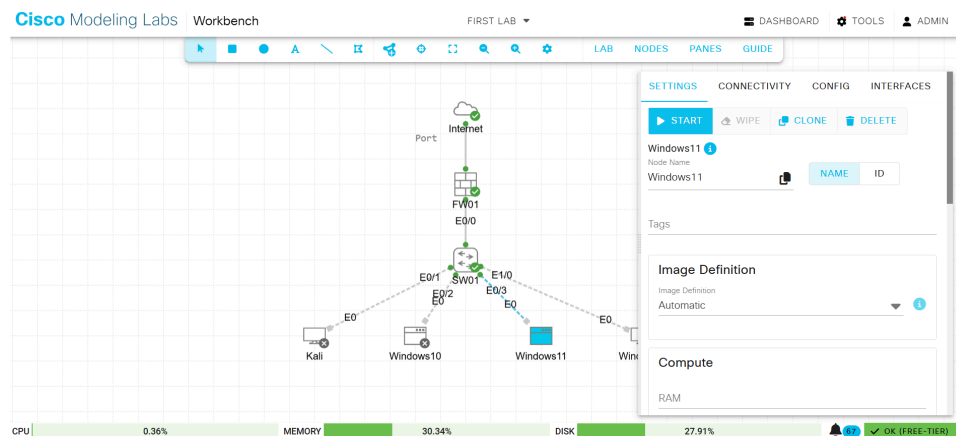
Step 20: Start Windows 7 VM

- Right-click Windows7 → Select Start.
- Wait for Windows 7 boot screen to appear.
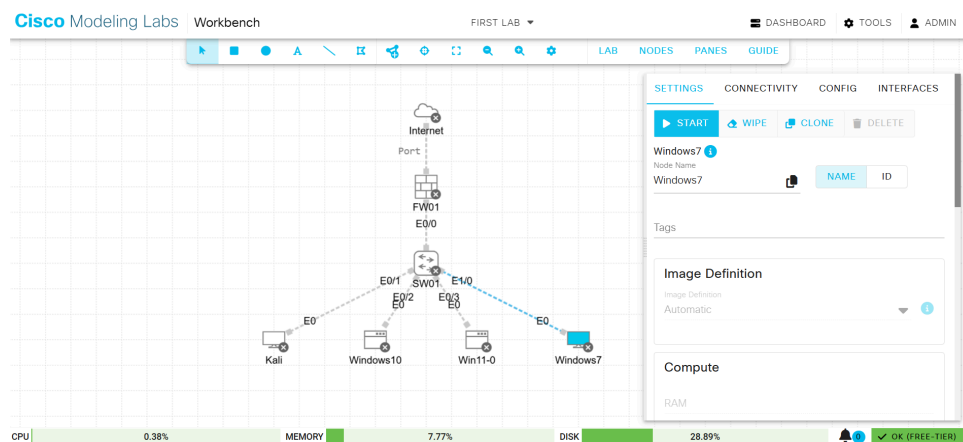
Step 21: Log in to Kali Linux
- Right-click Kali → Select Open Console.
- At the login prompt, enter:
- Username: cisco
- Password: cisco

Step 22: Set Password on Windows 7 (if prompted)
- After Windows 7 boots, you may be prompted to set a password.
- If so, click Next, then enter:
- Password: Passw0rd!
- Confirm: Passw0rd!
- Click Finish.
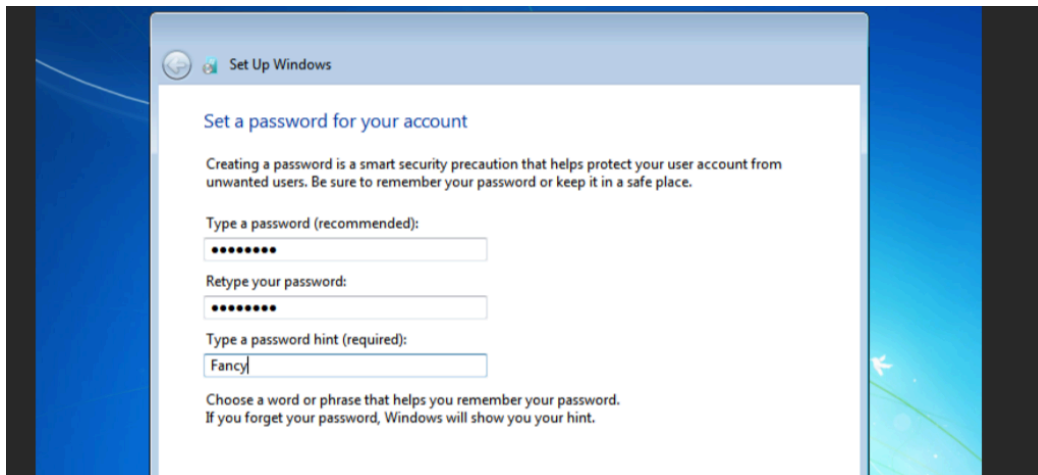
Step 26: Verify Firewall is Operational
- Right-click FW01 → Open Console.
- Make sure the login shows.

Cisco Modeling Labs | Workbench　　　　　　FIRST LAB ▾

>_ SW01　　>_ FW01

```
System is starting...
Starting system maintenance...

Scanning /dev/vda1... (0%)
Scanning /dev/vda1... (100%)

Scanning /dev/vda2... (0%)
Scanning /dev/vda2... (4%)
Scanning /dev/vda2... (12%)
Scanning /dev/vda2... (100%)
Serial number is FGVM01TM25002880


FW01 login:
```
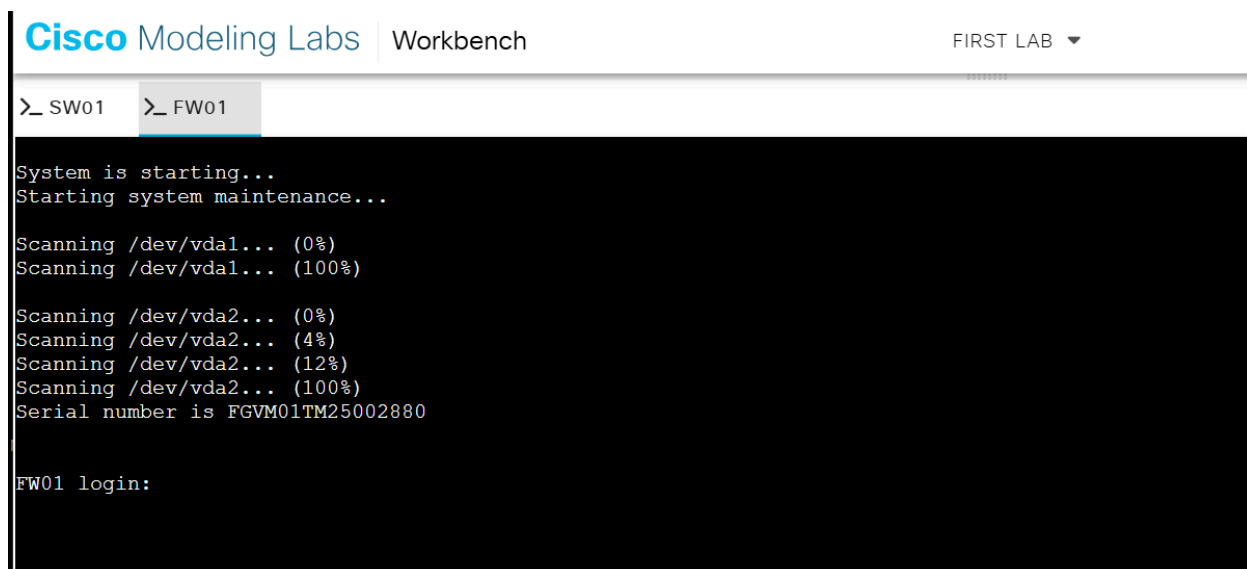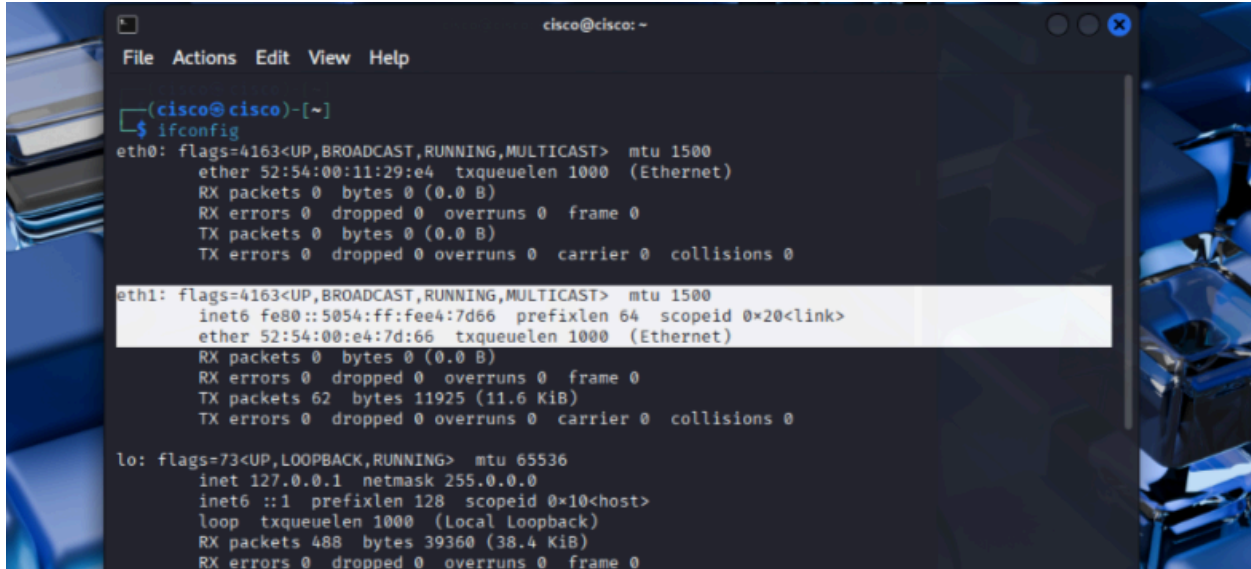
Step 27: Verify Switch is Operational

Right-click SW01 → Open Console.


```
However, the shell is currently disabled. You can enable
it on this terminal by typing
   'term shell'
You can also enable it for all terminals by configuring the
   'shell processing full'
command. There is additional information in the man command.
For more information, enable shell, and then enter:
'man IOS.sh'
SW01>term shell
SW01>fetch

*Sep 12 22:38:27.209: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/1 TDR=0, TRC=0
% Bad IP address or host name% Unknown command or computer name, or unable to find compute
SW01>
SW01>
*Sep 12 22:38:57.236: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/1 TDR=0, TRC=0
SW01>
*Sep 12 22:39:27.271: %AMDP2_FE-6-EXCESSCOLL: Ethernet0/1 TDR=0, TRC=0
SW01>
```

CPU　　　　　　　0.25%　　　　　　MEMORY　　　　　30.29%

Step 28: Verify Kali Linux is Connected
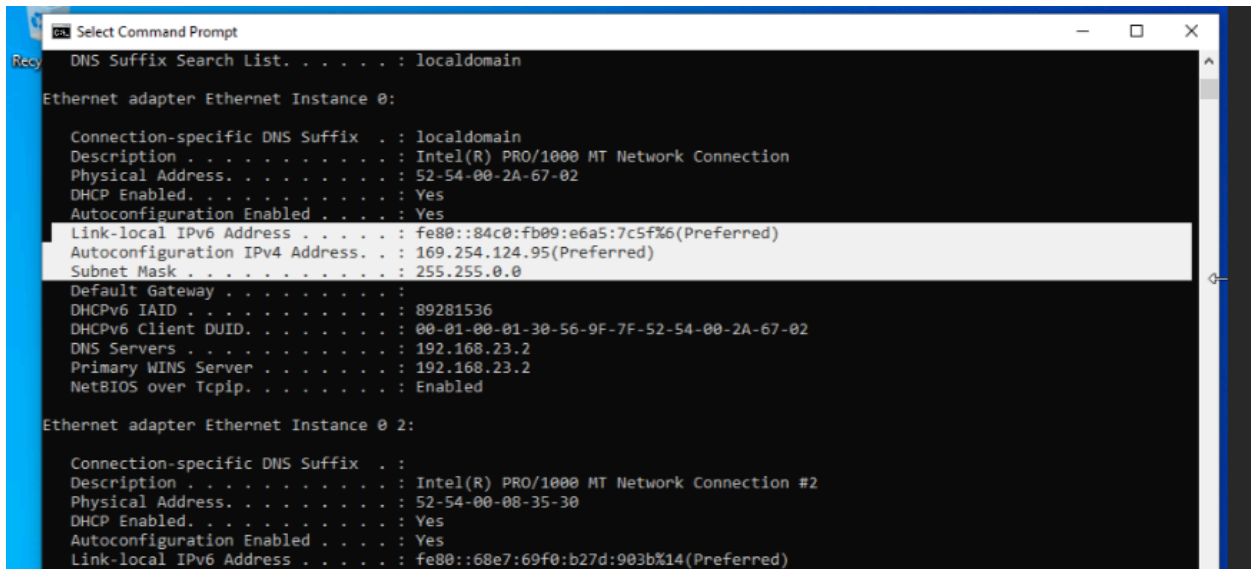
- In the Kali console (already logged in), type: ifconfig

Step 29: Verify Windows 10 is Connected

- In the Command Prompt, type: ipconfig

Step 30: Verify Windows 11 is Connected
In the Command Prompt, type: ipconfig

Step 31: Verify Windows 7 is Connected
In the Command Prompt, type: ipconfig

Finished Network Diagram and connected and ready for setup.