**NAME OF THE STUDENT**: SUDHARSHIYA GANESAN

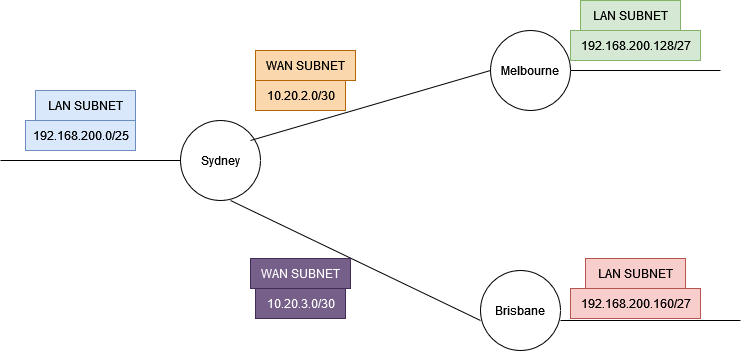
**COURSE**: NETWORKING

**STUDENT ID**: 20232004

### **ASSESSMENT ON**

**PROJECT: NETWORKING PRACTICE**

**TASK 1: Design a series of subnets**



**1a. Static Configuration of WAN Subnet between Melbourne and Sydney: 10.20.2.0/30**

Here, I have decided to give router IP address in Class A. I need only 2 hosts per WAN connection. So, I have increased the CIDR to 30.

Network address: 10.20.2.0/30

Broadcast address: 10.20.2.3/30

Subnet mask: 255.255.255.252

Ip addresses for the routers are:

Sydney router IP address external (WAN) interface:10.20.2.1

Melbourne router IP address external (WAN) interface:10.20.2.2

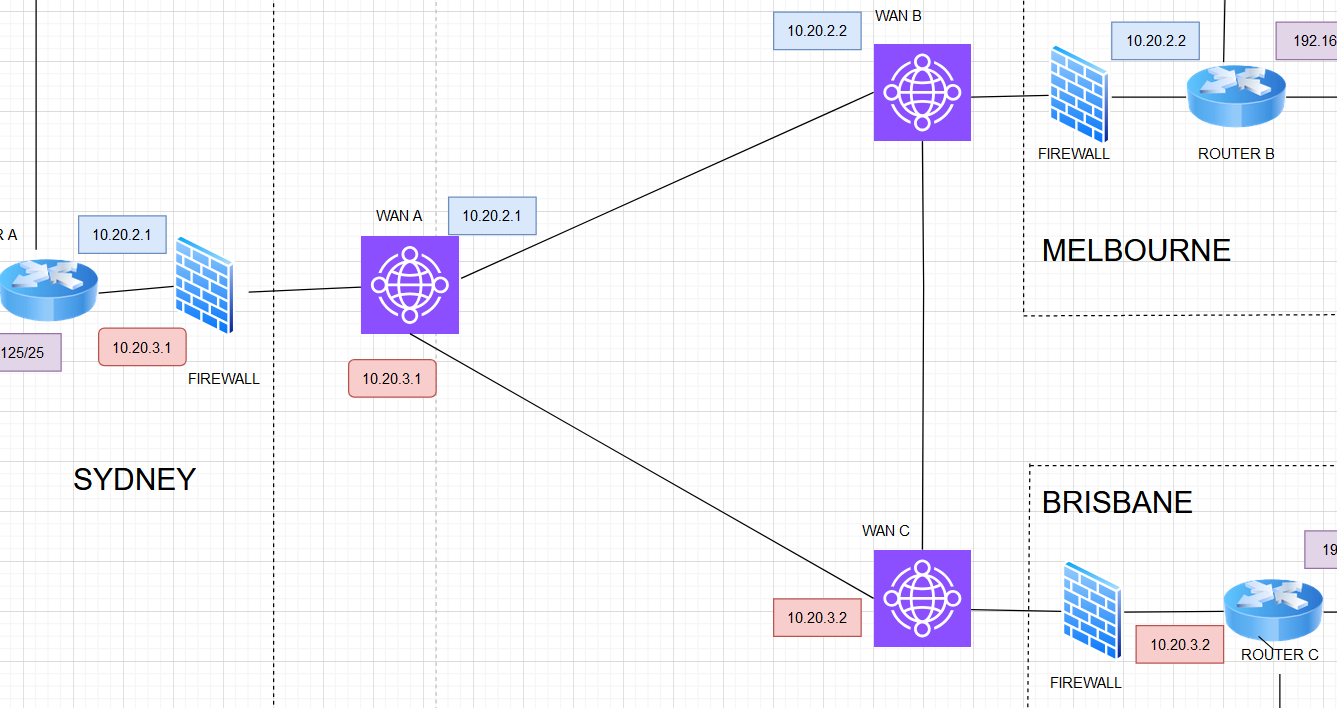


Fig 1.1 Wan subnet IP addresses of Sydney vs Melbourne in blue box (10.20.2.1, 10.20.2.2) and Wan subnet IP addresses of Sydney vs Brisbane in orange box (10.20.3.1, 10.20.3.2)

**1b. Static configuration of WAN Subnet between Brisbane and Sydney:10.20.3.0/30**

Network address: 10.20.3.0/30

Broadcast address: 10.20.3.3/30

Subnet mask: 255.255.255.252

Ip addresses for the routers are:

Brisbane router IP address external (WAN) interface: 10.20.3.1

Sydney router IP address external (WAN) interface: 10.20.3.2

**TASK 1.1: Design Server and IP addresses**

I need three subnets for three locations: Sydney, Melbourne and Brisbane in 192.168.200.0 IP address scheme.

**1.1a.** Sydney should accommodate at least 100users. In mindful of the extension of the staffs/PCs in the future, I have designed the site with 126 usable IP addresses.

Sydney local LAN: 192.168.200.0/25

Sydney WAN interface: 10.20.2.1/30(for Melbourne),

10.20.3.1/30(for Brisbane)

Broadcast address of LAN network: 192.168.200.127/25

Subnet mask of LAN network: 255.255.255.128

126 Usable IP addresses for Sydney LAN network: 192.168.200.1 to 192.168.200.126

Sydney Router LAN interface: 192.168.200.125/25

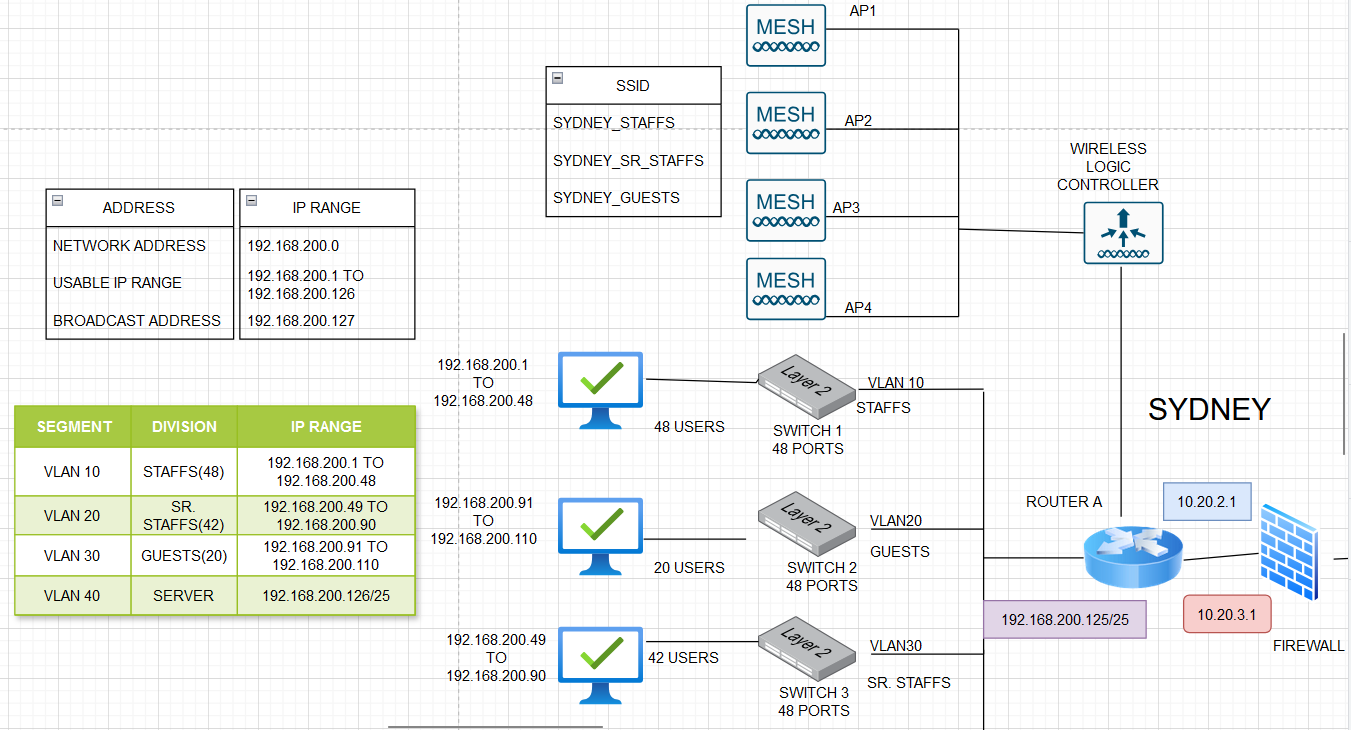


Fig 1.2 Sydney’s LAN network

**1.1b. Melbourne** has a maximum of 8 PCs. In mindful of the future extension, I have designed the site with 30 usable IP addresses

Melbourne local LAN: 192.168.200.128/27

Melbourne WAN interface: 10.20.2.2/30

Subnet mask of Melbourne LAN network: 255.255.255.224

30 Usable IP addresses for Melbourne LAN network: 192.168.200.129 to 192.168.200.158

Melbourne Router LAN interface: 192.168.200.155/27

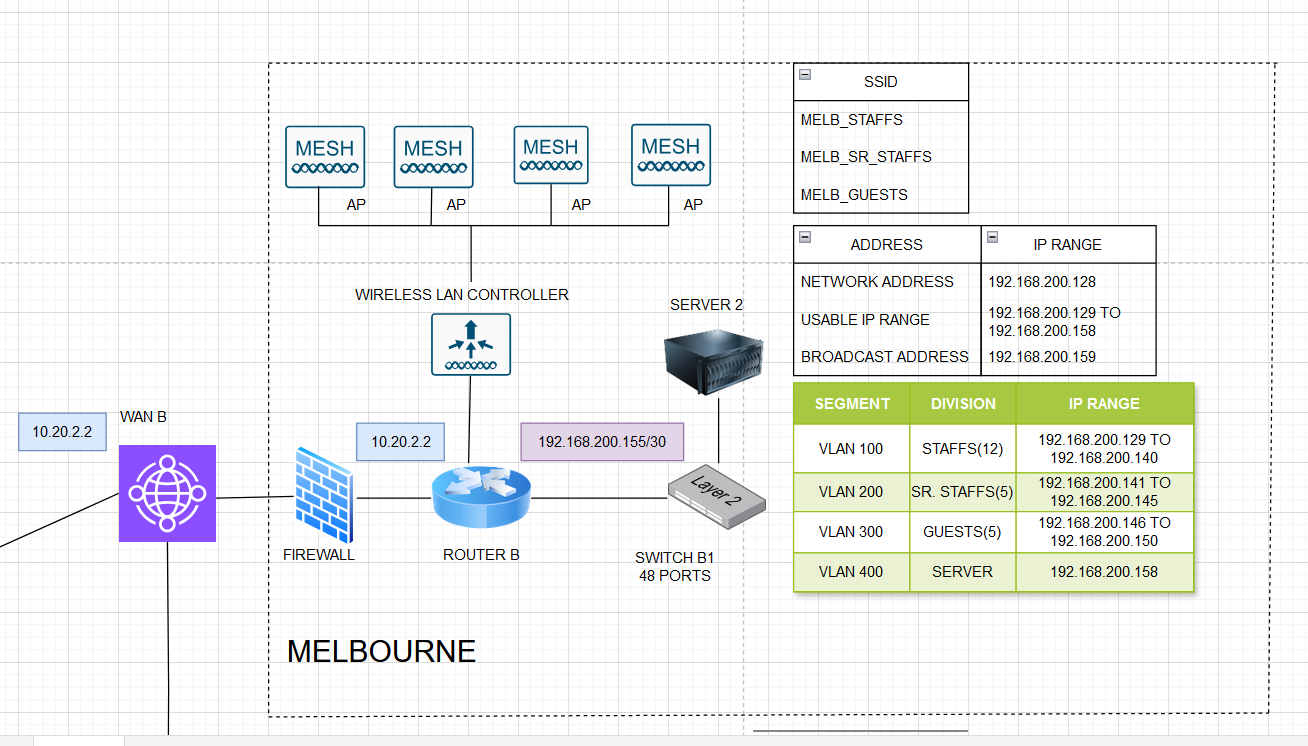


Fig 1.3 Melbourne’s LAN network

**1.1c. Brisbane** has a maximum of 8 PCs. In mindful of the future extension, I have designed the site with 30 usable IP addresses.

Melbourne local LAN: 192.168.200.160/27

Melbourne WAN interface: 10.20.3.2/30

Broadcast address of LAN network: 192.168.200.191/27

Subnet mask of LAN network: 255.255.255.224

30 Usable IP addresses for Brisbane LAN network: 192.168.200.161 to 192.168.200.190

Brisbane Router LAN interface: 192.168.200.185/27

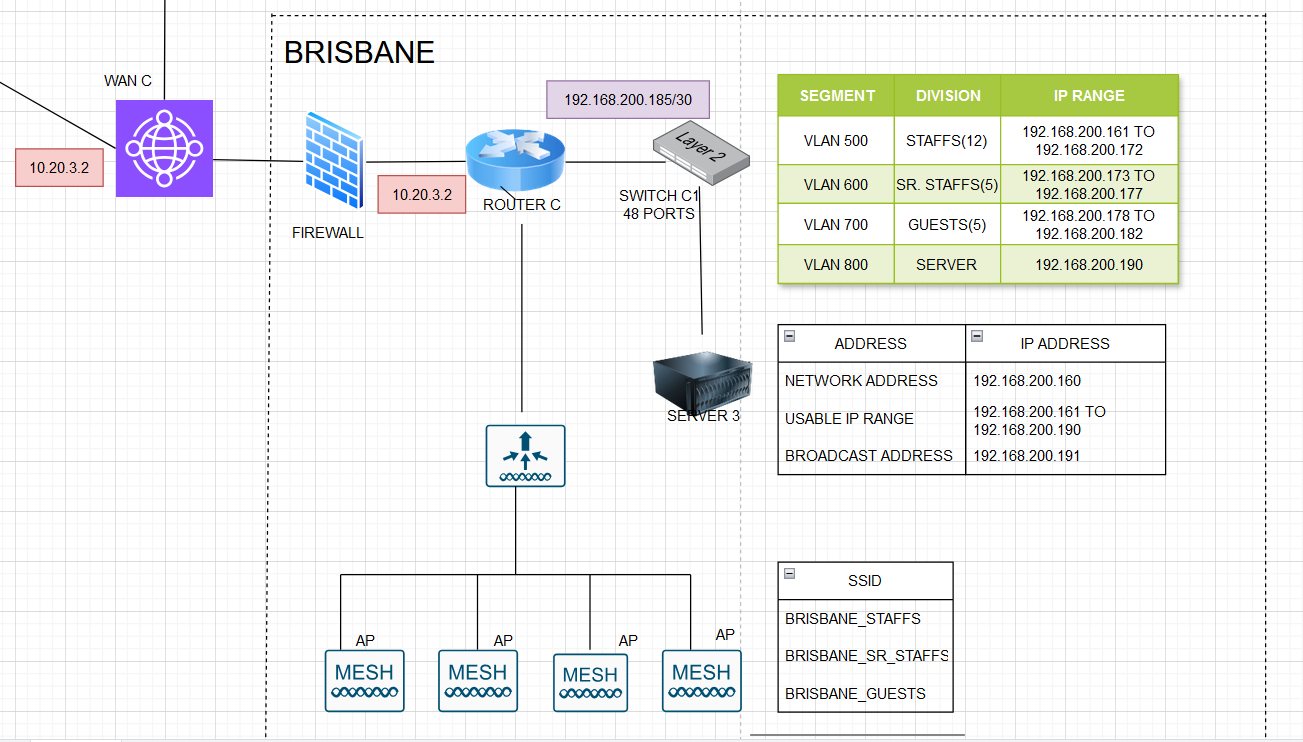


Fig 1.4 Brisbane’s LAN network

**IDENTIFY THE LOCATION AND THE DOMAIN CONTROLLERS AND SERVERS:**

Sydney site has one Domain Controller and the server is connected to domain name, SYD in IPv4 settings. SYD is primary, with Brisbane (BSB) and Melbourne (MLB) serving as additional Domain Controllers (ADCs). Totally 3 domain controllers and 3 servers, one for each site. Sydney will host the primary DNS server, while Brisbane and Melbourne will have secondary DNS servers, pulling zone data from Sydney through zone transfers.

* Sydney (Primary): Hosts the primary versions of services like VPN, DNS, DHCP, AD, HTTPS, FTP, SSH, Wireless LAN Controller (WLC), and SMTP.
* Brisbane and Melbourne (Secondary): These servers act as backups for redundancy, load balancing, and failover, ensuring business continuity.

|  |  |  |
| --- | --- | --- |
| Locations | Domain Controller | Server |
| Sydney | 1, SYD, Primary | 1, Primary |
| Melbourne | 1, MLB, secondary | 1, secondary |
| Brisbane | 1, BSB, secondary | 1, secondary |

**SERVER SERVICES:**

Running multiple services on a single server requires careful configuration to ensure that each service operates on its designated port without conflict.

Required services are:

* HTTP/HTTPS- 80, 443
* Active directory-
* DNS, DHCP
* VPN
* SSH

**Load Balancing**: Load balancing solutions can be introduced to distribute traffic across all three sites, reducing the load on Sydney.

**Automated Failover**: Each secondary site (Brisbane and Melbourne) will be set up to automatically take over services if the Sydney server becomes unavailable

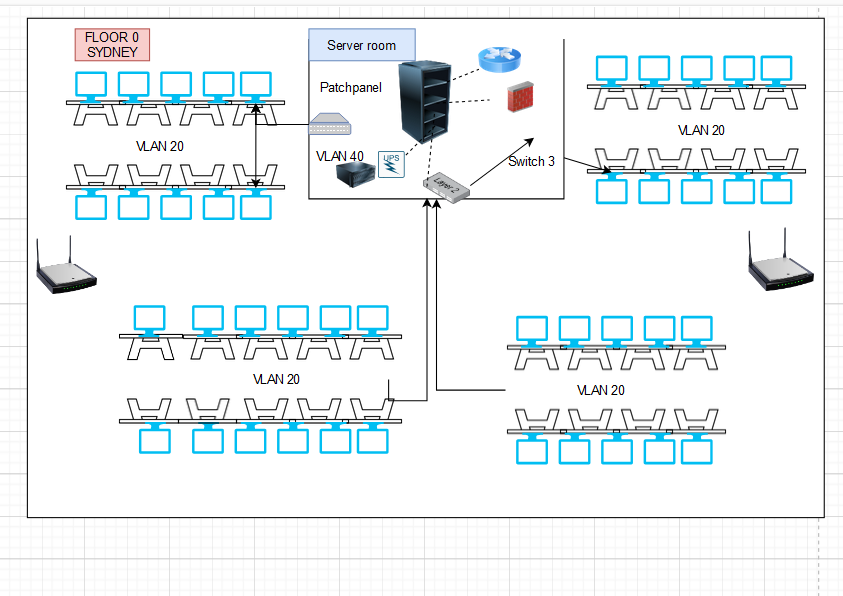
The selected server should be properly provisioned with enough CPU, memory, and storage to handle the load. So, I have selected HPE ProLiant DL380a Gen11 server of 3TB memory.

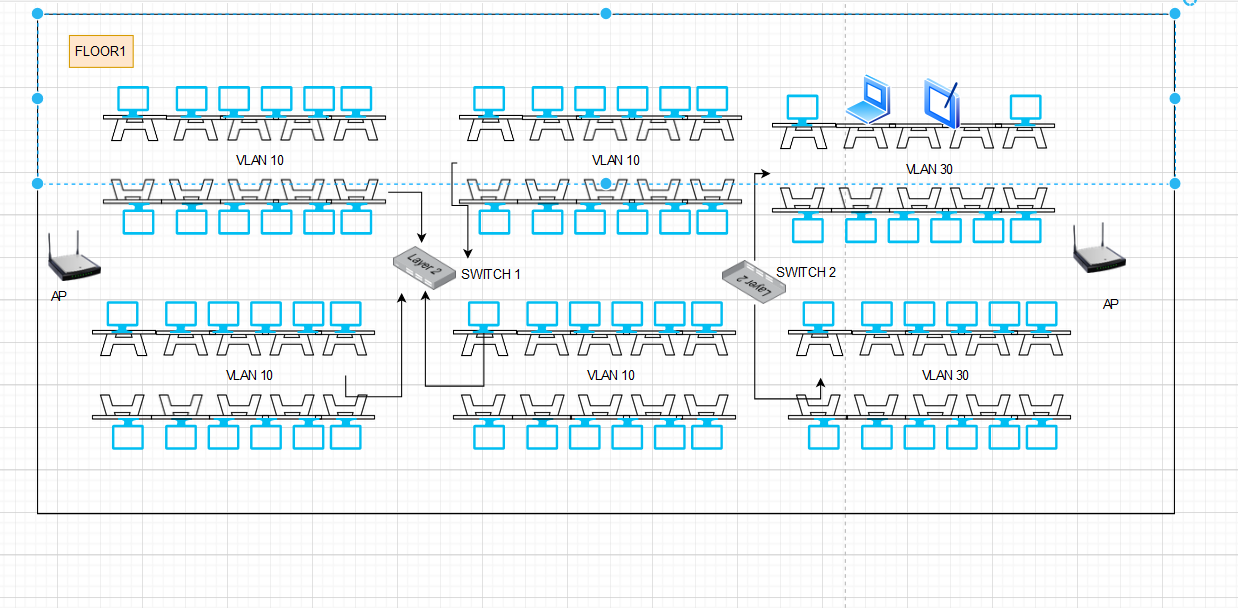
**TASK 1.2: Design Networking Equipment and Wireless**

**1.2a Networking/Physical Design floor plan**

Organize networking equipment within standardized racks to maximize space and improve manageability in each site’s server room.

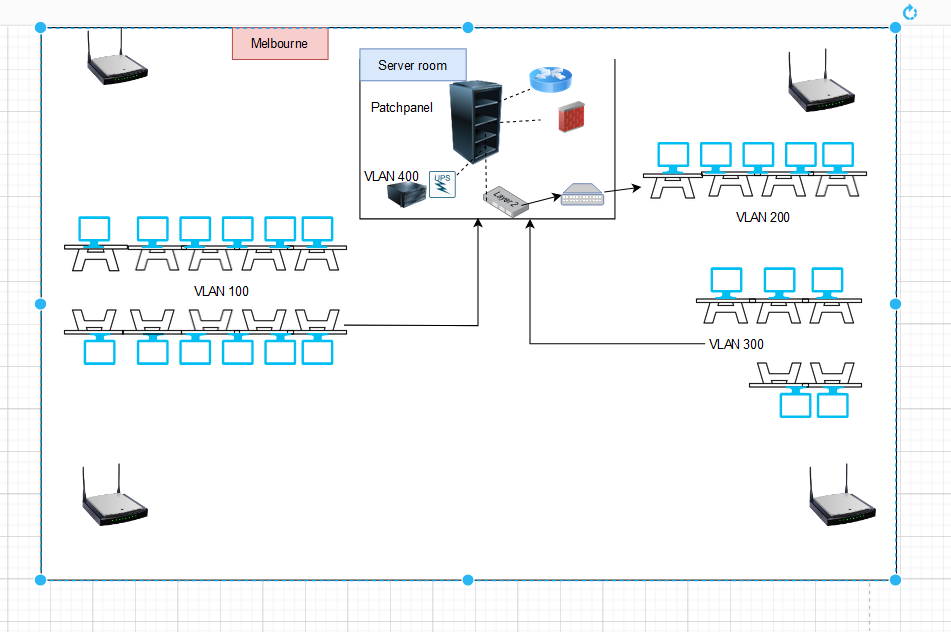
**Sydney site’s floor plan:** It has two floors in which the floor 0 has server room and PCs for senior or management staffs and they are connected to VLAN 20 and VLAN 40 for Senior staffs and server respectively.





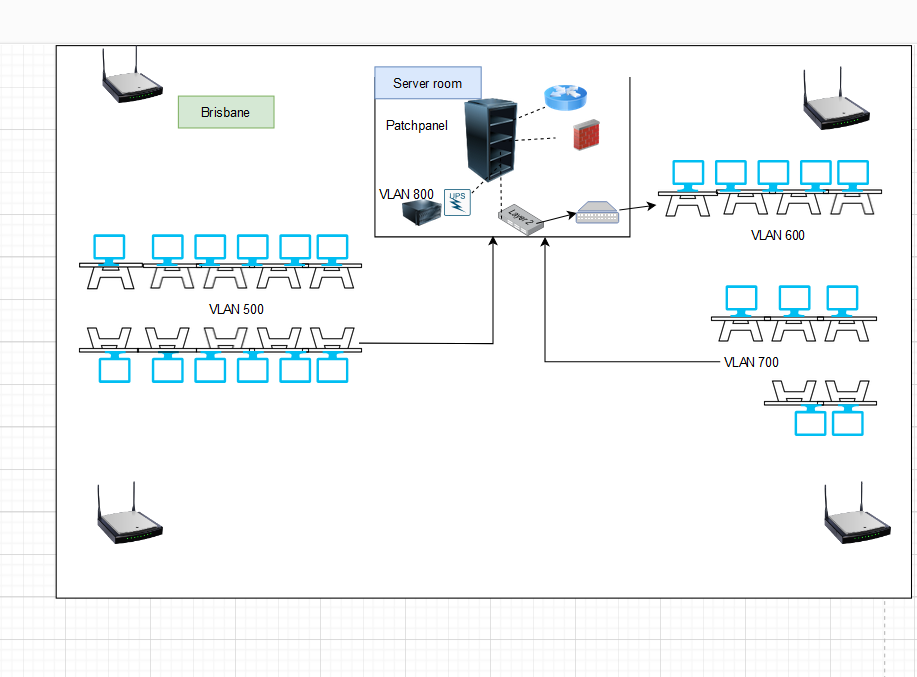
**Melbourne Floor plan:**

It is a single floor office with a secondary server and it is designed for 30 users with different VLAN segment to ensure security and manage network traffic.



**Brisbane Floor plan:**

It is a single floor office with a secondary server and it is designed for 30 users with different VLAN segment to ensure security and manage network traffic. It has a single 48 ports switch to manage the LAN network among users.



**1.2b Equipment to be installed and equipment installation plan:**

1. Switches (48 ports):

Model: Cisco Catalyst C9200-48P - 48 ports full PoE+

Link: <https://www.pbtech.co.nz/product/SWHCIS9200484/Cisco-Catalyst-9200L-48-port-PoE-4-x-10G-Network-E>

Installation: Mounted in server racks in each location’s server room.

1. Access Points (APs)\* 4 per site:

Model: Cisco CW9162I-x: Cisco Catalyst 9162 Series (In-built wireless controller)

Link: <https://www.cisco.com/site/us/en/products/networking/wireless/access-points/catalyst-9100-series/index.html>

Wi-Fi Alliance: Wi-Fi 6 (R2), Wi-Fi 6E, WPA3-R3, WPA3-Suite B, Enhanced Open Security

Installation: Ceiling-mounted in strategic locations to ensure maximum coverage.

3. Cisco Routers:

Model: Cisco ASR 1001-X

Installation: Installed in server racks next to switches.

4. Firewalls:

Model: Juniper SRX345 Firewall

Link: <https://www.juniper.net/us/en/products/security/srx-series/srx345-enterprise-firewall.html>

Installation: Mounted in server racks, connected with the router to protect the internet network

5. Servers:

#### Model: HPE ProLiant DL380a Gen11

Link: <https://buy.hpe.com/nz/en/accelerate-and-protect-with-intel?jumpid=in_smb_dm_intel>

Specification: 3 TB memory (1.5 TB per processor)- 2 processors, 5th Gen Intel Xeon Scalable processors.

Installation: Mounted in server racks in the respective server rooms in each location.

6. Server Rack

Link: <https://www.pbtech.co.nz/product/RACDNX1012/Dynamix-RST45-8X12-45RU-Server-Cabinet-1200mm-deep>

Specification: 1200 m deep to accommodate routers, switches and firewall

Installation: Standalone rack with 3 fixed shelves

7. Patch Panel: DYNAMIX 24 port 19’ Cat6 UTP Patch Panel

Model: PP-C6-24

Link: <https://dynamix.co.nz/pp-c6-24>

Installation: Fixed in the Server Rack for the office internal network LAN segment

8. Power Rail Surge

Model: Jackson RAC1200 2RU 12 Outlet Horizontal Power Rail Surge Protected 525J AU/NZ

Link: <https://www.pbtech.co.nz/product/CHSDNX1200/Jackson-RAC1200-2RU-12-Outlet-Horizontal-Power-Rai?qr=GShopping&gad_source=1&gclid=CjwKCAjw59q2BhBOEiwAKc0ijS85vpxygNBqBBVQxEzvNdDmc5DOn0EOROQ_dIoRCPAGI4JQPF9FERoC0HAQAvD_BwE>

Installation: Rack mounted in the server room

9. Cat6 305m cable box

Link: <https://www.pbtech.co.nz/product/CABDNX2916/Dynamix-C-C6-SLDBLUE-305m-Cat6-Blue-UTP-SOLID-Cabl?qr=popular_related_products>

Installation: Divide the cable to required length and connect with RJ45 which can be connected to the computers.

10. RJ45 (100 pieces)

Link: <https://www.pbtech.co.nz/product/ITPA-8P8C-100/Dynamix-RJ-45-R-JAR-RJ45-Plug-100pc-Jar>

Installation: Join with the cat6 cable which can be connected to the devices

11. UPS

Link: <https://www.pbtech.co.nz/product/UPSAPC0011/APC-Back-UPS-Pro-2200VA1320W-for-Gaming-230V-Pure>

Installation: Mounted in the server room to maintain power to server.

**1.2c Logical Design and Network diagram**

The logical design of the site with VLAN segmentation, IP addresses and SSID mapping to VLAN to ensure logical separation of traffic, enhance security, and optimize performance.

All the PCs connected to Switches are connected in **Star topology** and it is easy to implement cabling systems.

**Sydney site:**

In Sydney site, we are using 3 Cisco Catalyst 48 port POE switches. The first switch, SWITCH1 is used for 48 users of Staff division and they will be connected to SSID: SYDNEY\_STAFFS and they are mapped to VLAN10 of SWITCH1.

The second switch, SWITCH2 is used for guests and allocated 20 IP addresses for them but it has free ports in the switch for future extension and they are connected with VLAN30 and SYDNEY\_GUESTS SSID

The third switch, SWITCH3 is used for senior staffs and server and they have separate VLANs: VLAN20 and VLAN40 respectively. They have separate usable IP addresses for each device connected with the switches and they are listed in the table below and refer Fig 1.2.1

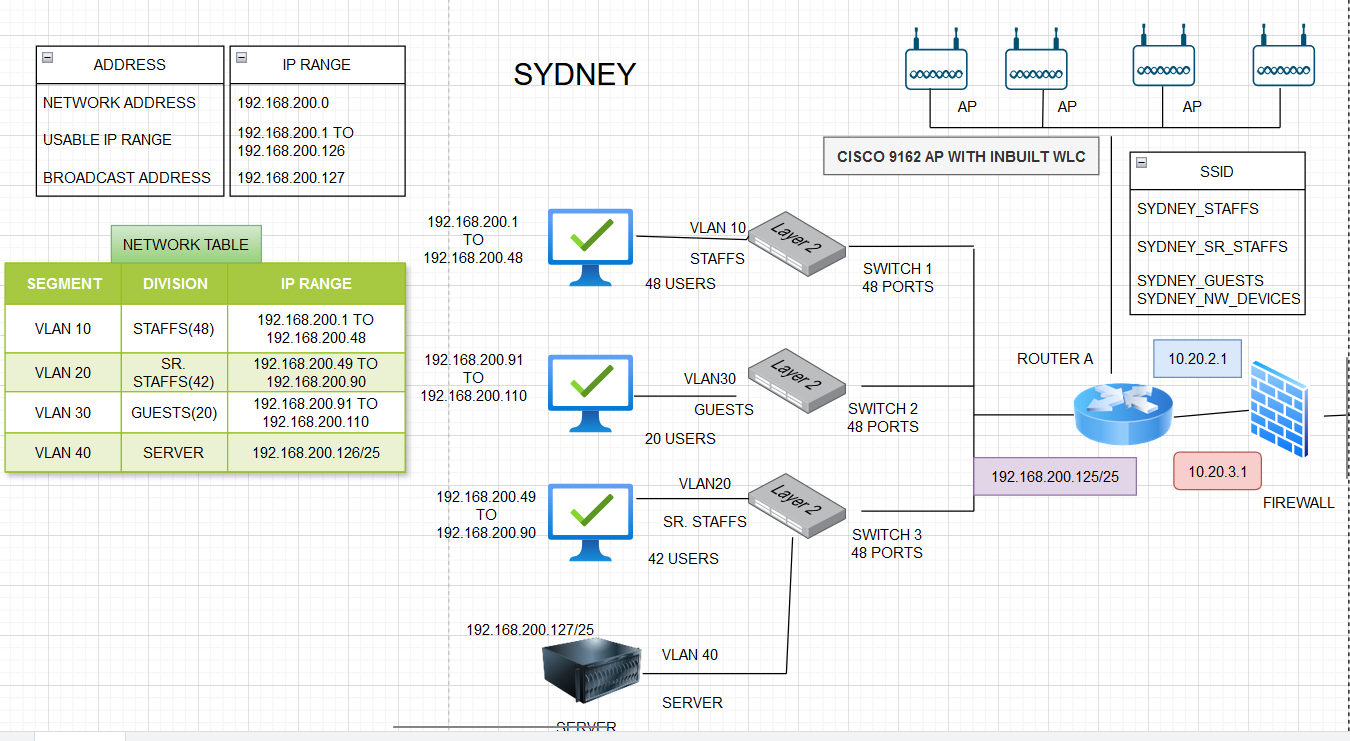


Fig 1.2.1 Sydney: Network diagram including VLAN, SSID, IP addresses.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SEGMENT | SWITCH | DIVISION | MAX USERS | SSID MAPPING TO VLAN | IP ADDRESSES |
| VLAN10 | SWITCH1 | STAFFS | 48 | SYDNEY\_STAFFS | 192.168.200.1 TO 192.168.200.48 |
| VLAN 20 | SWITCH3 | SENIOR STAFFS | 42 | SYDNEY\_SR\_STAFFS | 192.168.200.49 TO 192.168.200.90 |
| VLAN 30 | SWITCH2 | GUESTS | 20 | SYDNEY\_GUESTS | 192.168.200.91 TO 192.168.200.110 |
| VLAN 40 | SWITCH3 | SERVER | - | SYDNEY\_NW\_DEVICES | 192.168.200.126 |

TABLE 1.1 NETWORK TABLE: SYDNEY

**Configuration rules:**

1. Certificate management for remote access and VPN: For domain devices that travel between offices or require remote access, issue VPN certificates to secure remote connections. Devices will use these certificates for authentication when connecting to the network from external locations.
2. Configuration of Switches: In Brisbane and Melbourne site, a single 48 ports switch is divided into 4 VLANs. The proper configuration of the VLAN is required to maintain secured network among users, clients and guests.
3. Firewall configuration: Setting rules to avoid any unauthorised access into the internal network and establish ACL permissions.
4. Scalability and Flexibility: Usage of some cloud applications and switches with free ports help the network to adapt the growth of the business. Additional switches can be added easily and it has to be configured with the right VLAN type based on the Role based access type (Refer Table 1.2)

### Redundancy: Regularly back up all configurations and data to cloud-based application and document all redundancy configurations. Implement monitoring tools to detect and alert on any redundancy issues, such as failed links, degraded RAID arrays, or failed cluster nodes.

* + - RAID 1 for mirroring (critical data requiring high availability).
    - RAID 5/6 for a balance between performance, storage capacity, and redundancy.
    - RAID 10 for high performance and redundancy (combining mirroring and striping).

1. Primary and Secondary WAN Links: Configure multiple WAN links to provide redundancy. For example: Routing between Sydney and Brisbane can be done via Melbourne if there is any damage/failure in the shortest path.
2. Primary and Secondary Servers: To balance the loads of the services during downtime. For example: Sydney server is the primary server and other servers are secondary one. Usage of load balancers like Elastic load balancing to distribute application traffic across the three sites. (AWS load balancers[[1]](#endnote-22151))
3. Consistency in the Configuration: Use automated configuration management tools to maintain identical static routing settings across redundant devices. For example: Terraform

**Melbourne site:**

In Melbourne site, we are using one of the Cisco Catalyst 48 port POE switches. The SWITCH B1 is used for 12 users of Staff division and they will be connected to SSID: MELB\_STAFFS and they are mapped to VLAN100 of SWITCHB1.

Similarly, other VLANs: VLAN 200, VLAN 300, VLAN 400 are divided as segments from the same switch, SWITCH B1. They have separate usable IP addresses for each device connected with the switches and they are listed in the table (Table 1.3) and refer Fig 1.2.2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SEGMENT | SWITCH | DIVISION | MAX USERS | SSID MAPPING TO VLAN | IP ADDRESSES |
| VLAN100 | SWITCH B1 | STAFFS | 12 | MELB\_STAFFS | 192.168.200.129 TO 192.168.200.140 |
| VLAN 200 | SWITCH B1 | SENIOR STAFFS | 5 | MELB\_SR\_STAFFS | 192.168.200.141 TO 192.168.200.145 |
| VLAN 300 | SWITCH B1 | GUESTS | 5 | MELB\_GUESTS | 192.168.200.146 TO 192.168.200.150 |
| VLAN 400 | SWITCH B1 | SERVER | - | MELB\_NW\_DEVICES | 192.168.200.158 |

TABLE 1.2 NETWORK TABLE: MELBOURNE

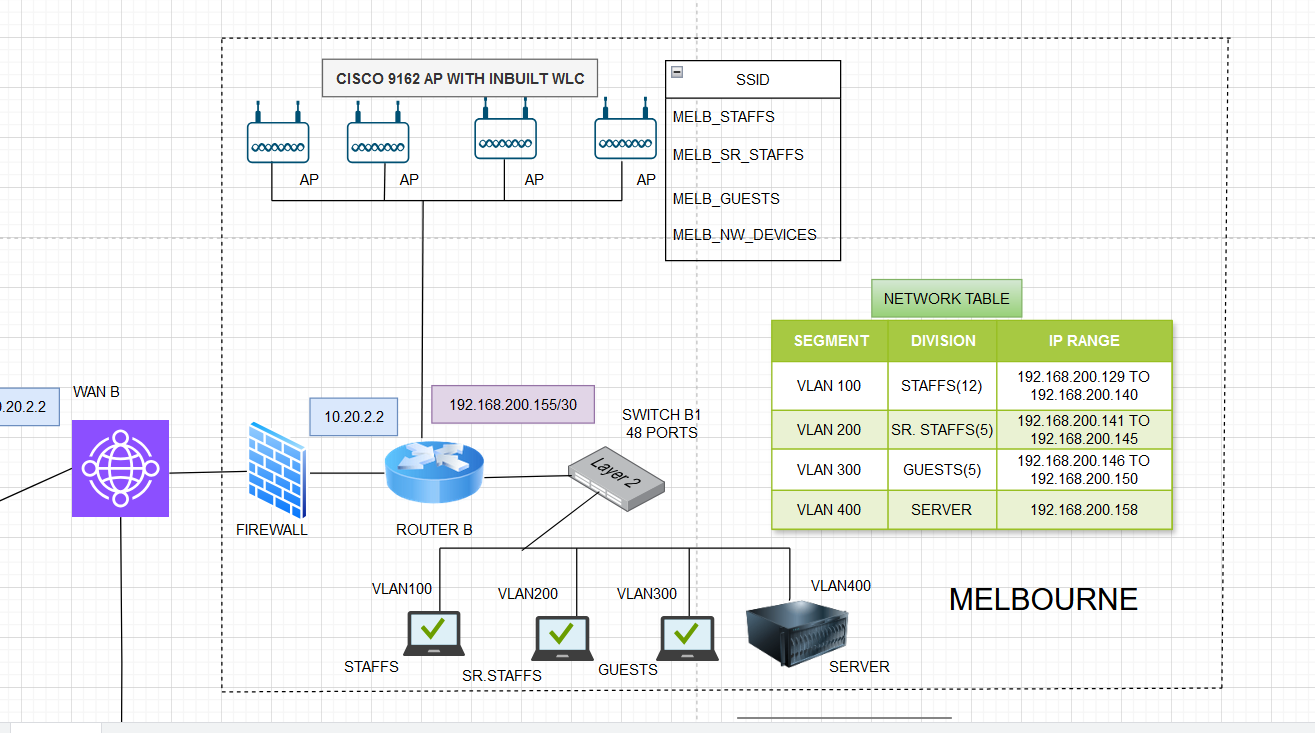


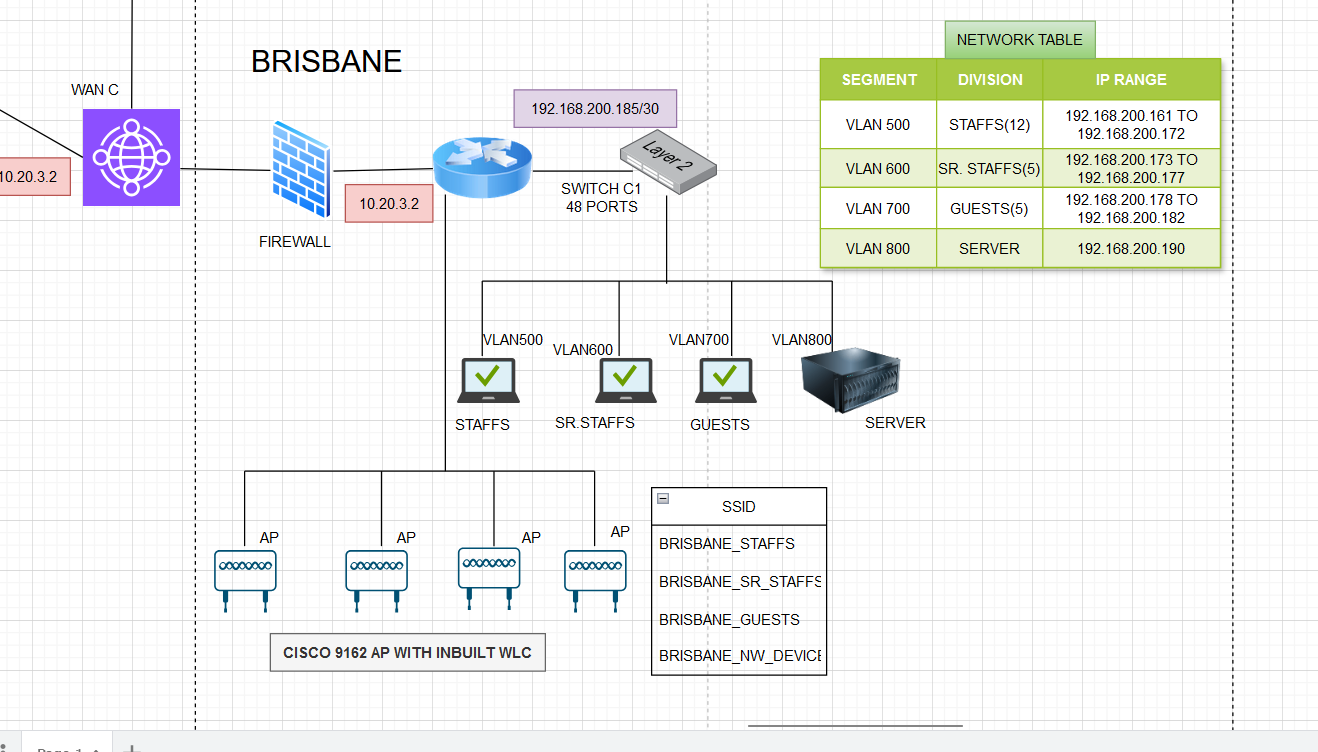
Fig 1.2.2 Melbourne: Network diagram including VLAN, SSID, IP addresses.

**Brisbane site:**

In Brisbane site, we are using one of the Cisco Catalyst 48 port POE switches. The SWITCH C1 is used for 12 users of Staff division and they will be connected to SSID: BRISANE\_STAFFS and they are mapped to VLAN500 of SWITCHC1. Similarly, other VLANs: VLAN 600, VLAN 700, VLAN 800 are divided as segments from the same switch, SWITCH C1. They have separate usable IP addresses for each device connected with the switches and they are listed in the table below and refer Fig 1.2.3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SEGMENT | SWITCH | DIVISION | MAX USERS | SSID MAPPING TO VLAN | IP ADDRESSES |
| VLAN500 | SWITCH C1 | STAFFS | 12 | BRISBANE\_STAFFS | 192.168.200.161 TO 192.168.200.172 |
| VLAN 600 | SWITCH C1 | SENIOR STAFFS | 5 | BRISBANE\_SR\_STAFFS | 192.168.200.173 TO 192.168.200.177 |
| VLAN 700 | SWITCH C1 | GUESTS | 5 | BRISBANE\_GUESTS | 192.168.200.178 TO 192.168.200.182 |
| VLAN 800 | SWITCH C1 | SERVER | - | BRISBANE\_NW\_DEVICES | 192.168.200.190 |

TABLE 1.3 NETWORK TABLE: BRISBANE

Fig 1.2.3 Brisbane: Network diagram including VLAN, SSID, IP addresses.

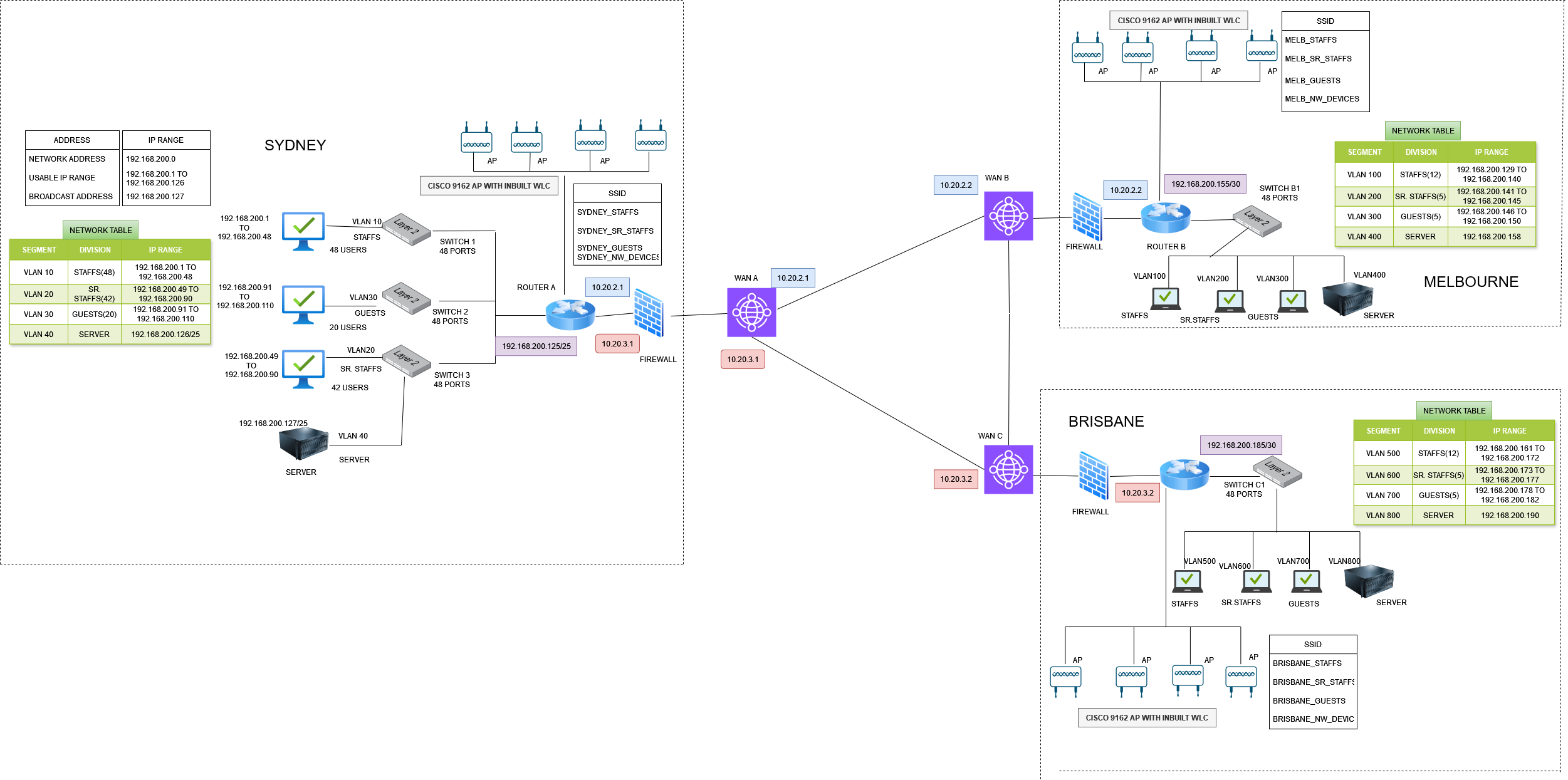


Fig1.2.4 Entire Network Diagram

**1.2e FIREWALL CONFIGURATION**

The Juniper SRX345 supports intrusion detection and prevention (IDP) services, SIEM using Juniper Secure Analytics and further we can use Juniper’s App Secure feature for deep packet inspection (DPI) and threat detection which inspect packets to block malicious payloads or unauthorized services.

|  |  |
| --- | --- |
| **Allowed services/ Ports** | **Blocked services** |
| HTTP. HTTPS (80,443) | Peer to Peer file sharing, gaming, gambling |
| FTP, SSH, VPN, DNS (53), DHCP | Netflix, Social media sites, |

**ACL for Firewall:**

It is performed by their respective IP addresses allocated to their devices based on their VLAN, SSID and defining security zones for each group.

##### Staff Access Policies: Staff can access the internal network (e.g., internal servers) and the internet. They should be restricted to access management resources.

##### Management/Senior staffs Access Policies: Management can access both the internal network and staff resources. They should get full internet access in 6GHZ.

##### Guest Access Policies: Guests have internet access only and they don't have access to internal resources or management.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Users | Documents/files (FTP) | Cloud based user  profiles | Intranet access | Internet  Access (HTTPS) | VPN |
| Staffs | Read | Enabled | Allow | Allow | Allow |
| Senior Staffs/Management | Read, Write | Enabled | Allow | Allow | Allow |
| Guests | deny | Deny | Deny | Allow | Deny |

TABLE 1.4 ACL PERMISSIONS FOR ALL SITES

Quality of service (QOS) and traffic shaping: Prioritise traffic for management and staff over guest traffic by applying traffic shaping rules or bandwidth limits on the guest VLAN.

Inbound Traffic (External to Internal): Define strict rules to limit inbound traffic to only necessary services and devices, such as web servers or VPN gateways.

Outbound Traffic (Internal to External): Control outbound traffic to block unauthorized or unwanted access to external websites, including gambling sites. Content Filtering using URL filtering or content filtering features to block gambling sites by category. Enable Web Filtering and block the "Gambling", “Adult/mature content” and “Pornography" category in the firewall's content filtering section and set them to “Block”

Logging and Monitoring: Enable logging for all denied and allowed traffic to monitor security incidents or policy violations.

**1.2f Monitoring and Maintenance:**

The implemented design will be monitored using a combination of:

* Network Monitoring Tools: Tools like Cisco DNA Center track network performance, bandwidth usage, latency, uptime, and device health.
* SNMP (Simple Network Management Protocol): SNMP will be enabled on network devices to provide real-time alerts for faults, device status, and performance metrics.
* Syslog and SIEM (Security Information and Event Management): Logs from switches, routers, firewalls, and servers will be centralized in a Syslog server or SIEM system to monitor suspicious activity, hardware issues, and software failures.

Routine maintenance ensures the continued health and performance of the network. Maintenance tasks will include:

* Firmware and Software Updates: Network devices (routers, switches, firewalls, APs) will be regularly checked for firmware and software updates. Security patches will be applied based on vendor advisories to mitigate vulnerabilities.
* Backup and Recovery: Configurations for all network devices will be backed up regularly. In case of hardware failure or misconfiguration, these backups can be quickly restored.

Automation: Network automation tools will be used to enforce configuration policies and automatically apply changes across devices, saving time and reducing errors.

Help Desk and IT Support: An IT service desk will be in place to manage user issues, escalate problems, and track resolutions.

Password Expiration: All network device local user accounts (e.g., on switches, routers, and firewalls) will have password expiration set to 60 days. Users will be prompted to change their passwords before expiration.

Automated Password Rotation: Automation tools or scripts will be used to enforce password rotation and notify administrators when passwords are about to expire.

**1.2g WLAN DESIGN:**

The Cisco 9162 Access Point supports both Wi-Fi 6 (802.11ax) and Wi-Fi 6E (802.11ax in the 6 GHz band).

* 6 GHz Band (Wi-Fi 6E): Utilize the 6 GHz band for high-density environments and latency-sensitive applications. This band is less congested, providing faster and more reliable connections.
* 5 GHz Band: Devices that support Wi-Fi 6 can be connected with 5 GHZ 2.4 GHz Band: For more coverage and less speed.

#### **SSID and VLAN Assignment**

Each SSID is mapped to a distinct VLAN for network segmentation and security as mentioned in the table 1.5 for Sydney site. Similarly, it is done for other sites Brisbane and Melbourne

**WPA3-R3** (WPA3-Enterprise) is the latest version of WPA3, providing enhanced security over WPA2. **WPA3-Suite B** provides stronger encryption and authentication mechanisms, suitable for sensitive data access by management users. **Enhanced Open** provides encryption even for open networks, without requiring a pre-shared key (PSK).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SSID Name** | **Wi-Fi Band** | **VLAN** | **Security** | **Purpose** |
| SYDNEY\_STAFFS | 5 GHz, 6 GHz | VLAN10 | WPA3-Enterprise (R3) | Access to internal resources |
| SYDNEY\_SR\_STAFFS | 5 GHz, 6 GHz | VLAN 20 | WPA3-Suite B | Access to sensitive resources |
| SYDNEY\_GUESTS | 2.4 GHz, 5 GHz | VLAN 30 | Enhanced Open (WPA3-Open) | Internet access only |
| SYDNEY\_NW\_DEVICES | 6 GHz | VLAN 40 | WPA3-Enterprise (R3) | Full access |

TABLE 1.5: SSID mapped with VLANs and their security mechanisms

**TASK 2 TROUBLEHOOTING AND ANALYSING THE NETWORK**

**TASK 2.1 WIRESHARK**

**PART 1: Capture and Analyse Local ICMP Data in Wireshark.**

Step 1: Ipconfig/all from my laptop. My IPV4 address is 192.168.0.179 and my LAN adapter physical address (MAC) is CC-47-40-A6-78-62

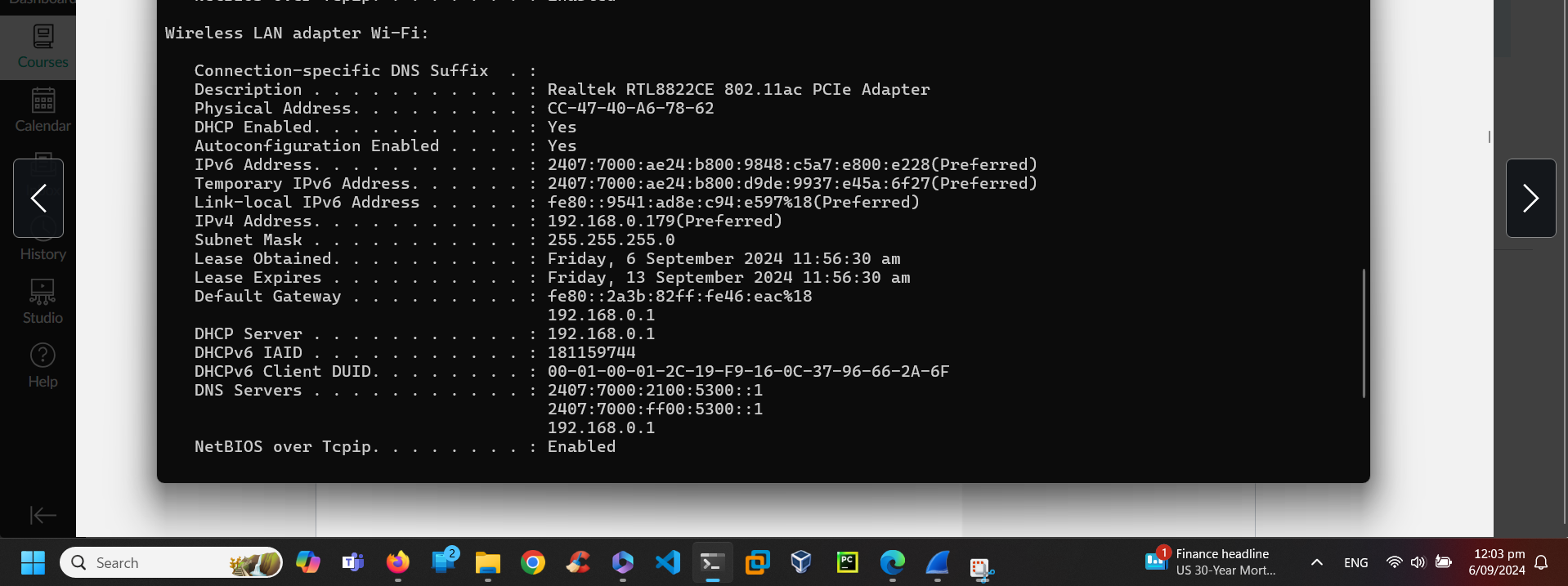
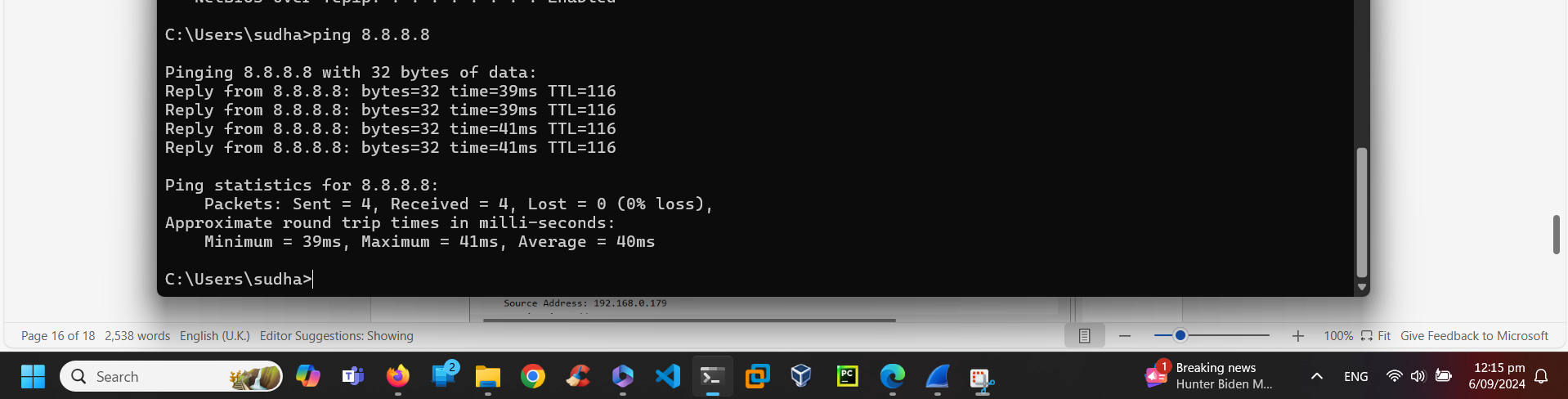
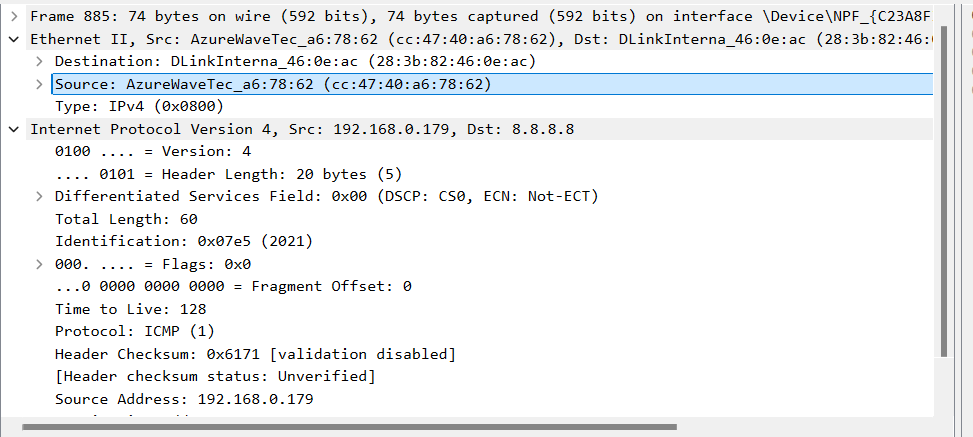
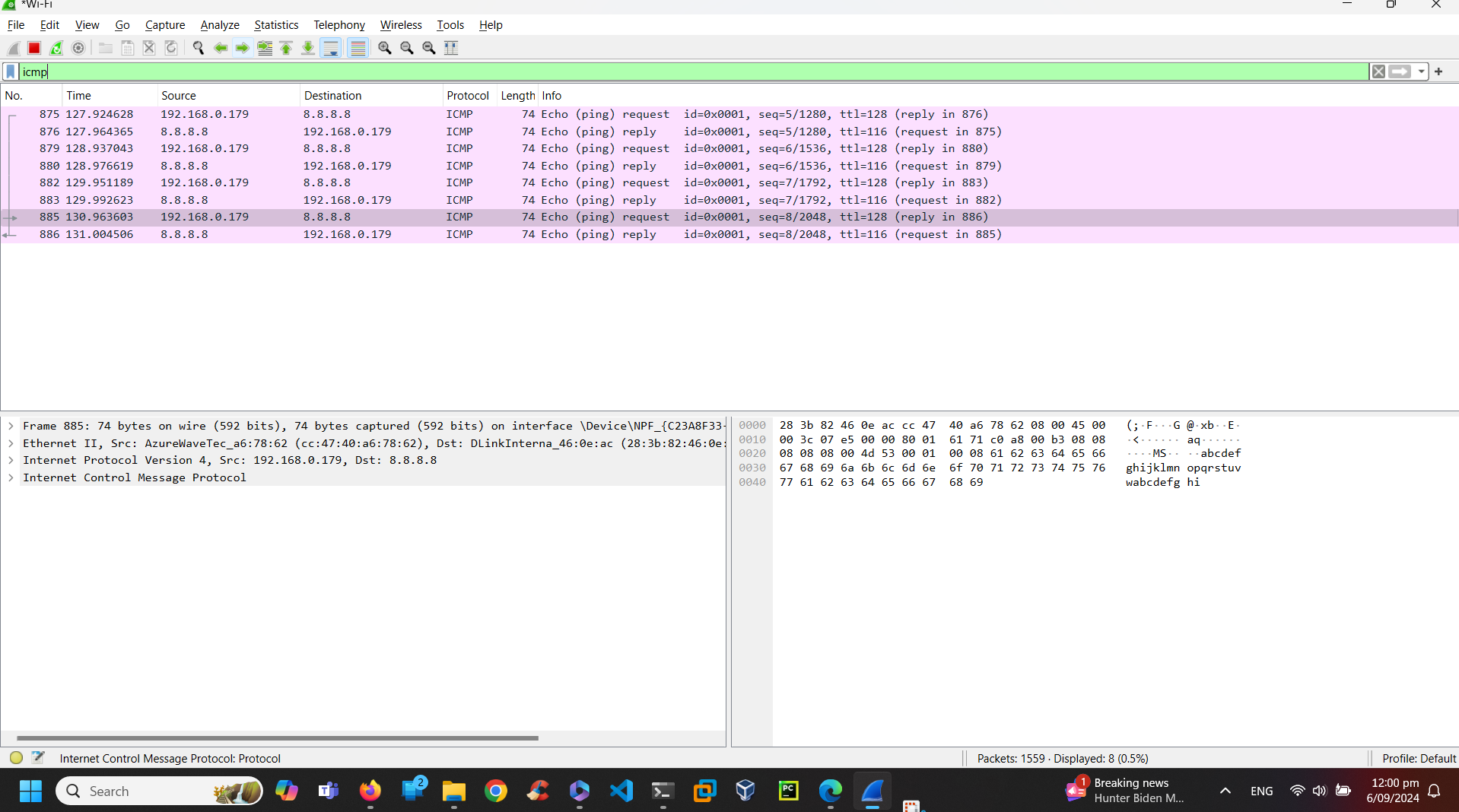


Fig 2.1 Ipconfig in Command Prompt

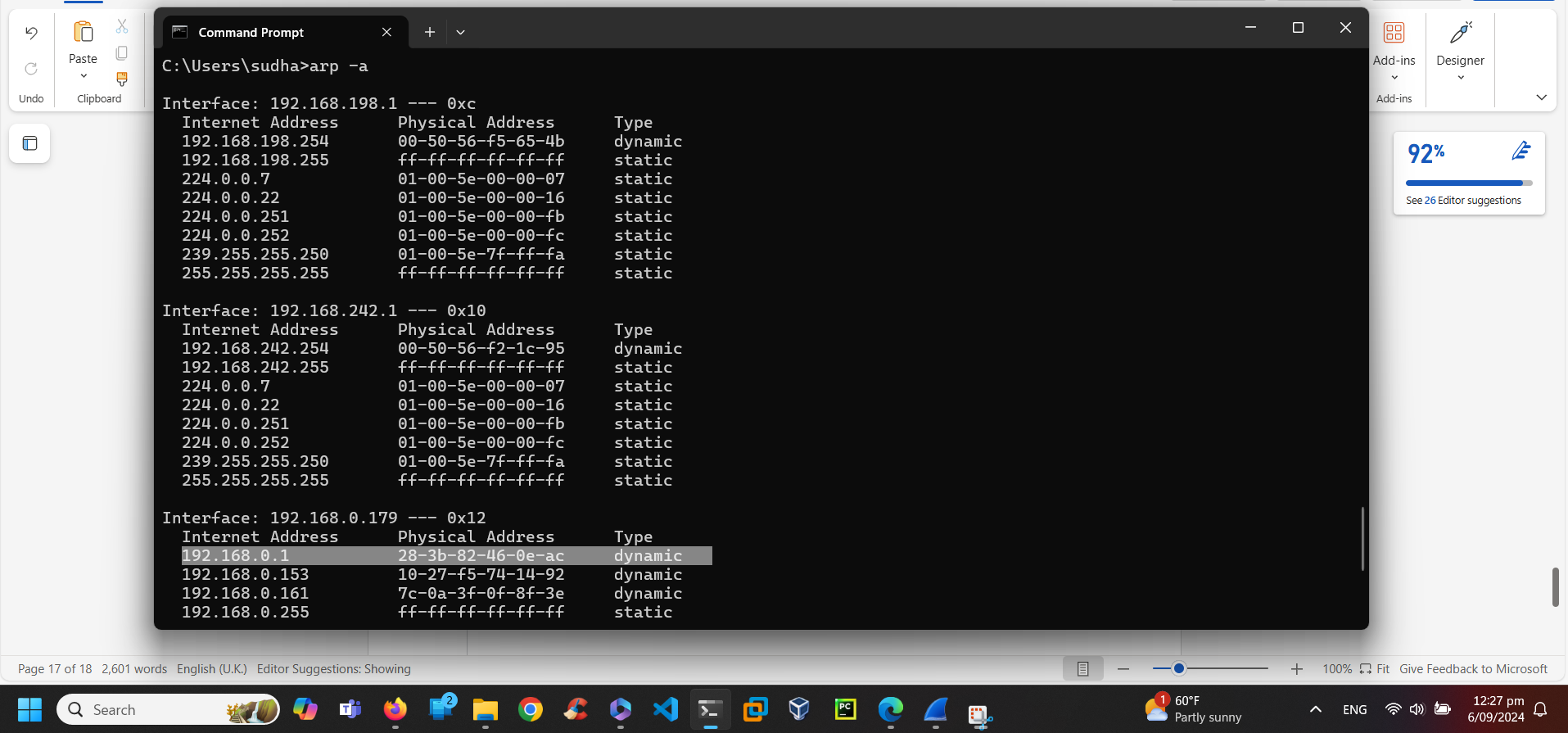
Step 2: When I tried to Ping 8.8.8.8 from my laptop and I filtered the ICMP protocol. I could the packets from my Ipv4 address is the source :192.168.0.179 and destination is 8.8.8.8. My LAN MAC address also matches. Refer fig 2.2, 2.3 and 2.4

Fig 2.2 Ping 8.8.8.8

Fig 2.3 My LAN adapter MAC address matches with the details in Ipconfig

 Fig 2.4 Filtering the ICMP protocol packets

Question1: Does the Source MAC address match your PC’s interface? Yes  
Question 2: Does the Destination MAC address in Wireshark match the MAC address of ? YES. Refer fig 2.2 and 2.5

  
Fig 2.5 arp -a

Question 3: How is the MAC address of the pinged PC obtained by your PC? It is found by ICMP protocol which checks the device with the IP address given.

**PART 2: Examining and analysing the data from remote hosts.**

1. List the destination IP and MAC addresses for all three locations in the space provided.  
   1st Location: IP: 172.16.16.128 MAC: Intel\_5b:7d:4a (00:21:6a:5b:7d:4a)  
   2nd Location: IP: 67.228.110.120 MAC: DLink\_21:99:4c (00:05:5d:21:99:4c)  
   3rd Location: IP:212.58.226.142 MAC: DLink\_21:99:4c (00:05:5d:21:99:4c)
2. What is significant about this information?

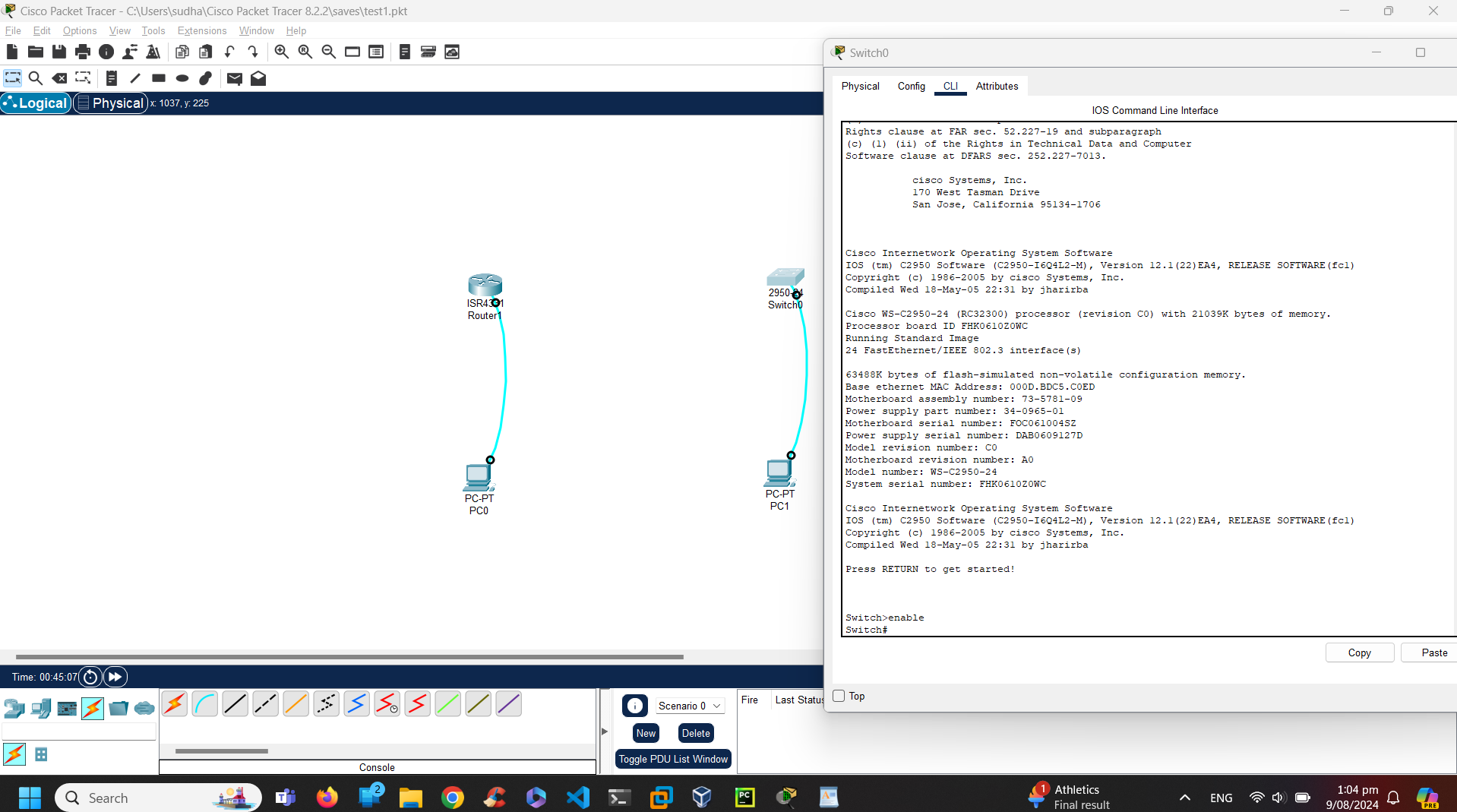
Ans: The MAC Addresses are same for 2nd and 3rd location

1. How does this information differ from the local ping information you received in First Part?

Answer: It differs by the protocol type and the second one has port numbers along with Protocol TCP 2826 port. It has Synchronisation and acknowledgement between source and destination.

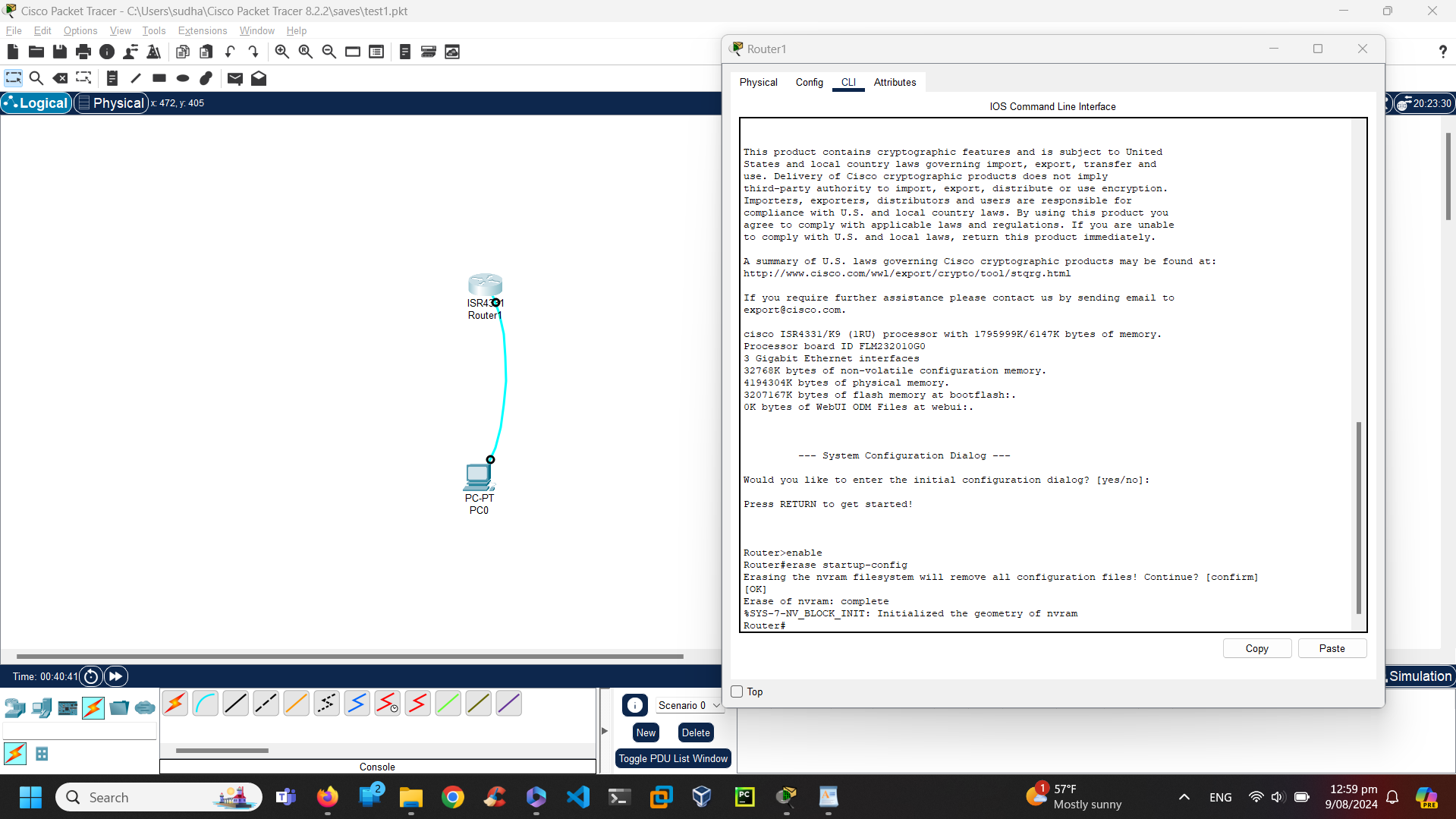
**TASK 2.2 PACKET TRACER**

**Part 1: Set up devices as shown in topology**

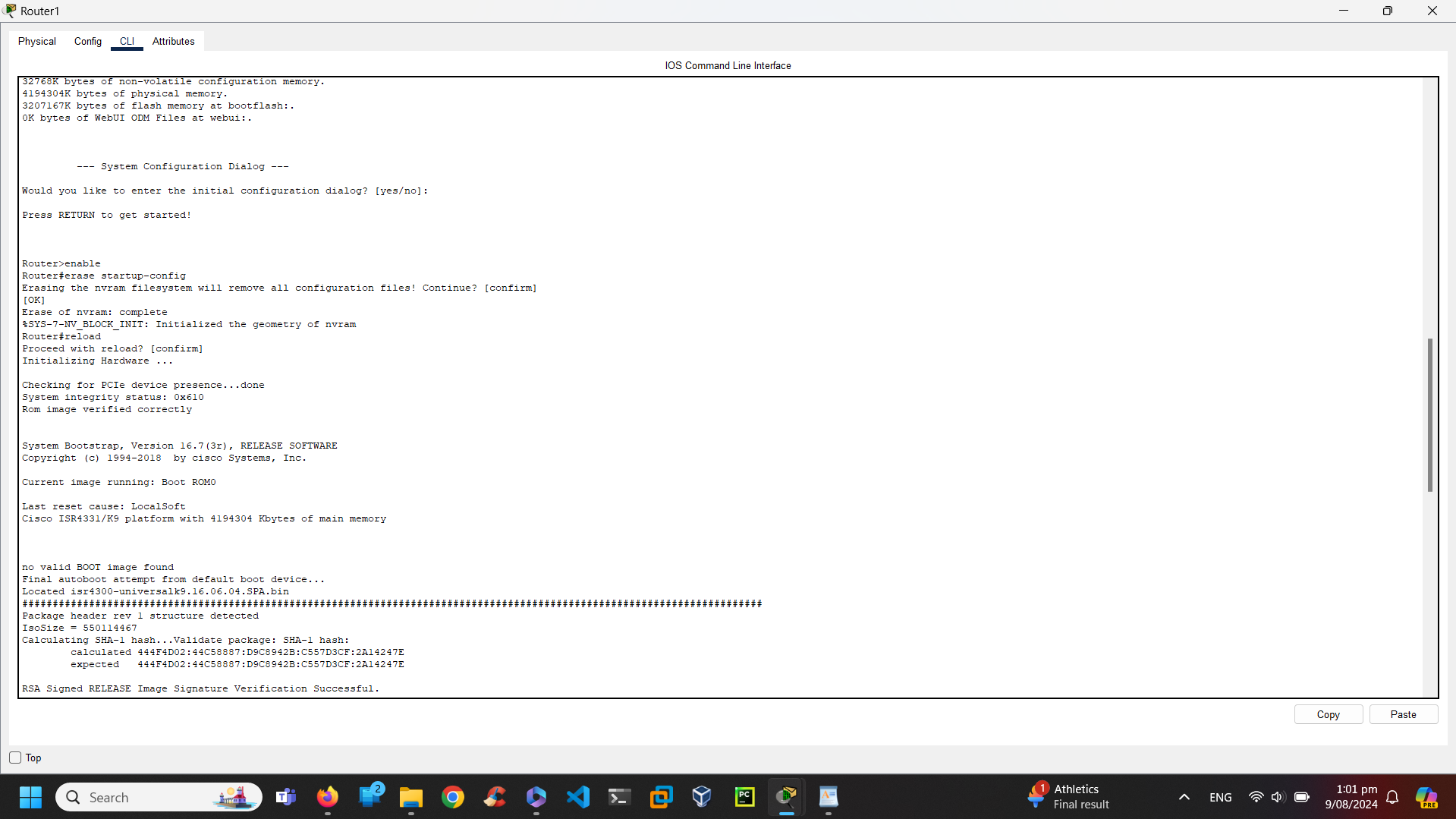
Fig 2.2.1 topology

PART 2: Initialise the router and reload

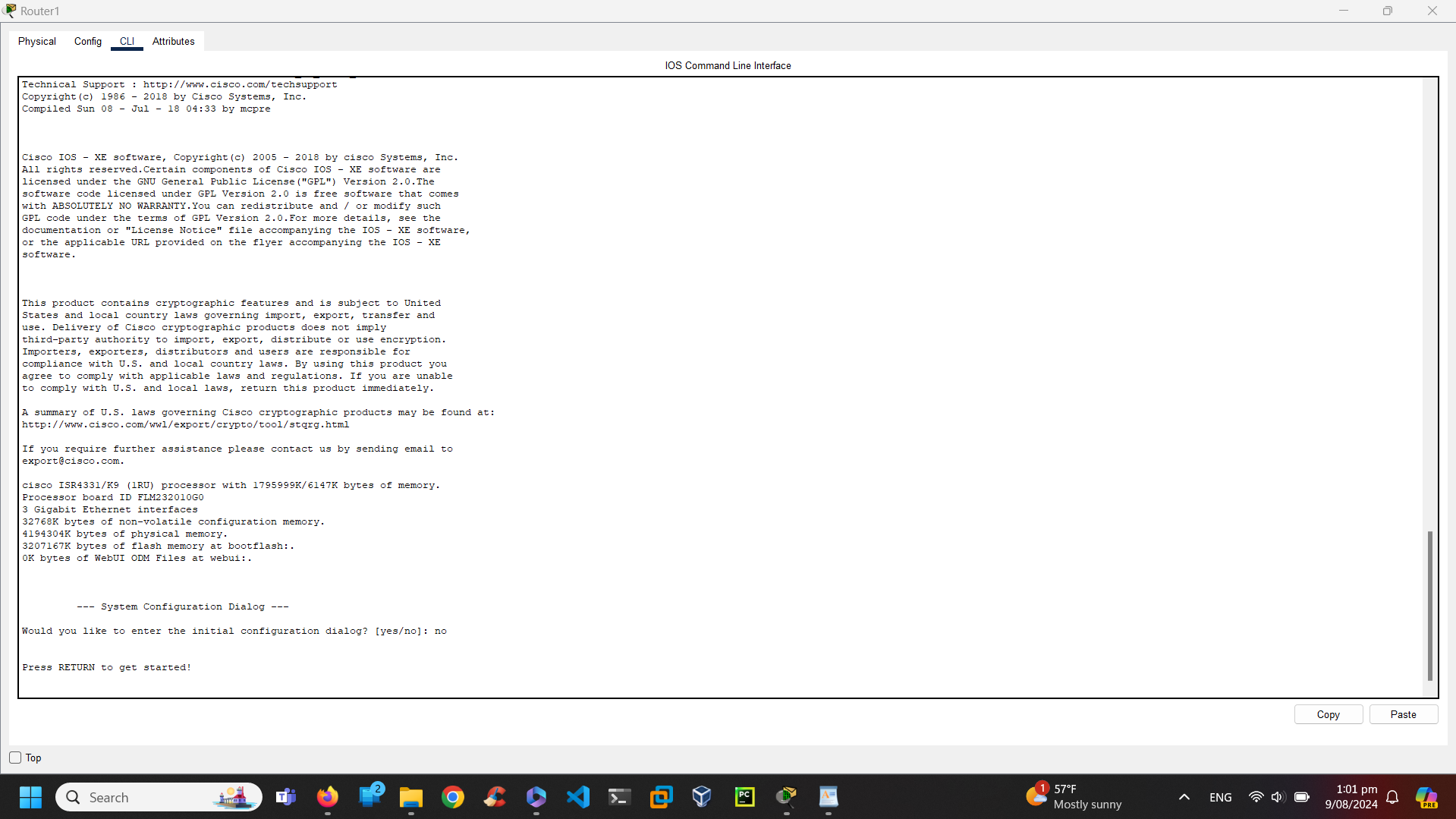
Step1: Enable the router and erase the NVRAM



Step 2: Reload the router

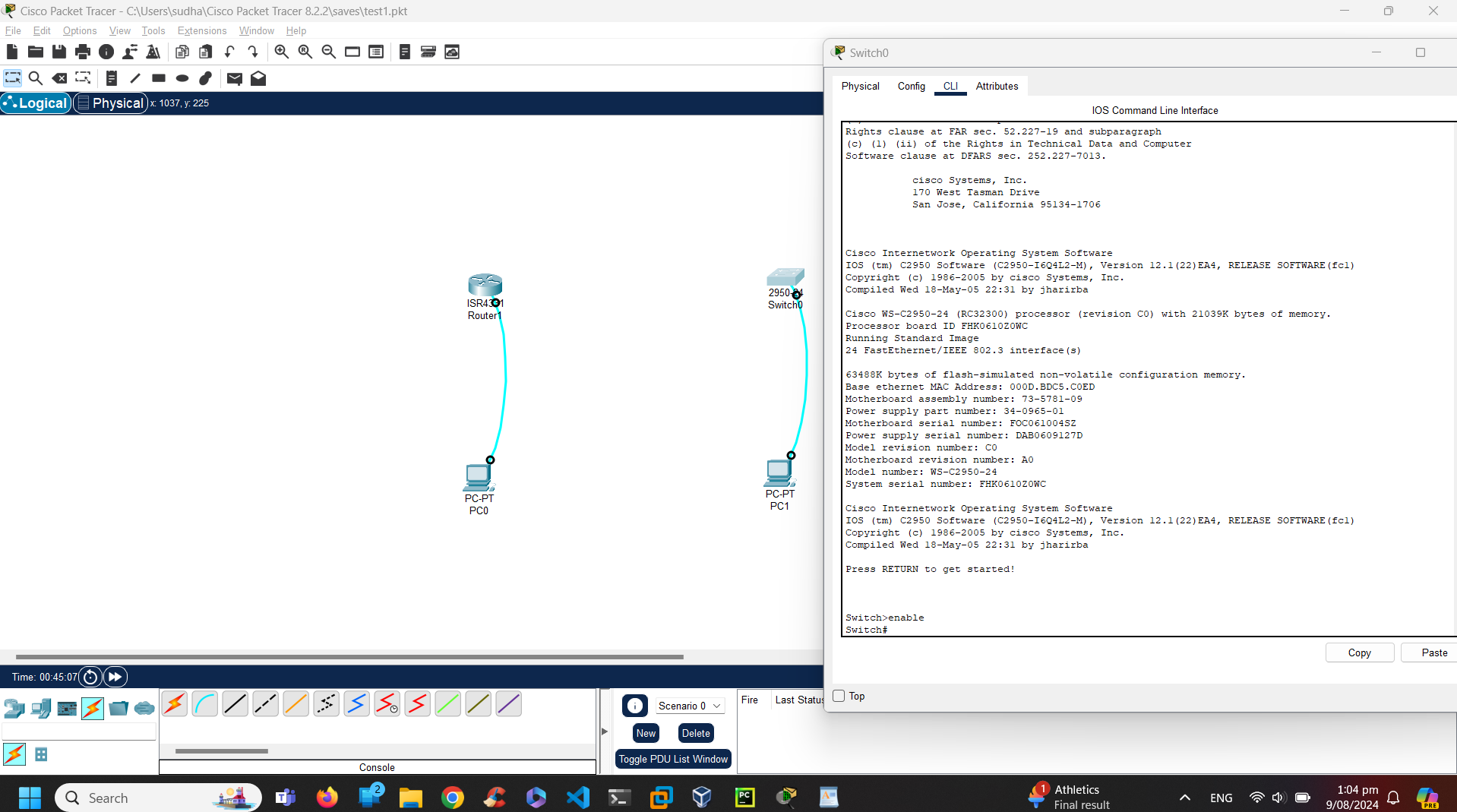


Step: 3 Bypass the initial configuration

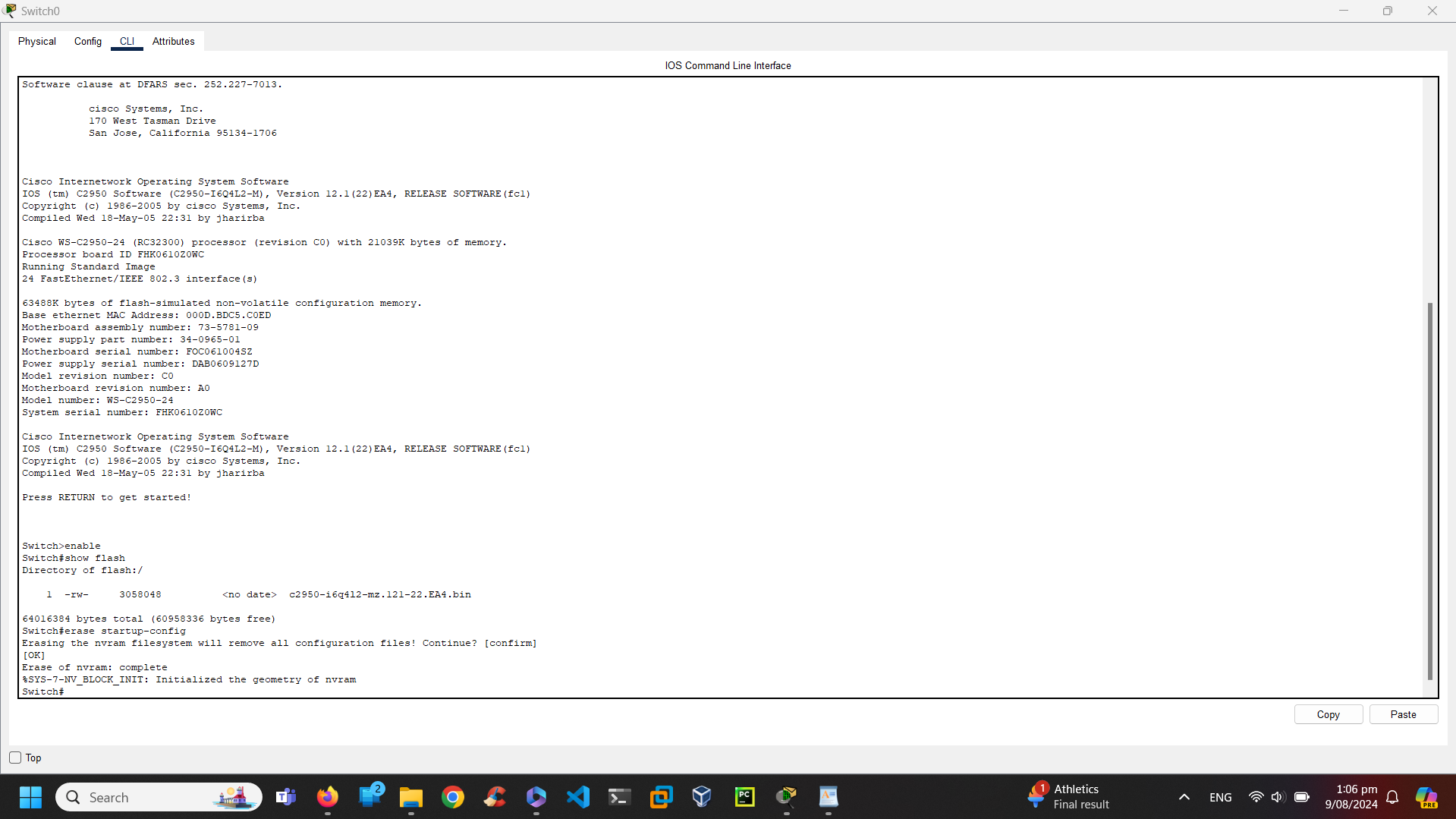


**Part 3: Initialise the switch and router**

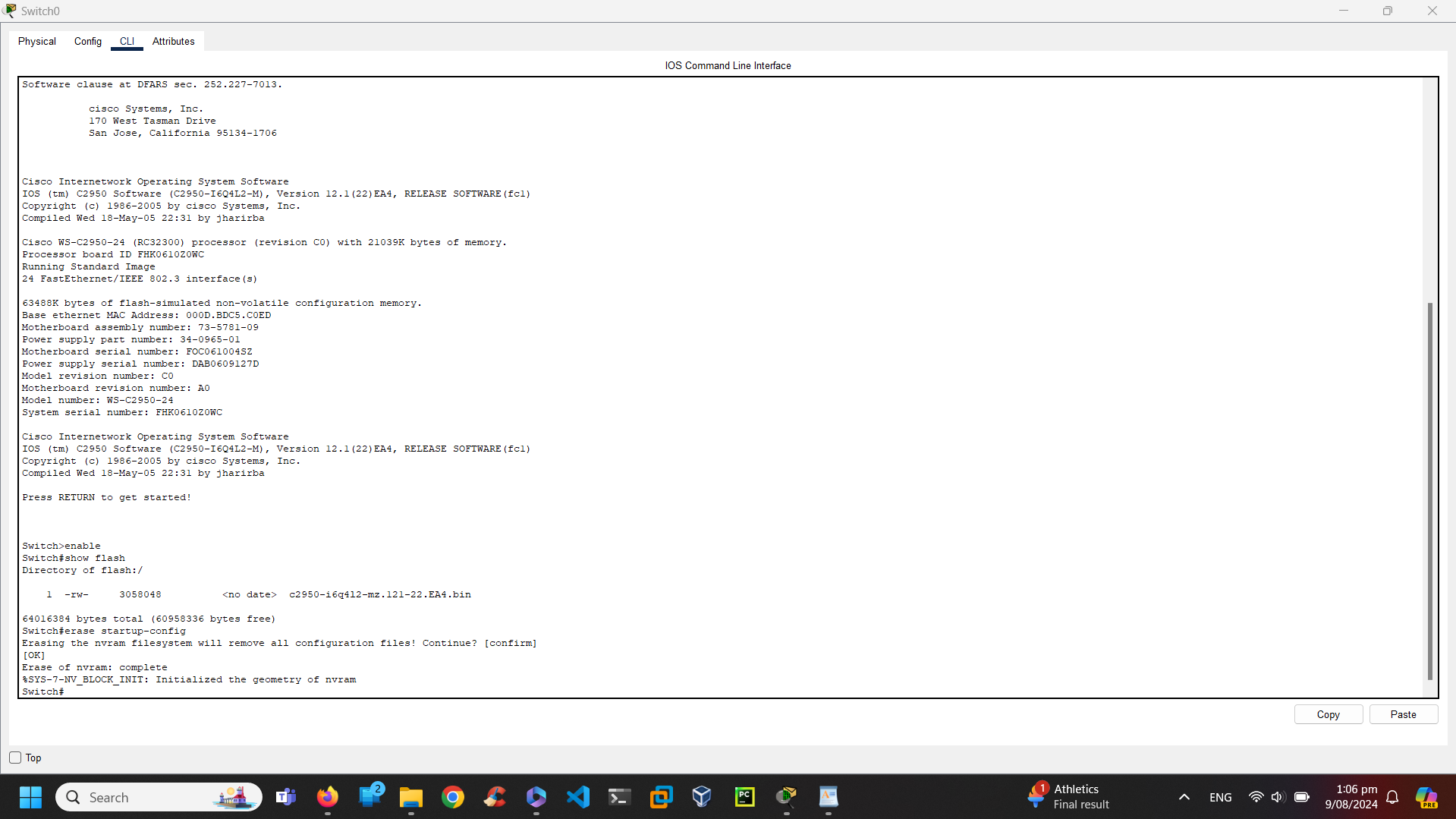
Step 1: Connect to the switch

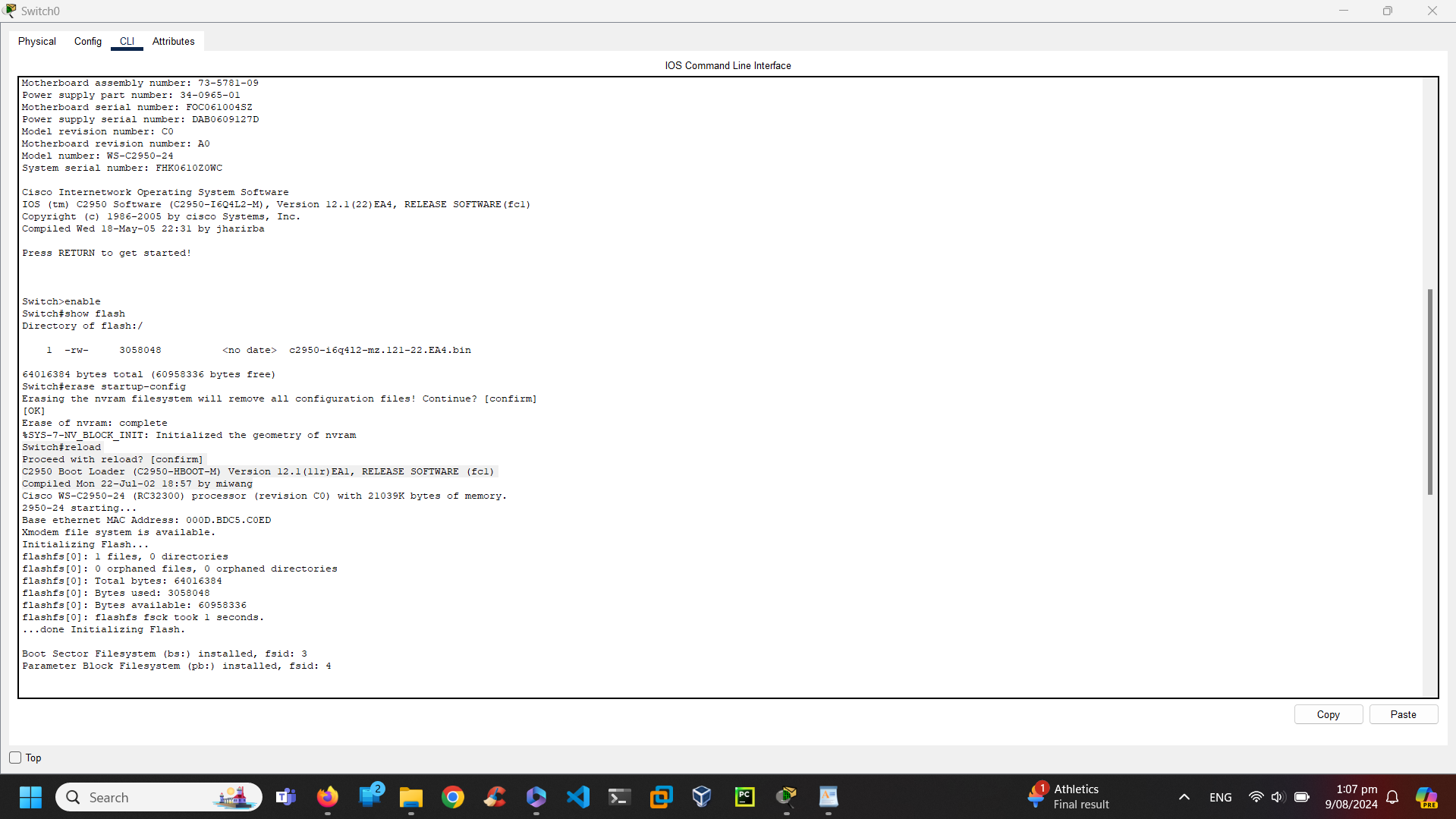
 Step 2: Find any VLAN created

There is no data about VLAN



Step 3: Erase the startup configuration file

Step 5: Reload the switch



1. Why is it necessary to erase the startup configuration before reloading the router?

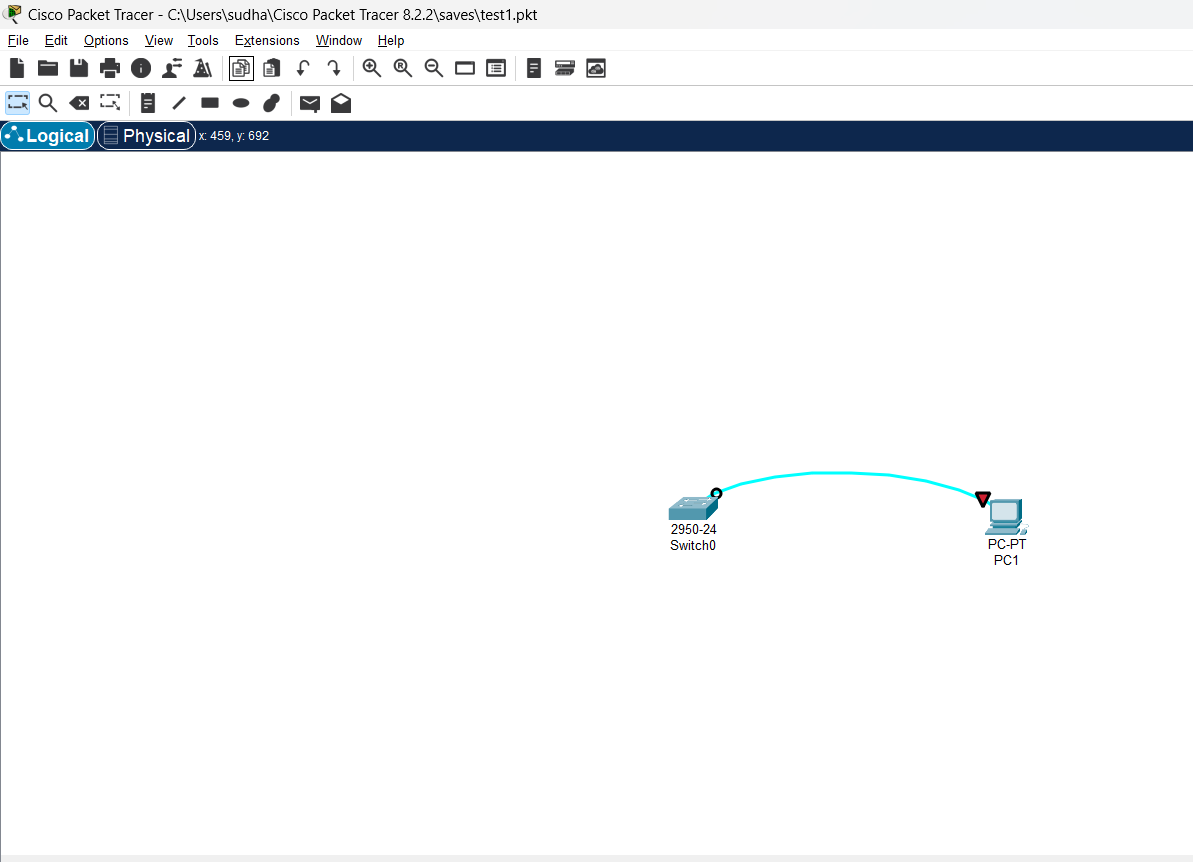
Answer: The old startup configuration may cause conflicts. So, to ensure the new setup is clean and error-free, erase the old one.  
2. You find a couple configurations issues after saving the running configuration to the startup configuration, so you make the necessary changes to fix those issues. If you were to reload the device now, what configuration would be restored to the device after the reload?

Answer: Saving the changes in NVRAM after the startup configuration helps to fix those issues.

**Lab- Configuring a Switch Management Access**

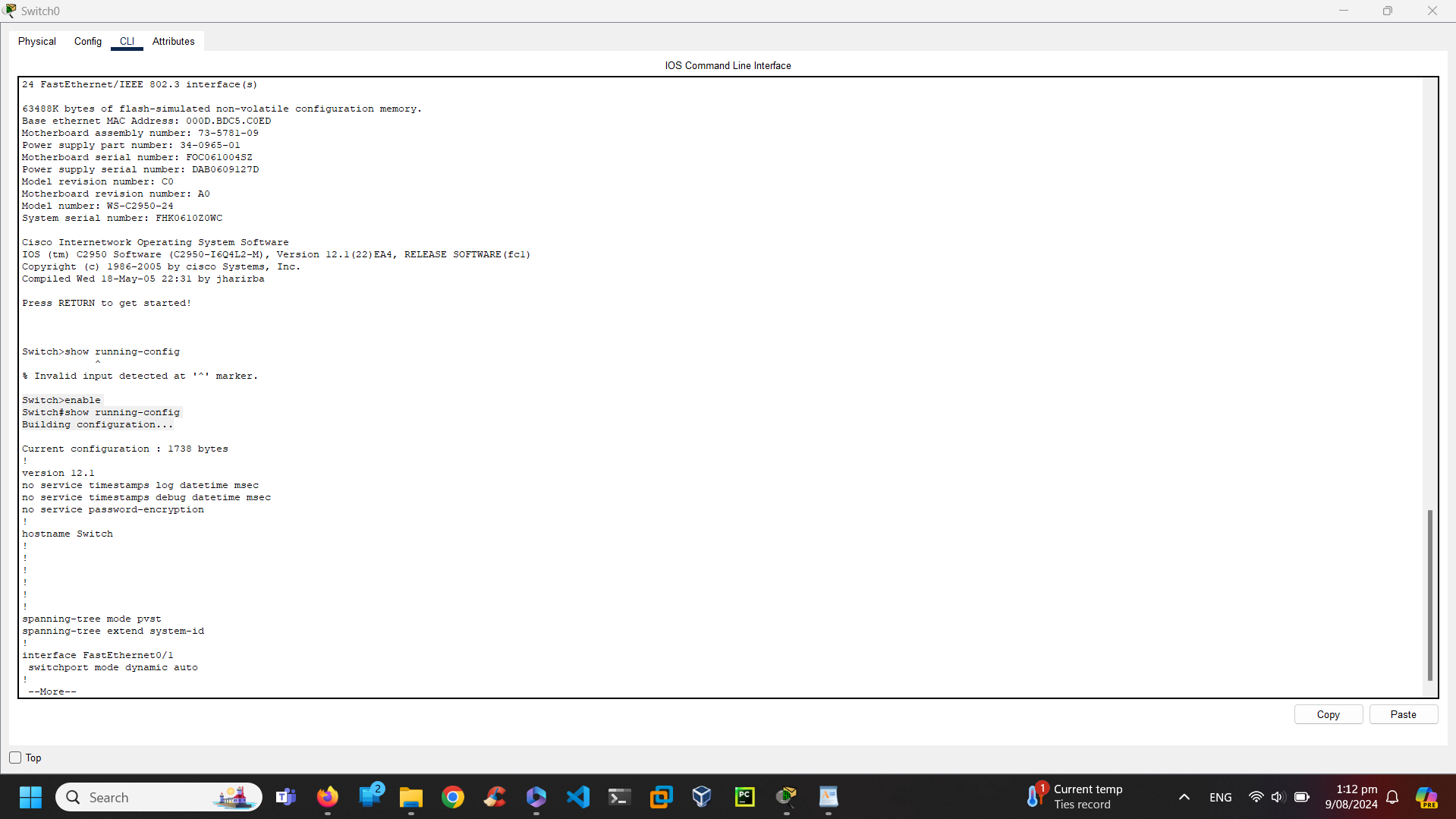
Part 1: Configure a basic network device

Step 1: Cable the network and establish the console connection



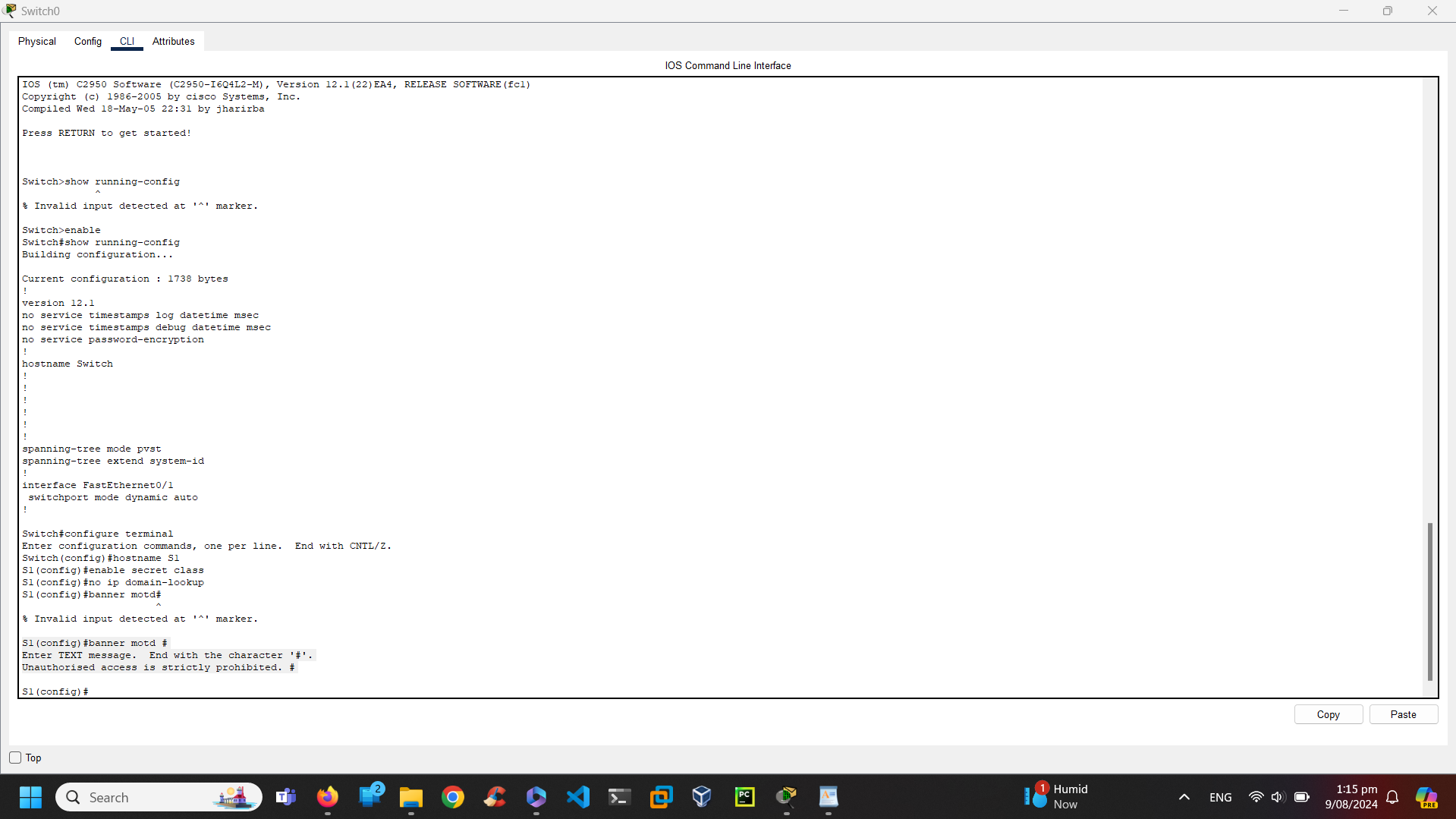
Step 2: Basic switch configuration

1. Enable and show running config

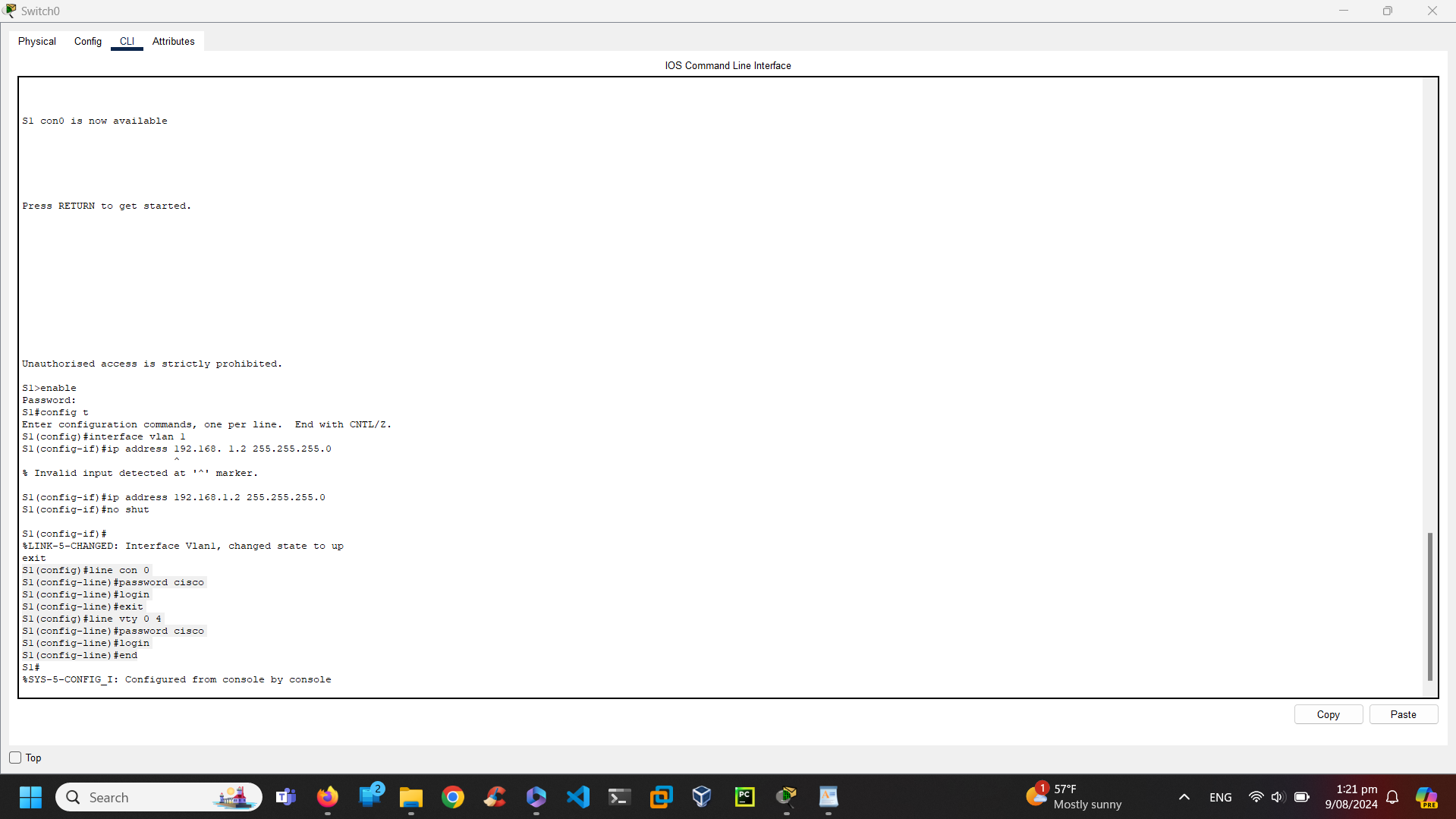
B. Assign the switch hostname S1

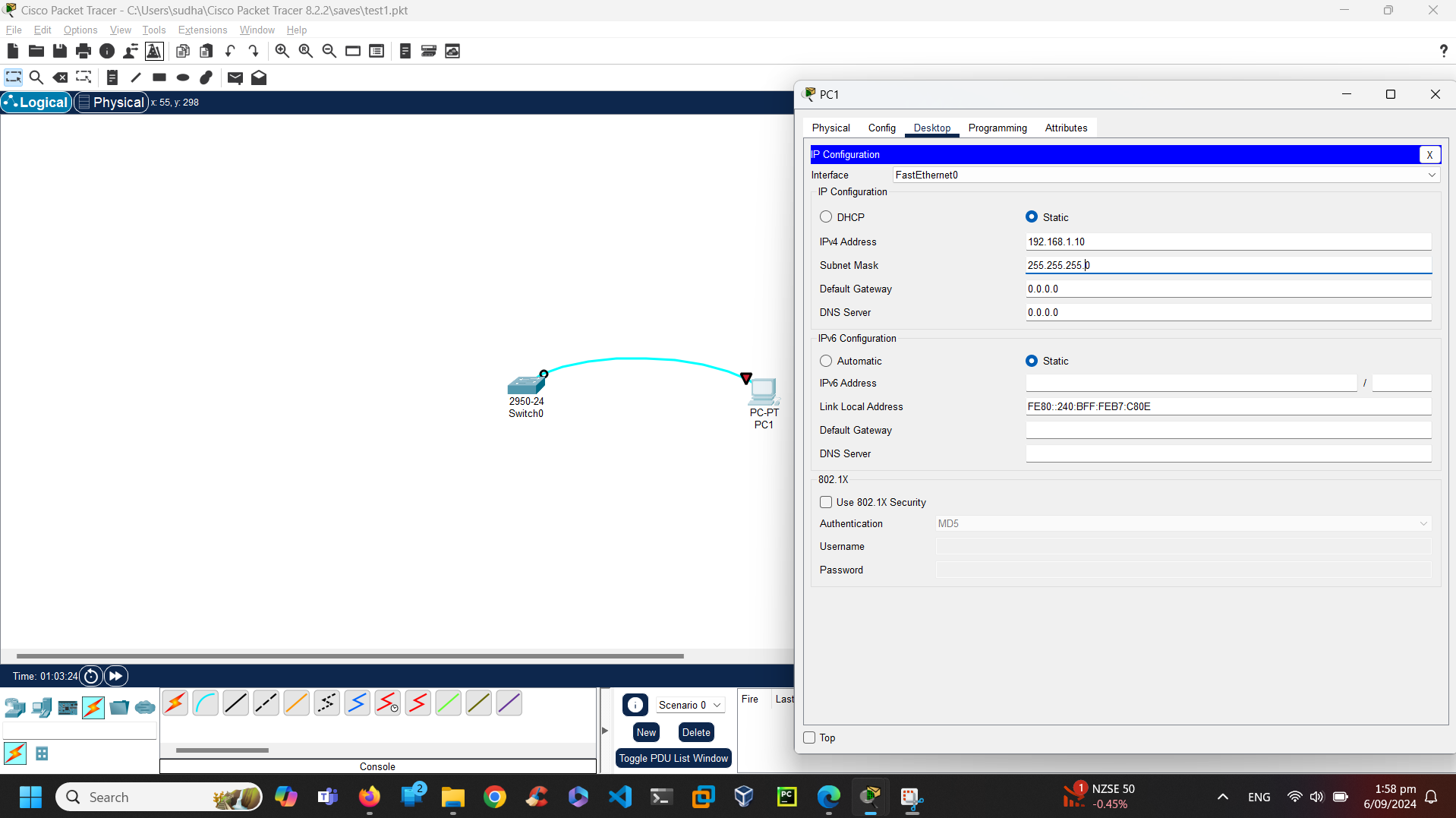
C. Enable secret class and no IP domain lookup to prevent unwanted DNS lookups

D. Message of the day banner.

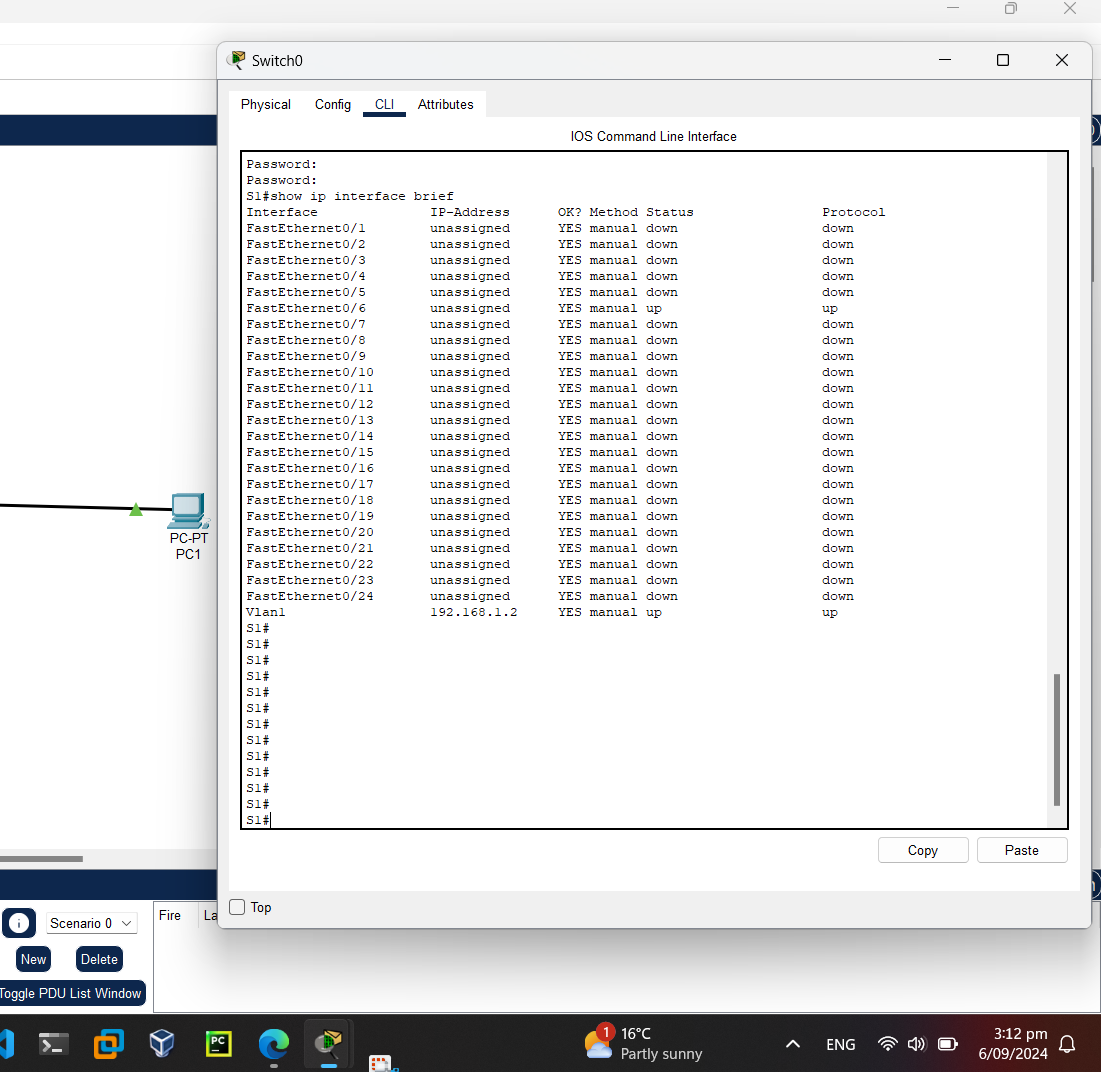
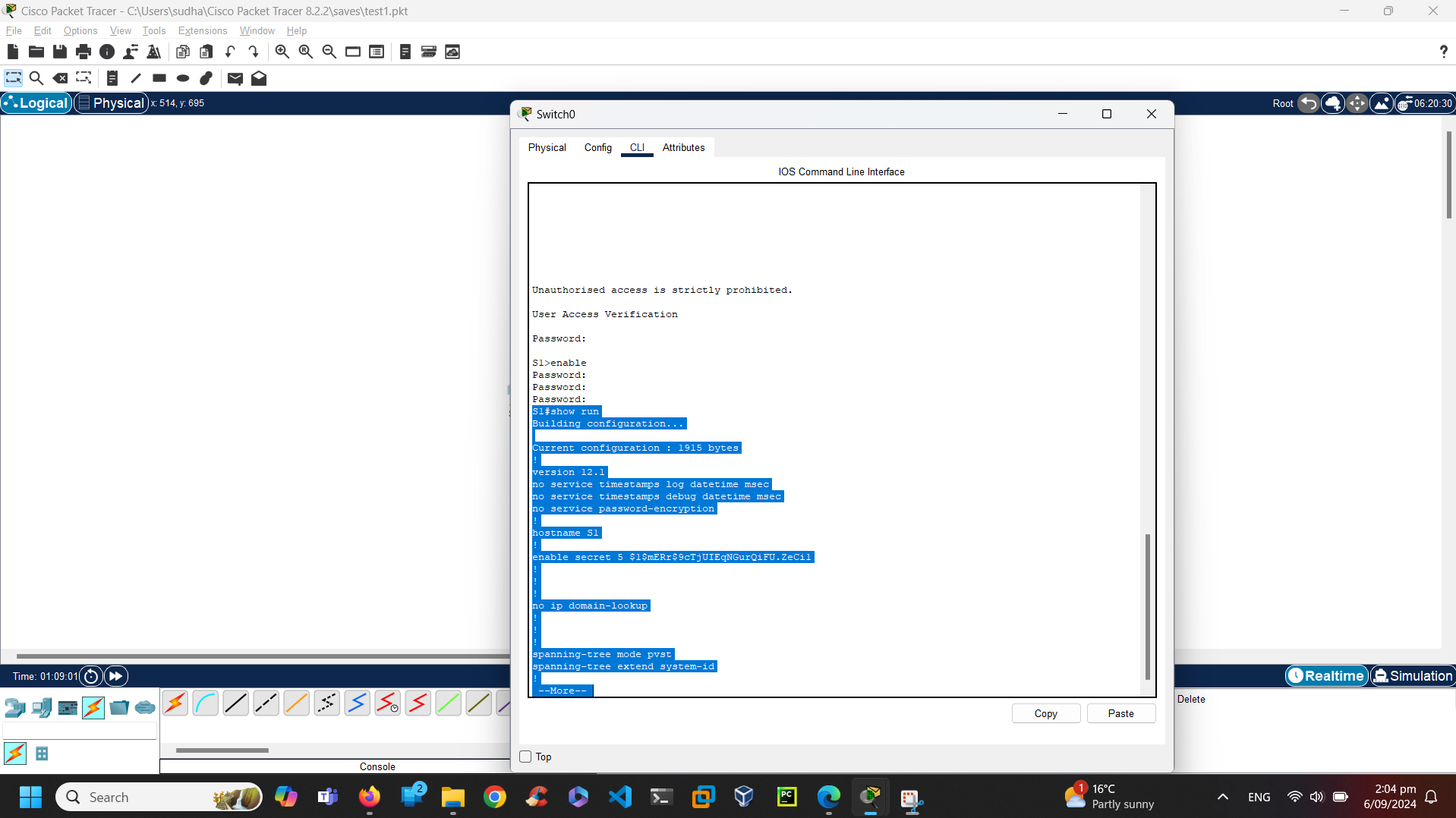
E. Setting up IP addresses and passwords in switch S1

What shortcut keys are used to go directly from global configuration mode to privileged EXEC mode? Exit or Control+Z

STEP 3: Configure an IP address on PC-A

PART 2: Verify and Test Network connectivity

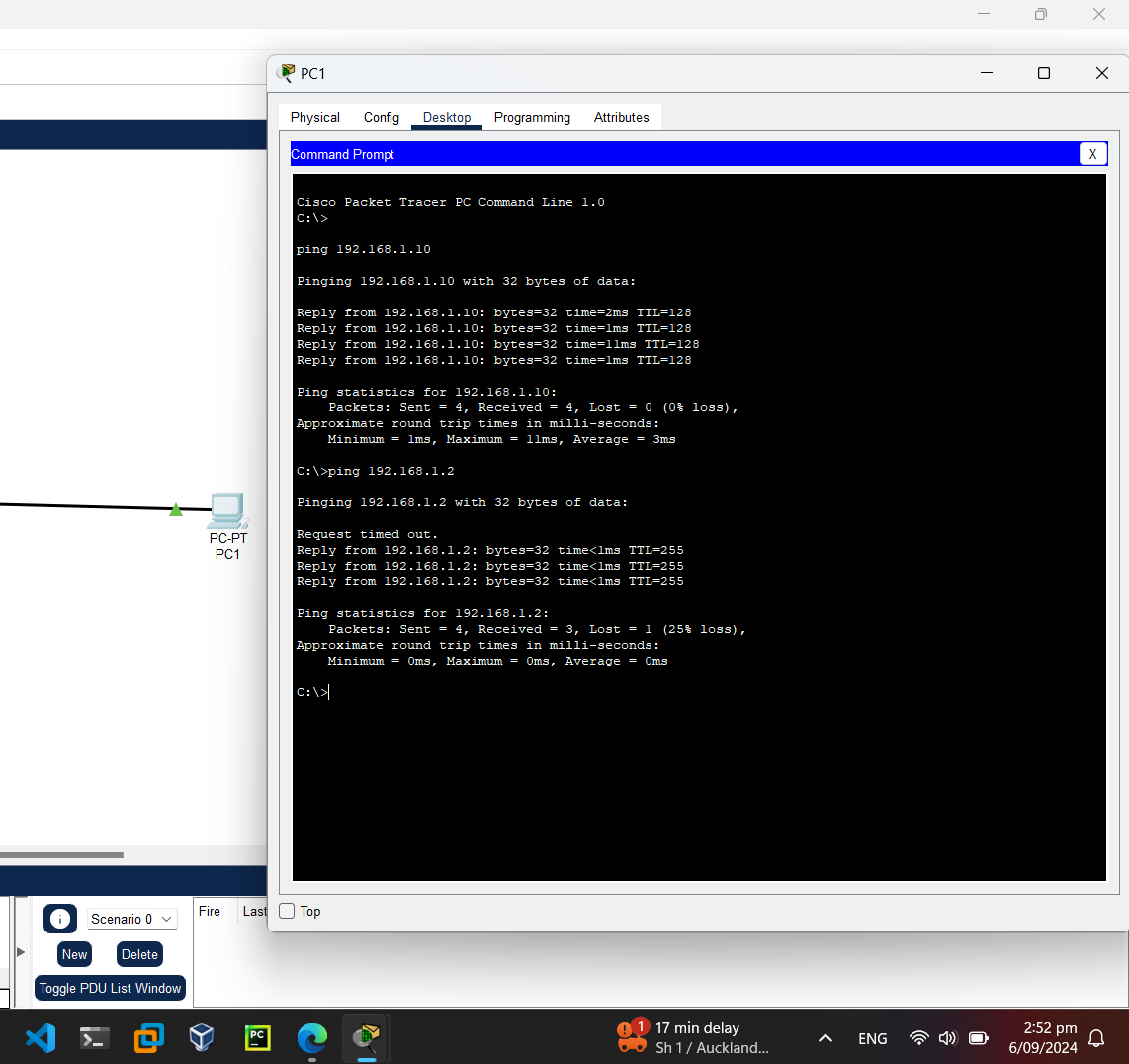
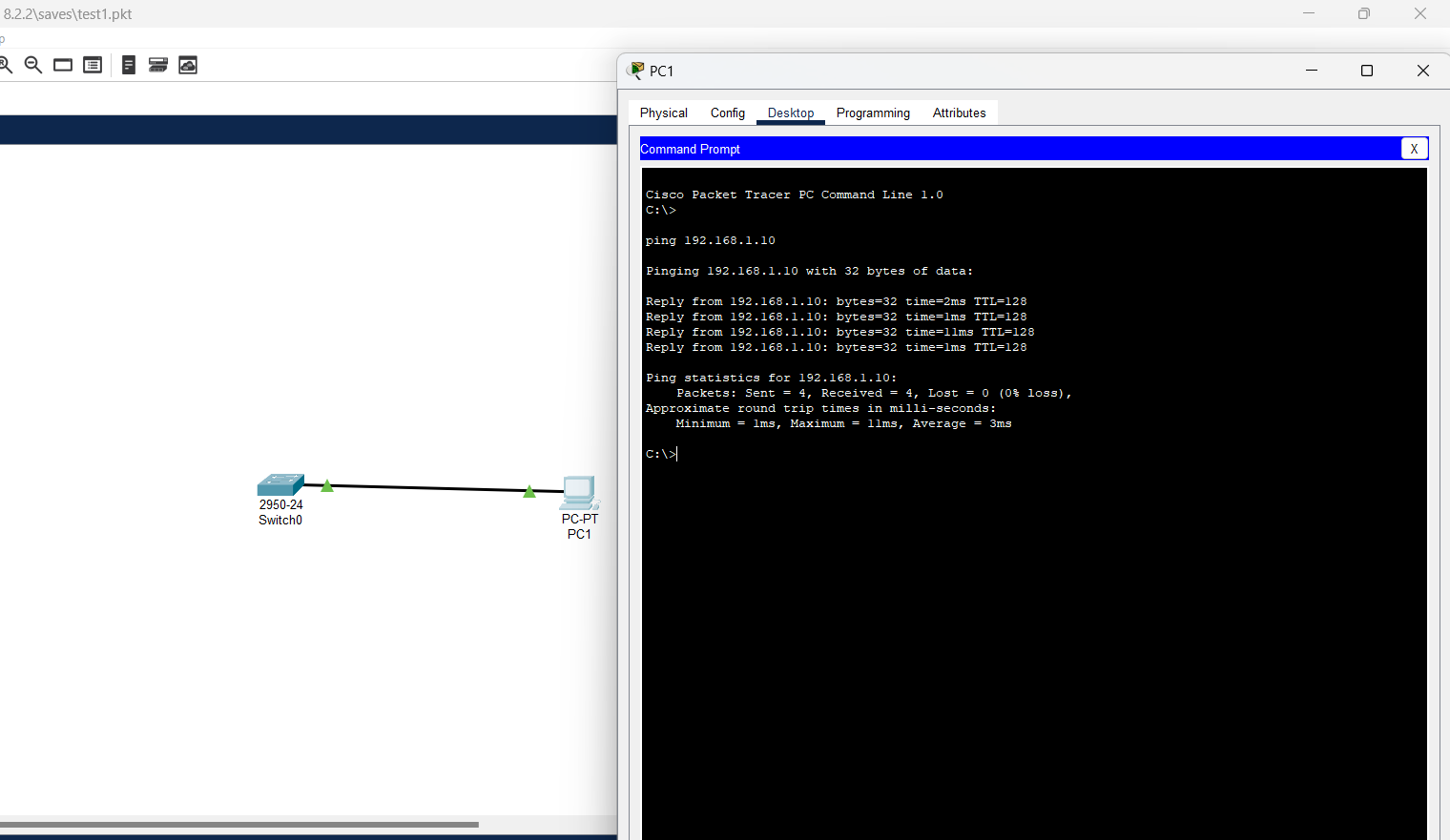
Step1: Display the S1 device configuration

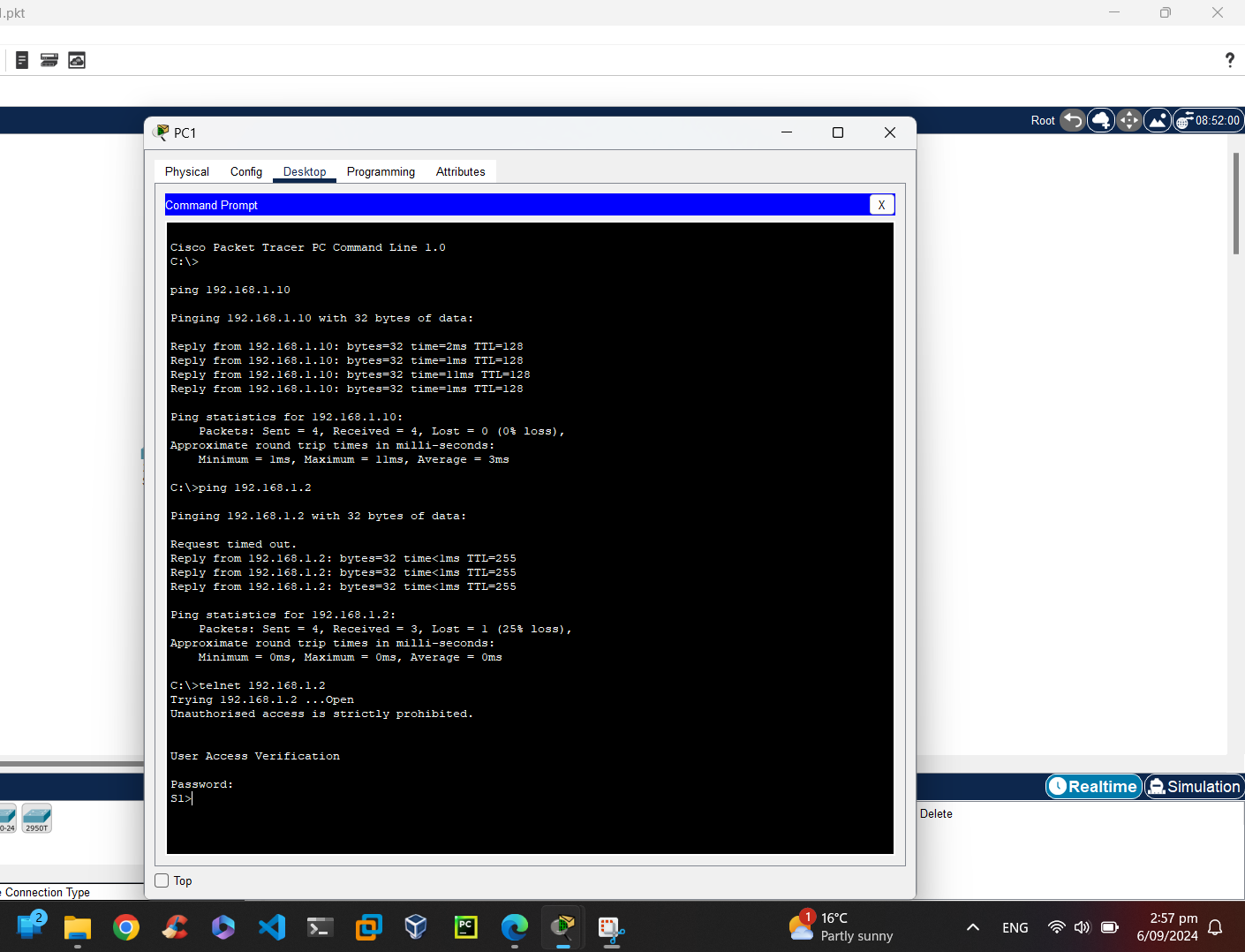


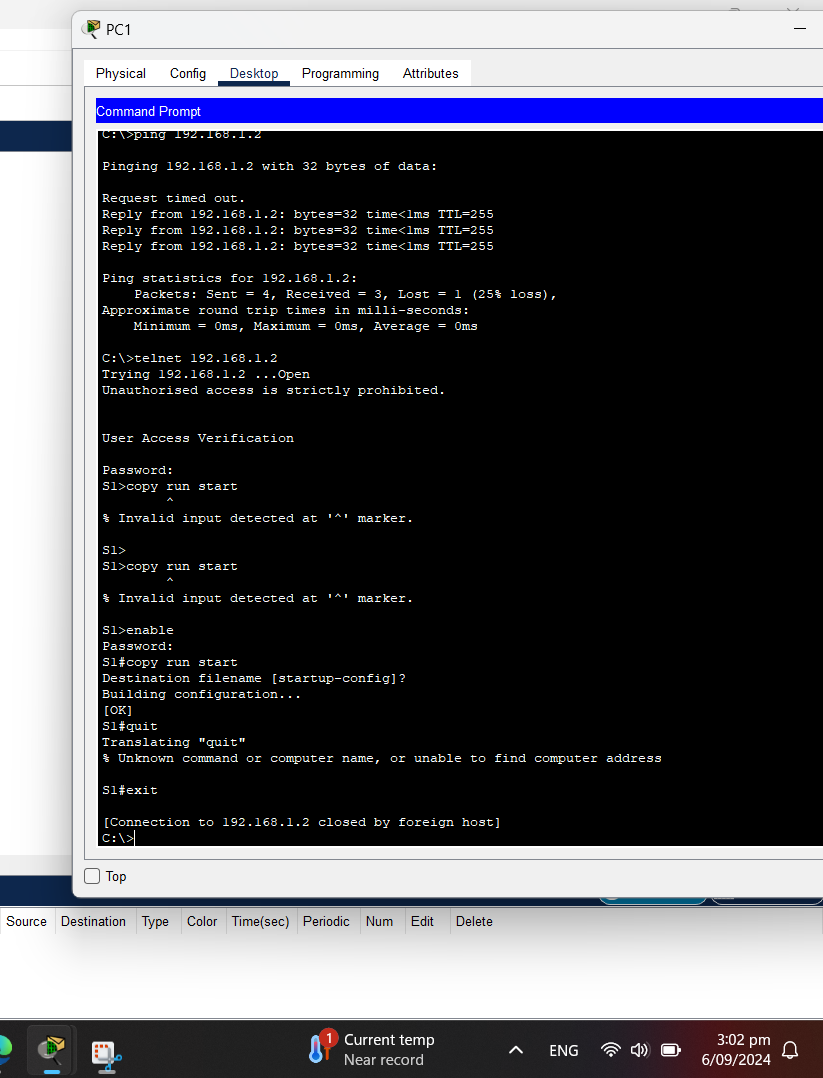
VLAN 1 interface should be up/up and have an IP address assigned. The switch port F0/6 is also up because PC-A is connected to it.

Step 2: Step end to end connectivity

Ping PCA itself and ping it to switch and the screenshots are shown below:

Step3: Test and verify the remote management of S1

Step 4: Save the configuration file



Why must you use a console connection to initially configure the switch? Why not connect to the  
switch via Telnet or SSH?

Answer: Telnet or SSH need network-based connection but switches are not pre-configured. The switches are configured using console connection in the beginning.

1. <https://aws.amazon.com/elasticloadbalancing/> [↑](#endnote-ref-22151)