BIRZEIT UNIVERSITY

Faculty of Engineering and Technology

Department of Electrical and Computer Engineering

ENCS3320 – Computer Networks

Project #2 (Cisco Packet Tracer)

Team members:

Heba Dababat	**ID : 1230151**	**Section: 1**
Hala Soboh	**ID : 1230286**	**Section: 1**
Lujain alawneh	**ID :1230127**	**Section: 1**

Instructor: Dr. Ahmed Shawahna

Submission Date: January/25/2026

Abstract

This project focuses on developing comprehensive competencies in computer network design and implementation. The primary goal is to build both theoretical understanding and hands-on expertise across key networking domains. Participants will design IP addressing schemes through subnetting techniques and utilize Cisco Packet Tracer for creating and simulating network topologies. The project encompasses configuring routing protocols, establishing wireless LAN infrastructures, and mastering essential network diagnostic commands. Beyond technical skills, emphasis is placed on cultivating professional documentation abilities through technical report writing and enhancing collaborative capabilities via team-based project execution. This multifaceted approach ensures participants gain practical experience in network architecture design, configuration, and analysis while developing critical professional competencies essential for careers in network administration and engineering.

Contents

List of Figures

List of Tables

Theory and Procedure

IP Address

An IP (Internet Protocol) address is a unique numerical label assigned to every device on a computer network, acting like a digital home address to identify devices and enable them to send and receive data, ensuring information reaches the correct destination across local networks or the global internet, with versions like IPv4 and the newer IPv6 providing vast address space

(Ref:[1])

Classless Inter-Domain Routing CIDR

A modern method for allocating and routing IP addresses that replaces the old class-based system to make address distribution more efficient. Instead of organizing IP addresses into fixed classes (like Class A, B, or C), CIDR uses a flexible prefix length written as an IP address followed by a slash and a number (for example, /24) to indicate how many bits define the network portion of the address. This classless system allows network administrators to create subnets of varying sizes based on actual needs, reducing wasted address space and improving routing efficiency. CIDR is widely used in today's IP networks because it supports variable-length subnet masking (VLSM) and makes better use of limited IPv4 addresses while simplifying routing on the internet.[6]

Subnetting

Subnetting is the process of dividing a large IP network into smaller logical networks called subnets. Each subnet allows devices to communicate efficiently, improving network performance, security, and manageability. By creating these segmented networks, organizations can optimize bandwidth utilization, reduce broadcast traffic, and implement granular access controls. Subnetting also facilitates logical network organization by grouping devices based on department, function, or geographic location, making troubleshooting and network administration more streamlined. Additionally, it enables more efficient use of IP address space by allocating addresses according to actual network requirements, preventing waste of valuable IP resources. This hierarchical approach to network design provides scalability and flexibility, allowing networks to grow and adapt to changing organizational needs while maintaining optimal performance and security standards.(Ref[2])

Why different subnet sizes are used?

Different subnet sizes are used because not all parts of the network need the same number of IP addresses. Some areas, like the Central LAN, have many devices and require a large subnet, while other parts, such as the ISP link between two routers, only need two IP addresses. By using different subnet sizes, we can allocate just the number of IPs each network needs without wasting addresses. This makes the network more organized, more efficient, and easier to expand in the future.

Subnet Mask

A subnet mask is a 32-bit number used in IP addressing to separate the network portion of an IP addresses from the host portion. It helps computers and devices determine which part of an IP address refers to the network they are present, and which part refers to their specific location or address within that network.(Ref [3])

Figure 1 : Subnet Mask example

Routers

A router is a networking device that controls how data moves between different networks by checking destination IP addresses and choosing the best path

- Forwards data packets between networks
- Works at Layer 3 (Network Layer) of the OSI model
- Selects the best route for data transfer

Routing of a data packet is done by analyzing the destination IP Address of the packet. Look at the below image:

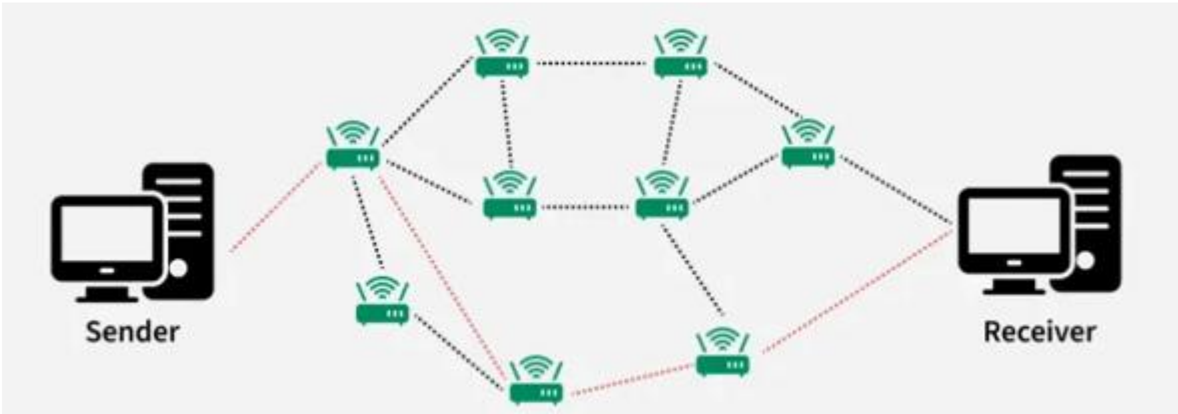


Figure 2 : Routing

The source node (sender) transmits a data packet onto the network, embedding the destination IP address within the packet header. The nearest router receives the packet and, based on routing metrics and its routing table, forwards the packet to the next appropriate router. This forwarding process occurs recursively as the packet travels across multiple routers until it finally reaches its intended destination node.

Router-PT

The Router-PT is a generic router model provided in Cisco Packet Tracer that represents a standard enterprise router with basic routing and interface capabilities. It supports essential networking functions such as IP addressing, static and dynamic routing , and inter-network communication.

Local Area Networking

A Local Area Network (LAN) is a computer network that interconnects devices within a limited geographical area, such as a home, office building, school, or campus. LANs enable multiple devices like computers, printers, servers, and smartphones to communicate and share resources efficiently through wired connections (typically Ethernet cables) or wireless technologies (Wi-Fi). The primary advantages of LANs include high-speed data transfer rates, low latency, enhanced security within the local environment, and cost-effective resource sharing such as printers, storage devices, and internet connections. LANs are typically owned, controlled, and managed by a single organization or individual, making them distinct from Wide Area Networks (WANs) which span larger geographical distances. Modern LANs commonly use TCP/IP protocols for communication and can be configured in various topologies including star, bus, or mesh configurations, with star topology being the most prevalent in contemporary networks due to its reliability and ease of troubleshooting.

There are several Common types of Local Area Networks (LAN) each designed for different usage environments and needs :

- Wired LAN
- Wireless LAN
- Virtual LAN
- Hybrid LAN

Wired Local Area Network (LAN)

A wired LAN connects devices such as computers, servers, IoT devices, and other electronic equipment to a company network using Ethernet cables and switches. In small organizations or businesses with a limited number of devices, a wired LAN may consist of a single unmanaged switch that provides Ethernet ports to connect all devices together. This type of network is widely used because it offers high speed, stable connections, and reliable performance, making it suitable for environments where devices remain in fixed locations, such as offices, labs, and data centers.[4]

wireless Local Area Network (LAN)

A wireless LAN (WLAN) is a wireless computer network that connects two or more devices using radio communication to form a local area network within a limited area such as a home, school, computer laboratory, campus, or office building. WLAN technology allows users to move freely within the coverage area while remaining connected to the network, providing flexibility and mobility that wired networks cannot offer. Through a wireless access point and a gateway, a WLAN can also provide connectivity to the wider Internet, enabling wireless devices such as laptops and smartphones to access network resources and online services efficiently. (Ref [4])

Switches

A switch is a network device used to connect multiple devices within the same local area network (LAN), such as PCs, laptops, servers, and access points. It works like an intelligent traffic controller: instead of sending data to all devices, it forwards each data frame only to the device that matches the destination MAC address. This makes communication faster and reduces unnecessary network traffic. Switches help improve network performance, support full-duplex communication, and make the network more organized and reliable, which is why they are essential in modern network designs .Ref[5]

Figure 3 : Switching

Procedure

The main ip address according to ID = 1230286

X = 02 and Y = 86

So the main IP is : 102.86.128.0/17

Based on the main IP address 102.86.128.0/17 and the number of required hosts for each subnetwork shown in Table 1, a Variable Length Subnet Masking (VLSM) approach was used to allocate IP address ranges efficiently. Table 2 presents the final subnetting plan, including the network address, broadcast address, usable IP range, and CIDR notation for each subnetwork.

Table 1 : Number of hosts for each network Table

Subnet	Hosts	Subnet Size	CIDR
C-LAN	500	512	/23
W-LAN1	200	256	/23
W-LAN2	260	512	/23
W-WLAN	480	512	/23
E-LAN1	112	128	/25
E-LAN2	150	256	/24
E-WLAN	550	1024	/22
ISP-Link	2	4	/30

Table 2 : Subnetworking Table

Subnetwork	CIDR	Network IP	First usable IP	Las usable IP	Broadcast IP
C-LAN	/23	102.86.132.0	102.86.132.1	102.86.133.254	102.86.133.255
W-LAN1	/24	102.86.138.0	102.86.138.1	102.86.138.254	102.86.138.255
W-LAN2	/23	102.86.136.0	102.86.136.1	102.86.137.254	102.86.137.255
W-WLAN	/23	102.86.134.0	102.86.134.1	102.86.135.254	102.86.135.255
E-LAN1	/25	102.86.140.0	102.86.140.1	102.86.140.126	102.86.140.127
E-LAN2	/24	102.86.139.0	102.86.139.1	102.86.139.254	102.86.139.255
E-WLAN	/22	102.86.128.0	102.86.128.1	102.86.131.254	102.86.131.255
ISP-Link	/30	102.86.140.128	102.86.140.129	102.86.140.130	102.86.140.131

Network Topology :

The network topology is designed to connect multiple areas (West, Main Campus, and East) using routers, with the Main Campus acting as the central network. Each area contains its own LAN that connects PCs and laptops through switches using wired connections, in addition to wireless access points that provide WLAN access for mobile devices such as smartphones and laptops.

Routers are used to route traffic between the different areas and to connect the internal network to an ISP. The network is segmented into different subnets, with each router interface assigned a static IP address to ensure organized addressing and efficient routing. Area 0 is used as the backbone to allow smooth communication between all parts of the network.

This topology improves network performance, reduces unnecessary traffic, and allows the network to be easily managed and expanded in the future.

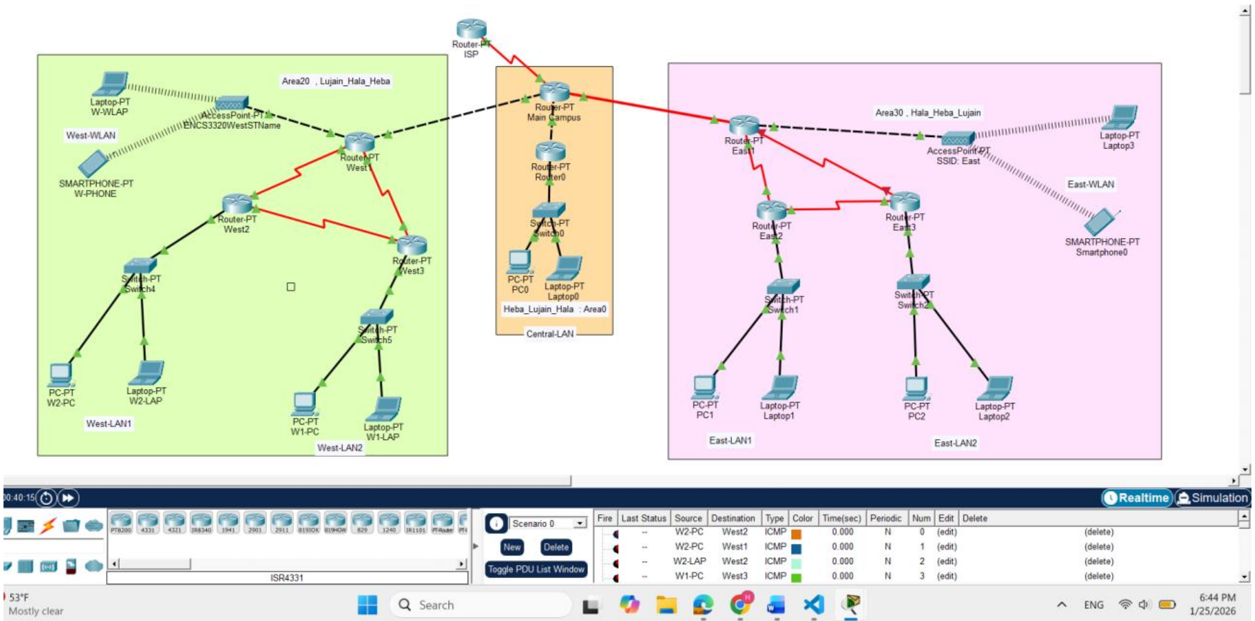


Figure 4 : Network Topology

Area 0 details :

It consists of one subnetwork (Central LAN) , Two Routers (Router-PT) , One switch (switch-PT) ,and two end devices with statics IP as follows :

- PC 200th host in the subnet : 102.86.132.200
- Laptop 350th host in the subnet : 102.86.133.95

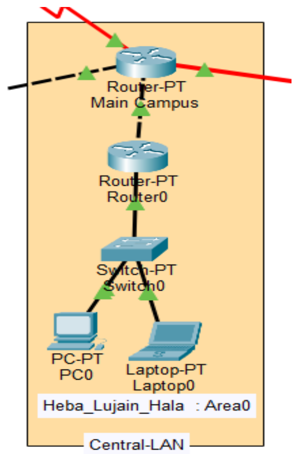


Figure 5 : Central Campus network (Area 0)

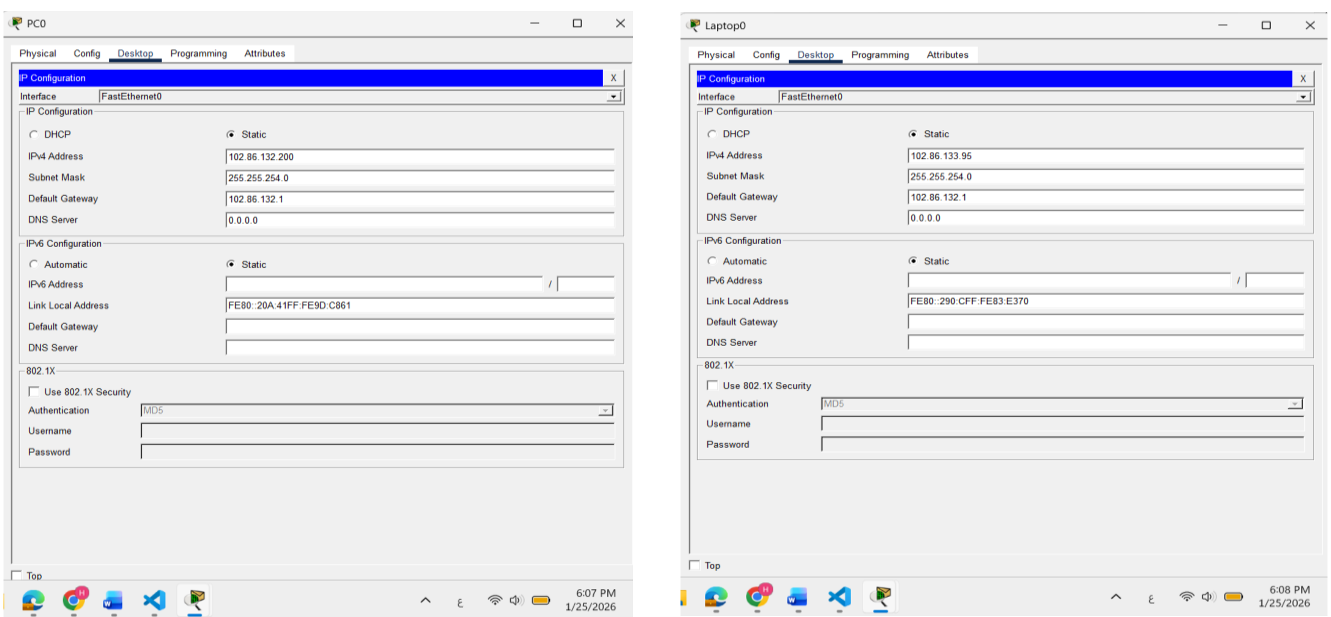


Figure 6 : Area 0 devices IPs

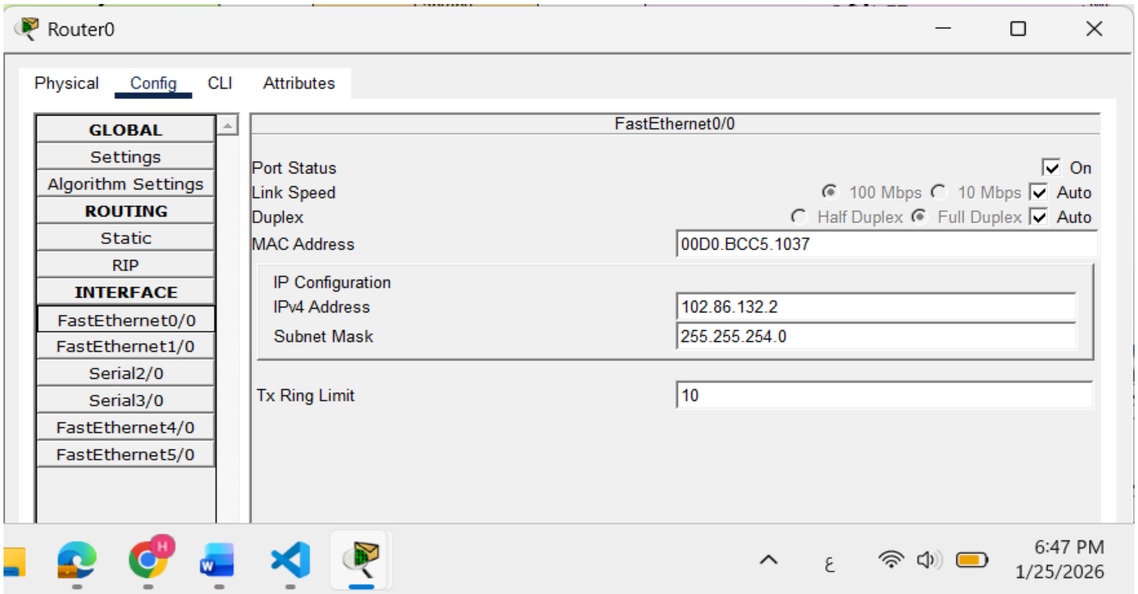


Figure 7 : Area0 Router IPs

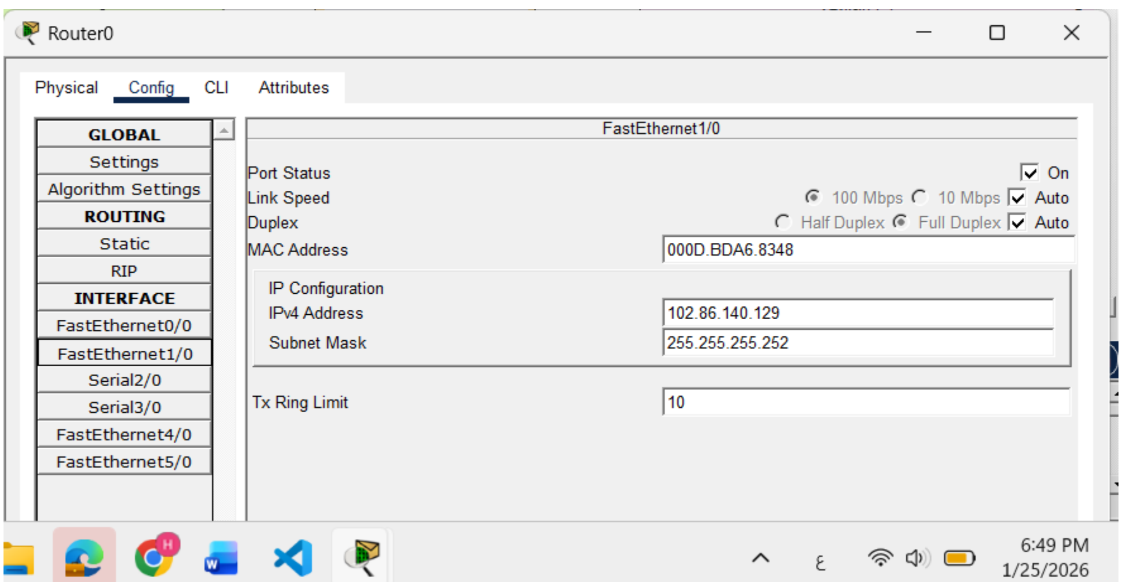


Figure 8 : Area0 Router Ips

Area 20 details :

It consists of three subnetworks (West LAN1, West LAN2 and West WLAN) , Three routers (Router-PT) , Two switches (Switch-PT) , One wireless access point (AccessPoint-PT) ,And other devices as follows :

West LAN1 :

- PC 50th host in the subnet : PC: 102.86.138.50
- Laptop 80th host in the subnet : Laptop: 102.86.138.180

West LAN2 :

- PC 114th host in the subnet : 102.86.136.114
- Laptop 258th host in the subnet : 102.86.137.2

West WLAN :

- PC 80th host in the subnet : 102.86.134.80
- Laptop 438th host in the subnet : 102.86.135.182

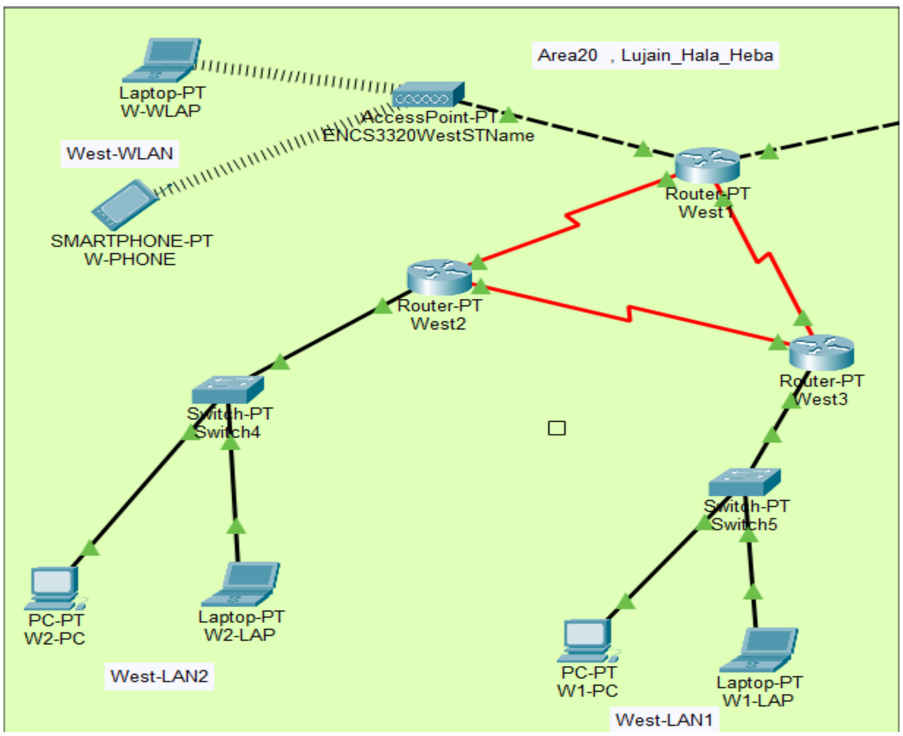
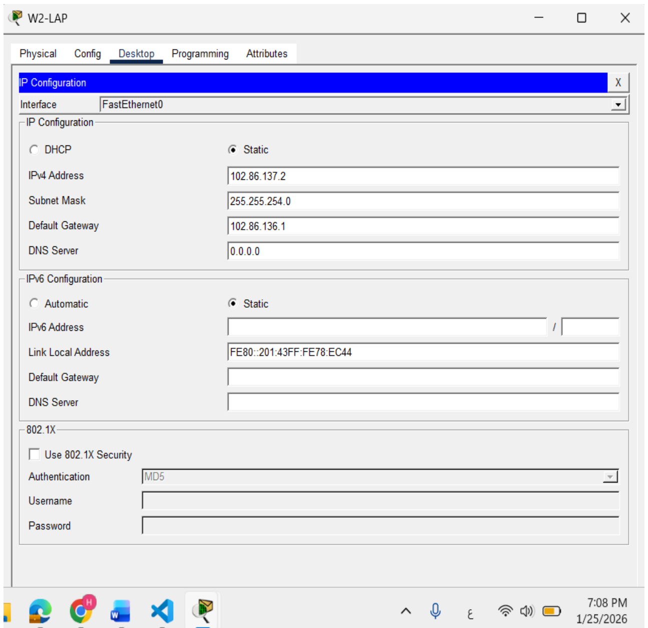


Figure 9 : West network (Area 20)

West-LAN2 devices :



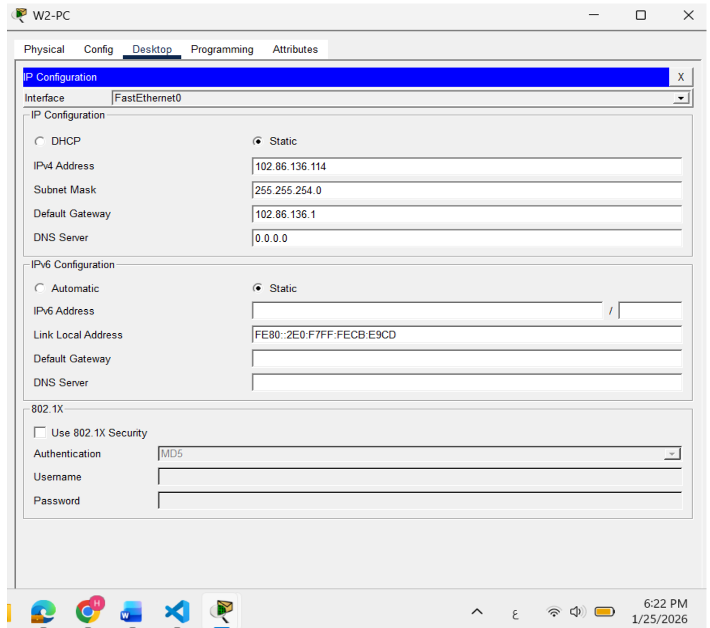
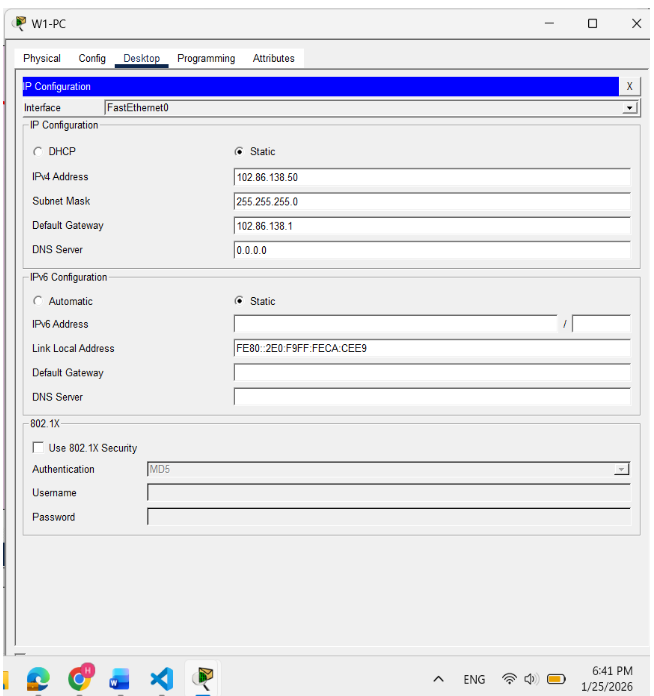


Figure 10 : West LAN2 devices IPs

West-LAN1 devices :



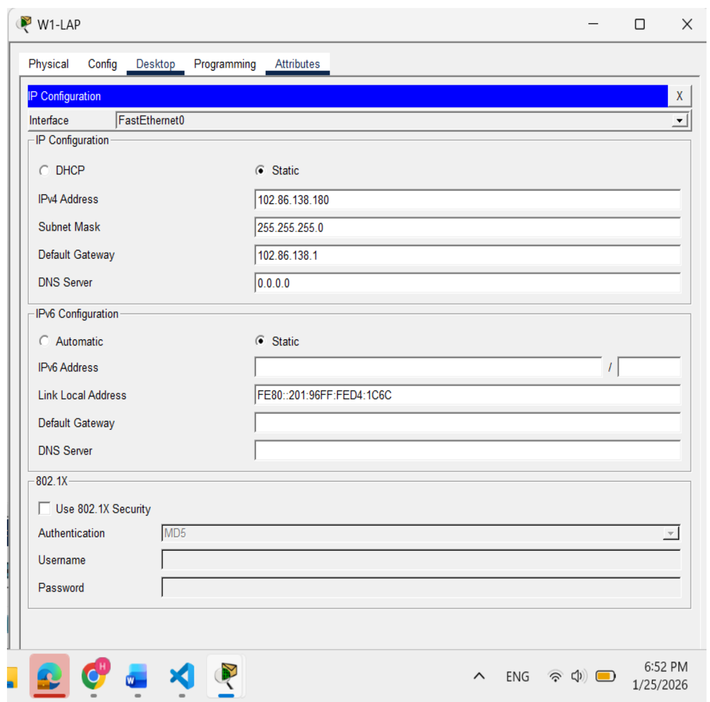


Figure 11 : West-LAN1 devices IPs

West-WLAN devices :

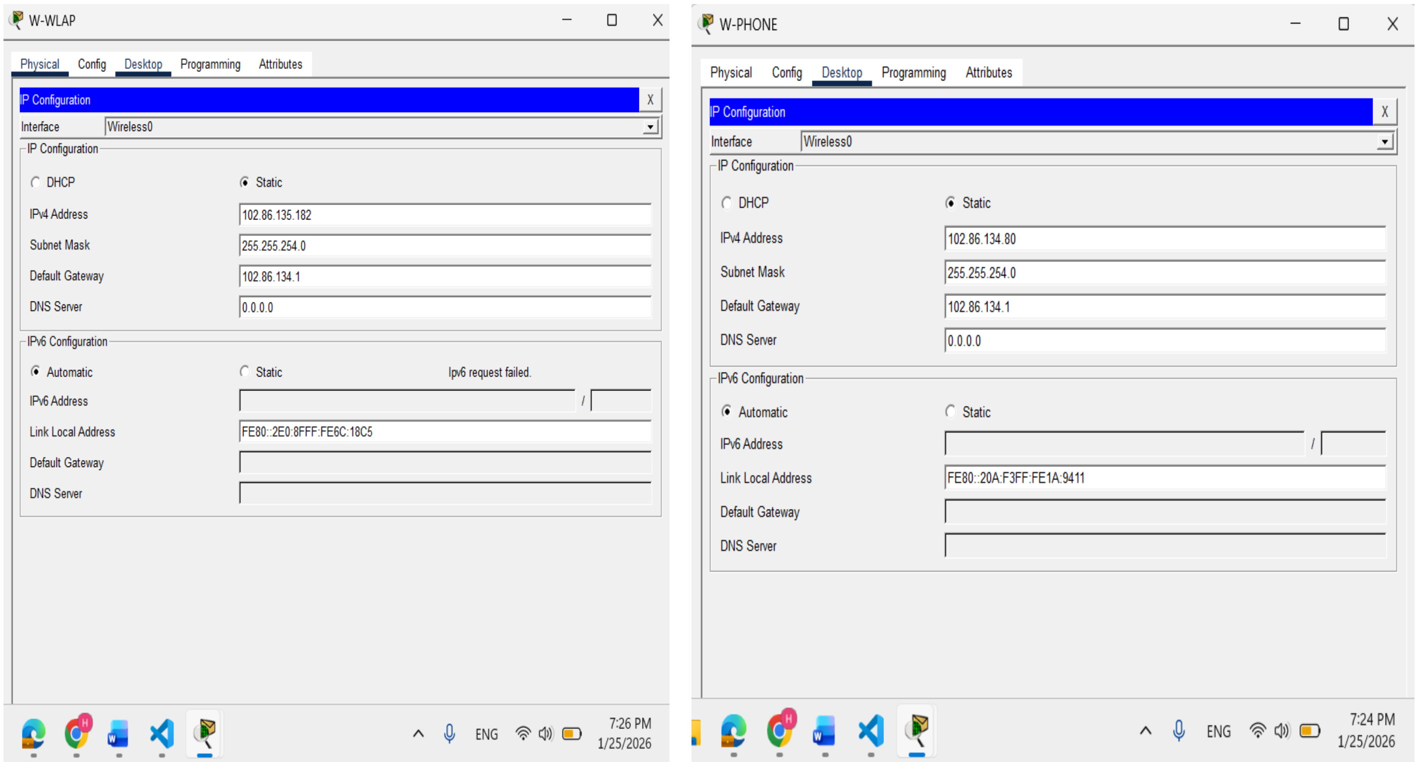


Figure 12 : West-WLAN devices IPs

West-LAN2 Router :

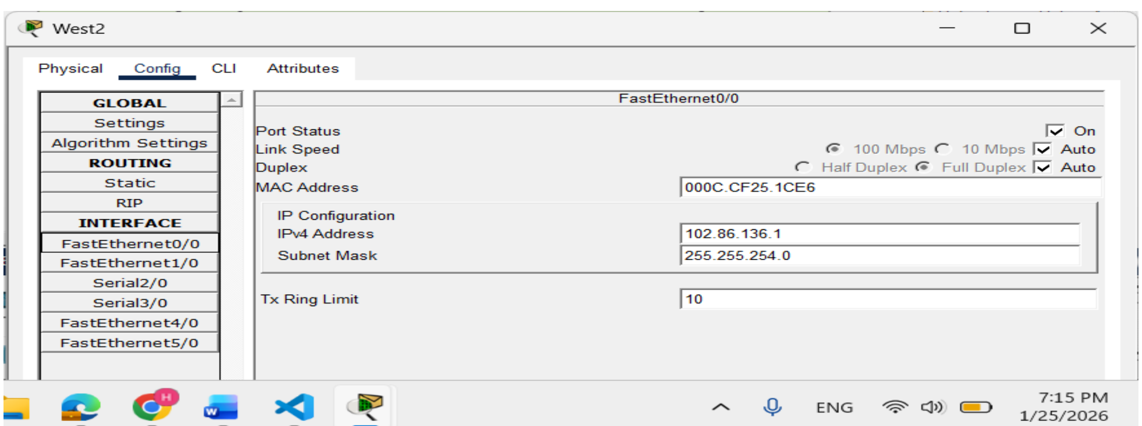


Figure 13 : West-LAN2 Router IPs configuration

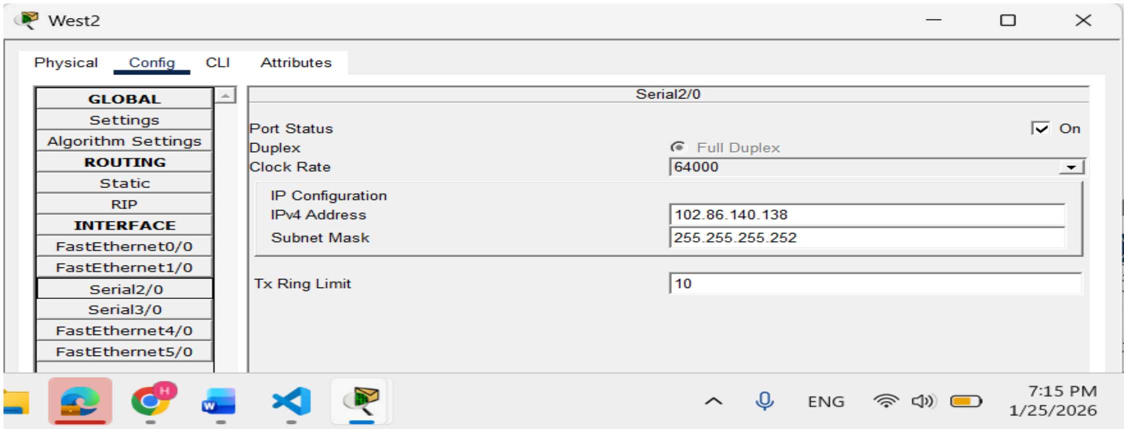


Figure 14 : West-LAN2 Router IPs configuration

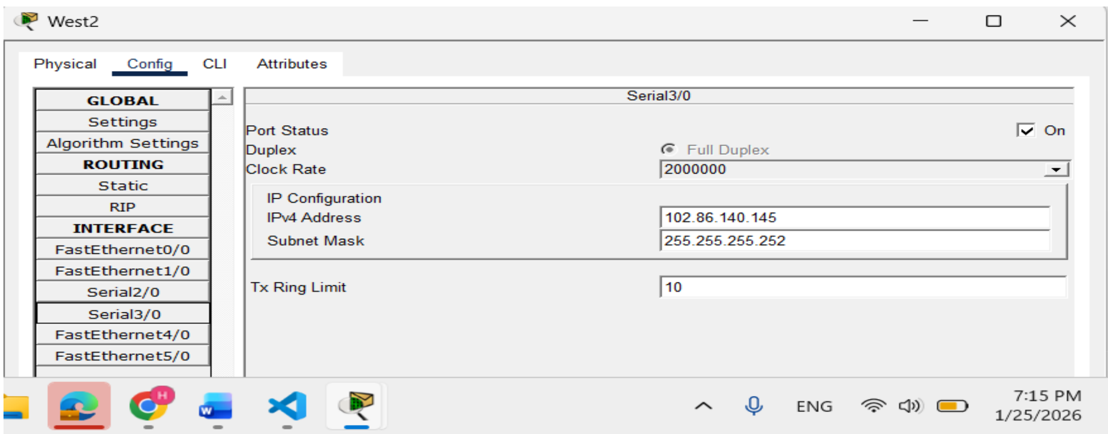


Figure 15 : West-LAN2 Router IPs configuration

West-LAN1 Router :

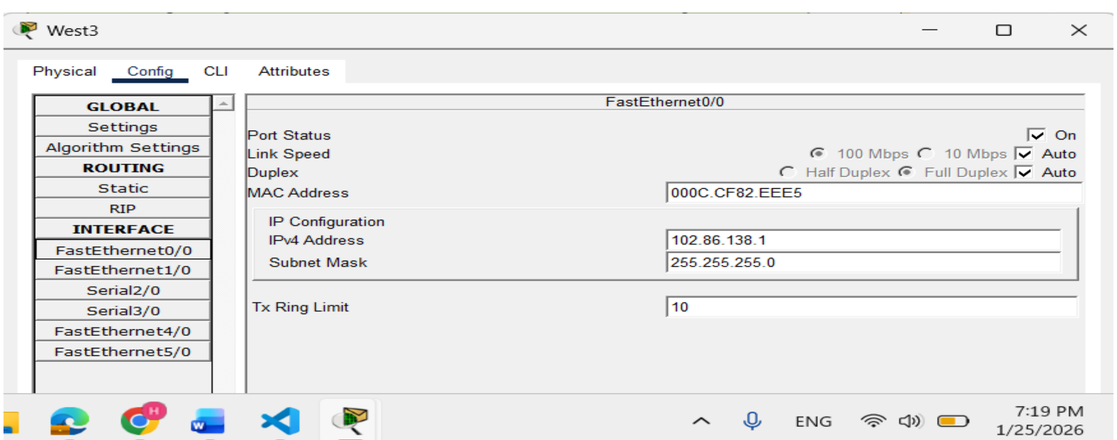


Figure 16 : West-LAN1 Router IPs configuration

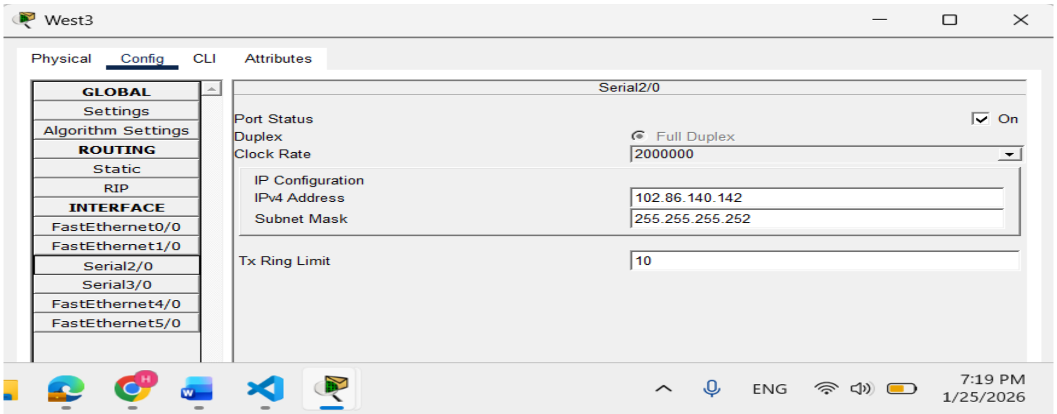


Figure 17 : West-LAN1 Router IPs configuration

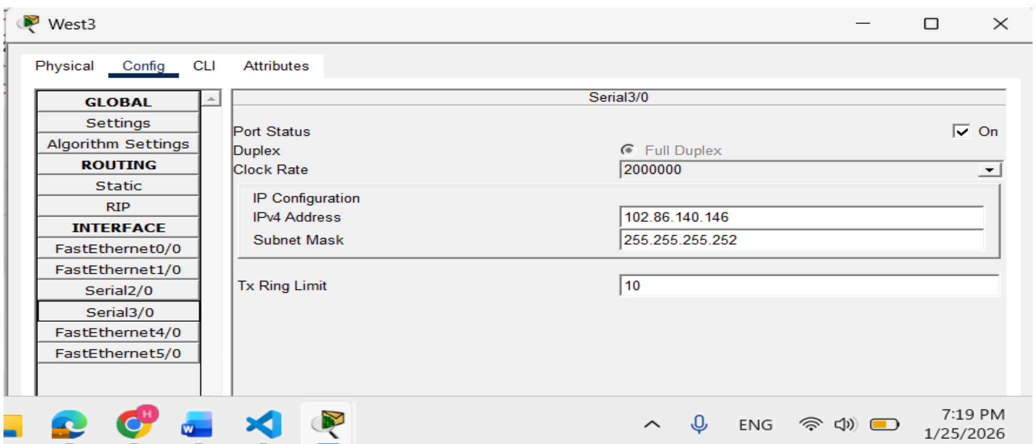


Figure 18 : West-LAN1 Router IPs configuration

West-WLAN Access Point :

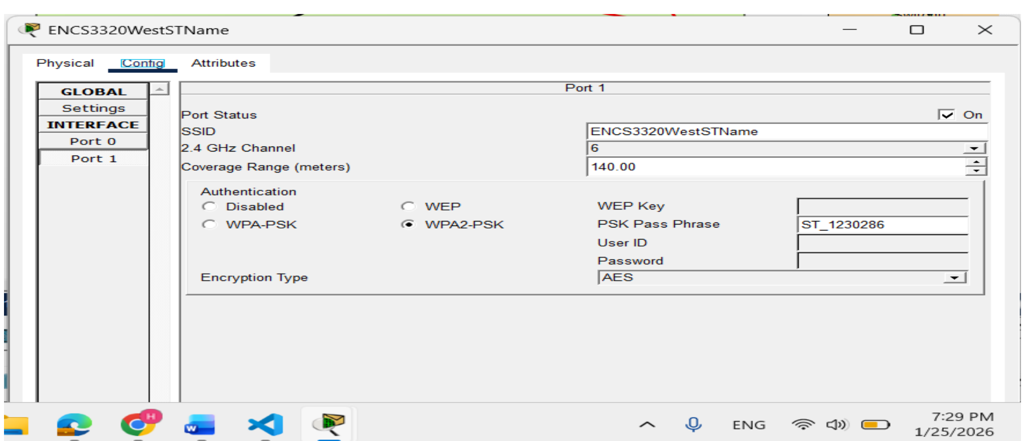


Figure 19 : West-WLAN Access Point

Area 30 details :

E-LAN1 :

- PC (30th host): 102.86.140.30
- Laptop (110th host): 102.86.140.110

E-LAN2 :

- PC (70th host): 102.86.139.70
- Laptop (145th host): 102.86.139.145

E-WLAN :

- PC (15th host): 102.86.128.15
- Laptop (540th host): 102.86.130.28

ISP Link :

- Campus router : 102.86.140.129
- ISP Router : 102.86.140.130

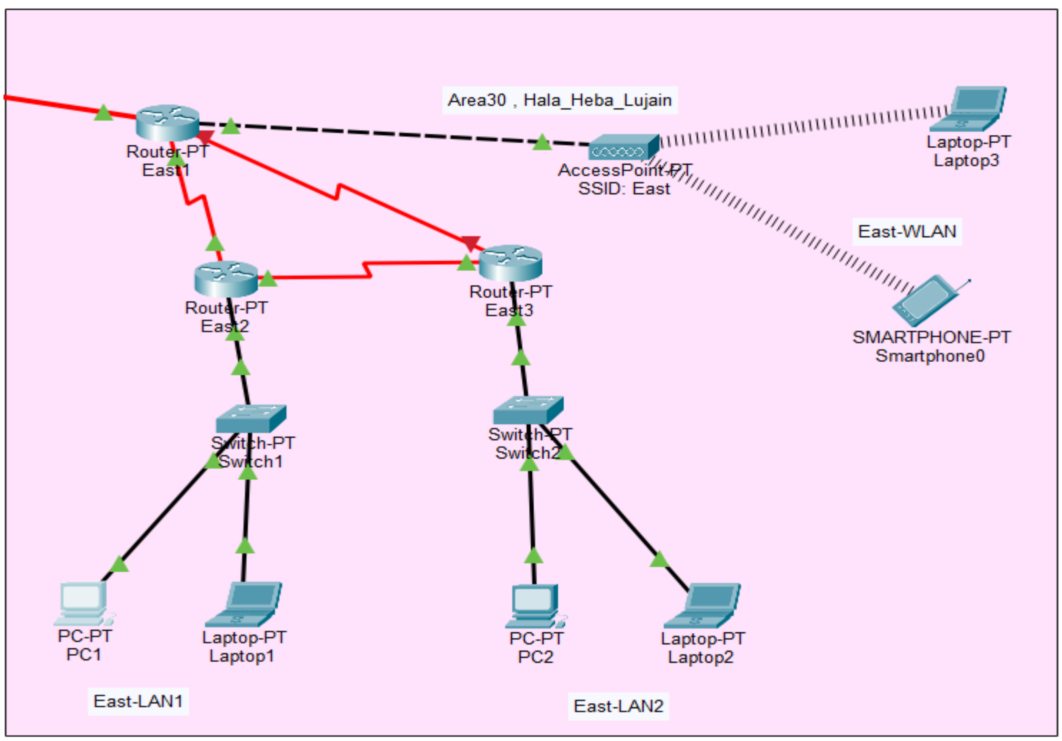
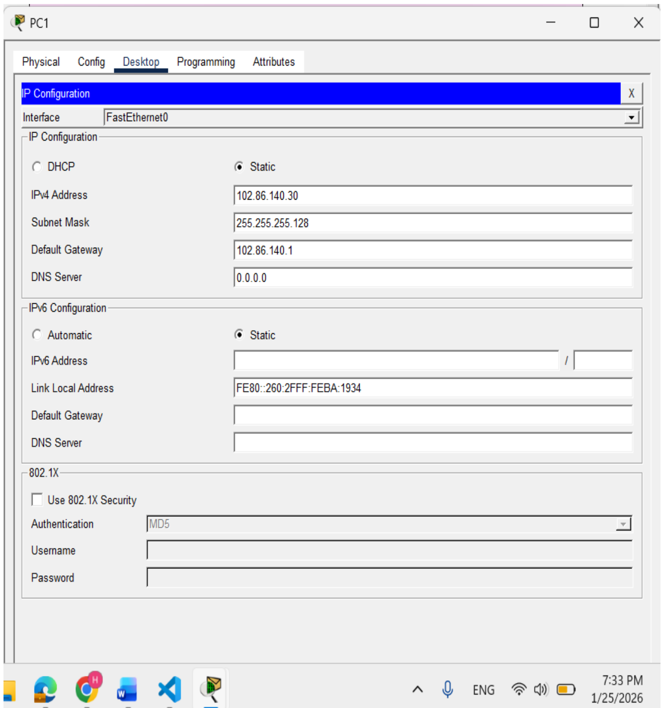


Figure 20 : East network (Area 30)

East-LAN1 devices :



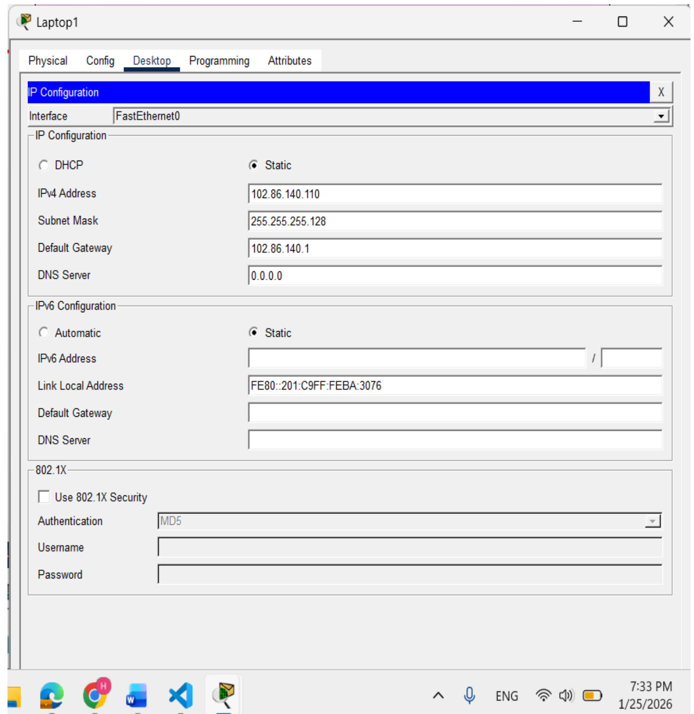
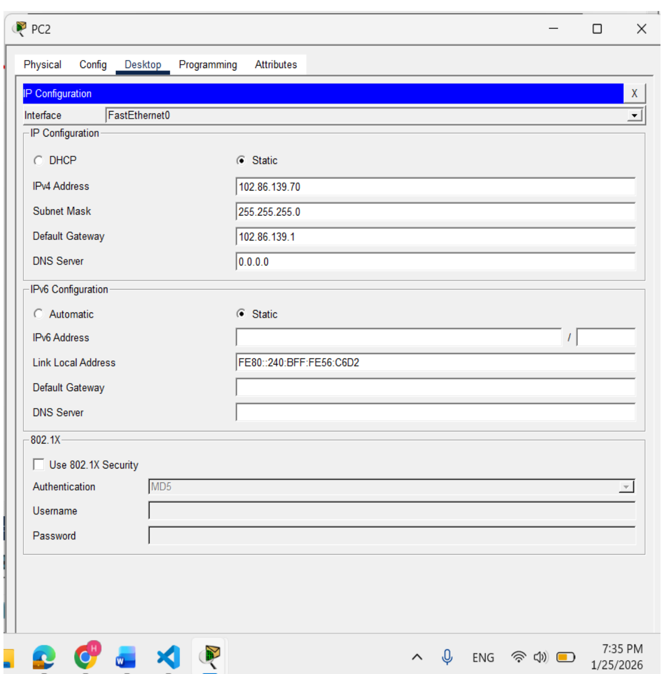


Figure 21 : East-LAN1 devices IPs

East-LAN2 devices :



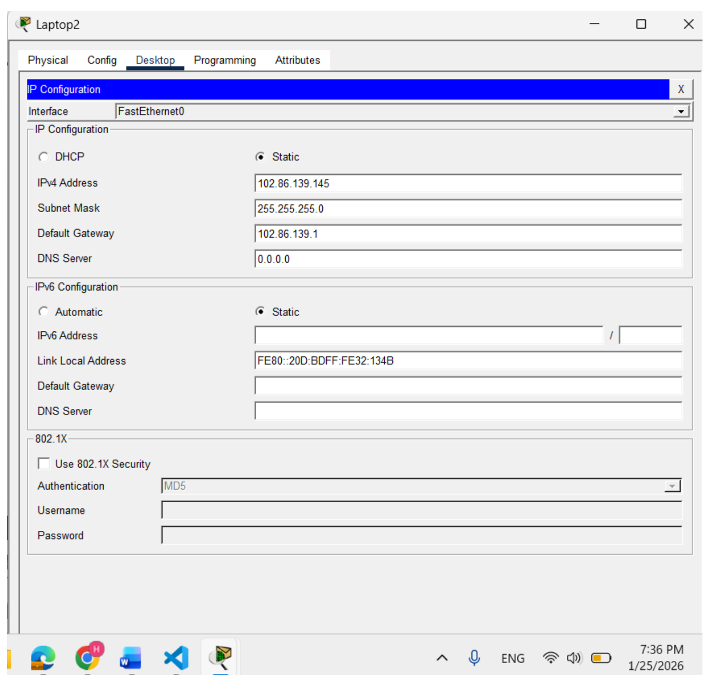


Figure 22 : East-LAN2 devices IPs

East-WLAN devices :

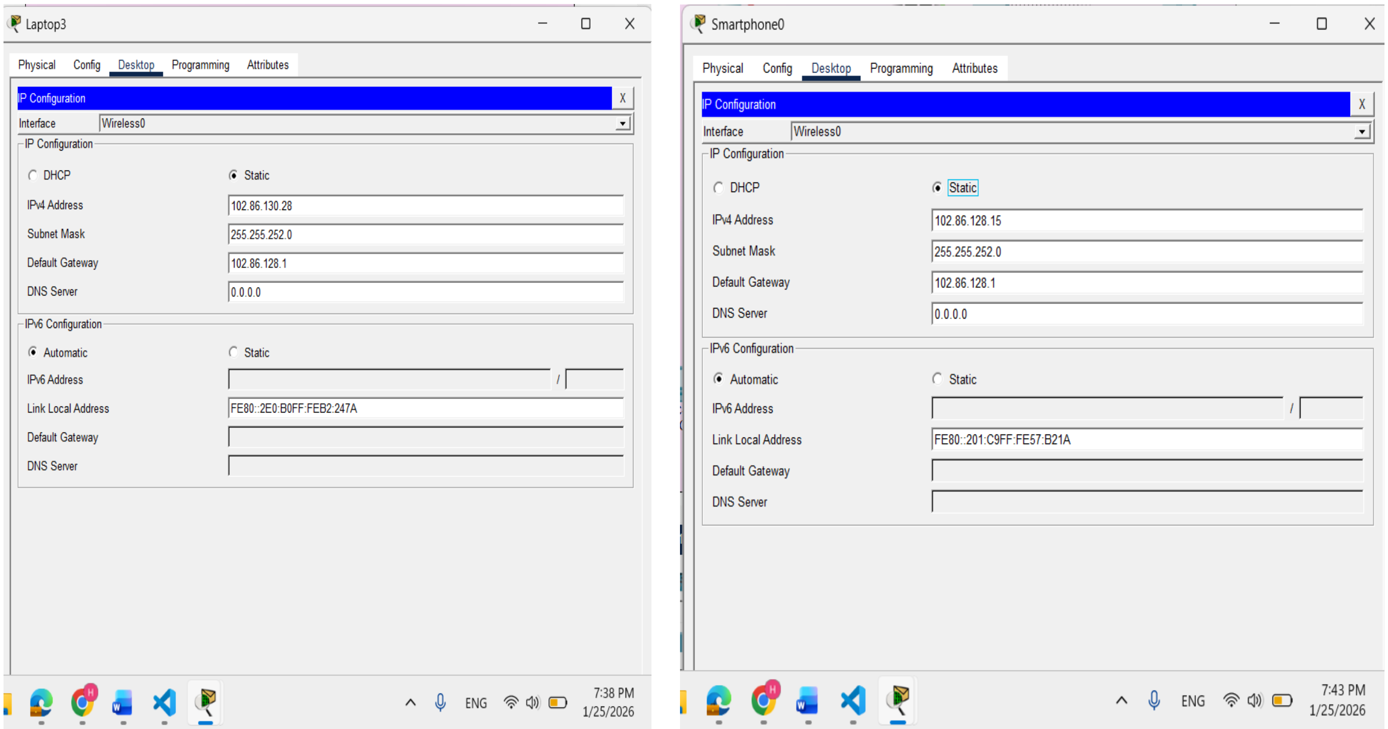


Figure 23 : East-WLAN devices IPs

East-LAN1 Router :

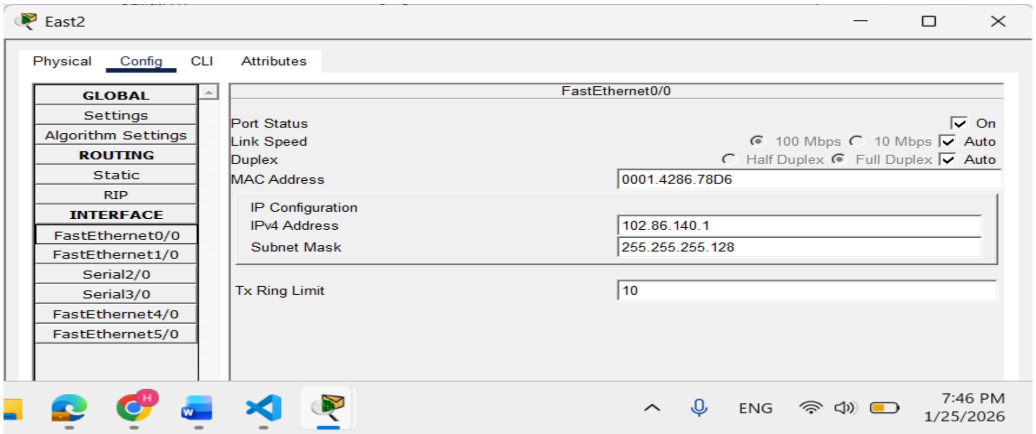


Figure 24 : East-LAN1 Router Ip configuration

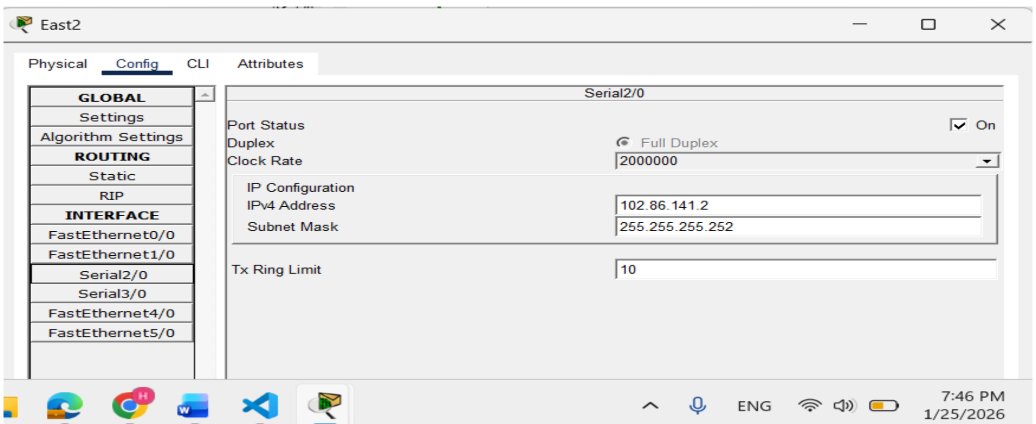


Figure 25 : East-LAN1 Router Ip configuration

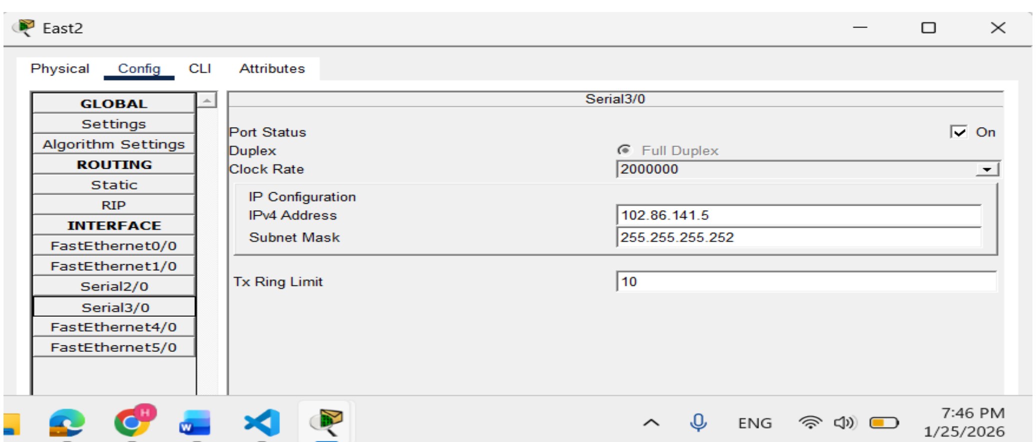


Figure 26 : East-LAN1 Router Ip configuration

East-LAN2 Router :

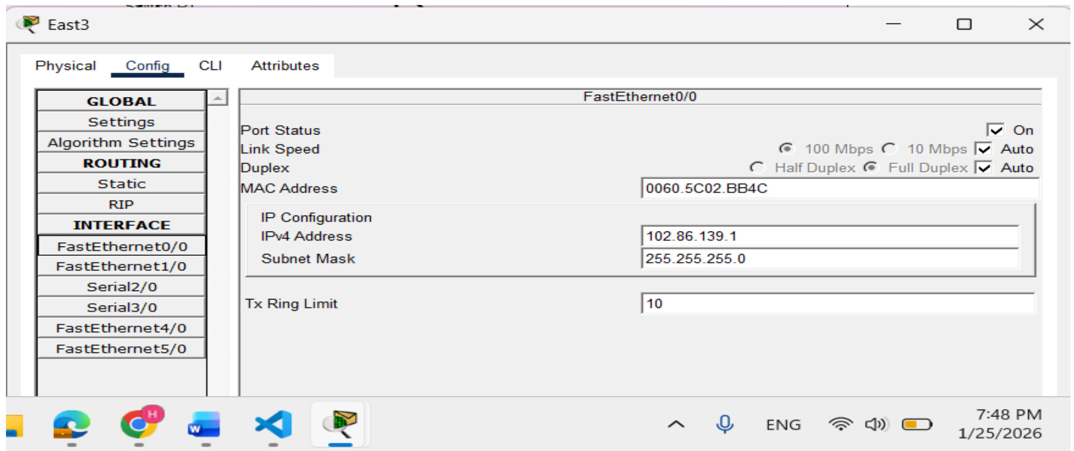


Figure 27 : East-LAN2 Router Ip configuration

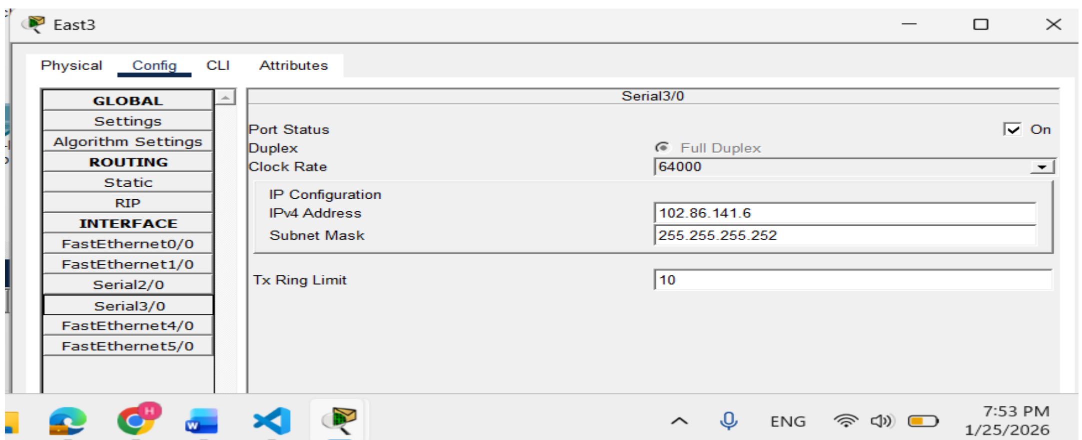


Figure 28 : East-LAN2 Router Ip configuration

//miss pic

East-WLAN Access Point :

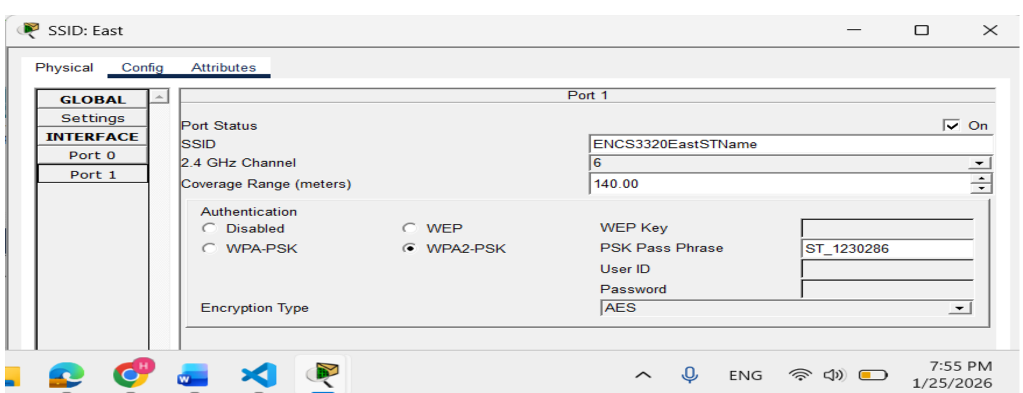


Figure 29 : East-WLAN access point

Main West Router :

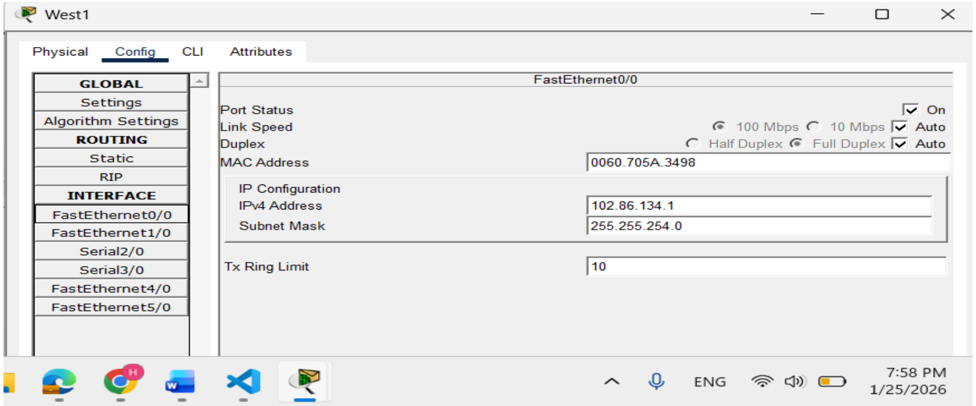


Figure 30 : West main Router Ips configuration

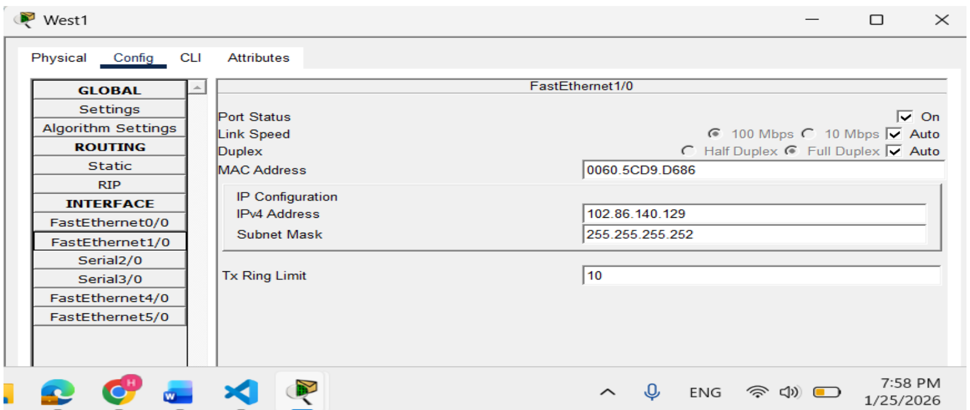


Figure 31 : West main Router Ips configuration

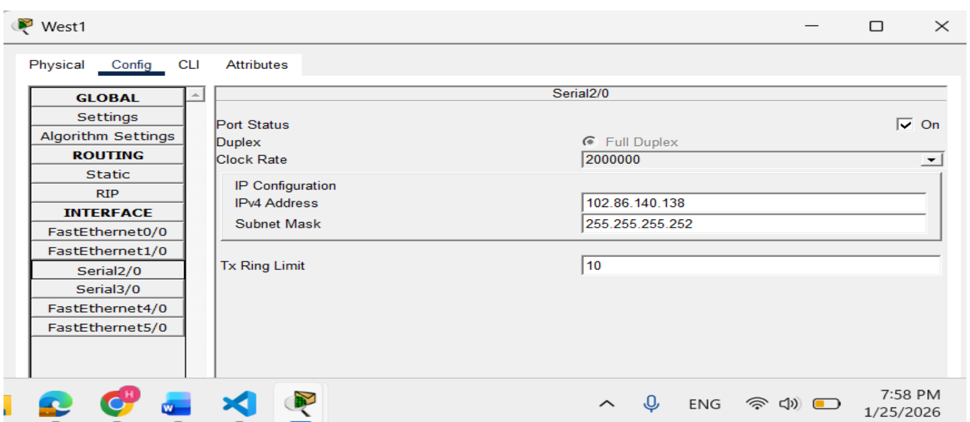


Figure 32 : West main Router Ips configuration

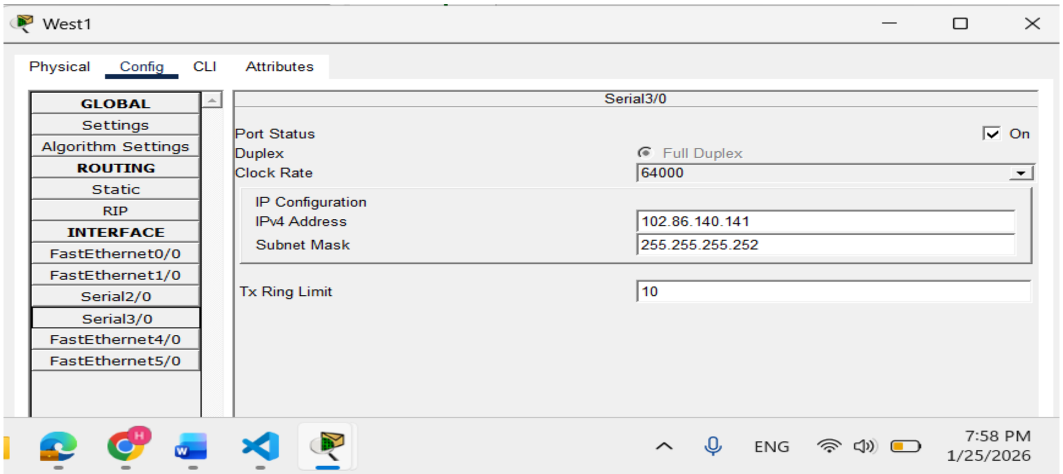


Figure 33 : West main Router Ips configuration

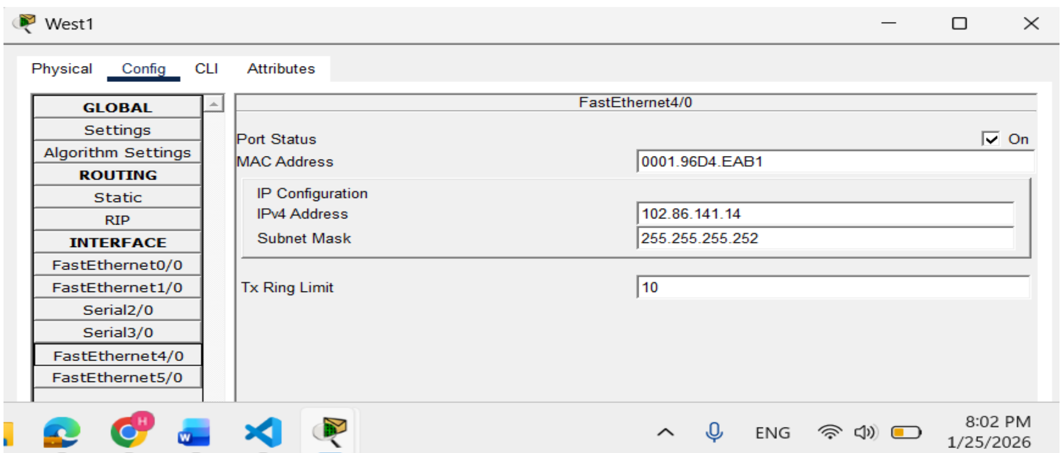


Figure 34 : West main Router Ips configuration

East Main Router :

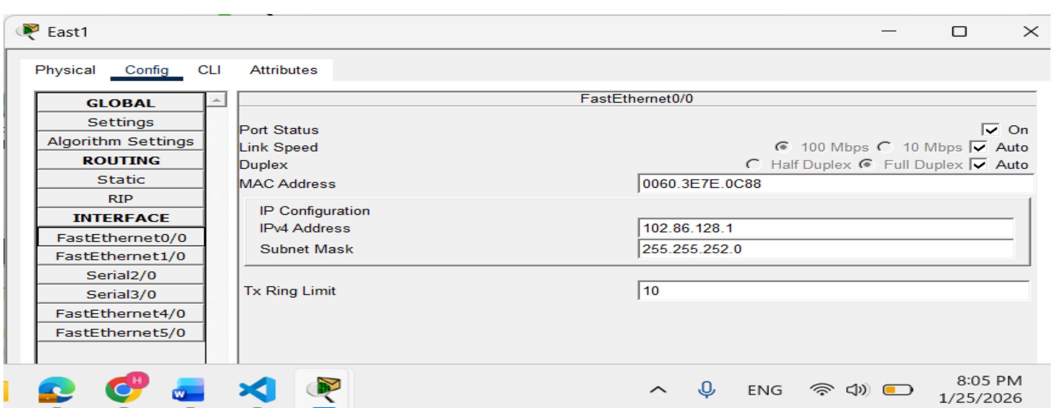


Figure 35 : East main Router Ips configuration

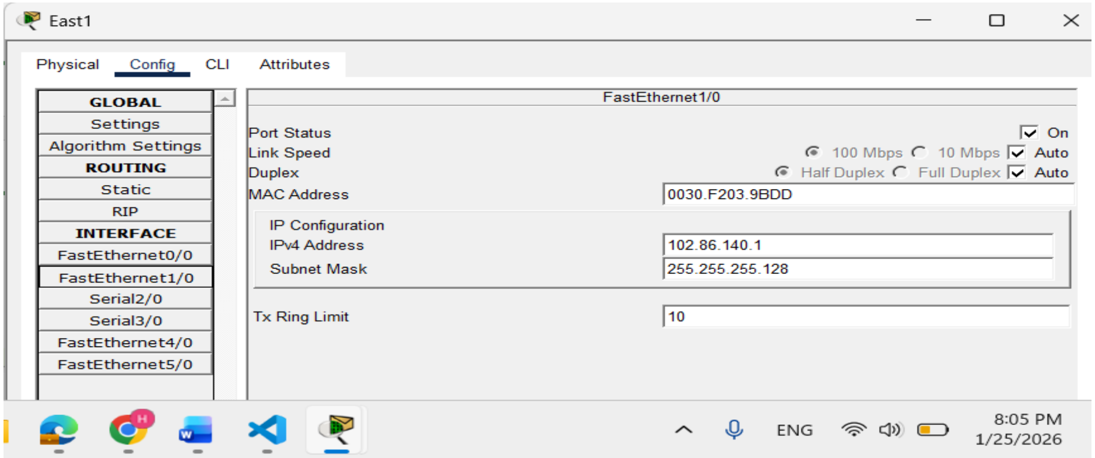


Figure 36 : East main Router Ips configuration

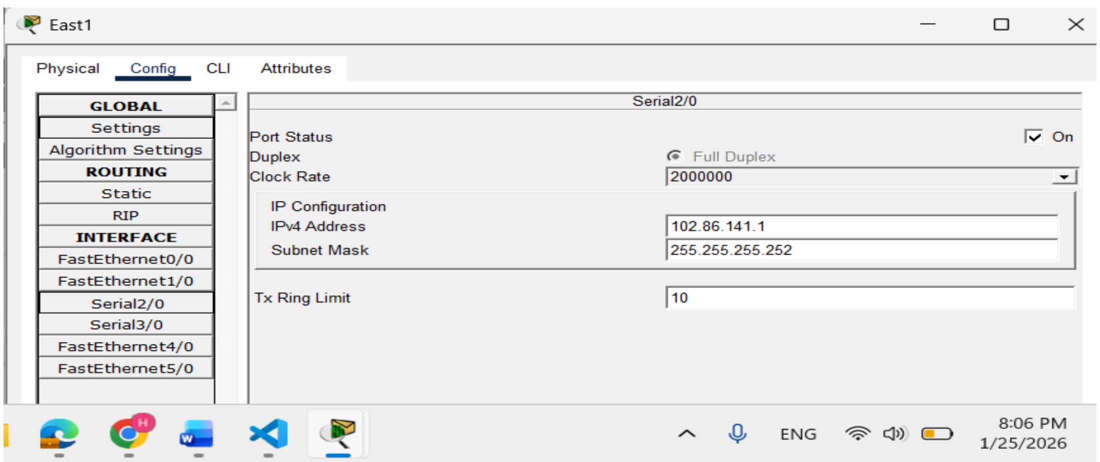


Figure 37 : East main Router Ips configuration

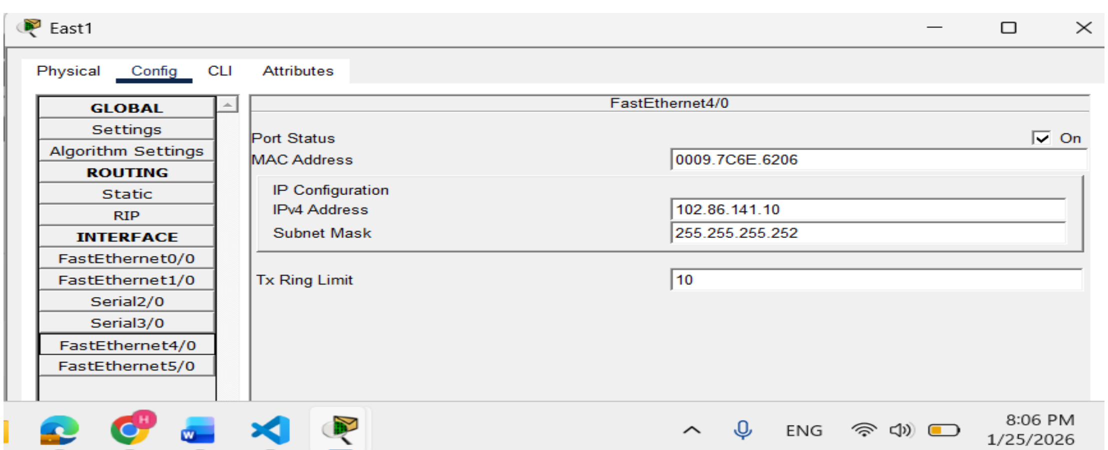


Figure 38 : East main Router Ips configuration

Main Campus Router Ips Configration :

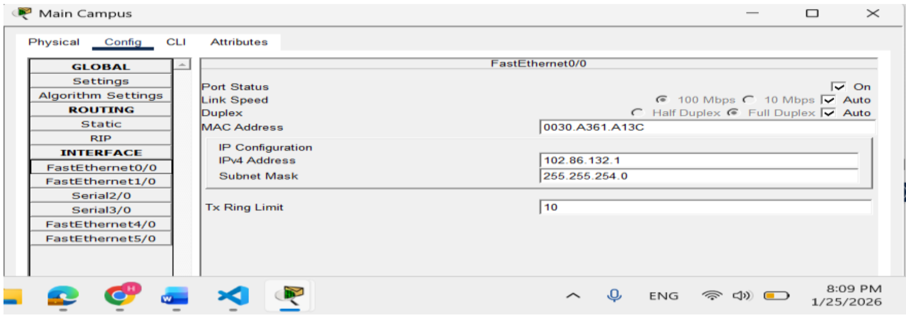


Figure 39 : Main Campus Router Ips Configuration

Figure 40 : Main Campus Router Ips Configuration

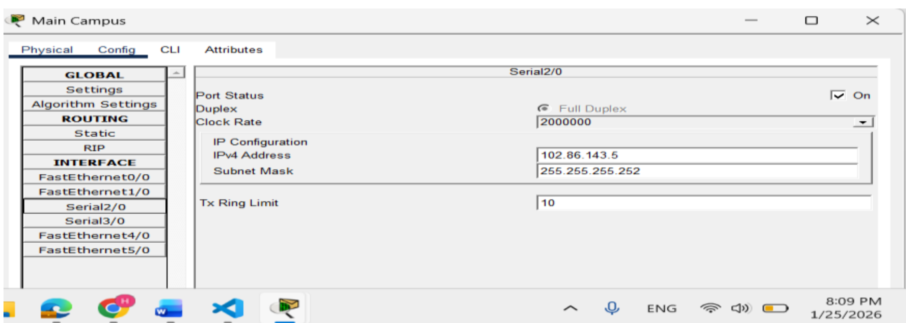


Figure 41 : Main Campus Router Ips Configuration

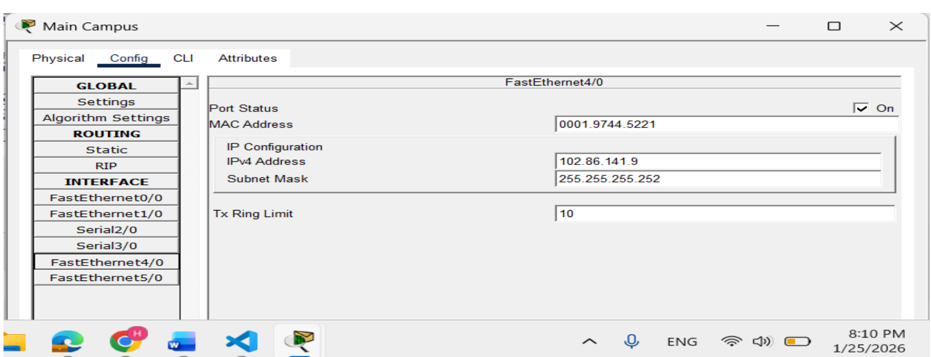


Figure 42 : Main Campus Router Ips Configuration

ISP Router IP configuration :

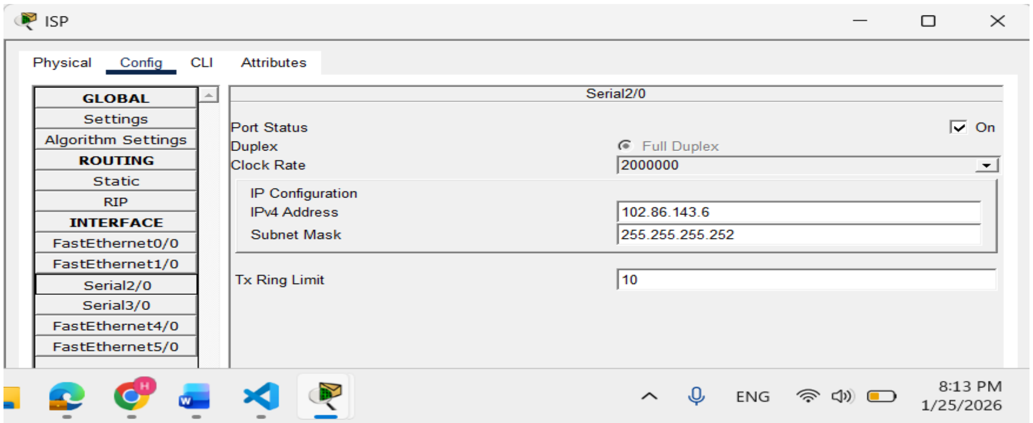


Figure 43 : ISP Router Ip configuration

Testing :

During the testing phase, some message tests failed on the first attempt, especially in the wireless network. However, when the same test was repeated, it worked successfully. This happens because wireless devices need a short time to establish the connection, complete authentication, and update ARP information. After this initial setup is completed, the network becomes stable and the tests succeed.

1- from smart phone in east to PC2 :

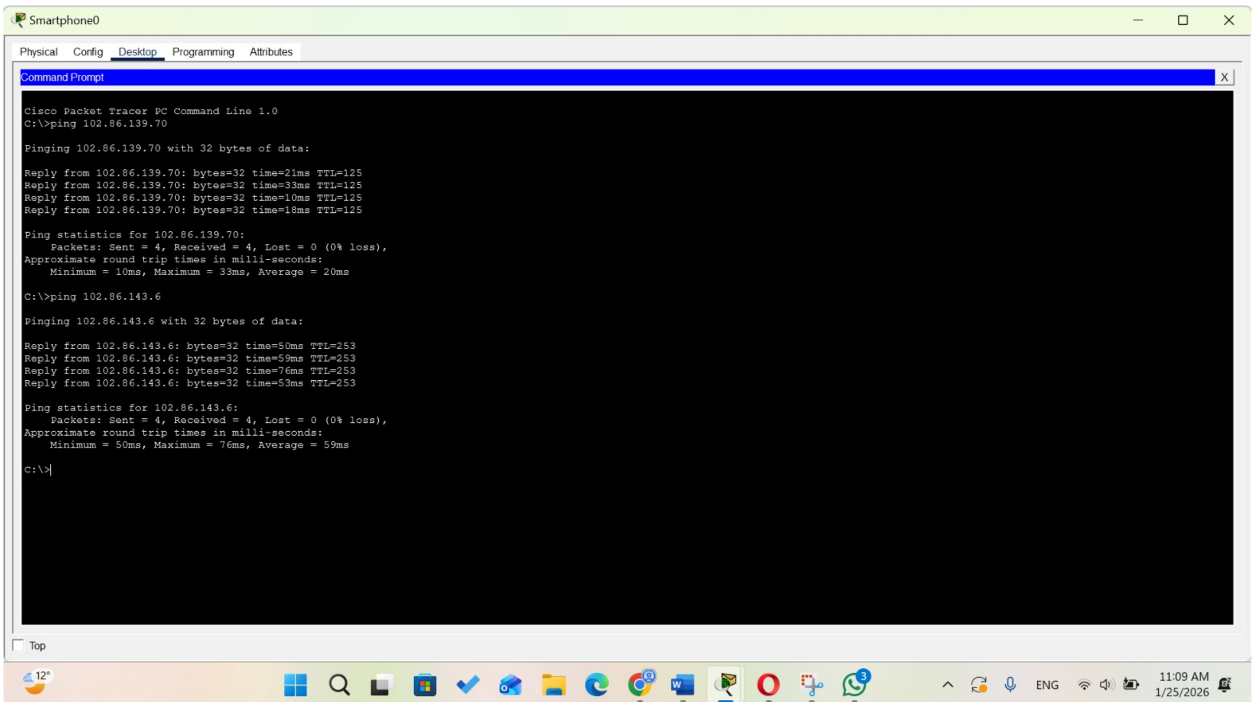


Figure 44 : Test 1 case : Within the same area connection

When testing the connection from Smartphone0 to PC2 by pinging IP address 102.86.139.70, the communication followed a specific path through the network infrastructure.

The smartphone, connected wirelessly to the "SSID: East" access point, sent ICMP echo request packets through the wireless connection. These packets were then forwarded from the access point to Router-PT East, which examined the destination address and determined the appropriate route. Since both devices are located in the eastern region, the router directed the packets to Switch-PT Switch2, which used PC2's MAC address to deliver them to the correct port.

PC2 received the packets and sent ICMP echo reply packets back through the same path in reverse: Switch2 -> Router East3 -> Access point -> Smartphone0. The test results showed 100%

success with all 4 packets transmitted and received with no loss. The round-trip times ranged from 10ms to 33ms with an average of 20ms, which is normal for a network combining wireless and wired connections. This demonstrates that the routing configuration and wireless integration are functioning correctly, allowing seamless communication between mobile and wired devices in the network.

2- From Laptop1 to laptop3 (In the same area communication)

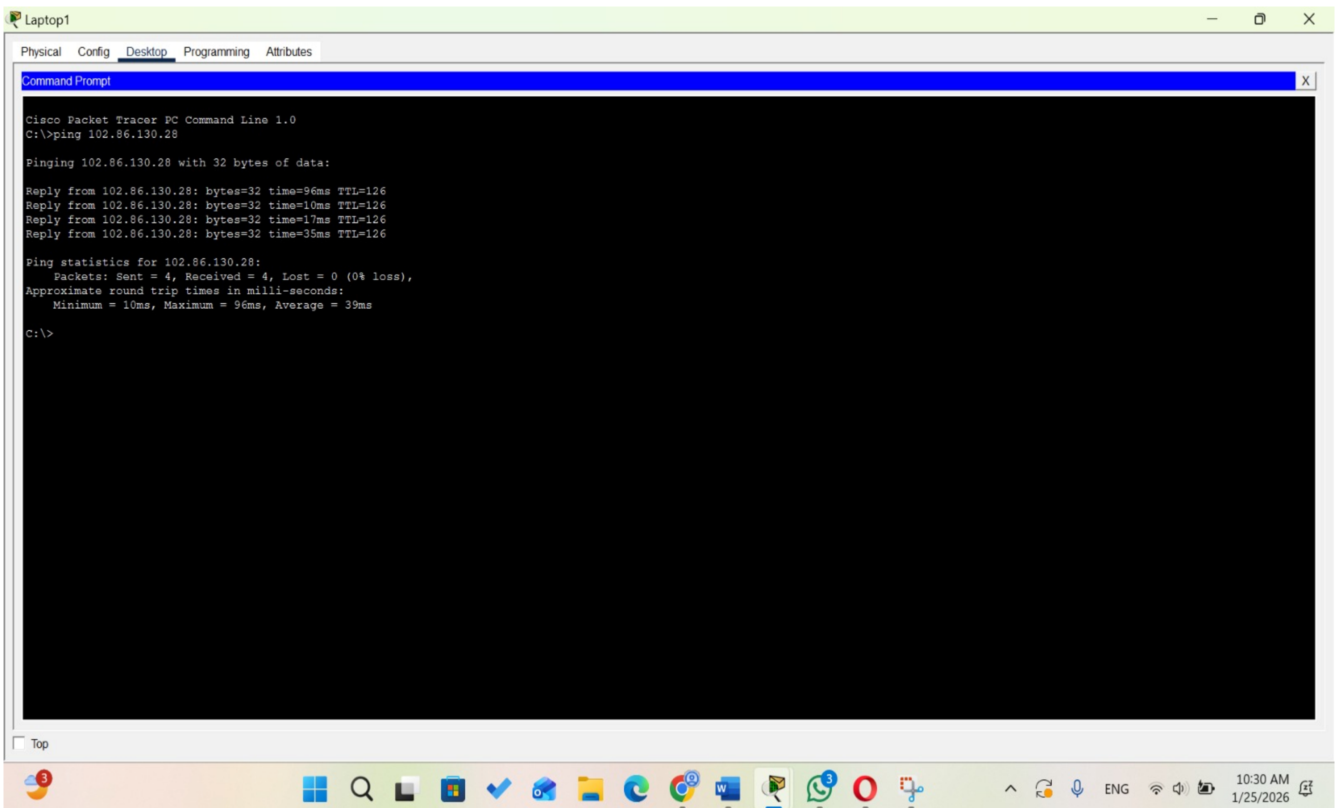


Figure 45 : Test case 2 , Within the same area

When pinging the IP address 102.86.130.28 from Laptop1 to test connectivity with Laptop3, the packets traveled through multiple network devices in the eastern region.

Laptop1 sent ICMP echo request packets to its gateway Router-PT East2, which forwarded them through the network path to reach Laptop3 connected to Switch-PT Switch2. Laptop3 received the packets and sent replies back through the same route.

The test showed 100% success with all 4 packets delivered and no packet loss. Round-trip times ranged from 17ms to 96ms with an average of 39ms. The higher latency compared to direct connections is normal since packets traveled through multiple routers and switches between different network segments. This confirms that the routing between devices in the eastern campus is working correctly.

3- From W2PC to East PC1 (Cross-Area Communication)

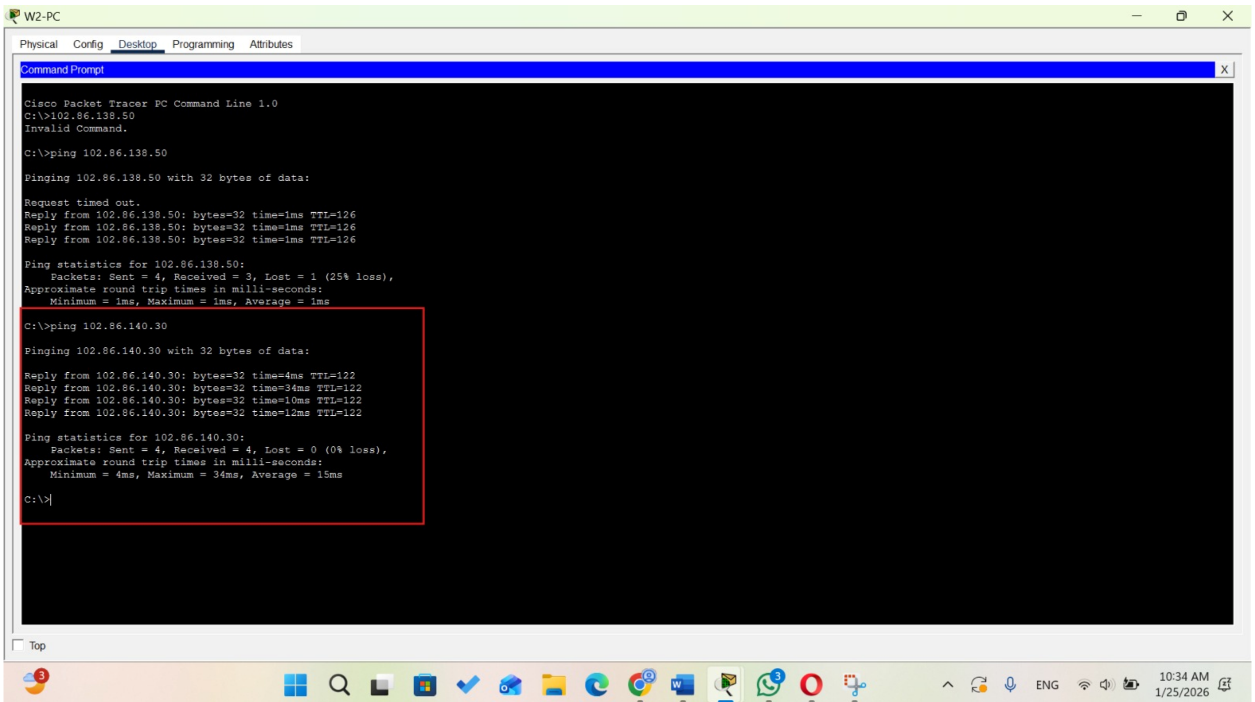


Figure 46 : Test case 3 , different areas Communication

4- From W-Wlap to Laptop1 in area0 (Cross-Area Wireless-to-Wired Communication)

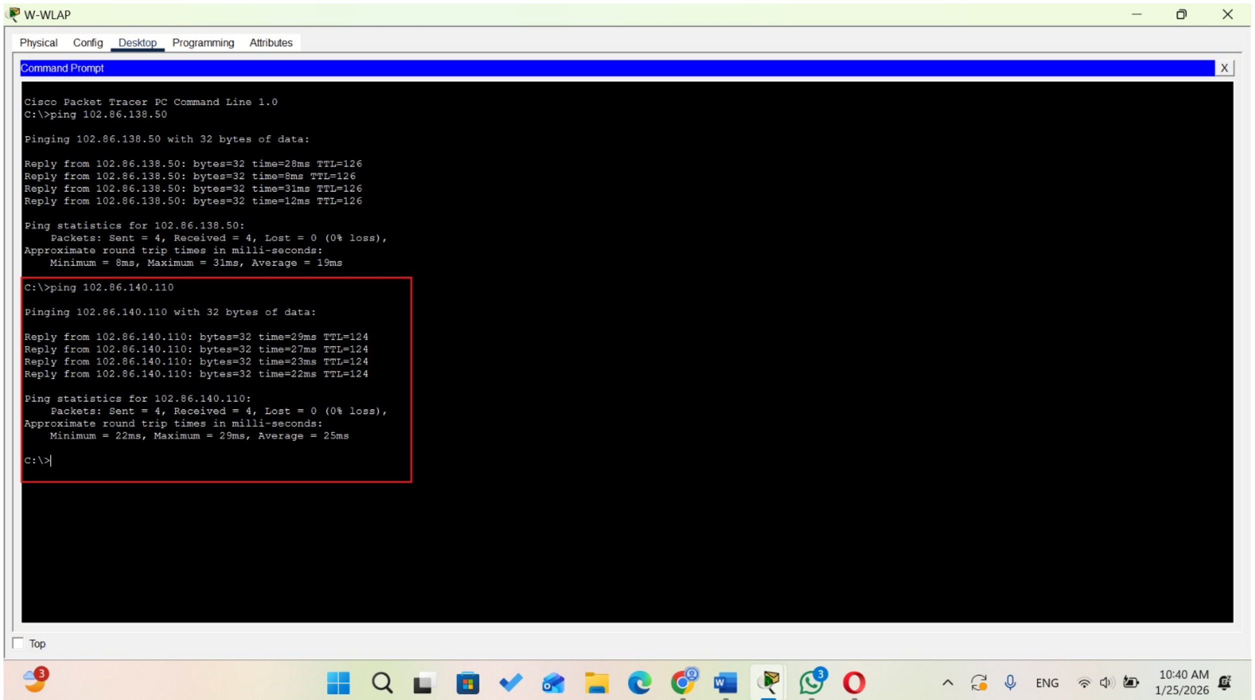


Figure 47 : Test case 4 , different areas wireless to wired communication

In this test, I pinged IP address 102.86.140.110 from W-WLAP, a wireless laptop in the western region, to reach Laptop1 in the eastern region. This demonstrates communication between wireless and wired devices across different campus areas.

W-WLAP, connected to the western wireless network, sent ICMP packets through its access point to Router-PT West2. Since the destination is in the eastern region, the router forwarded the packets through the campus backbone, likely passing through Router-PT Main Campus before reaching the eastern routers. The packets then traveled to Switch-PT Switch1 where Laptop1 is connected. Laptop1 received the requests and sent replies back through the same path.

The results show 100% success with all 4 packets delivered and no loss. Round-trip times ranged from 22ms to 28ms with an average of 25ms. This excellent performance is significant because it proves that the wireless infrastructure in the west can reliably communicate with wired devices in the east. The consistent latency demonstrates stable routing across areas and efficient wireless connectivity, which is crucial for mobile users accessing resources throughout the campus network.

5- From laptop2 in the East to W-2laptop in the West

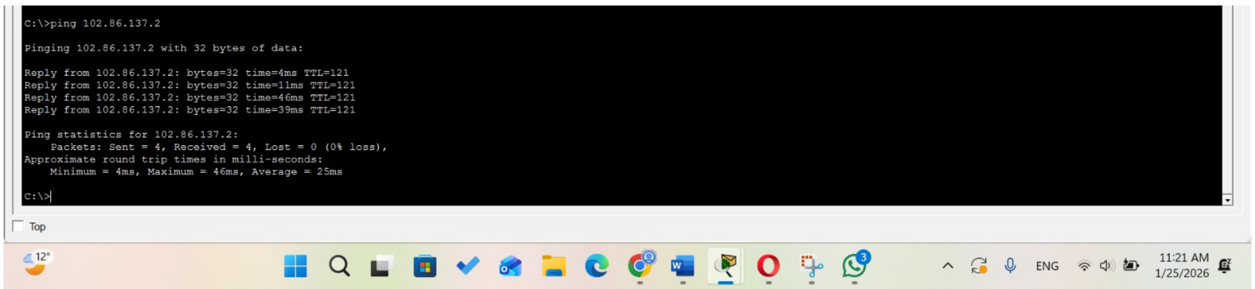


Figure 48 : Test case 5 , East and West communication

When testing the connection from Laptop2 to W2-LAP by pinging the IP address 102.86.137.2, the communication was successfully delivered across the network. Laptop2 generated ICMP echo request packets and forwarded them to its default gateway, where the router examined the destination IP and selected the correct route toward the West subnet that contains 102.86.137.2. The packets were then carried through the routing infrastructure until they reached the target LAN, where the local switch used the destination device's MAC address to forward the traffic to W2-LAP. After receiving the requests, W2-LAP returned ICMP echo reply packets back to Laptop2 through the same path in reverse. The results show 100% success, with 4 packets sent and 4 received (0% loss). The round-trip times ranged from 10 ms to 29 ms with an average of 21 ms, which indicates stable connectivity and normal delay across the network.

6- From W1PC to ISP router

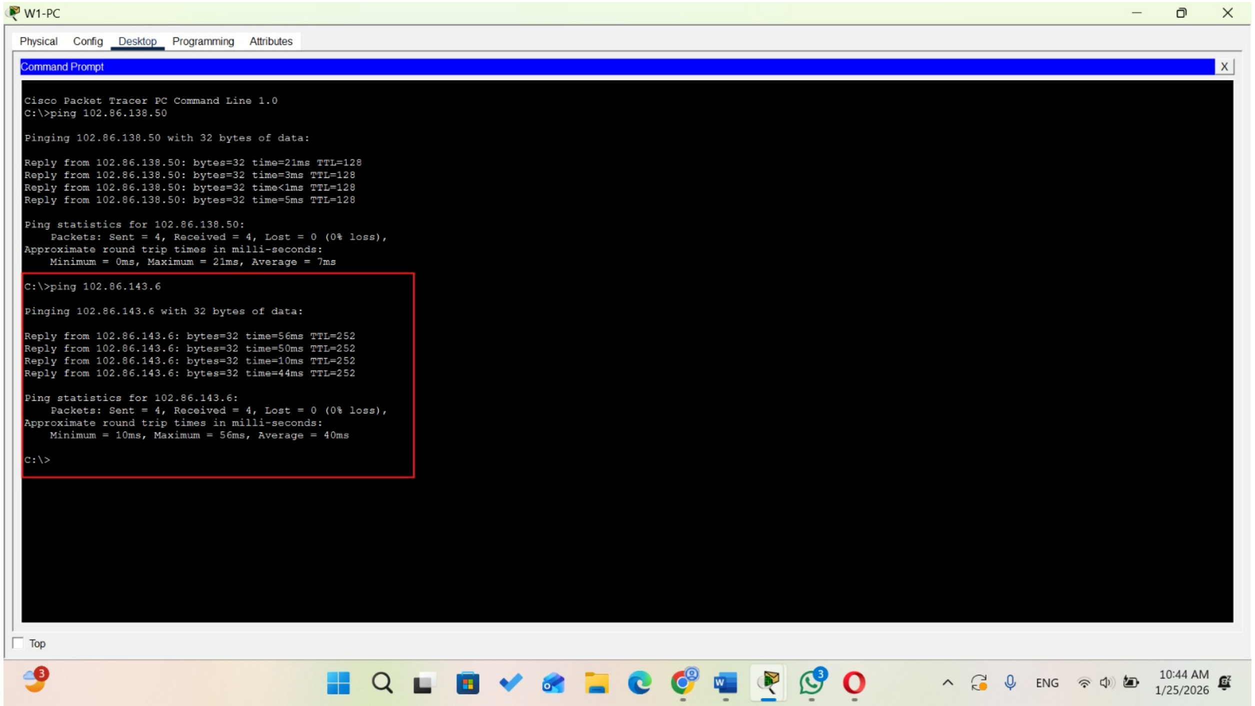


Figure 49 : Test case 6 , from device to ISP router

When testing connectivity from W1-PC to the ISP router, two ping tests were performed. First, W1-PC successfully pinged 102.86.138.50, confirming correct communication within the West LAN through the local switch. Then, W1-PC pinged the ISP router at 102.86.143.6, which is located in a different network. The ICMP packets were forwarded to the default gateway (102.86.138.1) and then routed across the network until reaching the ISP router, with the echo replies returning through the same path in reverse. Both tests achieved 100% success with no packet loss, and the round-trip times were within normal ranges, confirming that both local connectivity and upstream routing to the ISP are functioning correctly.

7- From smart phone in east with ISP

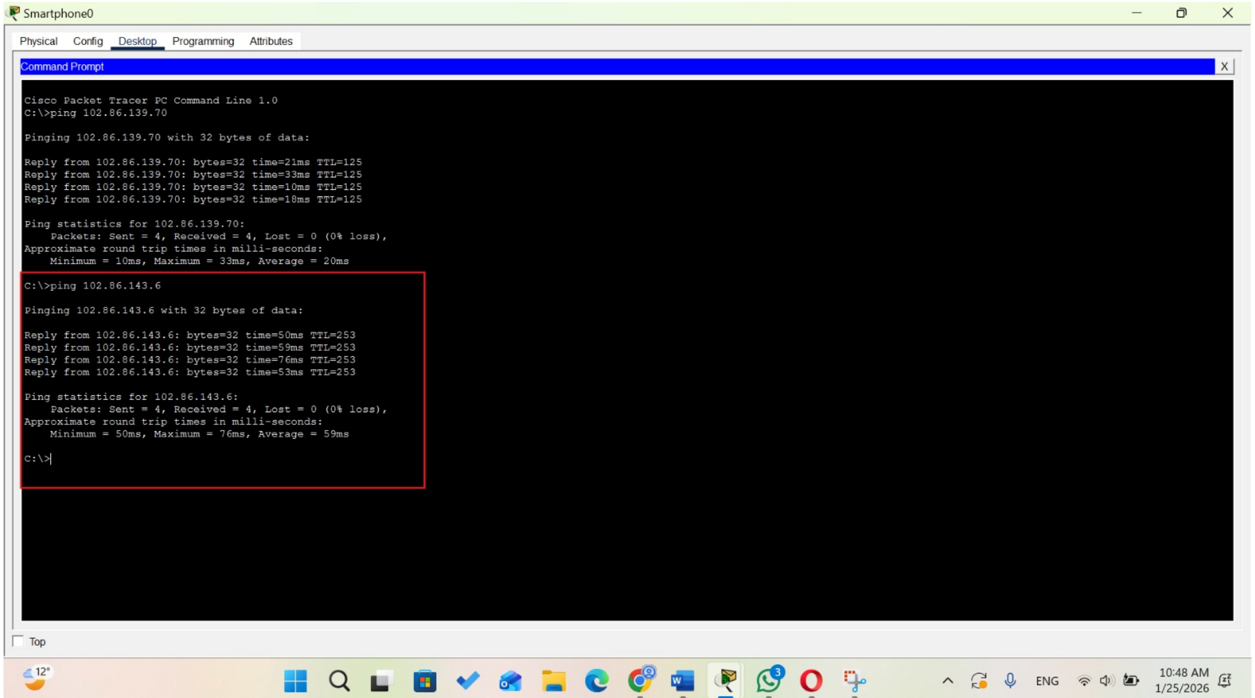


Figure 50 : Test case 7 , Wireless with ISP communication

When testing connectivity from Smartphone0 in the East network to the ISP router, two ping tests were performed to verify both wireless access and upstream routing. First, Smartphone0 successfully pinged 102.86.139.70, confirming correct communication within the East wireless network through the access point. Then, Smartphone0 pinged the ISP router at 102.86.143.6, which is located in a different network. The ICMP packets were sent over the wireless link to the access point, forwarded to the East router (default gateway), and then routed through the network until reaching the ISP router, with replies returning through the same path in reverse. Both tests achieved 100% success with no packet loss, and the round-trip times were within normal ranges, demonstrating that wireless integration and routing to the ISP are functioning correctly.

8- From W2-PC to W1-PC

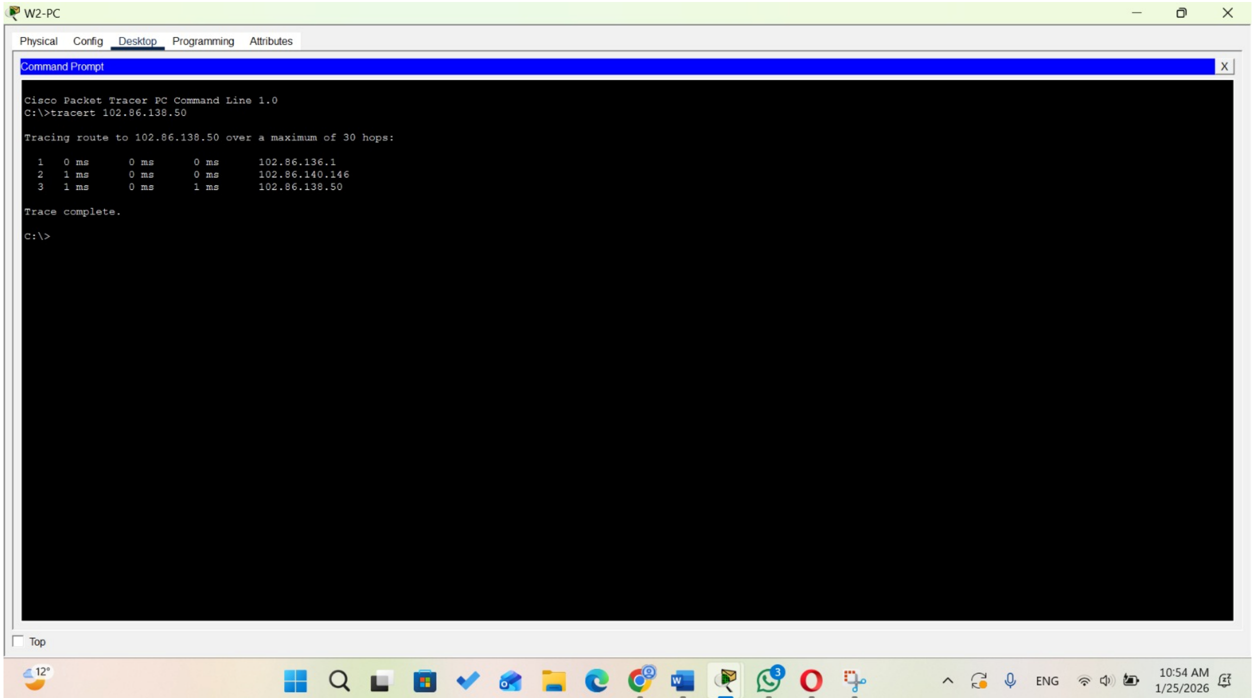


Figure 51 : Test case 8 ,

When performing a traceroute from W2-PC to W1-PC (102.86.138.50), the path taken by the packets through the network was clearly identified. The trace first reached the default gateway 102.86.136.1, then passed through the intermediate router 102.86.140.146, before finally arriving at W1-PC. The traceroute completed successfully in three hops, with very low response times at each hop. This confirms that routing between the West networks is correctly configured and that packets are being forwarded through the intended network path.

9- Traceroute Test 4: W1-PC → East Network Device

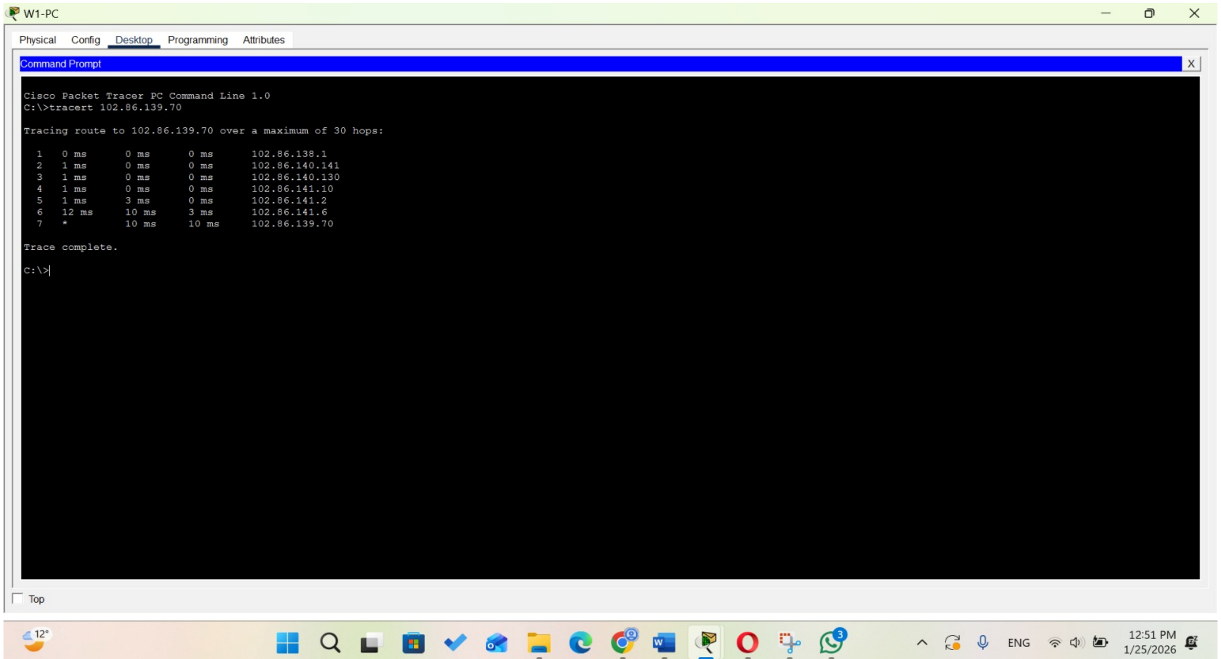


Figure 52 : Test case 9 , traceroute

tracert 102.86.139.70//Traceroute from W1-PC to East device (102.86.139.70):

In this test, the traceroute command was used from W1-PC to trace the path to IP address 102.86.139.70 in the East network. The results show that the packets passed through several intermediate routers, starting from the local West gateway and then through multiple backbone and East routers before reaching the destination. The trace completed successfully with all hops responding and low delay values. This confirms that inter-region routing between the West and East networks is correctly configured and that packets follow the intended path across the network.

10- W1_PC with main campus

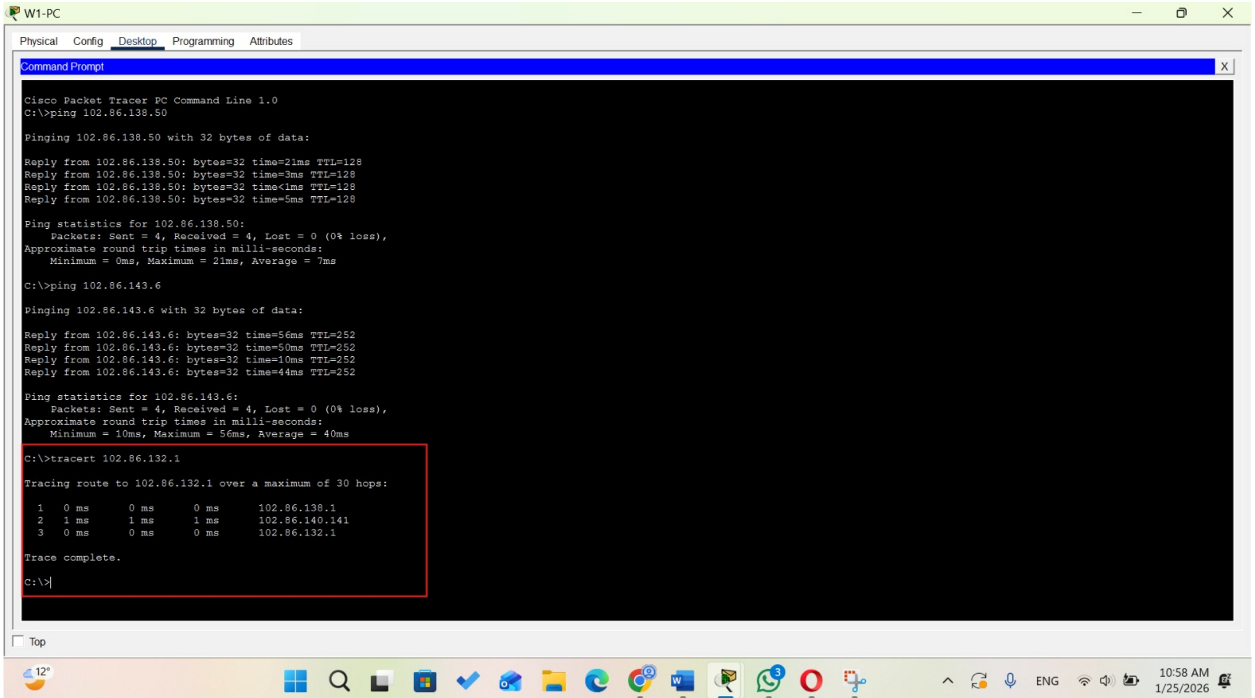


Figure 53 : Test case 9 , from west 1pc to the main campus router

In this test, the traceroute command was used from W1-PC in the West network to trace the path to the Main Campus router (102.86.132.1). The results show a short route of three hops: the first hop is the local gateway, the second hop is an intermediate router (102.86.140.141), and the third hop is the destination router (102.86.132.1). All hops responded with very low delay values, which indicates stable links and efficient forwarding. This is significant because it confirms that devices in the West region can reach the Main Campus through a correct and direct routing path, ensuring reliable access to central campus services and resources.

Testing Demonstration Video

To clearly demonstrate the correctness of the testing process, a screen-recorded video was included. The video shows the execution of the message and connectivity tests after the initial setup was completed, where all tests worked successfully. This visual demonstration confirms that the network configuration is correct and that the earlier failed attempt was a temporary behavior related to the first-time initialization, not a configuration error.

https://drive.google.com/file/d/1tG8LsMe9oU4O8jODztMJ9jOJcBgLHZAG/view?usp=sharing

Routing configuration using show IP Route command Main Campus

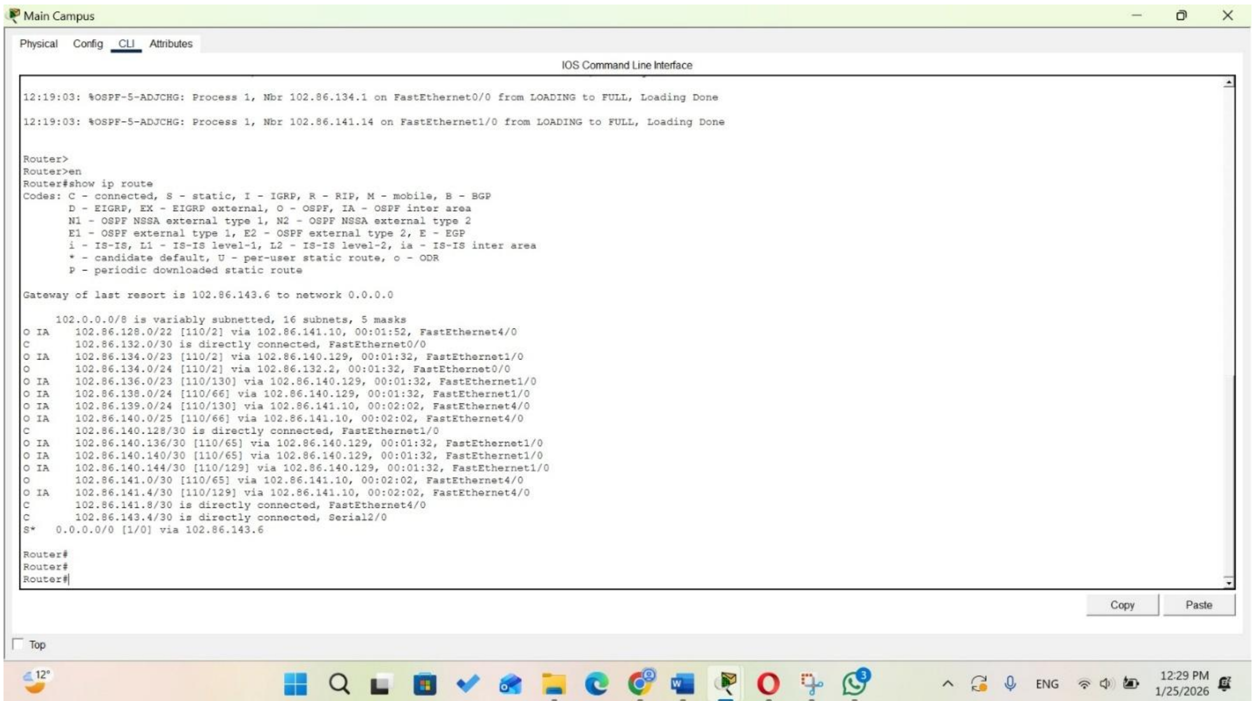


Figure 54 : Routing configuration using show ip route command.

The routing configuration was verified using the show ip route command on the Main Campus router. The routing table shows several directly connected networks (C), such as 102.86.132.0/30, 102.86.140.128/30, and 102.86.141.8/30, confirming that the router's local interfaces are correctly configured and active. In addition, multiple routes marked as OSPF routes (O and O IA) are present, indicating that the router has successfully learned routes to remote networks in the West and East regions through OSPF. The table also shows a default route (0.0.0.0/0) pointing to 102.86.143.6, which confirms proper connectivity to the ISP. Overall, this output confirms that OSPF is functioning correctly and that the Main Campus router can forward traffic to all internal networks and external destinations.

Routing configuration using show IP Route command East 1

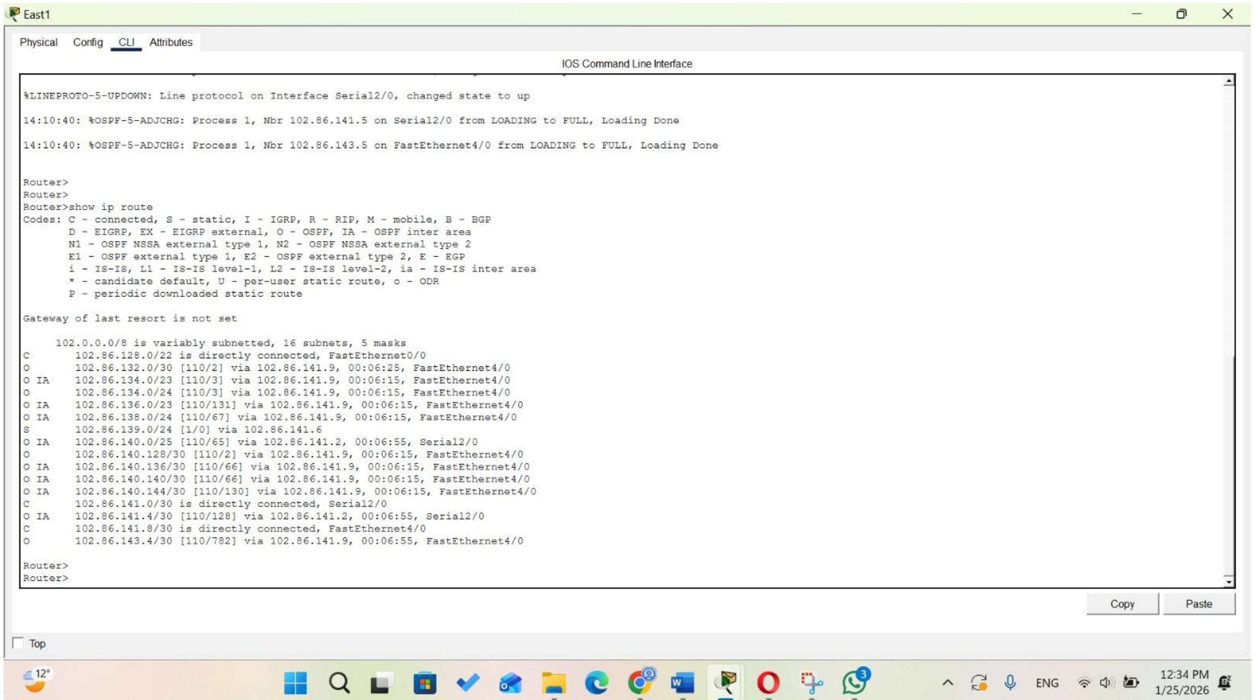


Figure 55 : Routing configuration using show ip route command.

The routing configuration on the East1 router was verified using the show ip route command. The routing table shows several directly connected (C) networks, such as 102.86.128.0/22, 102.86.141.0/30, and 102.86.141.8/30, confirming that the router's interfaces are correctly configured and operational. In addition, multiple routes marked as OSPF (O) and OSPF inter-area (O IA) are present, indicating that East1 is successfully exchanging routing information with neighboring routers through OSPF. The OSPF adjacency messages at the top of the output further confirm stable OSPF neighbor relationships. Overall, this verifies that East1 can correctly route traffic within the East region and communicate with other network areas.

Routing configuration using show IP Route command West 1

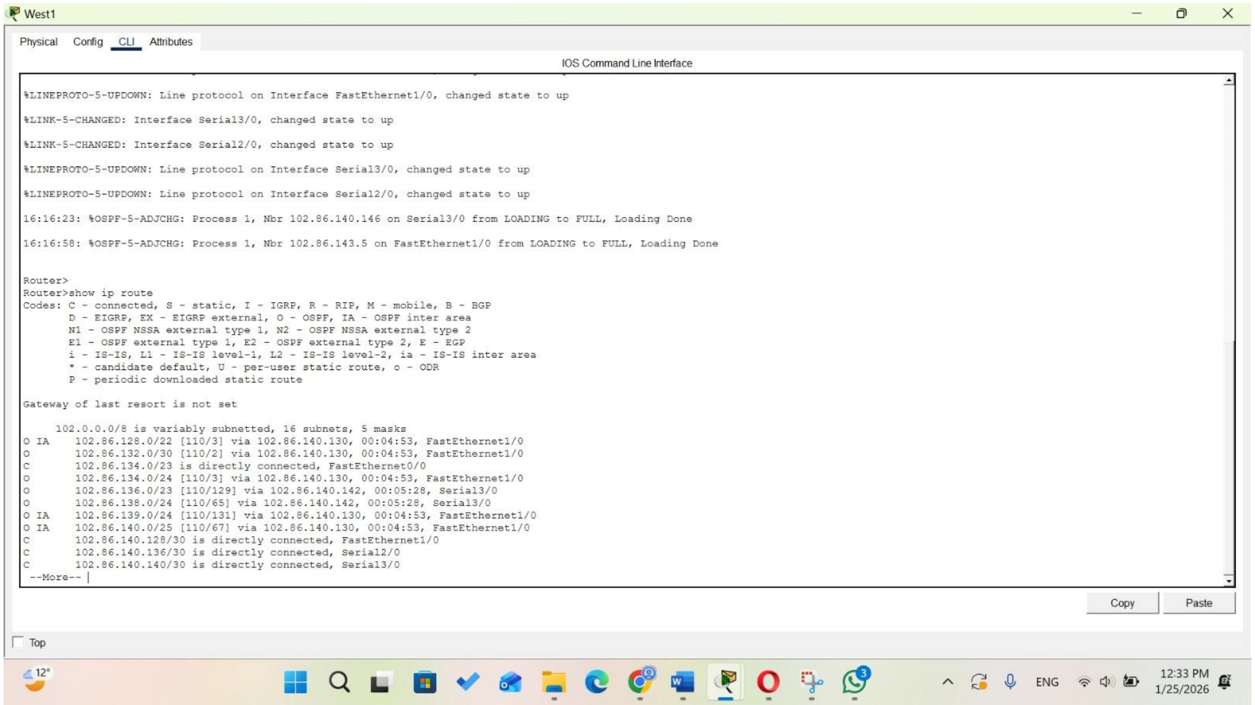


Figure 56 : Routing configuration using show ip route command.

The routing configuration on the West1 router was verified using the show ip route command. The routing table shows several directly connected networks (C), such as 102.86.134.0/23, 102.86.140.128/30, 102.86.140.136/30, and 102.86.140.140/30, confirming that the router's local interfaces are correctly configured and active. In addition, multiple routes marked as OSPF (O) and OSPF inter-area (O IA) are present, indicating that West1 has successfully learned routes to remote networks through OSPF. The presence of OSPF neighbor adjacency messages at the top of the output further confirms successful OSPF operation. Overall, this routing table verifies that West1 can correctly route traffic within the West region and communicate with other network areas through dynamic routing.

Routing configuration using show IP Route command Router0

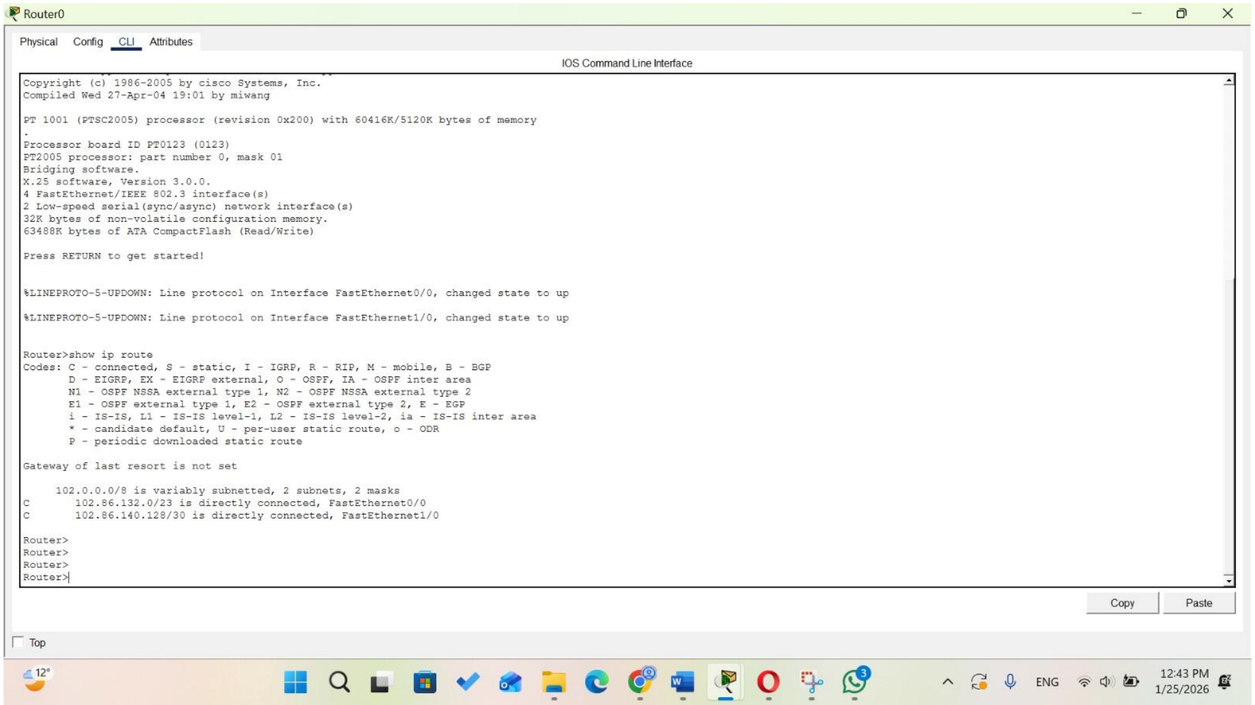


Figure 57 : Routing configuration using show ip route command.

The routing configuration on Router0 was verified using the show ip route command. The routing table shows two directly connected (C) networks: 102.86.132.0/23 on FastEthernet0/0 and 102.86.140.128/30 on FastEthernet1/0, confirming that Router0's interfaces are correctly configured and active. Since no OSPF-learned routes are present, Router0 currently only routes traffic for its directly connected networks. This indicates that Router0 is functioning as a local gateway between the main campus network and its adjacent link.

Issues and Limitations

Throughout this project, we found the experience both interesting and enjoyable, but we encountered several challenges along the way. One of the main difficulties was getting familiar with the Cisco Packet Tracer application, as we were still learning how to use its various features effectively. After completing all the necessary connections in our network topology, we faced a frustrating situation when we encountered an error that we couldn't immediately identify. It took us a considerable amount of time to troubleshoot and locate the source of the problem, which delayed our progress significantly. Additionally, time management proved to be a major limitation for our team. We were working on this project during a particularly busy period, juggling multiple other projects and midterm exams simultaneously, which made it difficult to dedicate sufficient time to fully explore and perfect our network design. Another challenge we faced was coordinating as a team, since each member had a different schedule. We couldn't find a common time for all of us to work together, so only three of us were able to meet during our practical lab sessions. As a result, we had to work individually whenever each person had free time and then combine our efforts later. Despite these challenges and time constraints, we managed to complete the project successfully, and overall, it was a fun and educational experience that helped us better understand network design and troubleshooting.

Teamwork contributions

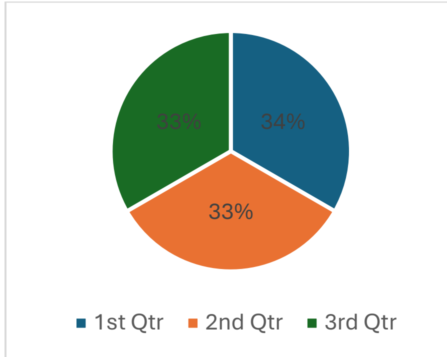


Figure 58 : Team work

This project was developed through continuous teamwork and coordination between all team members. Initially, the project implementation was completed during a team meeting to ensure that everyone clearly understood all parts of the network and how they connect together. After that, a second team meeting was held, during which the report writing, testing, and debugging tasks were completed. During this meeting, Heba handled the report organization, structure, and the addition of figures and written sections. Hala prepared and followed up on the test cases and documented the results using screenshots, while Lujain focused on analyzing the test cases and fixing the errors that appeared during testing. To be honest, the workload was shared equally, and all members contributed actively, supported each other, and exchanged ideas. This collaborative work during the second meeting helped finalize the project efficiently and improved the overall quality of the final submission.

Here we got a screen shot during our work :

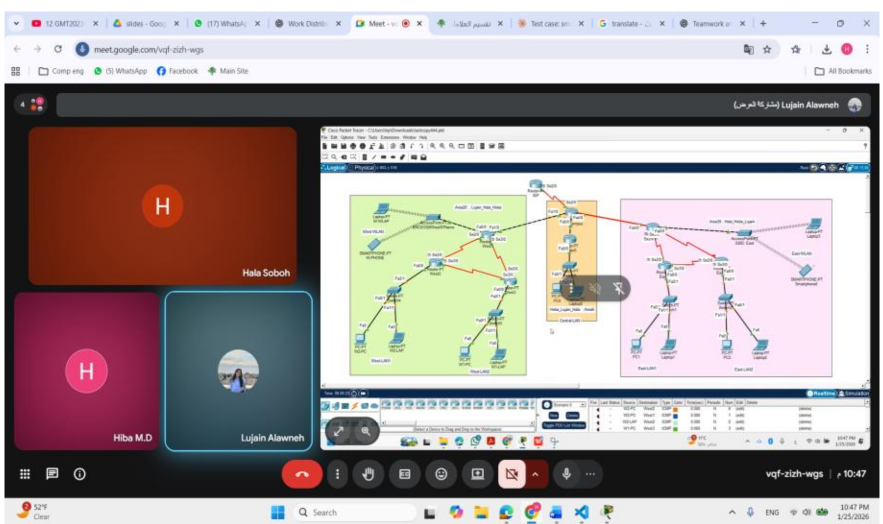


Figure 59 : meating work

References

[1] IP address : https://www.geeksforgeeks.org/computer-science-fundamentals/what-is-an-ip-address/ (accsed on 22/1/2026 , 5:40 am)

[2] : Subnetting and mask : https://www.geeksforgeeks.org/computer-networks/introduction-to-subnetting/ (accsed on 22/1/2026 , 5:56 am)

[3] Routing : https://www.geeksforgeeks.org/computer-networks/what-is-routing/ (accsed on 22/1/2026 , 5:58 am)

[4] LAN : https://en.wikipedia.org/wiki/Wireless_LAN (accsed on 22/1/2026 , 6:05 am)

[5] Swiches : https://www.geeksforgeeks.org/computer-networks/what-is-a-network-switch-and-how-does-it-work/ (accsed on 22/1/2026 , 6:11 am)

[6] CIDR : https://www.geeksforgeeks.org/computer-networks/classless-inter-domain-routing-cidr/