Birzeit University

Faculty of Engineering and Technology

Department of Electrical and Computer Engineering

Second Project
COMPUTER NETWORKS

Prepared by

Hasan Qarmash 1210611

Ahmad Hussin 1210326

Abdallah audah 1210571

Supervised by

Dr.Abdalkarim Awad & Dr.imad Tartir

Abstract:

This report encapsulates the construction and configuration of a simulated network topology using Cisco Packet Tracer, aimed at enhancing practical skills in IP subnetting, device configuration, and OSPF routing protocol application. The project was steered by the need to translate theoretical networking concepts into real-world practice. Following a systematic subnetting approach based on a unique student identifier, the topology was crafted to include a variety of network devices and subnetworks, each meticulously assigned with static IP addresses. Key network services—DNS, HTTP/WEB, and email—were configured and tested for functionality. The project culminated in the successful demonstration of interconnectivity and service accessibility across the network, signifying the attainment of the educational objectives and readiness for tackling complex networking tasks in professional settings.

Table of contents

Table of Figures

1)Part 0:

In this part we are required to do the subnetting of a network with this IP address: 200.3.10.0/25, we chose the octet 3 based on the ID of our teammates which is: 1210326 we chose the digits 03 from the number, after preparing the IP address we started subnetting it to 9 networks each network of them with different number of devices based on the topology in the Figure as well as the Table shown below:

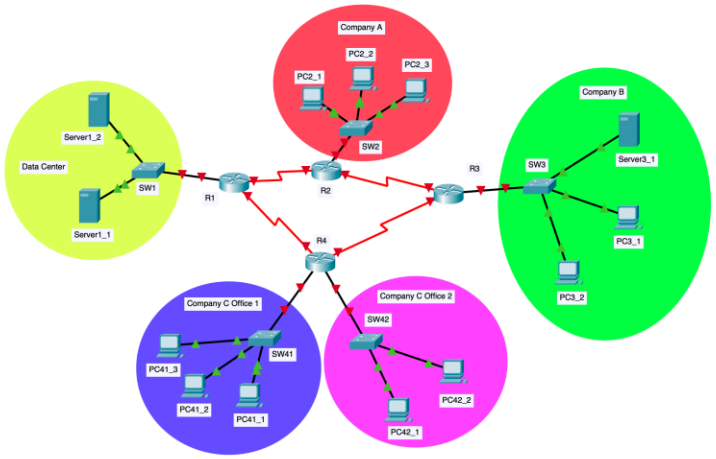


Figure1: Topology

Network	Number of End Devices (PCs and Servers)
Data Center	5
Company A	26
Company B	24
Company C Office 1	10
Company C Office 2	14

Table1: number of devices

After finishing the subnetting process we filled the following table with our results. We filled the subnet mask, network ip, ip, first device ip, last device ip, and the maximum number of devices in each subnet.

Subnet	Subnet Mask	Network IP	Broadcast IP	First IP	Last IP	Maximum number
Company A	255.255.255.224/27	200.3.10.0/27	200.3.10.31	200.3.10.1	200.3.10.30	30
Company B	255.255.255.224/27	200.3.10.32/27	200.3.10.63	200.3.10.33	200.3.10.62	30
Company C Office 1	255.255.255.240/28	200.3.10.64/28	200.3.10.79	200.3.10.65	200.3.10.78	14
Company C Office 2	255.255.255.240/28	200.3.10.80/28	200.3.10.95	200.3.10.81	200.3.10.94	14
Data Center	255.255.255.240/28	200.3.10.96/28	200.3.10.111	200.3.10.97	200.3.10.110	14
R1-R2 link	255.255.255.252/30	200.3.10.112/30	200.3.10.115	200.3.10.113	200.3.10.114	2
R2-R3 link	255.255.255.252/30	200.3.10.116/30	200.3.10.119	200.3.10.117	200.3.10.118	2
R3-R4 link	255.255.255.252/30	200.3.10.120/30	200.3.10.123	200.3.10.121	200.3.10.122	2
R4-R1 link	255.255.255.252/30	200.3.10.124/30	200.3.10.127	200.3.10.125	200.3.10.126	2

Table2: our results

2)Part 1:

In this part we constructed the topology using packet tracer based on the subnetting result in part0, we set 4 routers of model Router-PT as well as a switch device in each edge subnet each switch of model switch-PT in addition to that we connected a web and DNS servers in the Data Center subnet each of them has the model Server-PT as well as another Mail server with the same model in the company B subnet, after that we connected PC devices with model PC-PT inside the subnets as required in the project, the following figure shows our construction

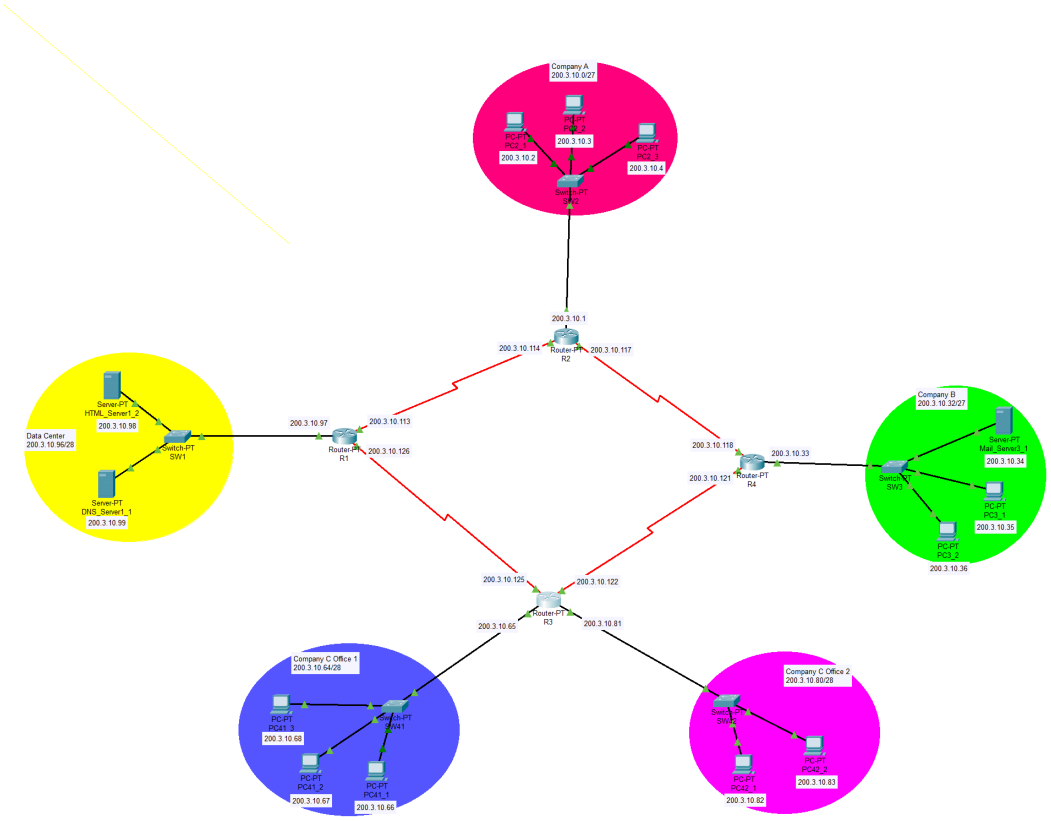


Figure2: our construction of the Topology

After building the topology we configured the interfaces of the routers and it was as follows:

⇒ Router1 (R1)

The following three snapshots (Figure-3) shows the configuration of the R1

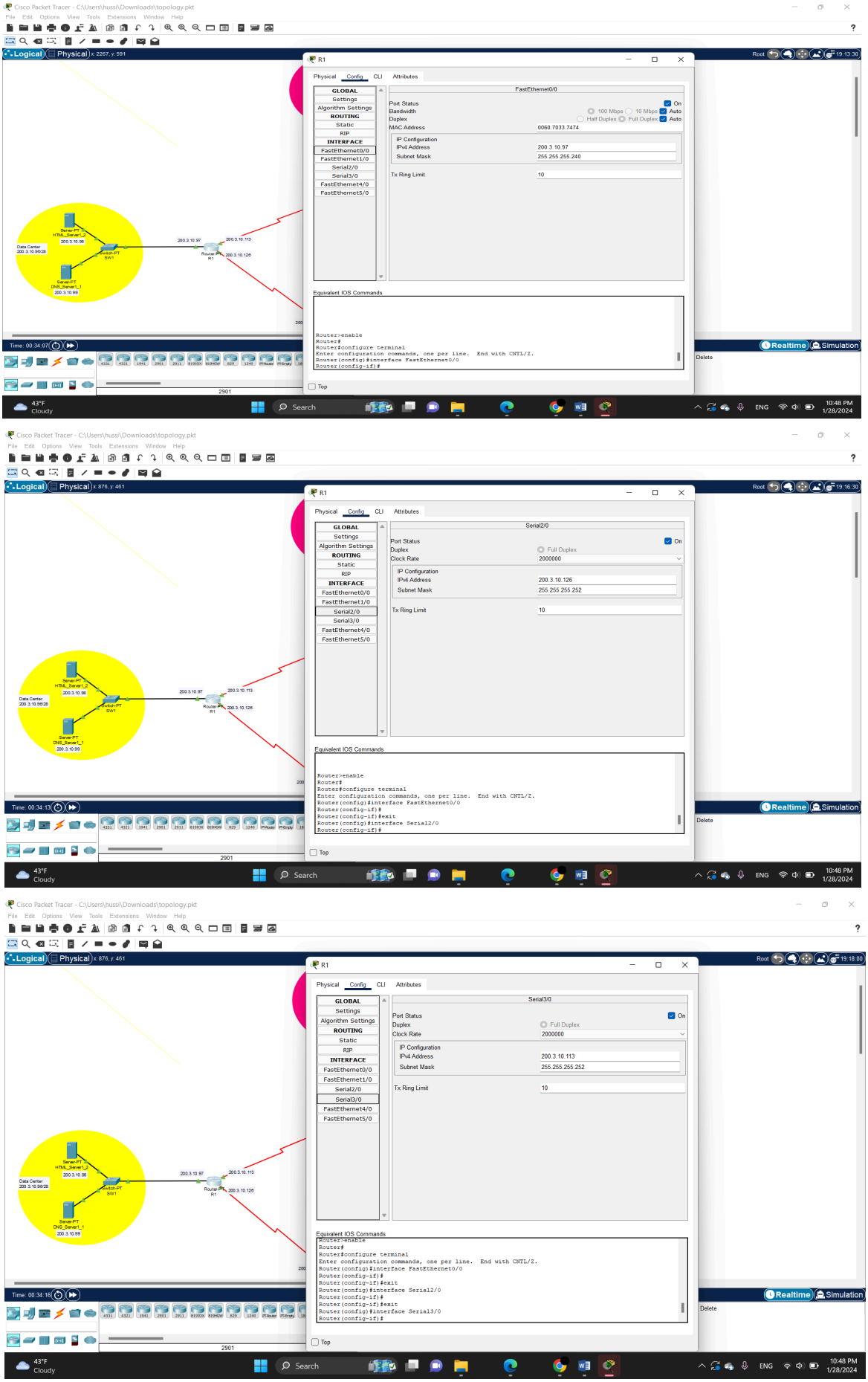


Figure3: Configuration of R1

⇒ Router2 (R2)

The following three snapshots (Figure-4) shows the configuration of the R2

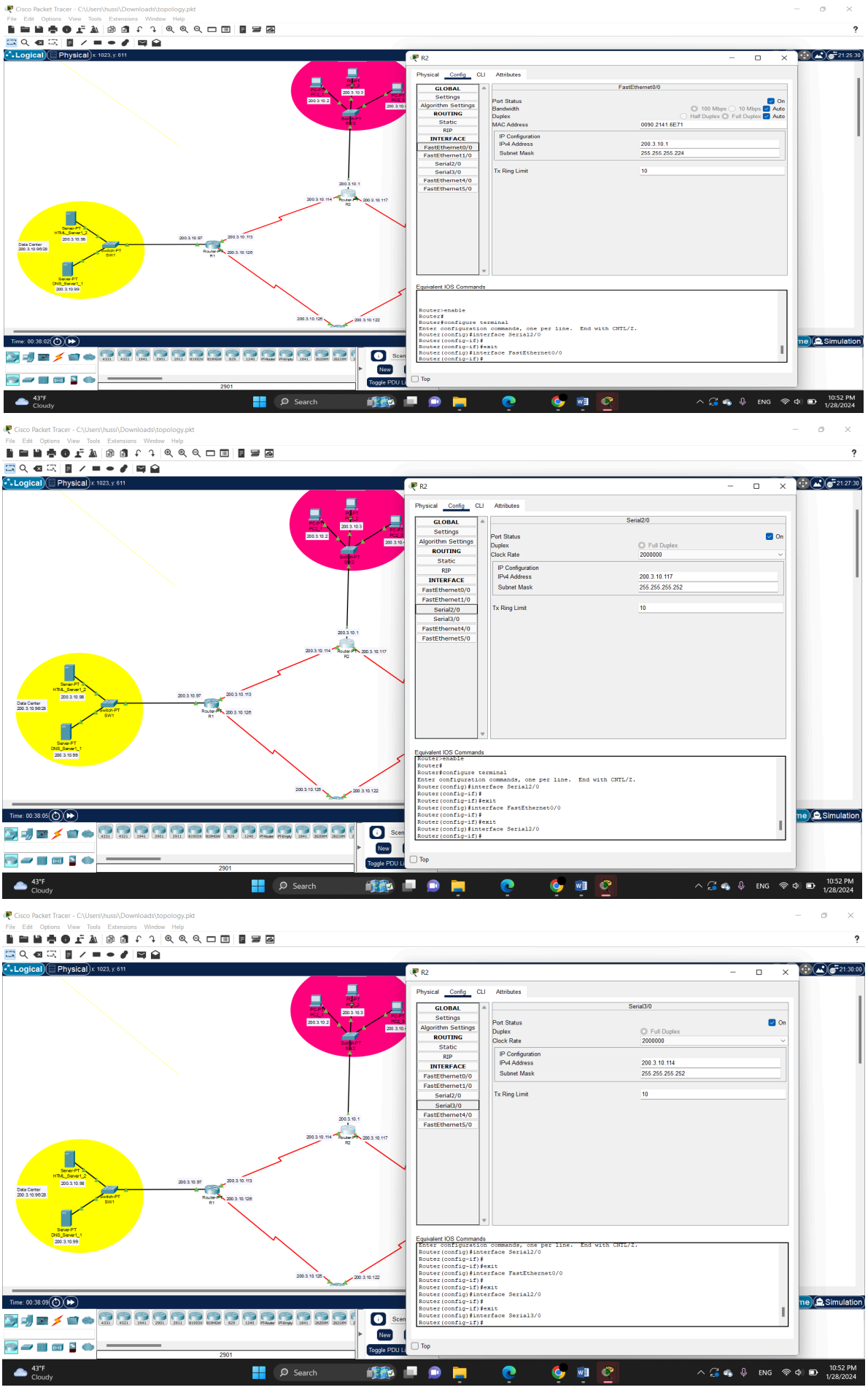
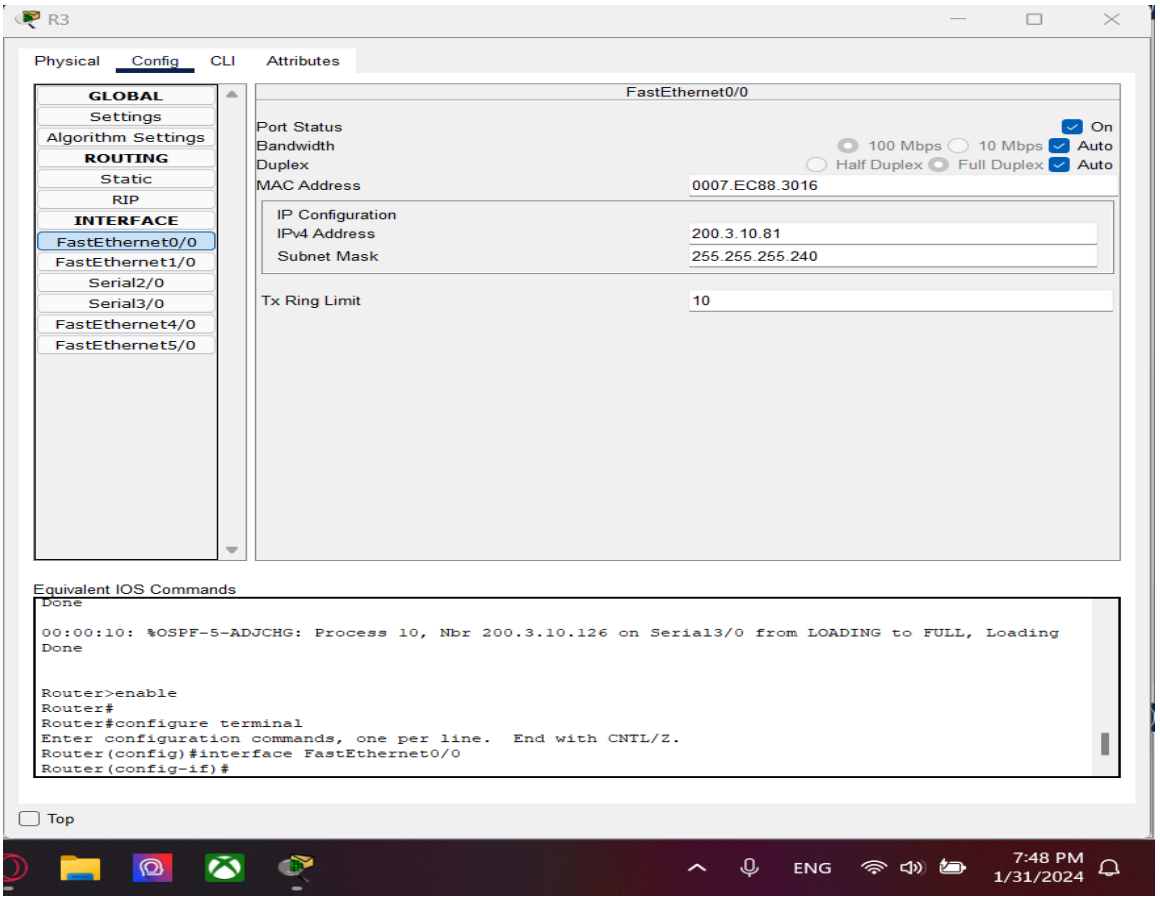
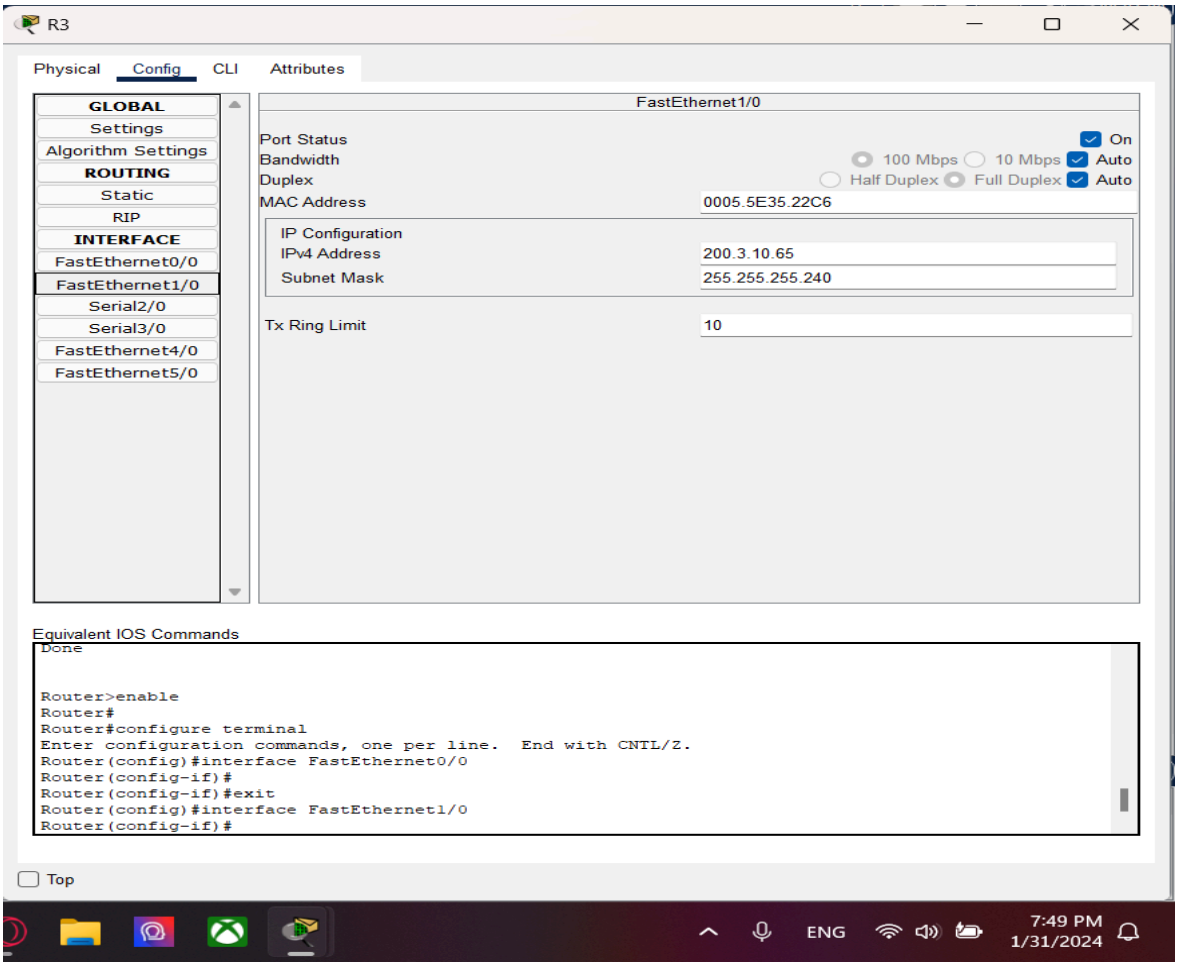


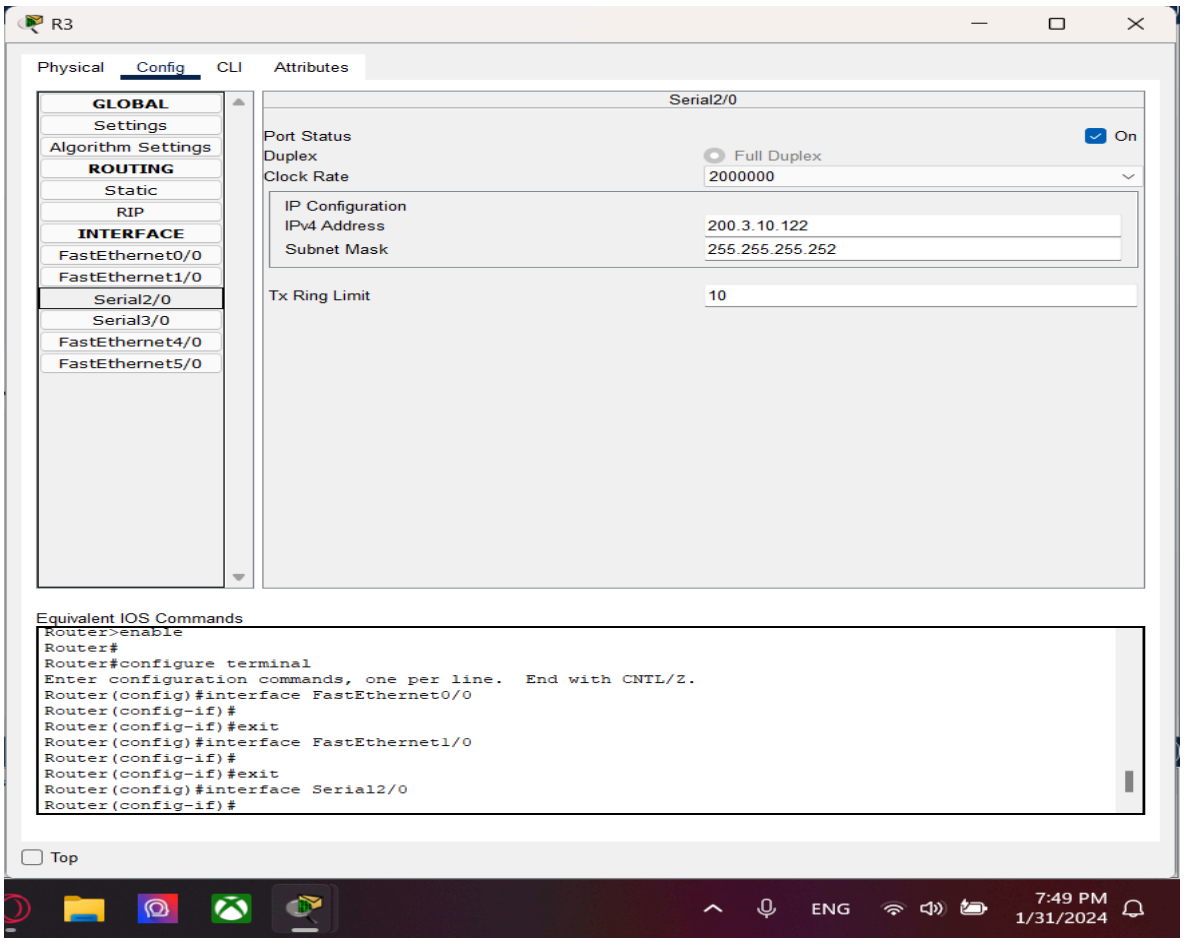
Figure4: Configuration of R2

⇒ Router 3 (R3)

The following four snapshots (Figure-5) shows the configuration of the R3







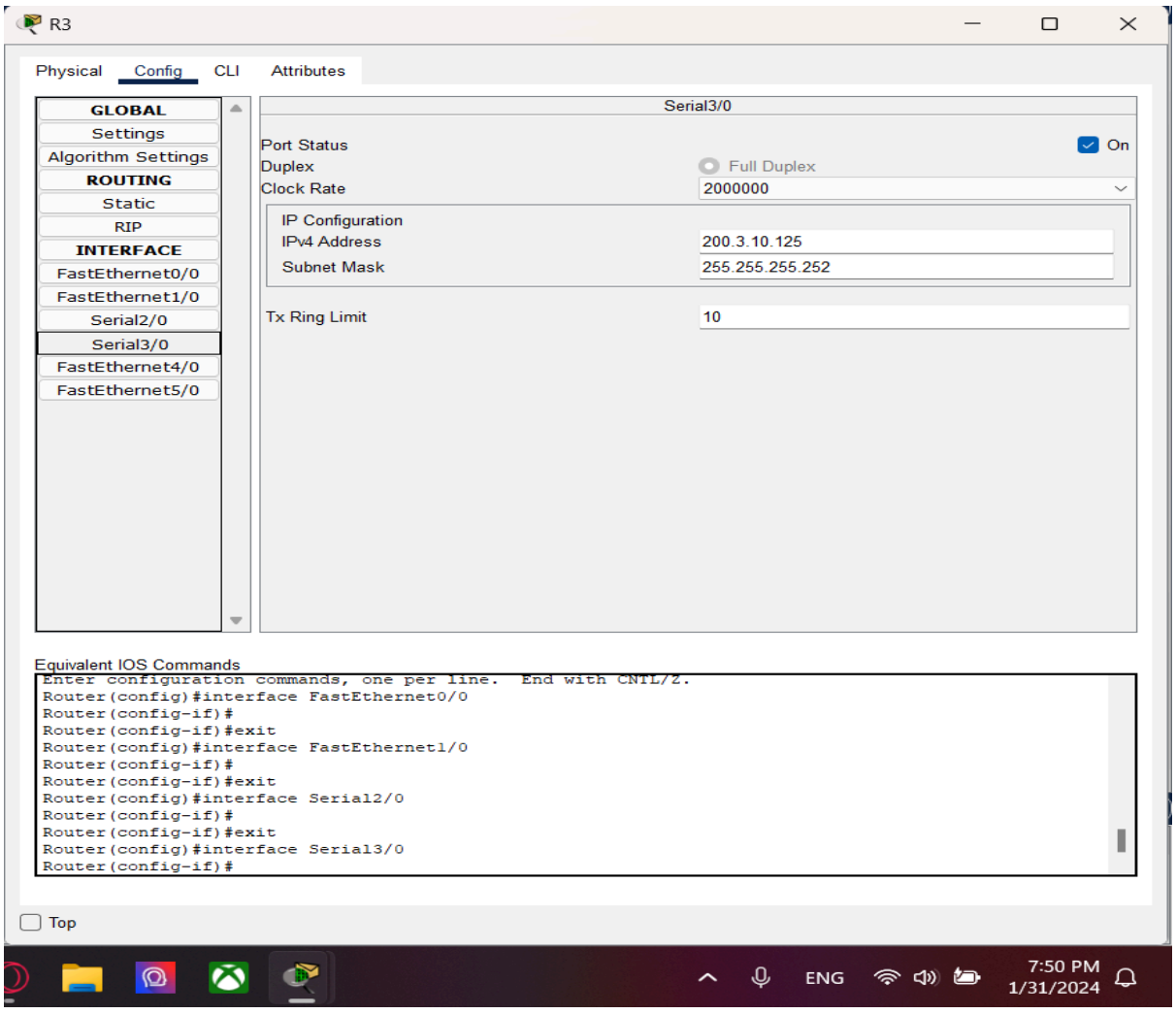
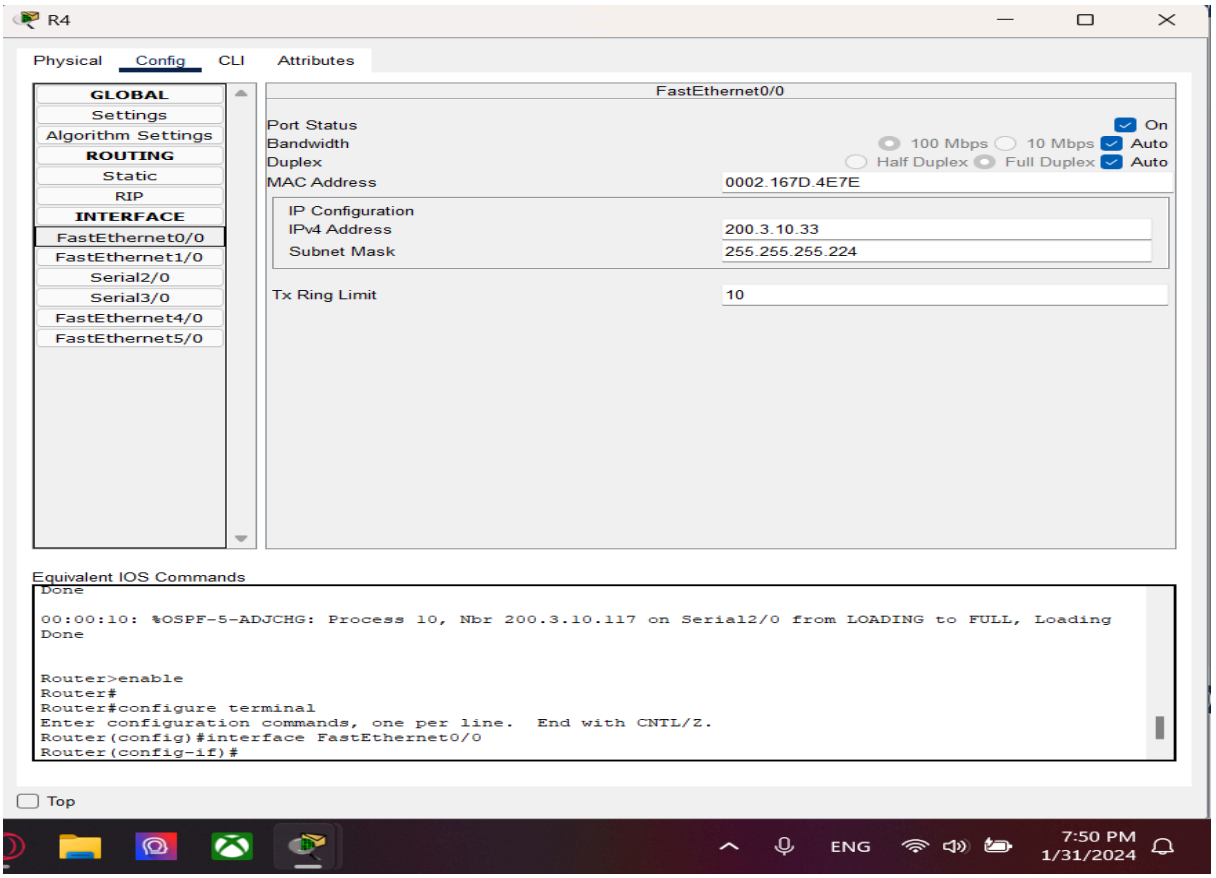
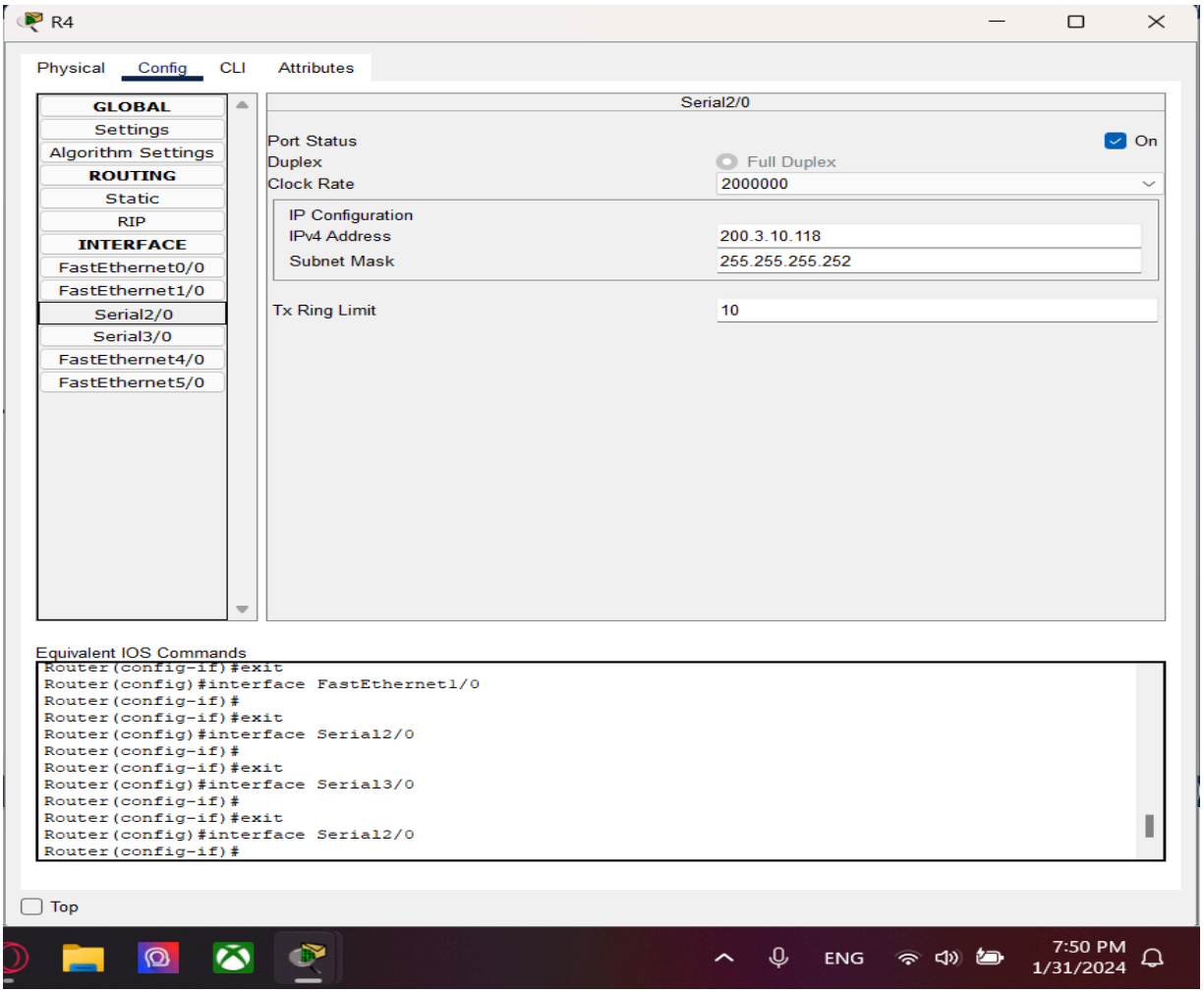


Figure5: Configuration of R3

⇒ Router 4 (R4)

The following three snapshots (Figure-6) shows the configuration of the R4





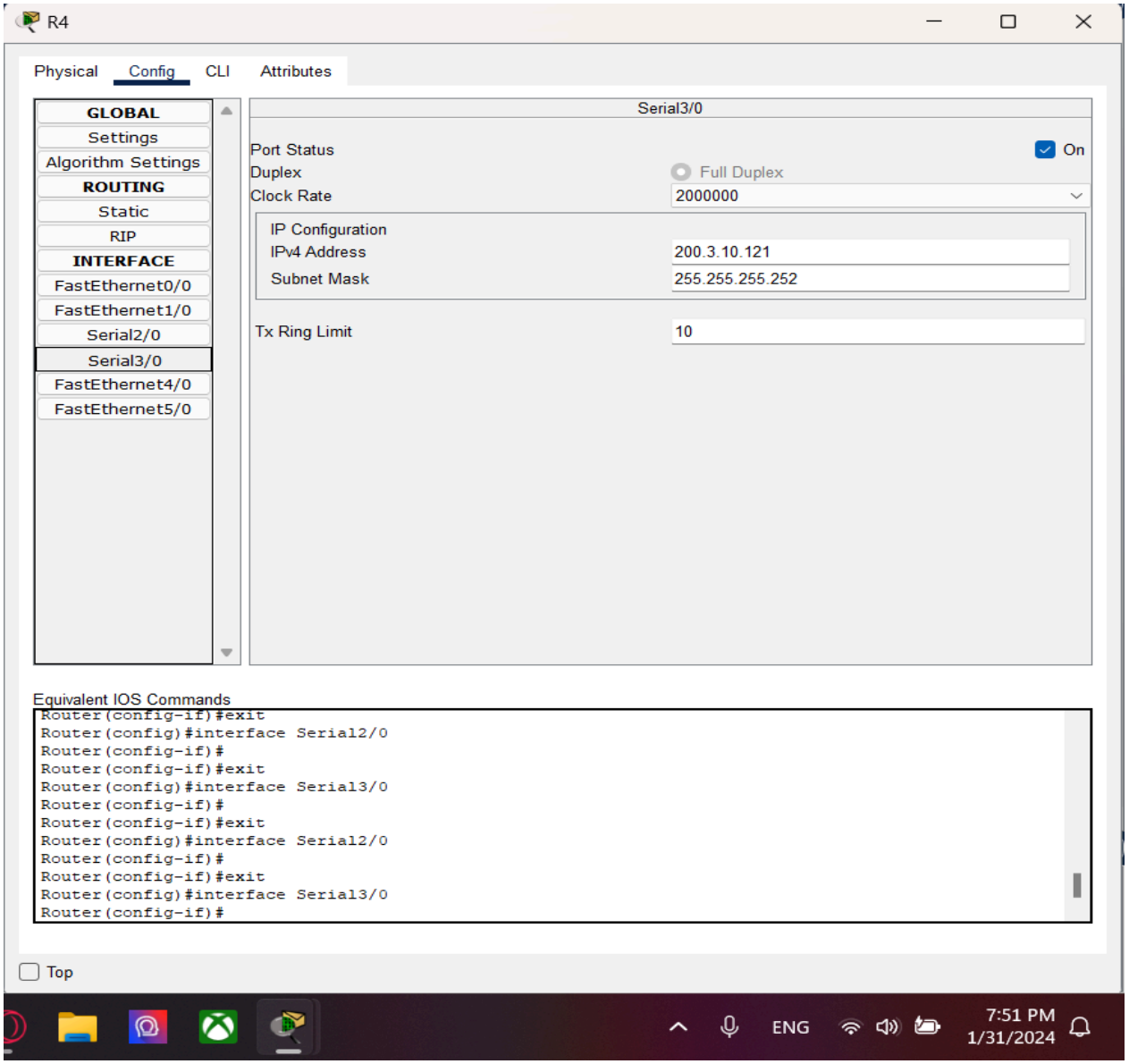


Figure6: Configuration of R4

After configuring the routers we configured the PCs as well as the servers:

⇒ Company A

The following three snapshots (Figure-7) shows the configuration of all PCs in company A

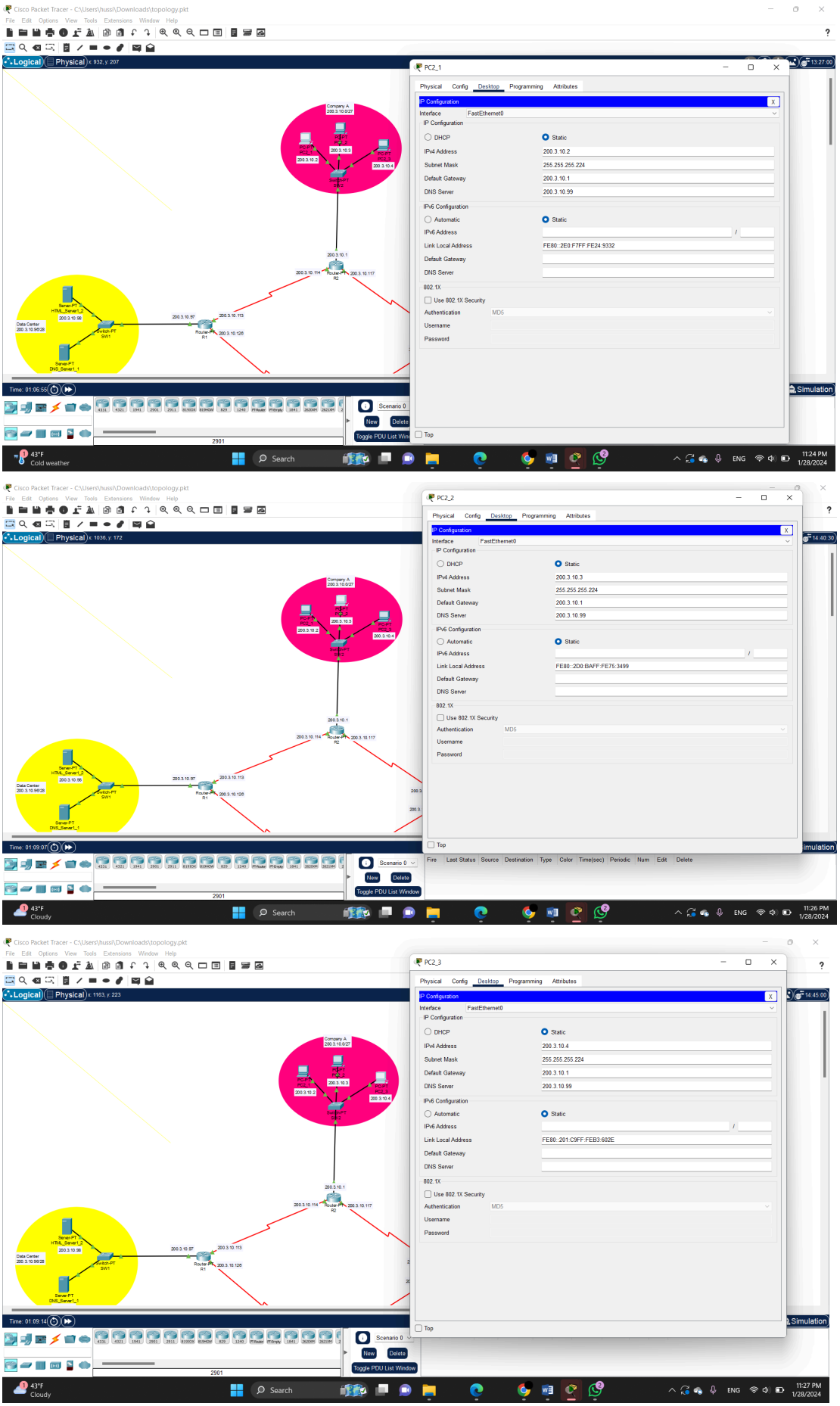


Figure7: Configuration of PCs in company A

⇒ Company B

The following three snapshots (Figure-8) shows the configuration of all PCs in company B as well as the mail server

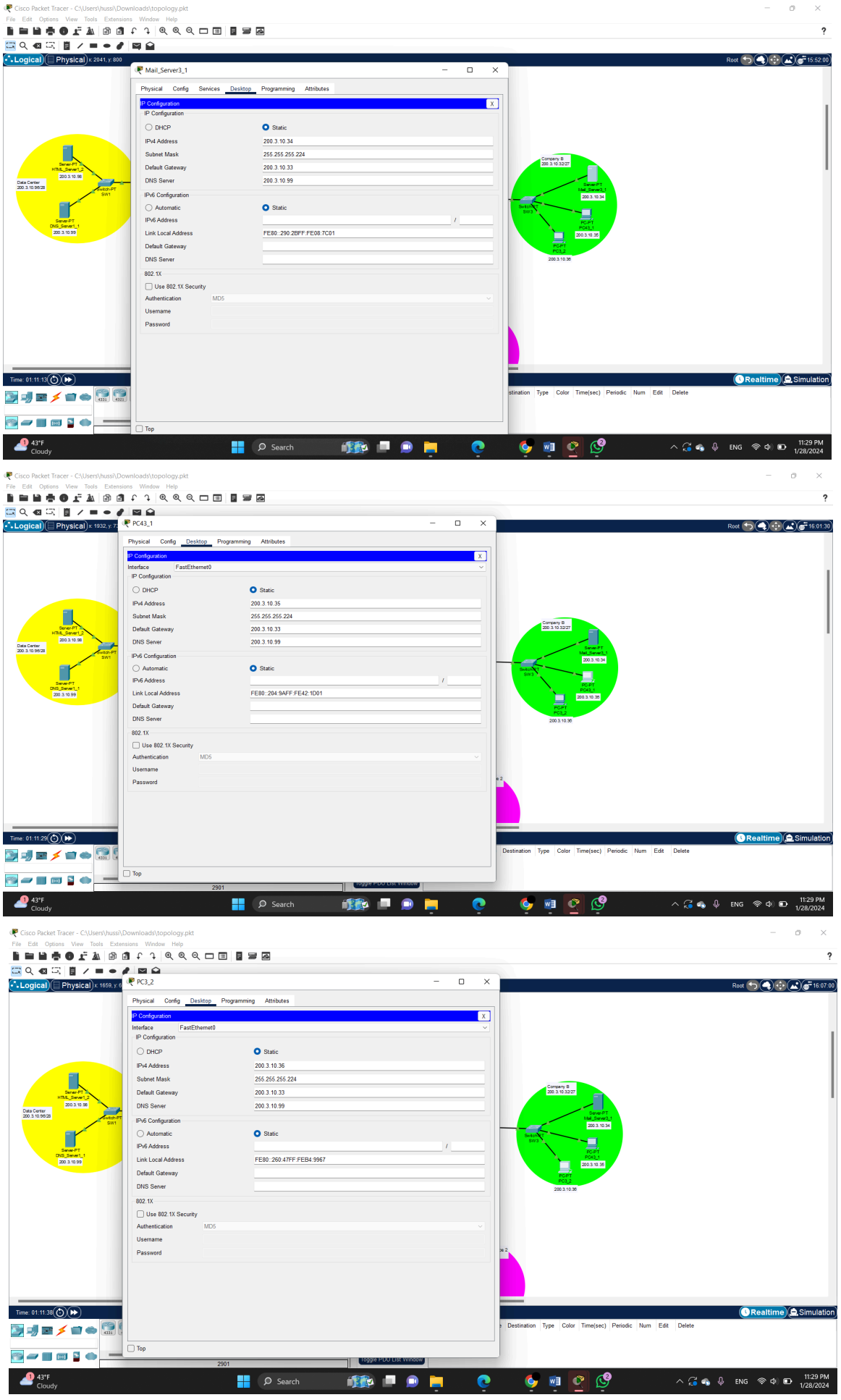


Figure8: Configuration of PCs in company B

⇒ Company C office2

The following two snapshots (Figure-9) shows the configuration of all PCs in company C office2.

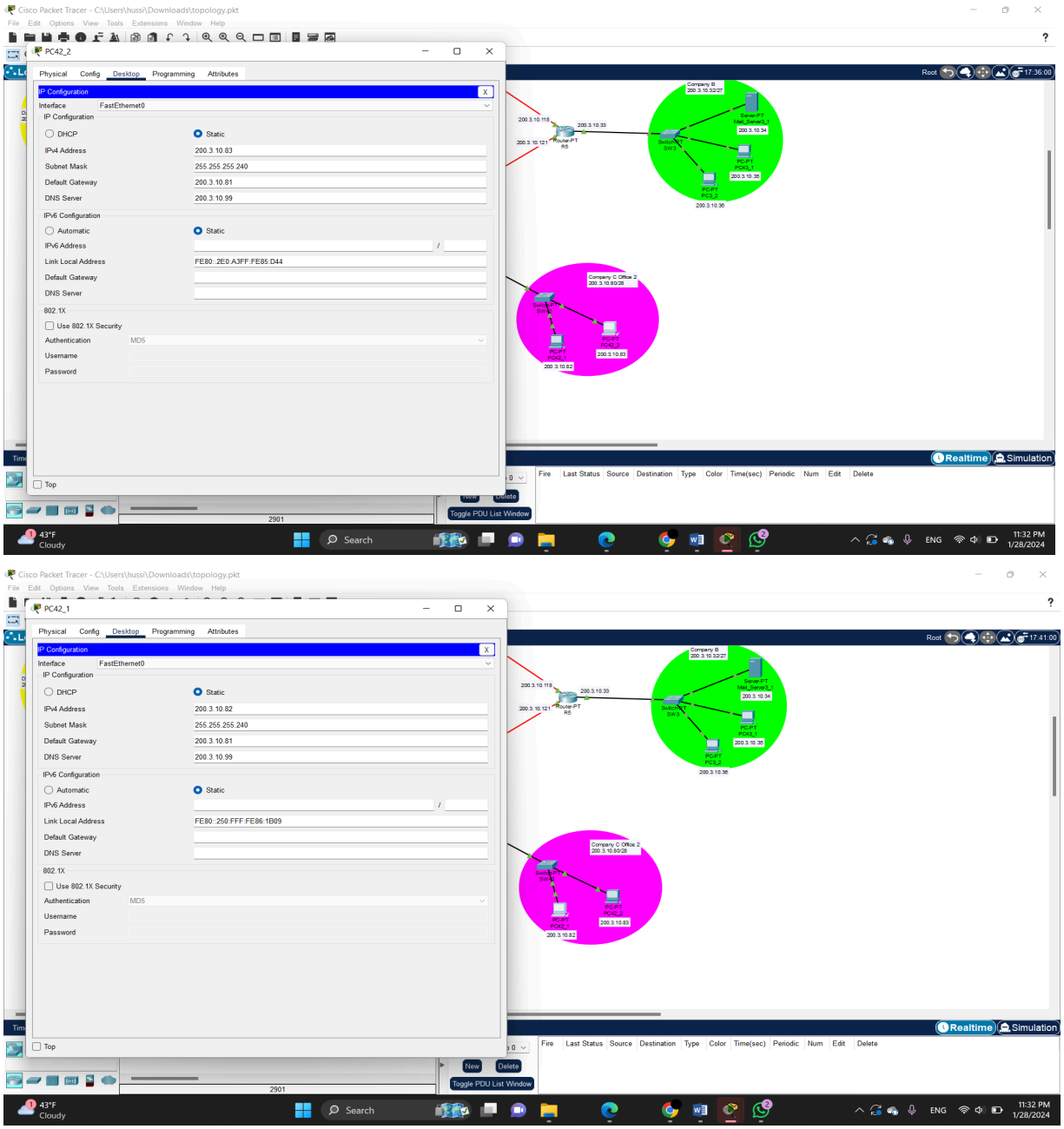


Figure9: Configuration of PCs in company C office2

⇒ Company C office1

The following three snapshots (Figure-10) shows the configuration of all PCs in company C office1.

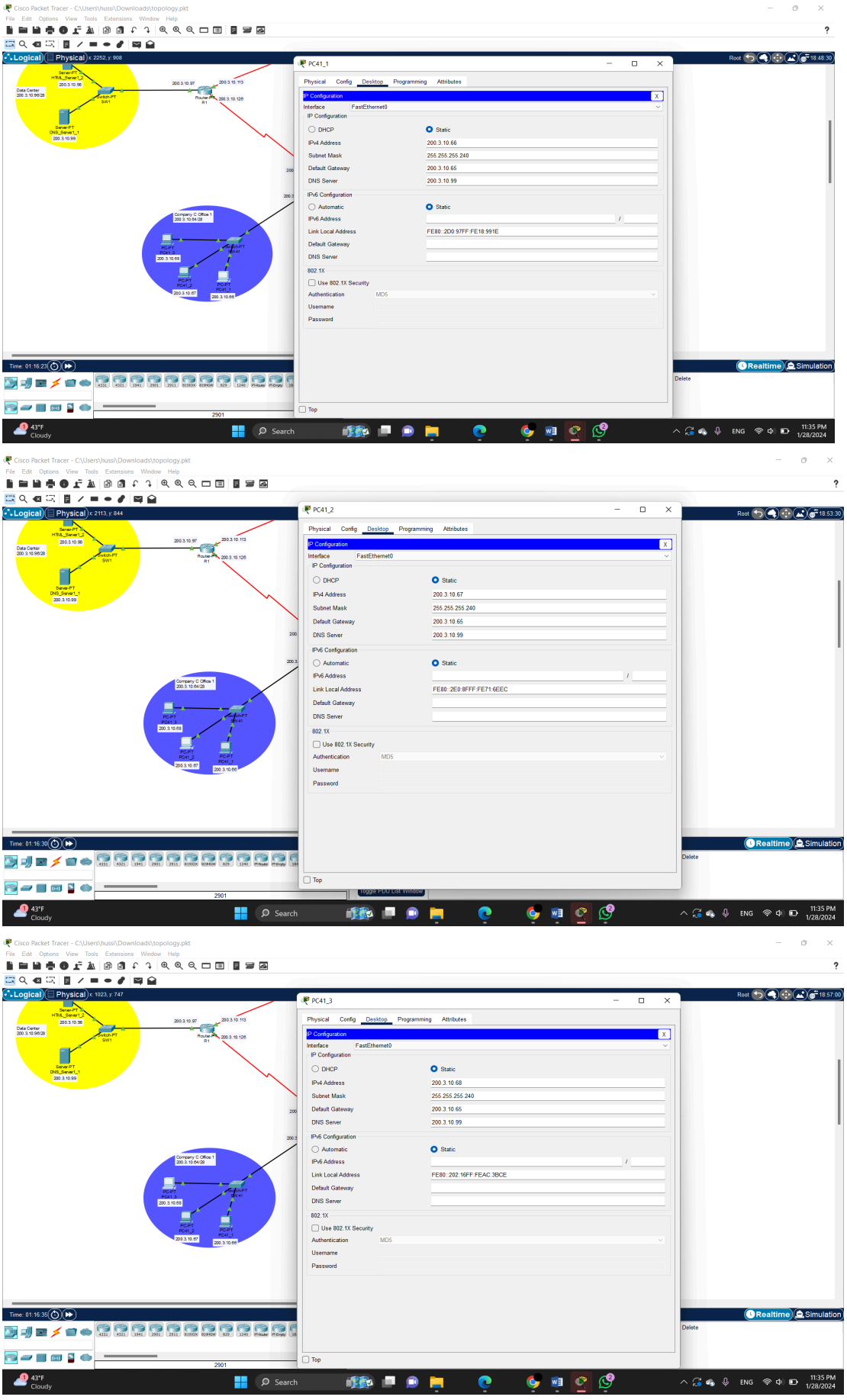


Figure10: Configuration of PCs in company C office1

⇒ Data Center

The following three snapshots (Figure-11) shows the configuration of all servers in the Data Center.

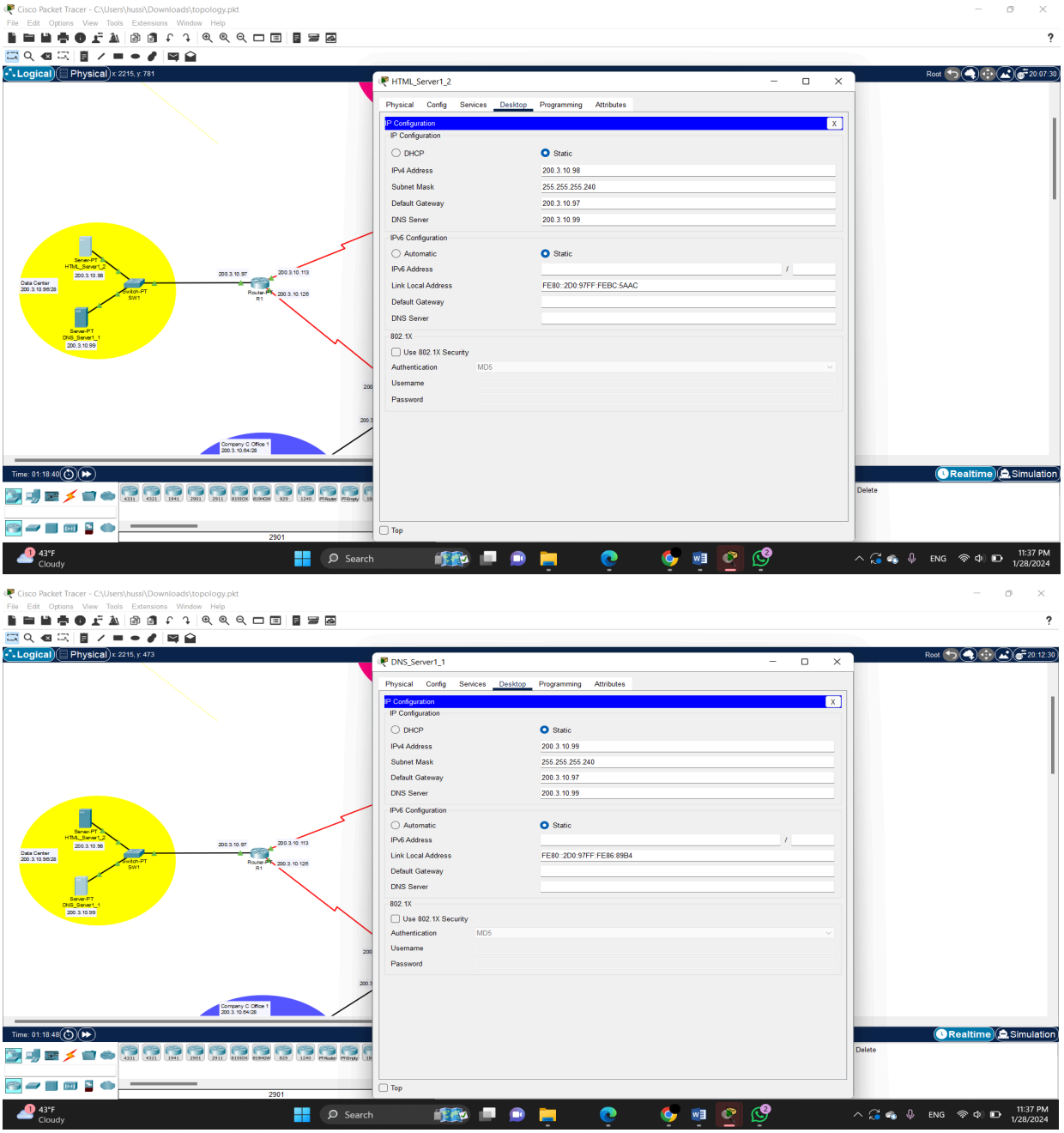


Figure11: Configuration of servers in the data center

3)Part 2:

The provided instructions outline the setup of a network with three servers: an HTTP/Web server and a DNS server in a Data Center, and a mail server in Company B's network. Key tasks include:

Configuring the DNS and Web servers with the domain www.FirstSem2024.com.
Developing a website on the HTTP server, featuring a specific title, a welcome message with red text, group member details, and additional information about their backgrounds and interests.
Setting up email accounts on the email server (ENCS3320.edu) for specified PCs, using unique usernames derived from the device names and a common password “A2024”.
These steps involve both technical configurations of network services and creative design of a website.

⇒ company A:

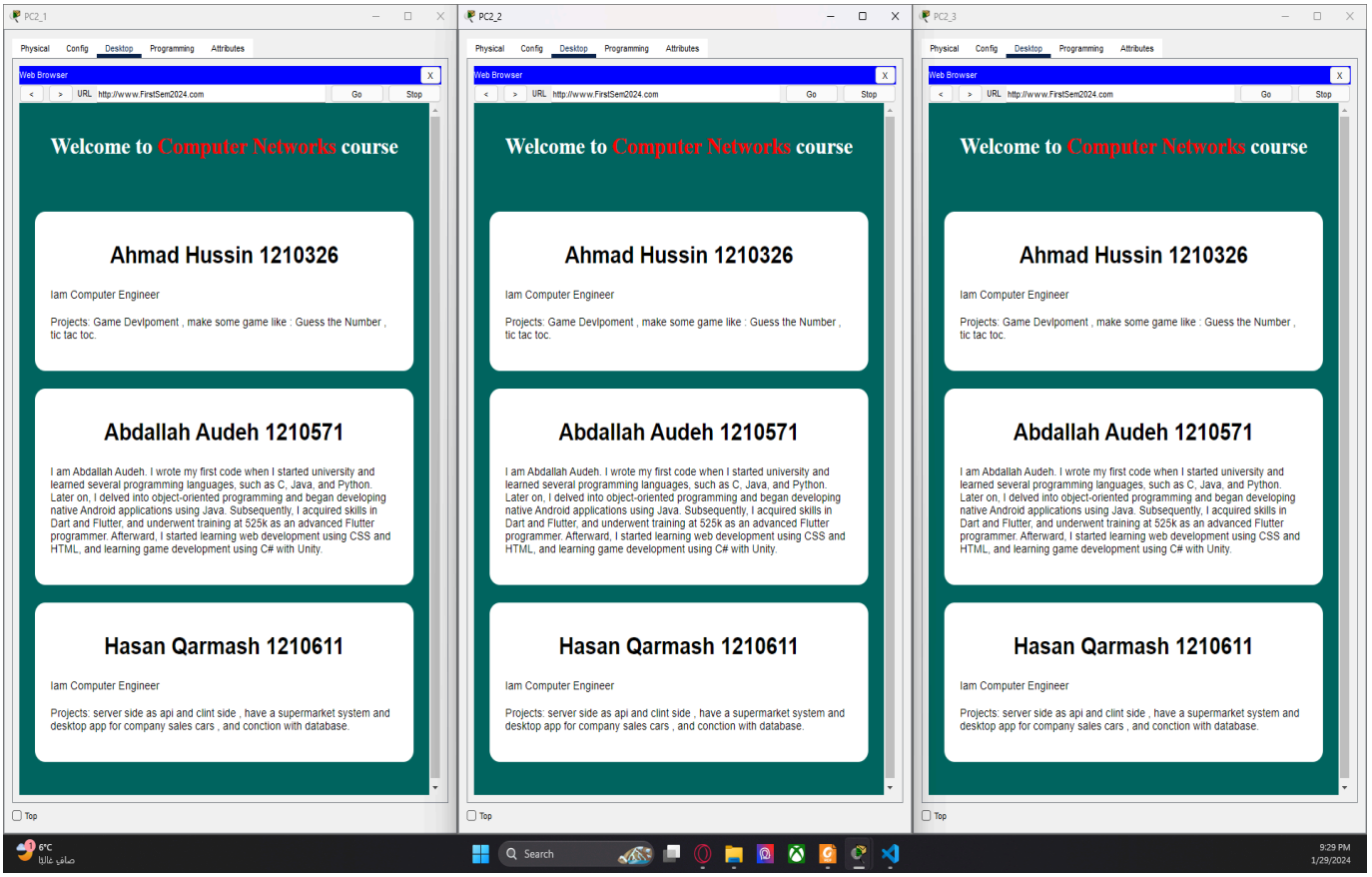


Figure12: Accessing the web page from Company A PCs

The webpage displayed in a browser within Company A's network. It shows a course website with a title, a welcome message where "Computer Networks" is likely in red, and a list of group members with their IDs and project information. This aligns with the task of modifying the index.html on the HTTP server to include specific course-related information and member details.

⇒ company B:

Similar to Company A, this image shows the course website accessed from a different location, presumably within Company B's network. The content is the same, indicating that the DNS server configuration is correctly directing requests for www.FirstSem2024.com to the appropriate HTTP
server, and the webpage is accessible across different networks.

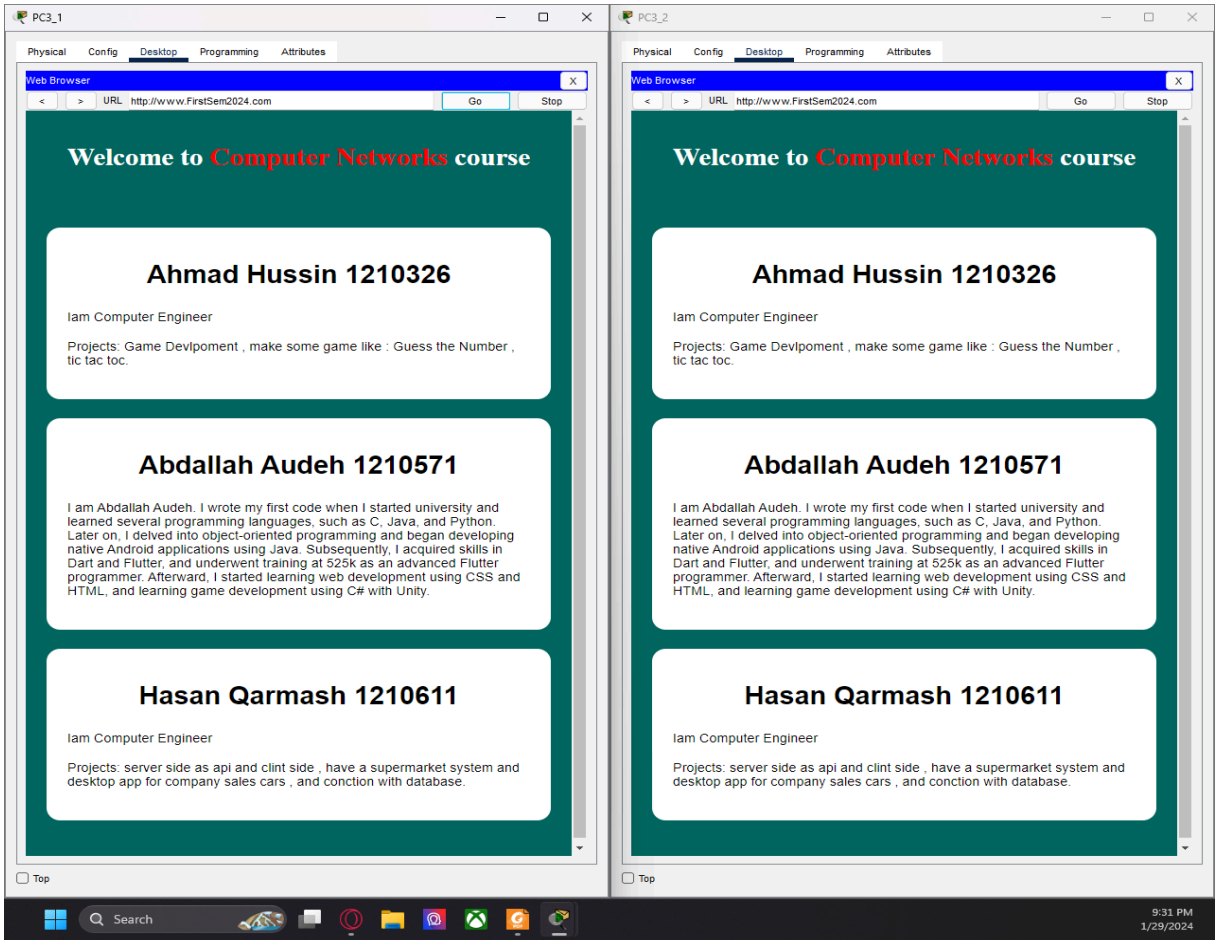


Figure13: Accessing the web page from Company B PCs

⇒ company c office 1:

This again shows the course website accessed from an office location within Company C's network. The consistency of the webpage's appearance across different companies suggests that the web and DNS servers are correctly set up and serving the content as intended.

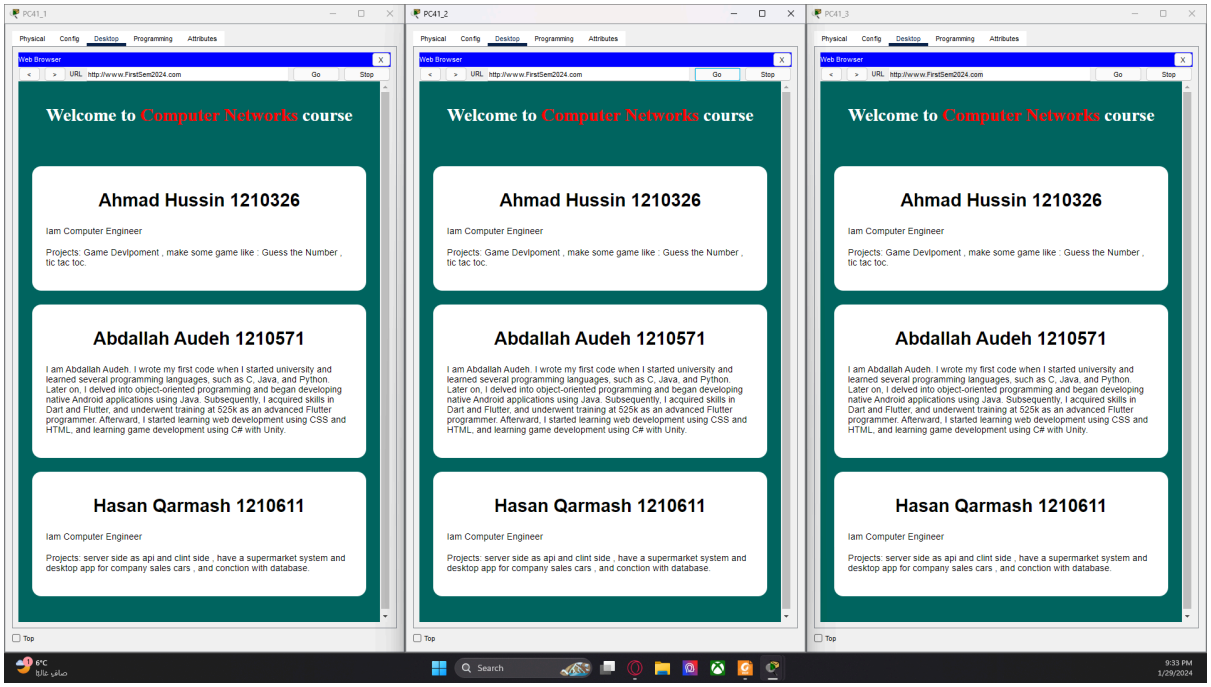


Figure14: Accessing the web page from Company C office1 PCs

⇒company c office 2

Another access point within Company C's network, with the same web page displayed. This indicates that the network configuration is robust, allowing multiple users in different locations to access the web server.

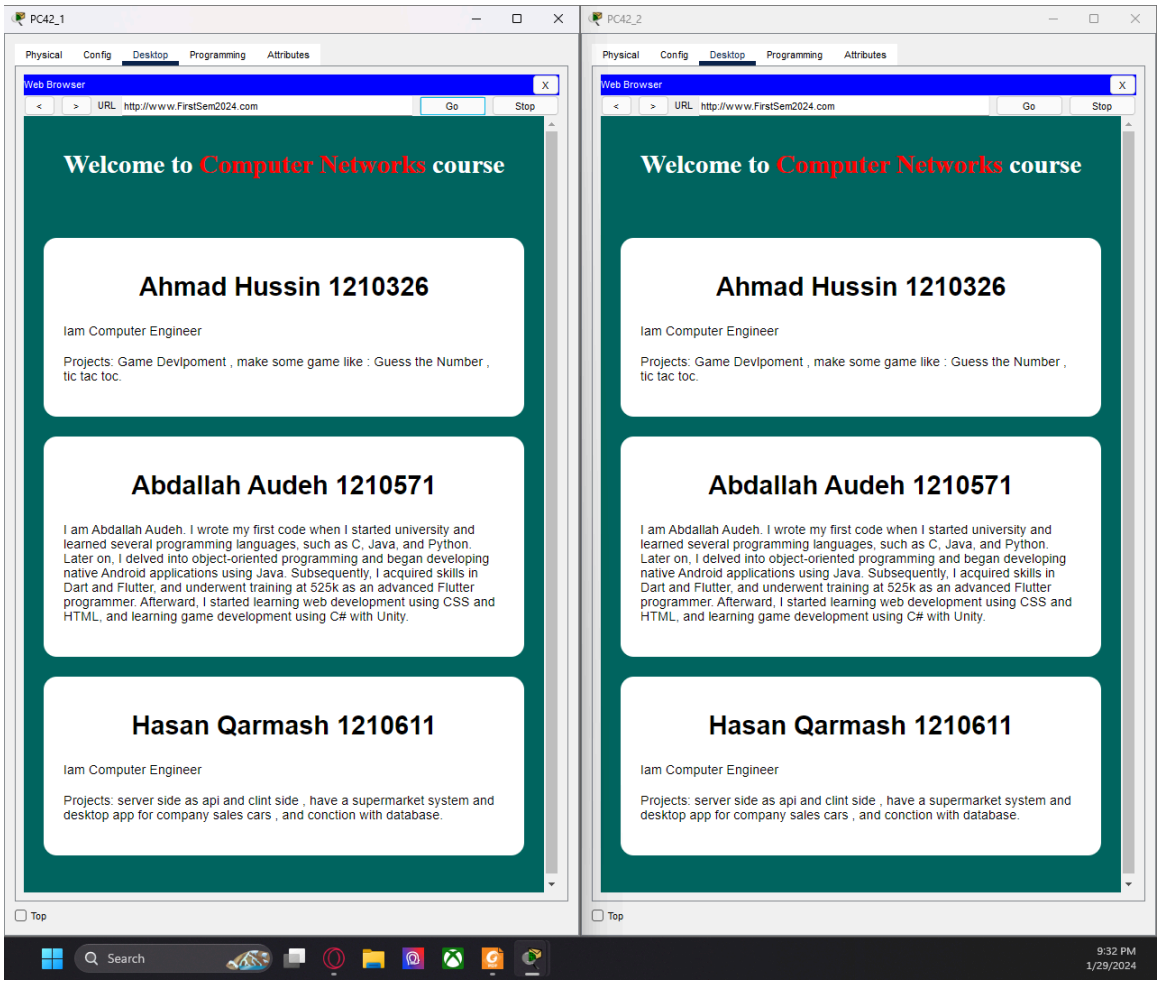


Figure15: Accessing the web page from Company C office2 PCs

The website displayed in these images meets the specified requirements, such as having a title, a welcome message with a portion in red, listing group members and their information, and providing additional details about the group members' backgrounds. The appearance of the website on all computers suggests that the DNS server is correctly resolving the domain name across the network and that the HTTP server is serving the webpage without any location-based restrictions.

⇒ configuring the Web server

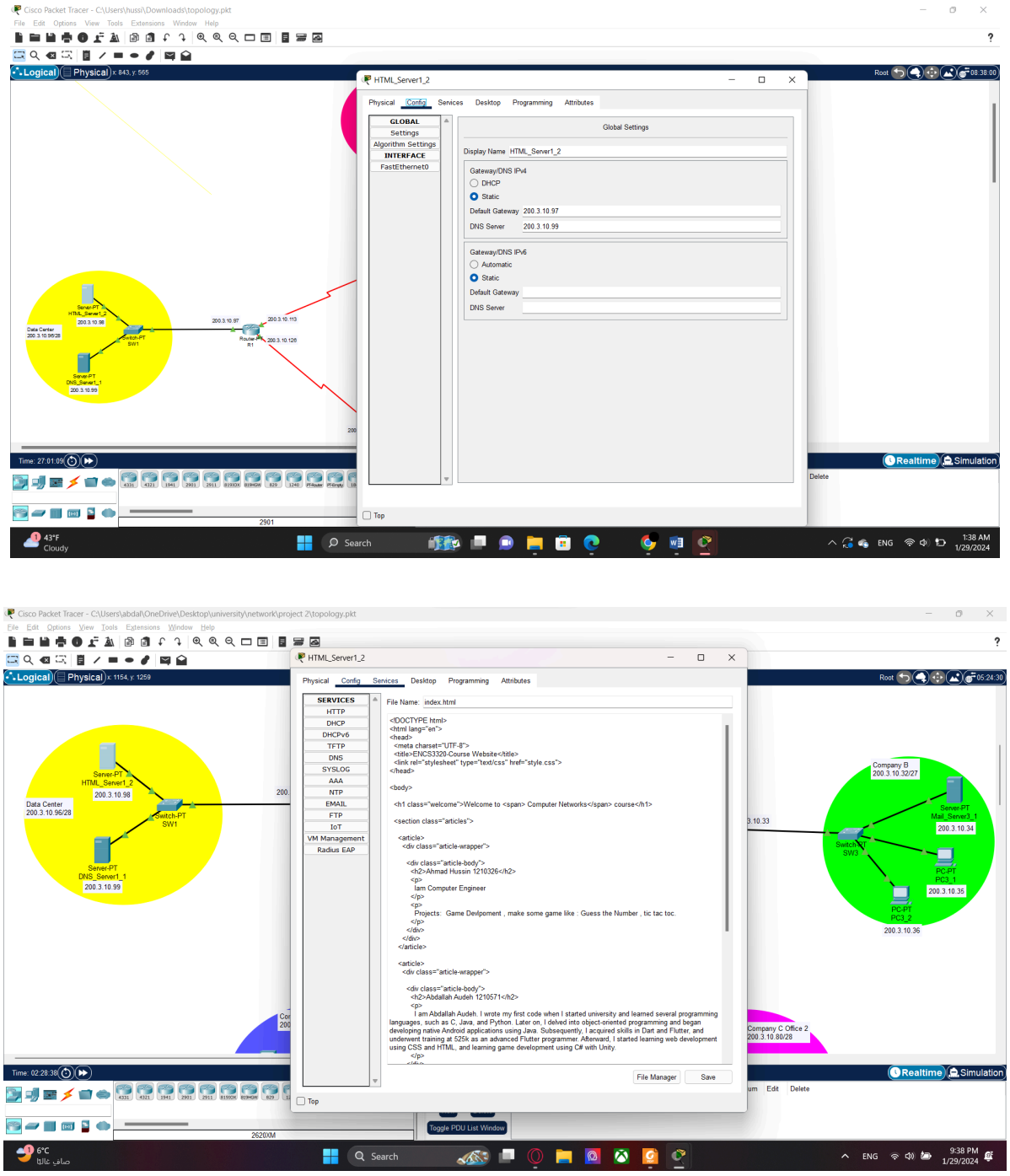


Figure16: configuration of the web server

⇒ configuring the DNS server

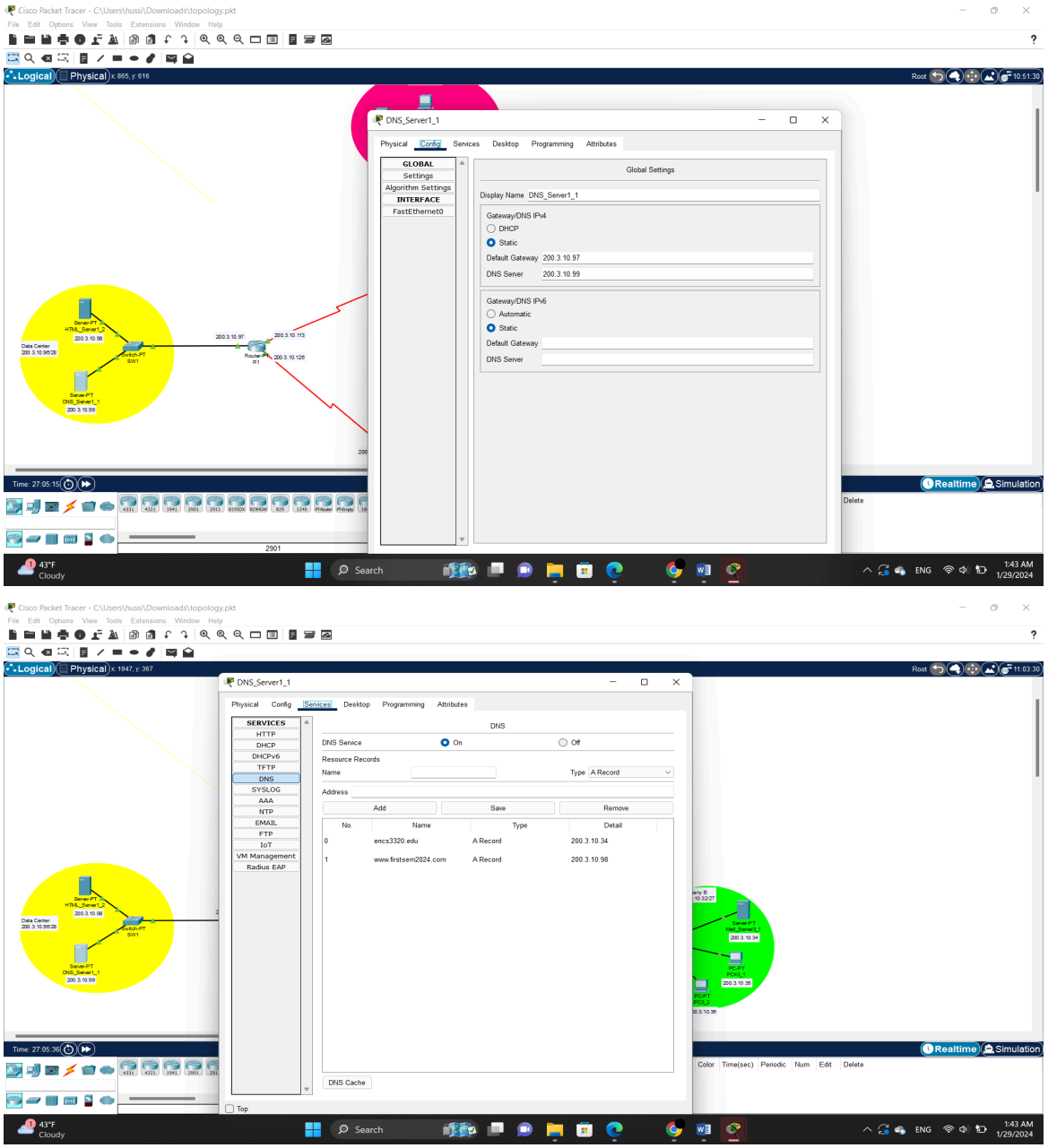


Figure17: configuration of the DNS server

⇒ configuring the Mail server

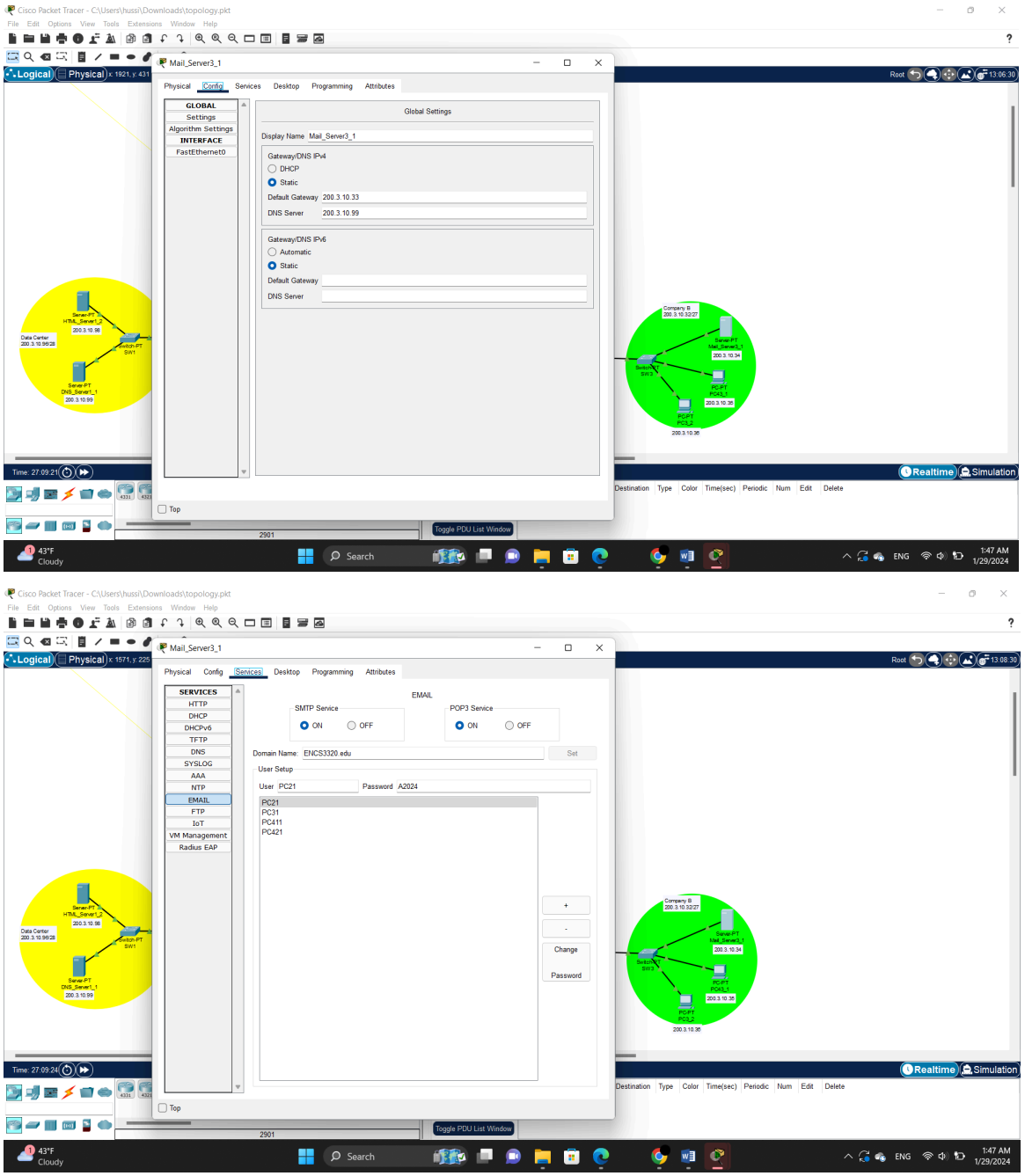


Figure18: configuration of the Mail server

4)Part3:

In our network configuration, we have implemented the OSPF routing protocol across all routers to enhance the efficiency and management of our network traffic. We have designated the process ID as 10 for uniformity across the entire network. The OSPF areas have been strategically assigned to correspond with the different segments of our network infrastructure: the Data Center is labeled as area 1, Company 1 as area 2, Company 2 as area 3, and Company 3 is segmented into area 4. The core network serves as the backbone area 0, which is a crucial component in OSPF for ensuring all areas can communicate effectively. By utilizing OSPF, we ensure that the shortest path is always taken for data packets traveling across our network, resulting in improved performance and reliability.

in the following snapshots we will show that the OSPF works on all routers:

⇒ Router1 (R1)

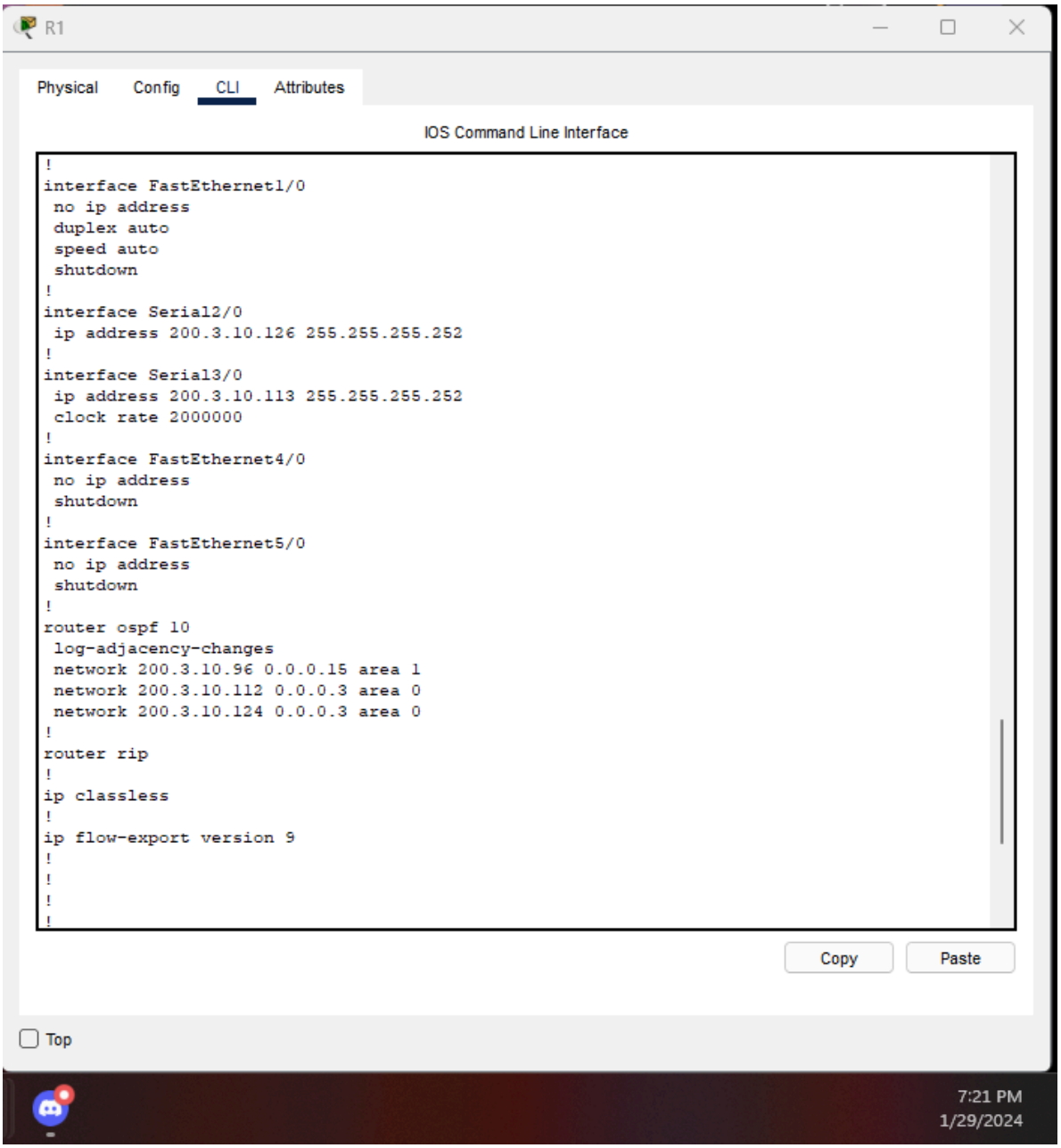


Figure19: checking OSPF for R1

⇒ Router2 (R2)

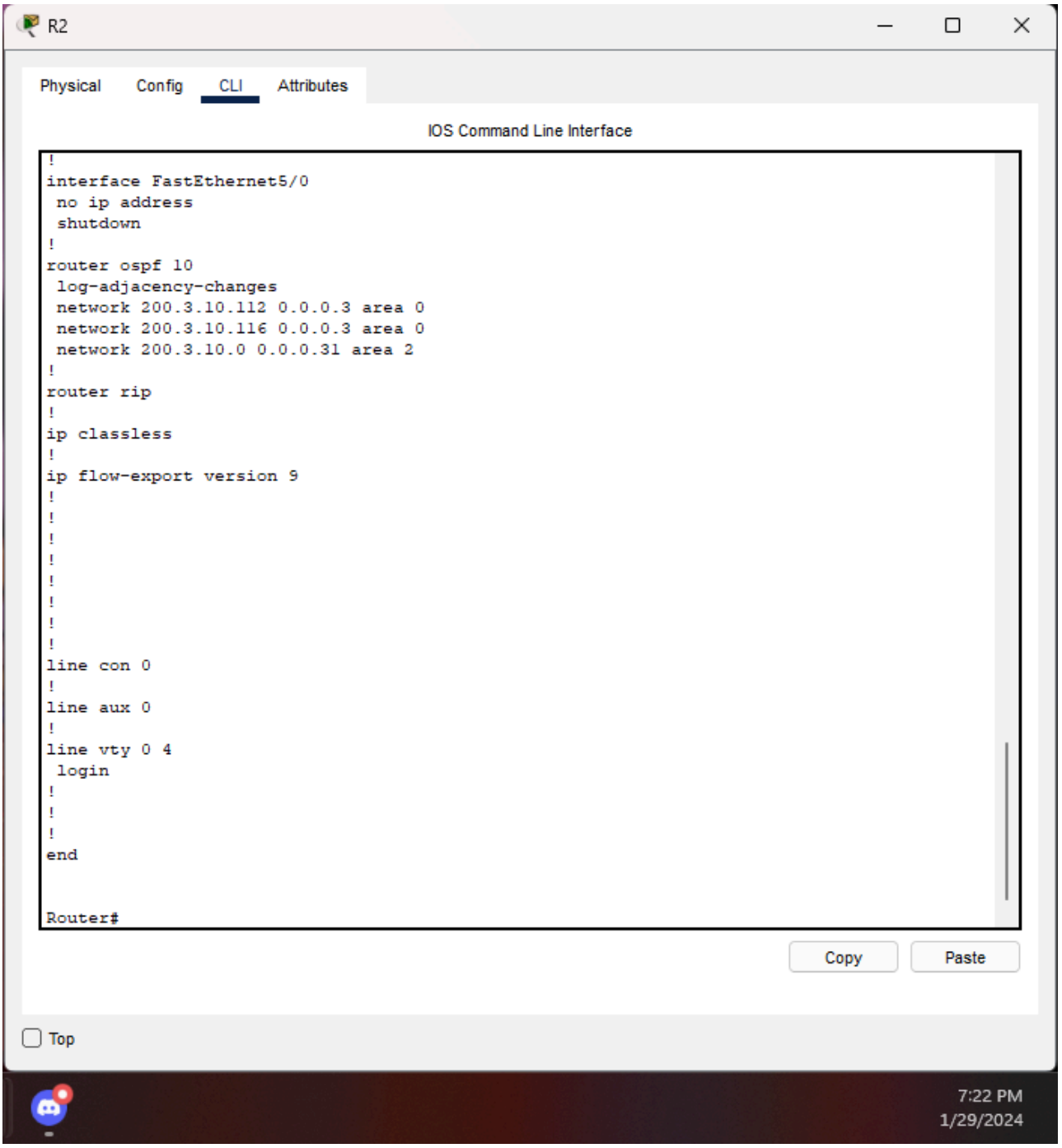


Figure20: checking OSPF for R2

⇒ Router 3 (R3)

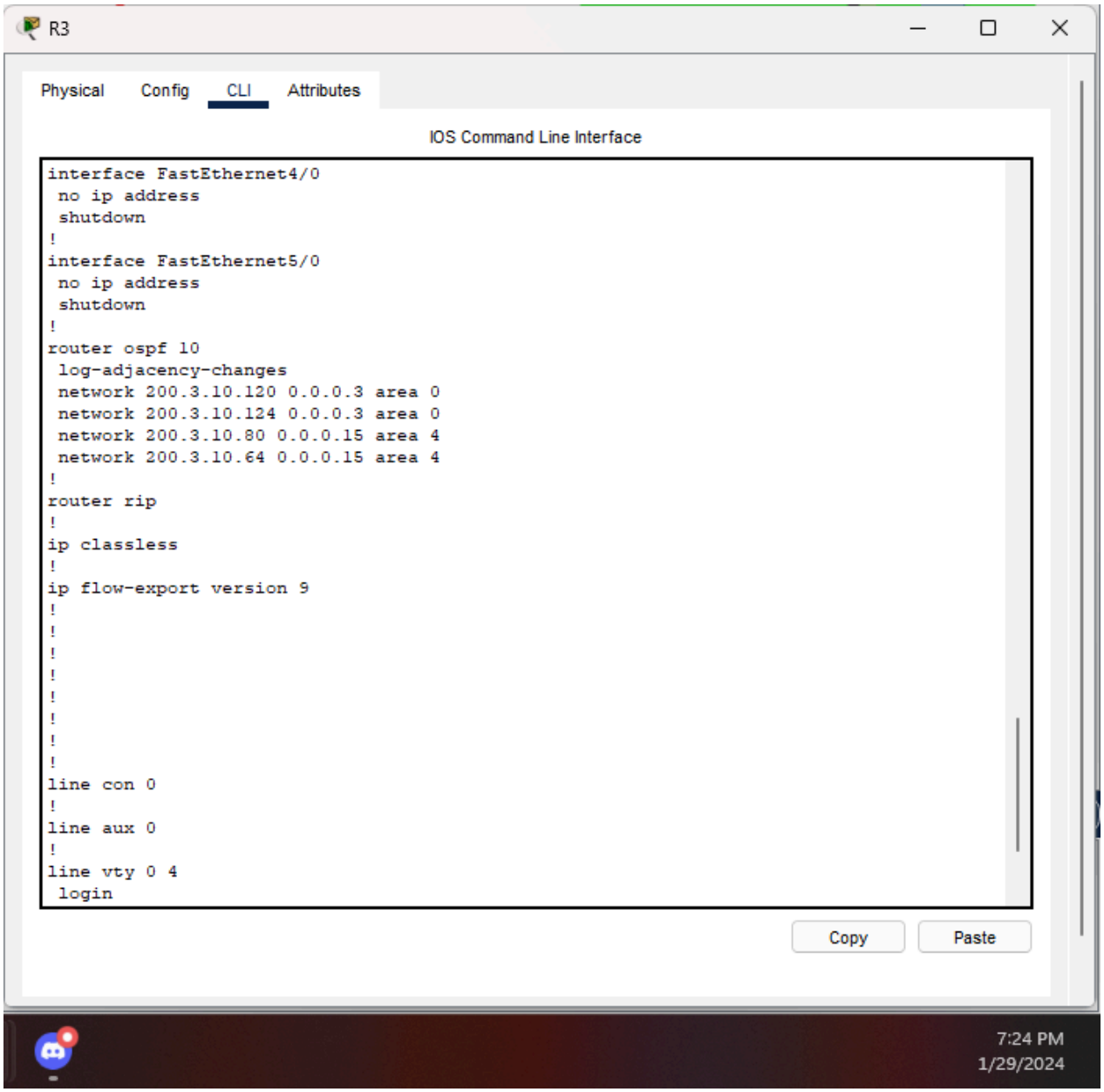


Figure21: checking OSPF for R3

⇒ Router 4 (R4)

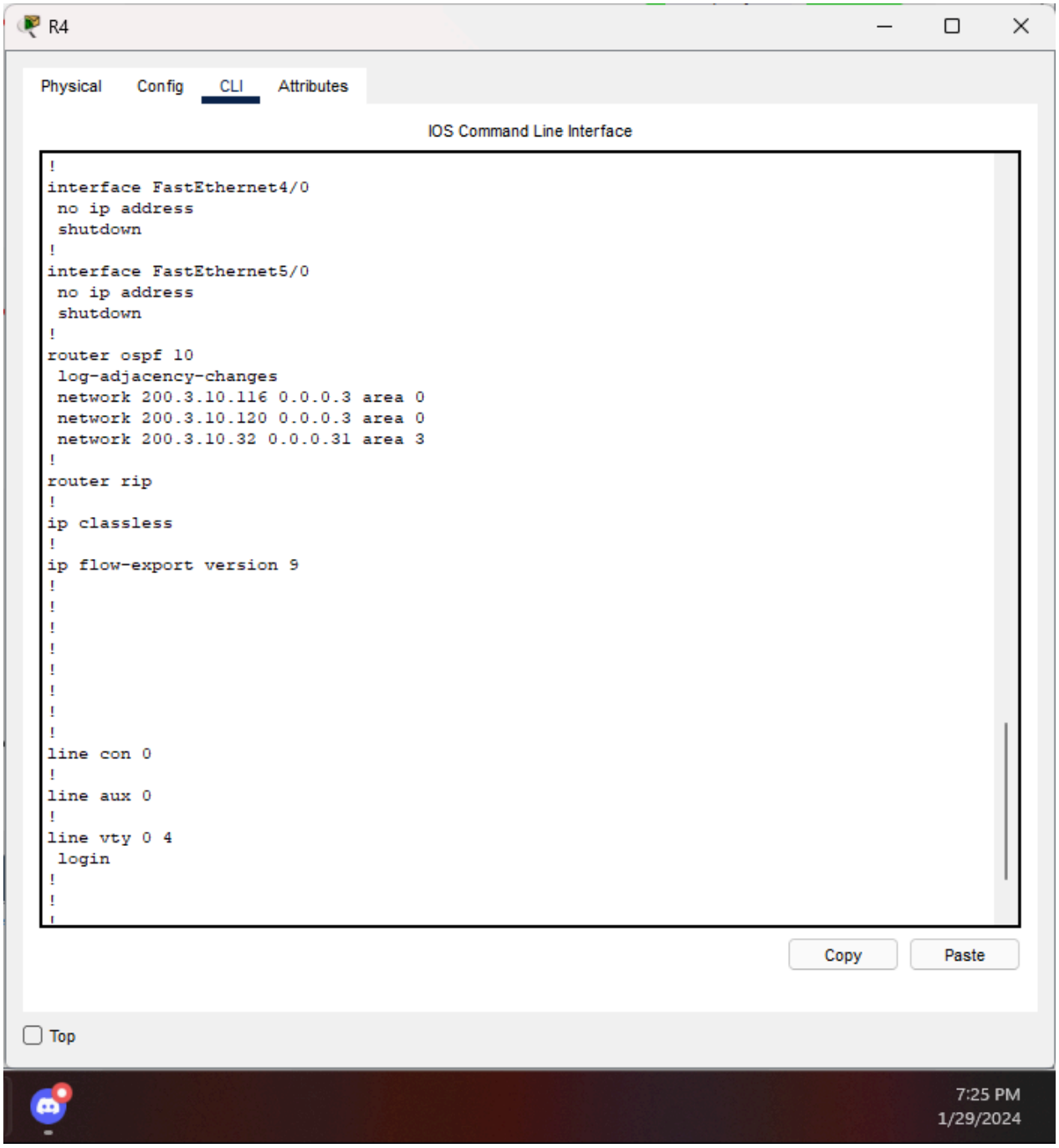


Figure22: checking OSPF for R4

5) Part 4:

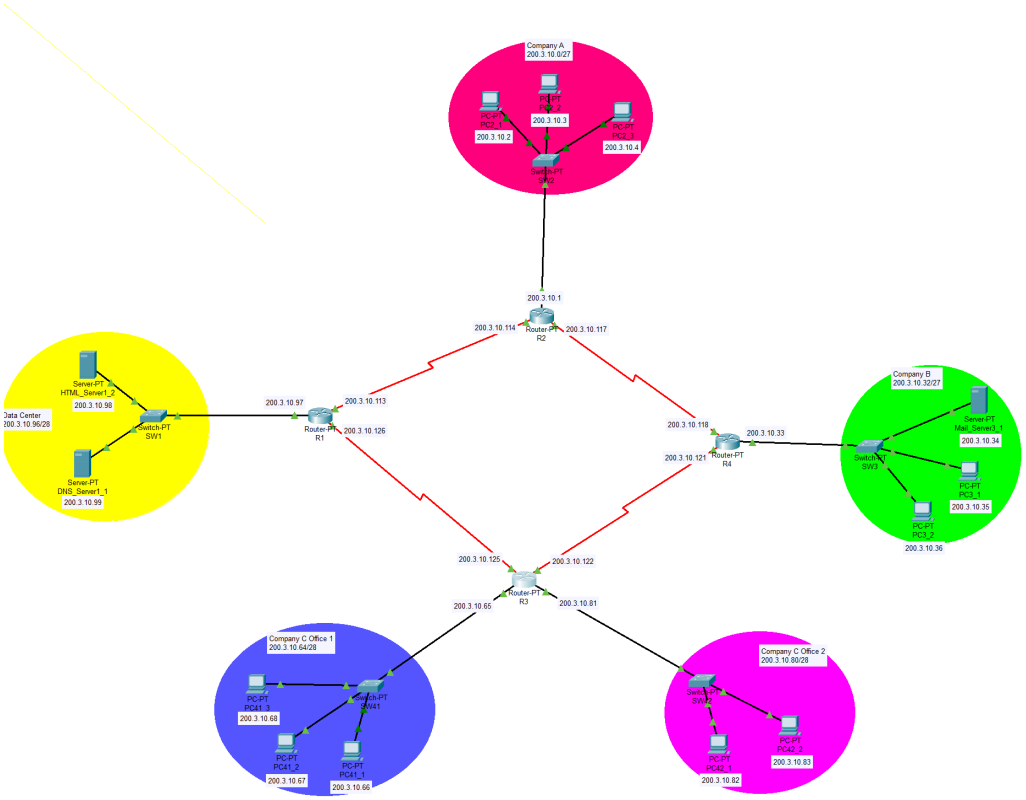
In Part 4 of our network project, we have conducted a comprehensive testing phase to validate the connectivity, routing efficiency, and accessibility of our website and email services across the entire network topology. We began by testing the connectivity between all PCs across the various networks—Data Center, Company A, Company B, and both offices of Company C. To ensure accuracy and accountability, we captured snapshots of the results from our ping and traceroute commands, which provided insights into the network's performance and the path data packets took between devices.

Furthermore, we accessed our website 'www.FirstSem2024.com' from all PCs to verify that the DNS and web server configurations were correct and that the site was reachable from multiple points in the network. Snapshots were taken during this process to document the website's accessibility from each location.

Network	Number of End Devices (PCs and Servers)
Data Center	5
Company A	26
Company B	24
Company C Office 1	10
Company C Office 2	14

We also meticulously recorded the results of these tests, including the snapshots, and provided detailed explanations within our report. This not only demonstrated the operational status of our network but also served as a reference for the network's topology and the number of hosts within each network segment, as outlined in Table 2. This table excludes the router interface to focus solely on end devices, offering a clear view of the network's scale and distribution of resources.

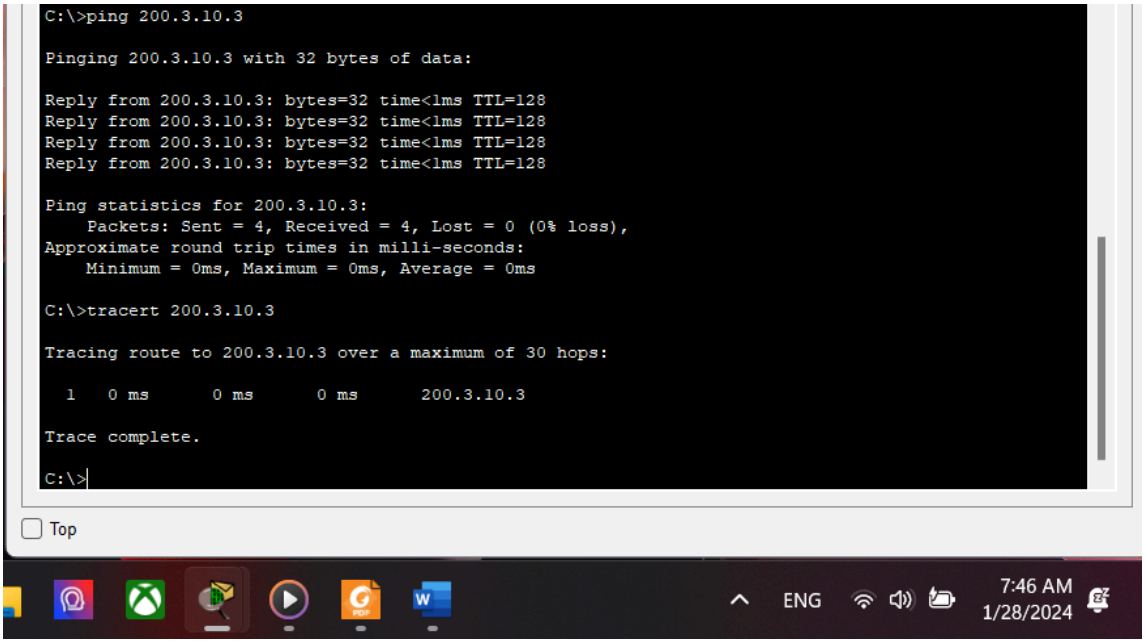
Our careful documentation and analysis have affirmed the network's integrity and our readiness for deployment. We have successfully established a robust and reliable network environment that meets our connectivity, routing, and accessibility requirements.



for your question: Test the connectivity between all PCs. You need to take snapshots of the results for ping and tracert commands between all PCs :

Company A:

⇒ PC 2_1 To PC 2_2:



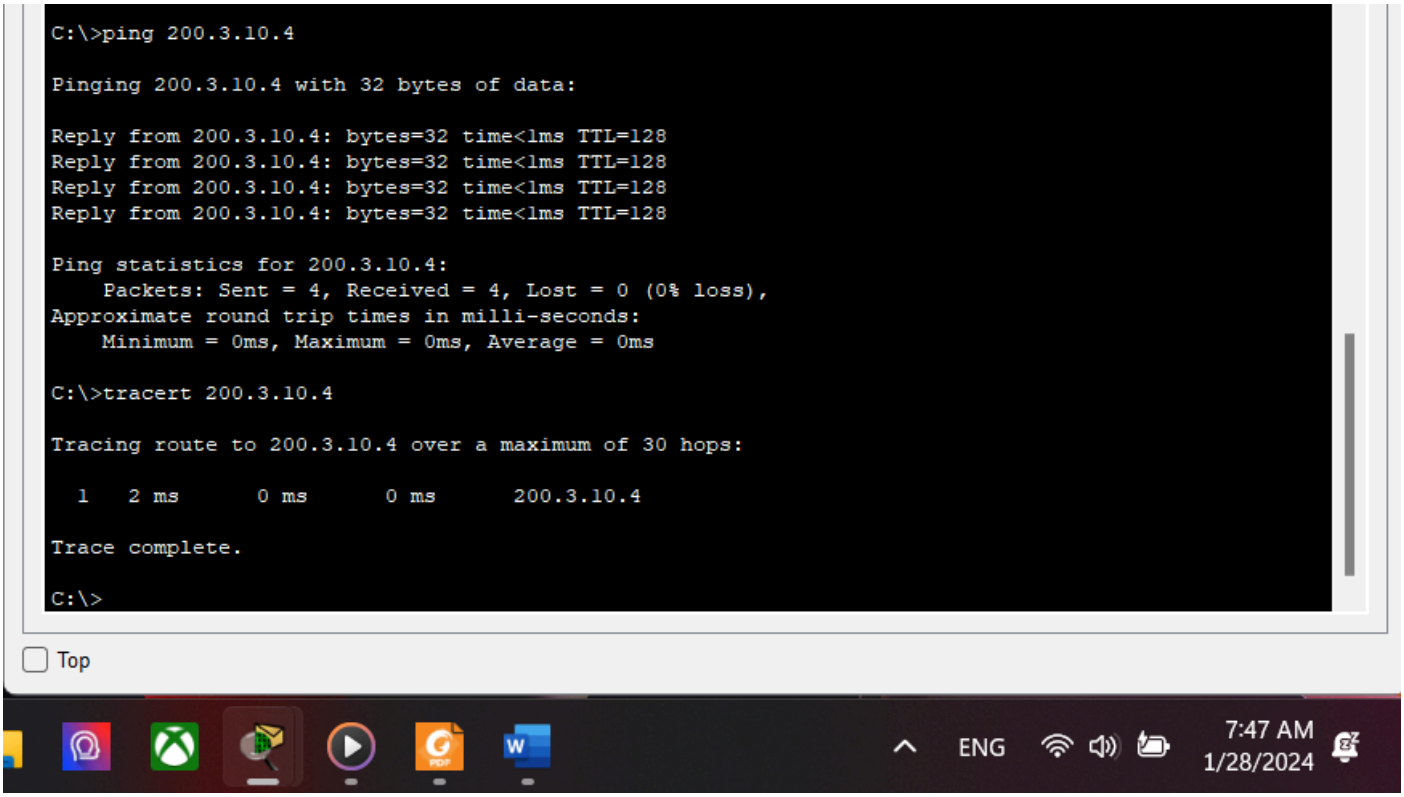
Ping Command:

The ping command is a diagnostic tool used to test the connectivity between the current host (the computer where the command is being run) and the target host (identified by the IP address 200.3.10.3).
The output indicates that four packets of data were sent to the IP address 200.3.10.3 and all four were received back, which means there was no packet loss. This implies a stable connection to the target IP address.
The time<1ms indicates the latency between the hosts is less than one millisecond, which is extremely fast, suggesting that the target is very close on the network, possibly on the same local network or even the same machine.
TTL=128 is the Time to Live for the packet, which decrements on each router it passes; starting at 128 suggests that the target is quite close because very few decrements have occurred.

Tracert Command:

The tracert (short for traceroute) command is used to determine the route taken by packets to reach a specific IP address from the host. It shows each hop and the time taken to reach it.
In this case, the output is very short, showing only one hop, which is the destination itself (200.3.10.3), and the time taken to reach it is 0 milliseconds. This again indicates that the destination is on the local network or the same host, as there are no intermediate routers listed.

⇒ping and tracert result From PC 2_1 To PC 2_3:



Ping Command:

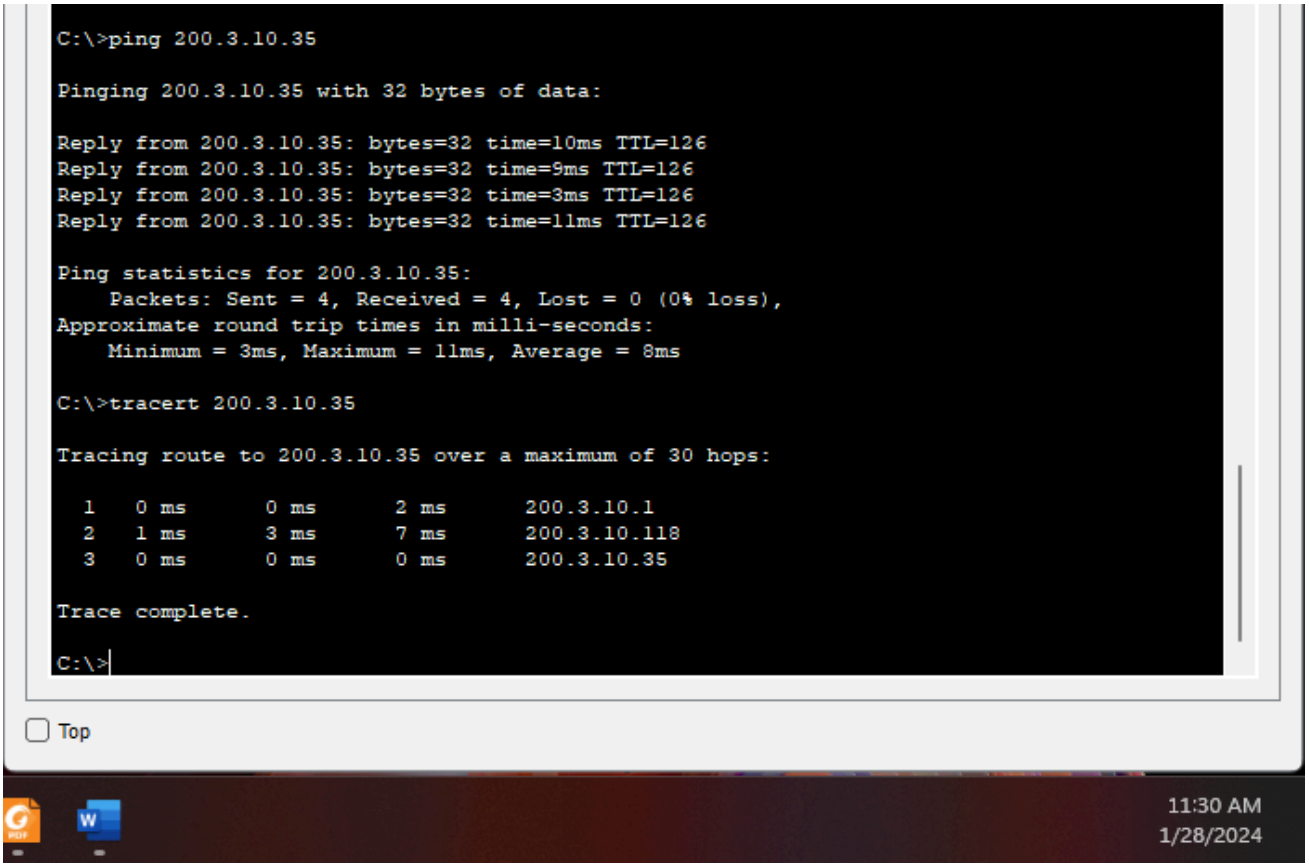
The ping command output shows that all four packets sent to the IP address 200.3.10.4 were successfully received back with no loss, which means the network connection to the target IP is stable.
The round-trip time recorded as <1ms suggests that the latency is less than one millisecond, indicating that the target device is very close within the network, likely on the same local area network (LAN) or the same physical machine.

TTL=128 indicates the Time to Live value, which is the number of hops a packet can traverse before being discarded. The high TTL value suggests that the packet has not passed through many routers, if any, which is consistent with a local network connection.

Tracert Command:

The tracert command is displaying the route taken by packets to reach the IP address 200.3.10.4. It shows only one hop, which is the destination address itself, with a very minimal delay of 2 milliseconds. The fact that there's only one hop suggests that there are no intermediate routers between the source and the destination, or that the destination is on the same subnet.
This single-hop trace with a very short delay is typical when the destination IP address is on the same local network or subnet.

⇒ ping and tracert result From PC 2_1 To PC 3_1



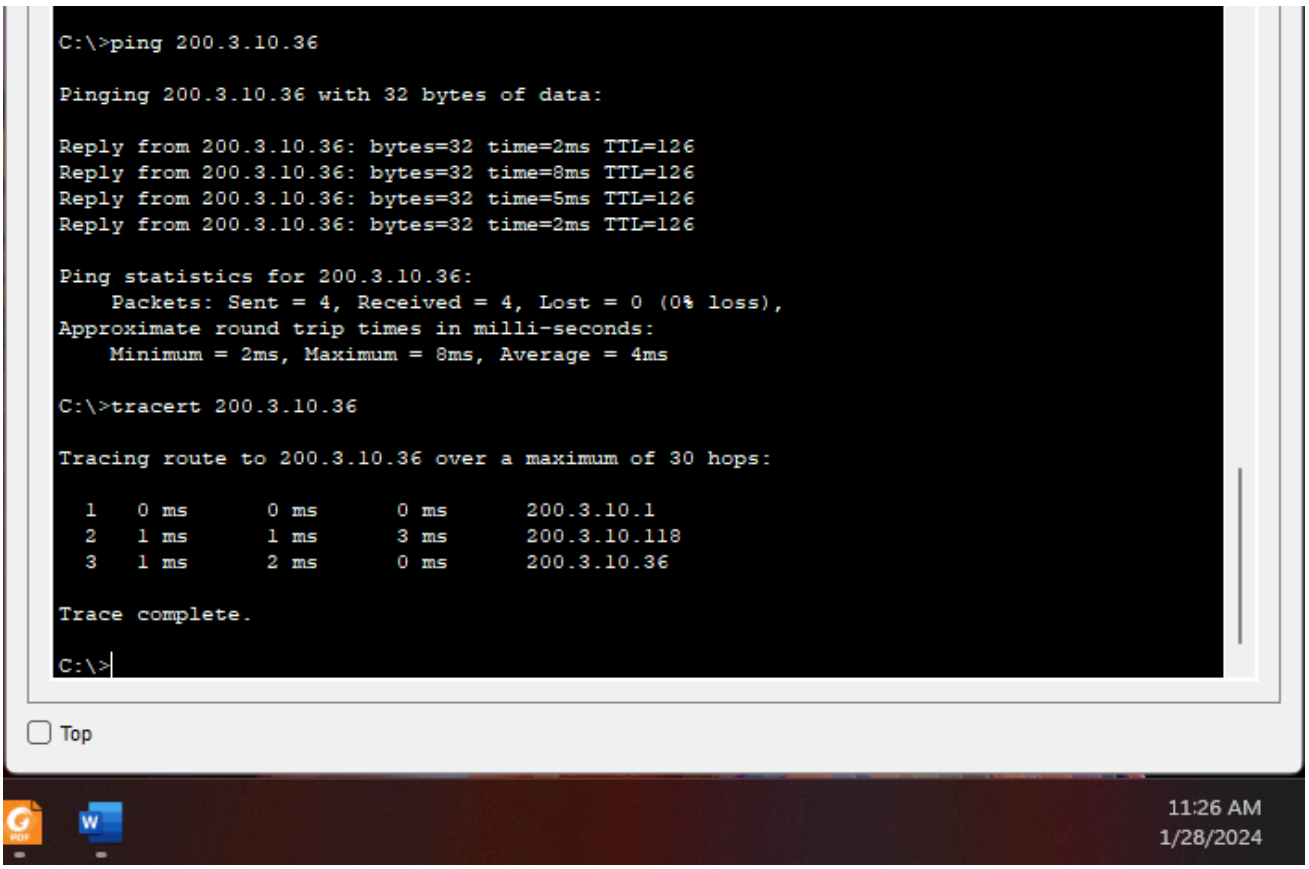
Ping Command:

The ping command is used to test the connectivity to the IP address 200.3.10.35. The output indicates that the destination is reachable, with all four packets sent having been received, resulting in 0% loss.
The round-trip times (the time for a signal to go to the destination and back) vary from 1ms to 9ms, which is still very low, suggesting that the destination is not far from the source, likely within the same local network.
The Time to Live (TTL) values are 126 and 128, suggesting that the destination is a few hops away since the TTL value has decreased slightly from the default (usually 128 or 255), indicating the packets have passed through a couple of routers.

Tracert Command:

The tracert command shows the route that packets take to reach the IP address 200.3.10.35. In this case, there are three hops. The first hop is to 200.3.10.1, the second to 200.3.10.118, and the final hop is to the destination 200.3.10.35.
The times next to each hop indicate how long it took for the response from each hop. The first hop was immediate (0 ms), the second took a total of 7 ms (1 ms for the first response, 3 ms for the second, and 3 ms for the third), and the final hop to the destination had no delay (0 ms).

⇒ ping and tracert result From PC 2_1 To PC 3_2



Ping Command:

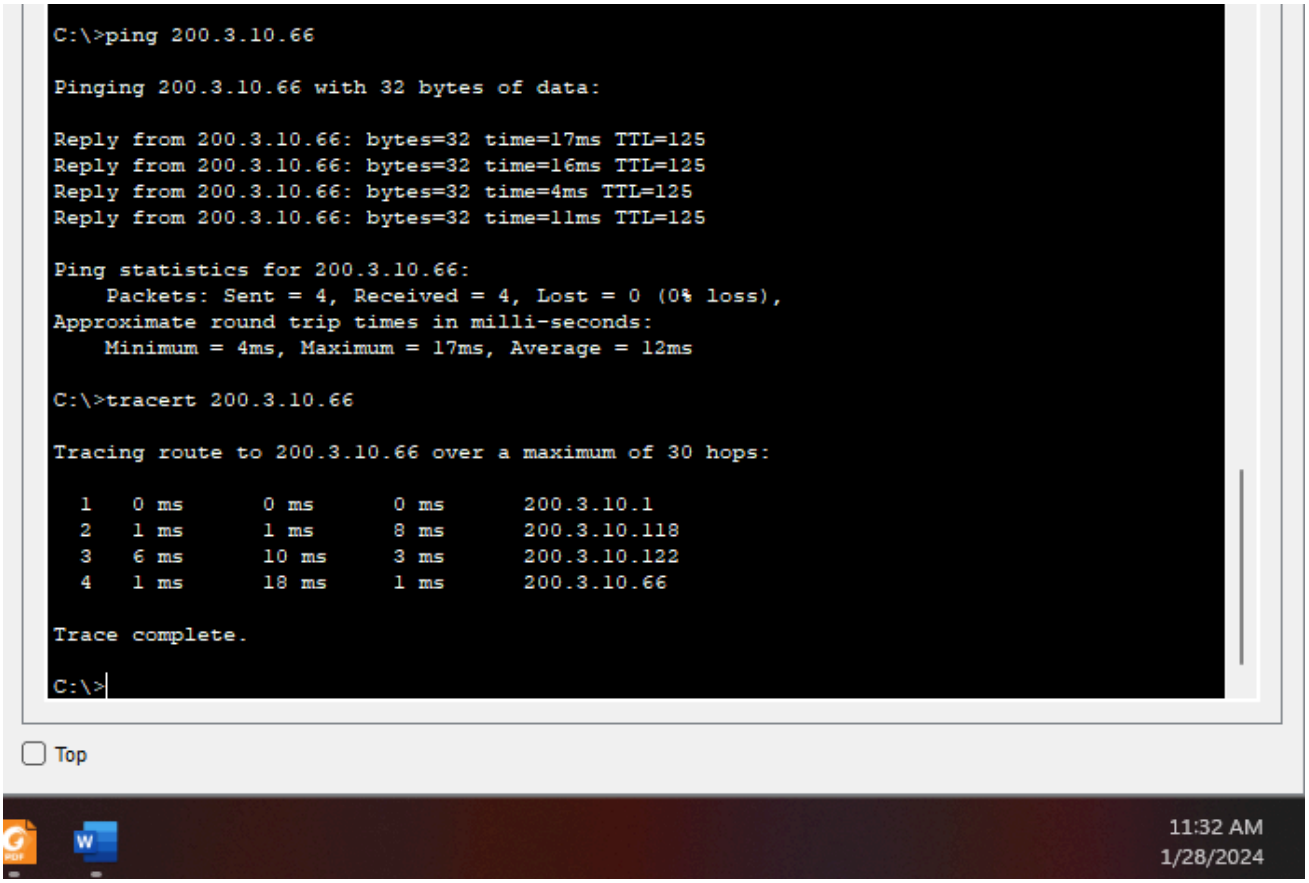
The ping command is used to check the reachability of the IP address 200.3.10.36. It shows that all packets sent were received back, indicating no packet loss and a stable network connection to the target IP.
The round-trip times, which indicate latency, range from 2ms to 8ms. These are relatively low, suggesting that the destination is geographically close or has a good connection to the host.
The Time to Live (TTL) value is 126, which means the data packets can be forwarded by up to 126 more network devices before the packet is discarded. A high TTL value typically indicates that the destination is not many hops away.

Tracert Command:

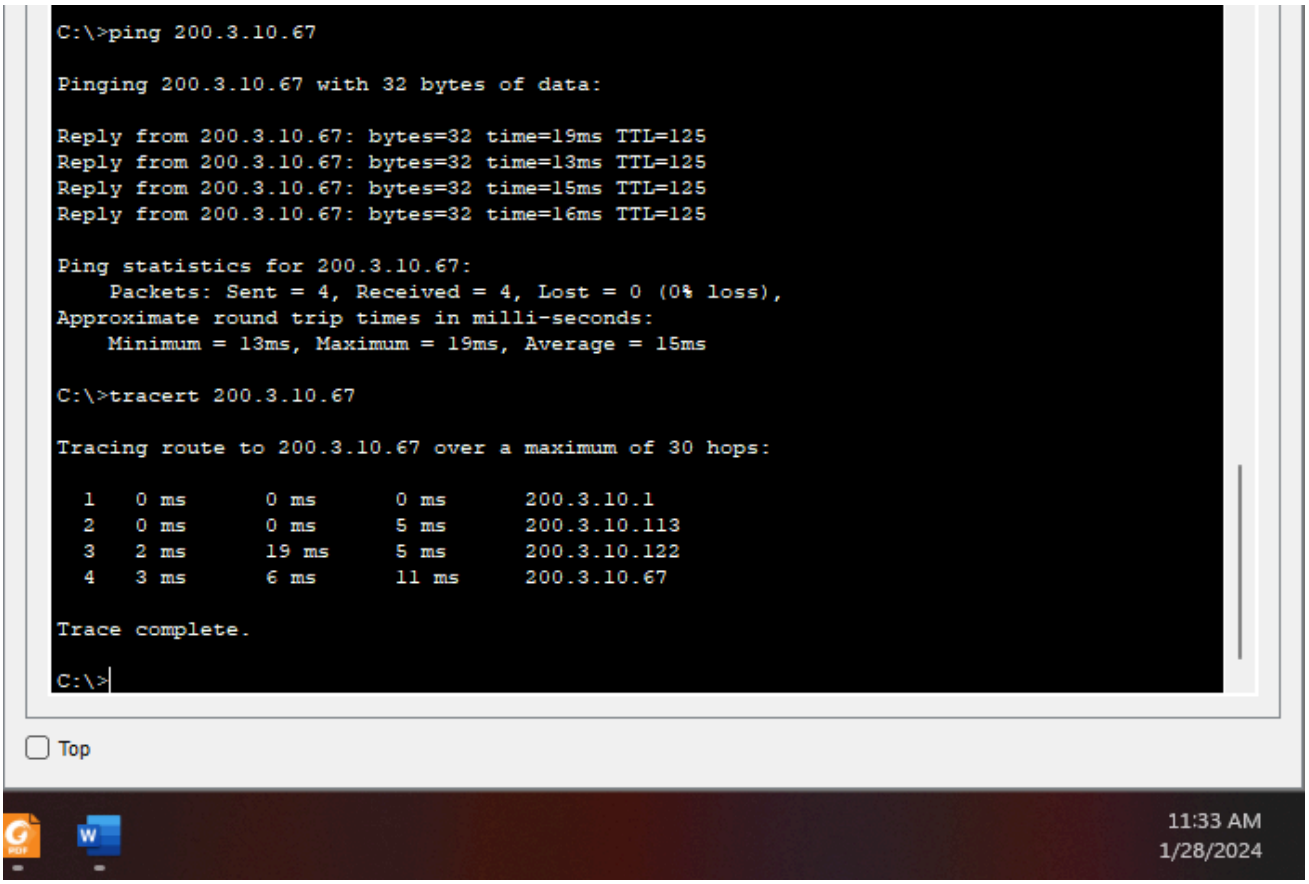
The tracert (or traceroute) command is showing the path that data packets take to reach the destination IP address 200.3.10.36. The trace is short, which typically indicates a network with few routers or switches between the source and destination.
The first hop to 200.3.10.1 is immediate (0 ms), which might be the network's default gateway or a switch.
The second hop to 200.3.10.118 has a delay of 3ms, indicating an intermediate device on the network.
The final hop to the destination IP, 200.3.10.36, has a minimal delay of 1-2ms.

Note: All the following images are in the same style, and we will suffice with the explanation above.

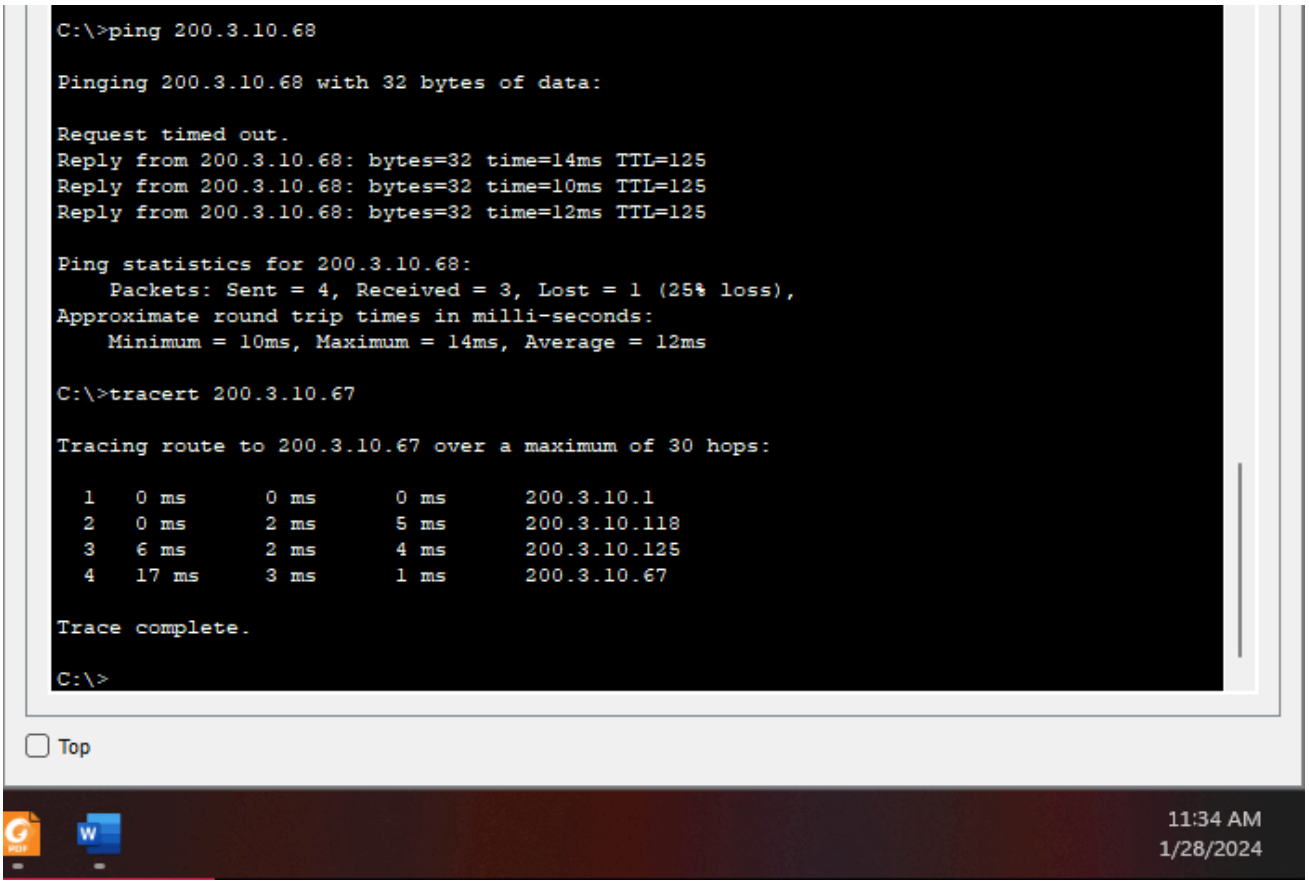
⇒ ping and tracert result From PC 2_1 To PC 41_1 :



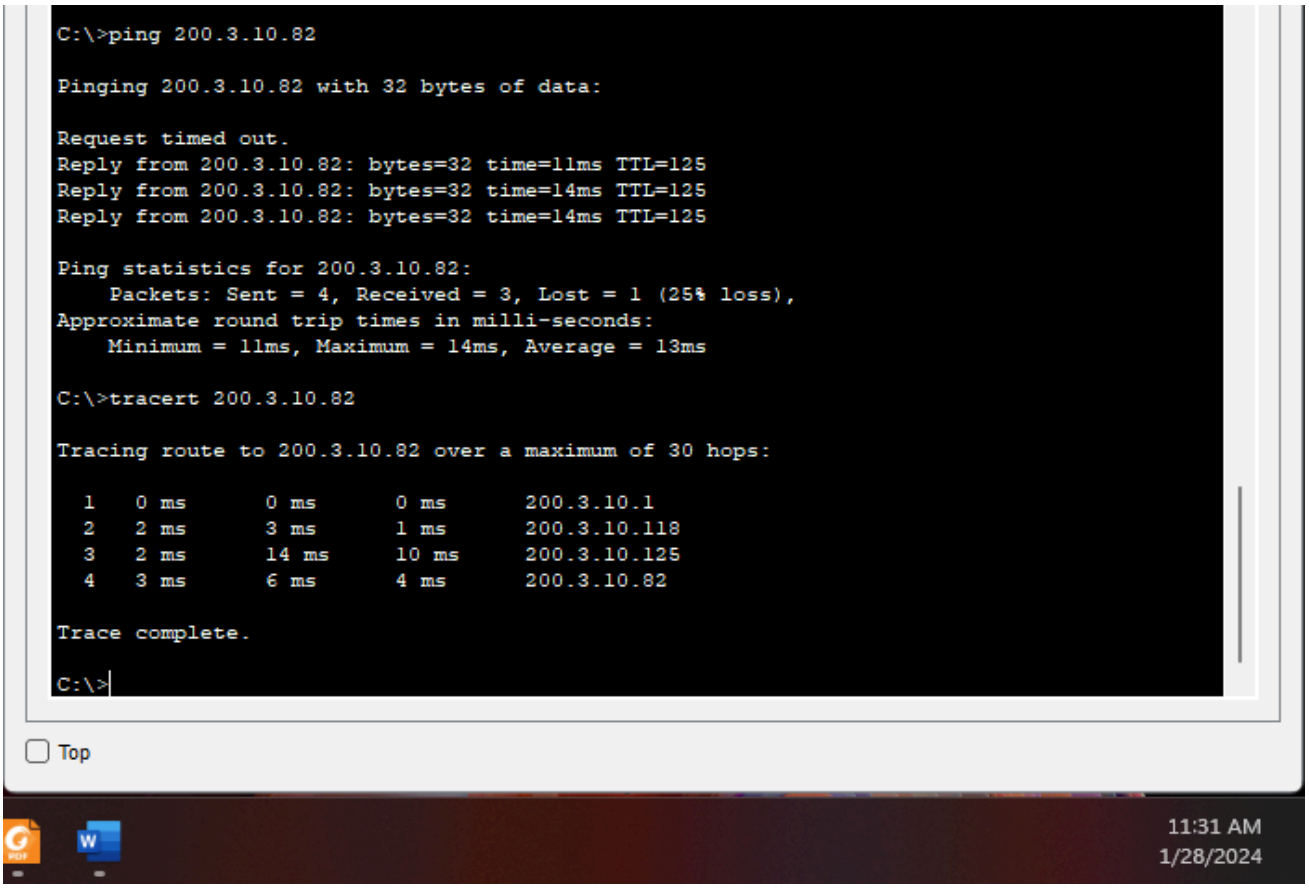
⇒ping and tracert result From PC 2_1 To PC 41_2:



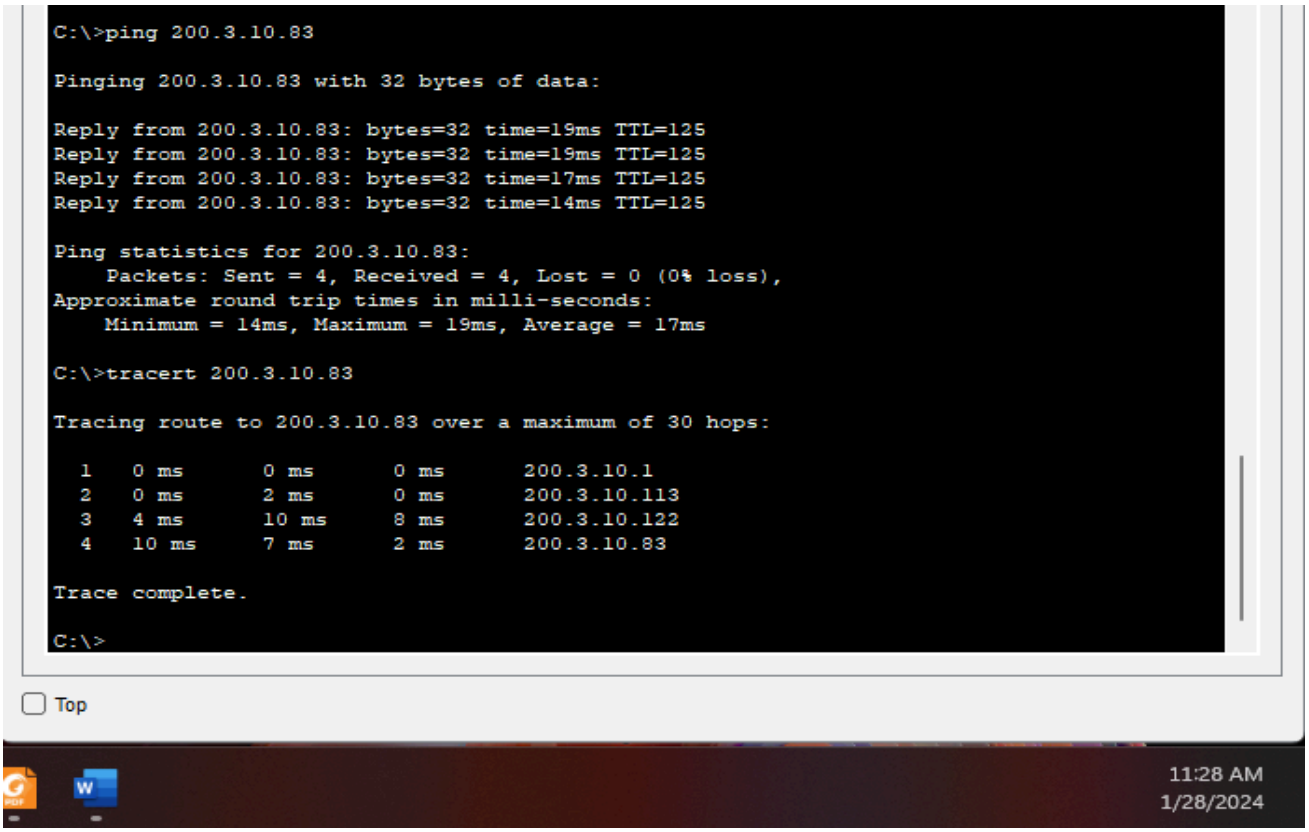
⇒ ping and tracert result From PC 2_1 To PC 41_3



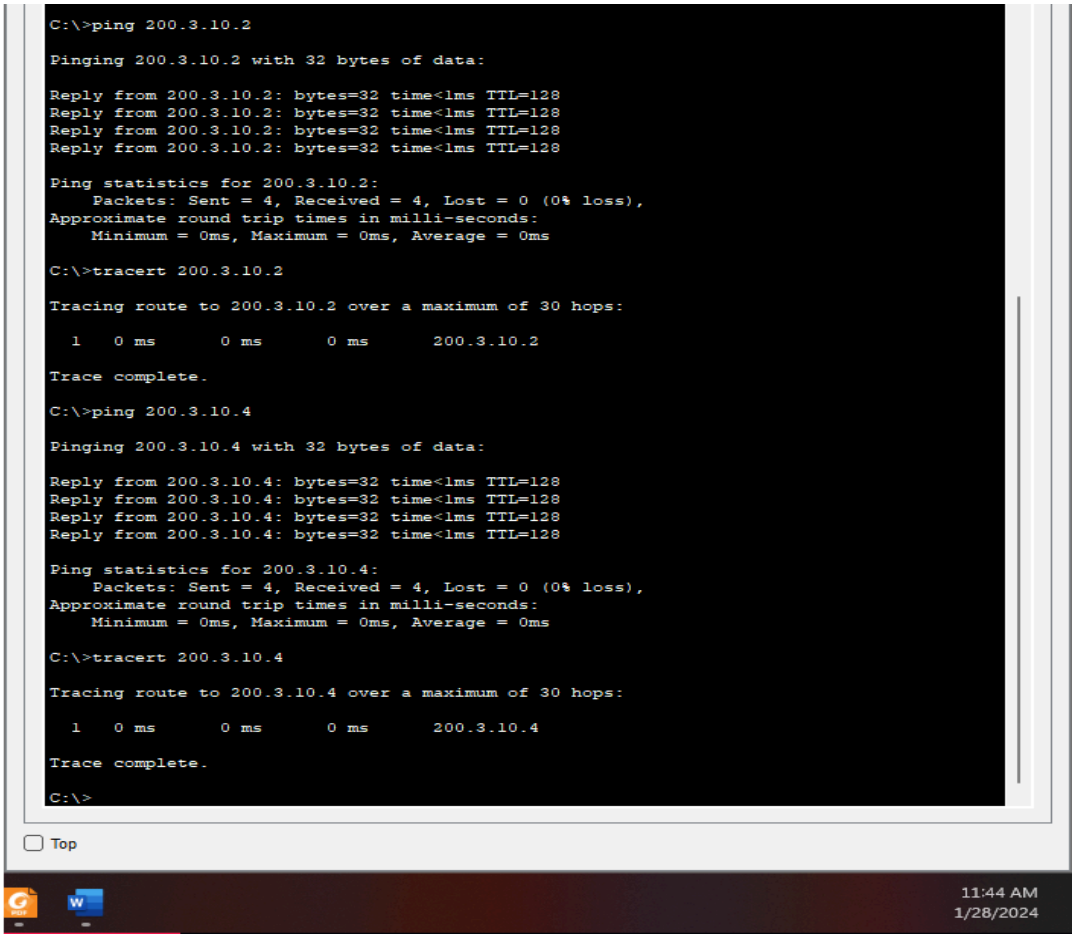
ping and tracert result From PC ⇒2_1 to PC 42_1 :



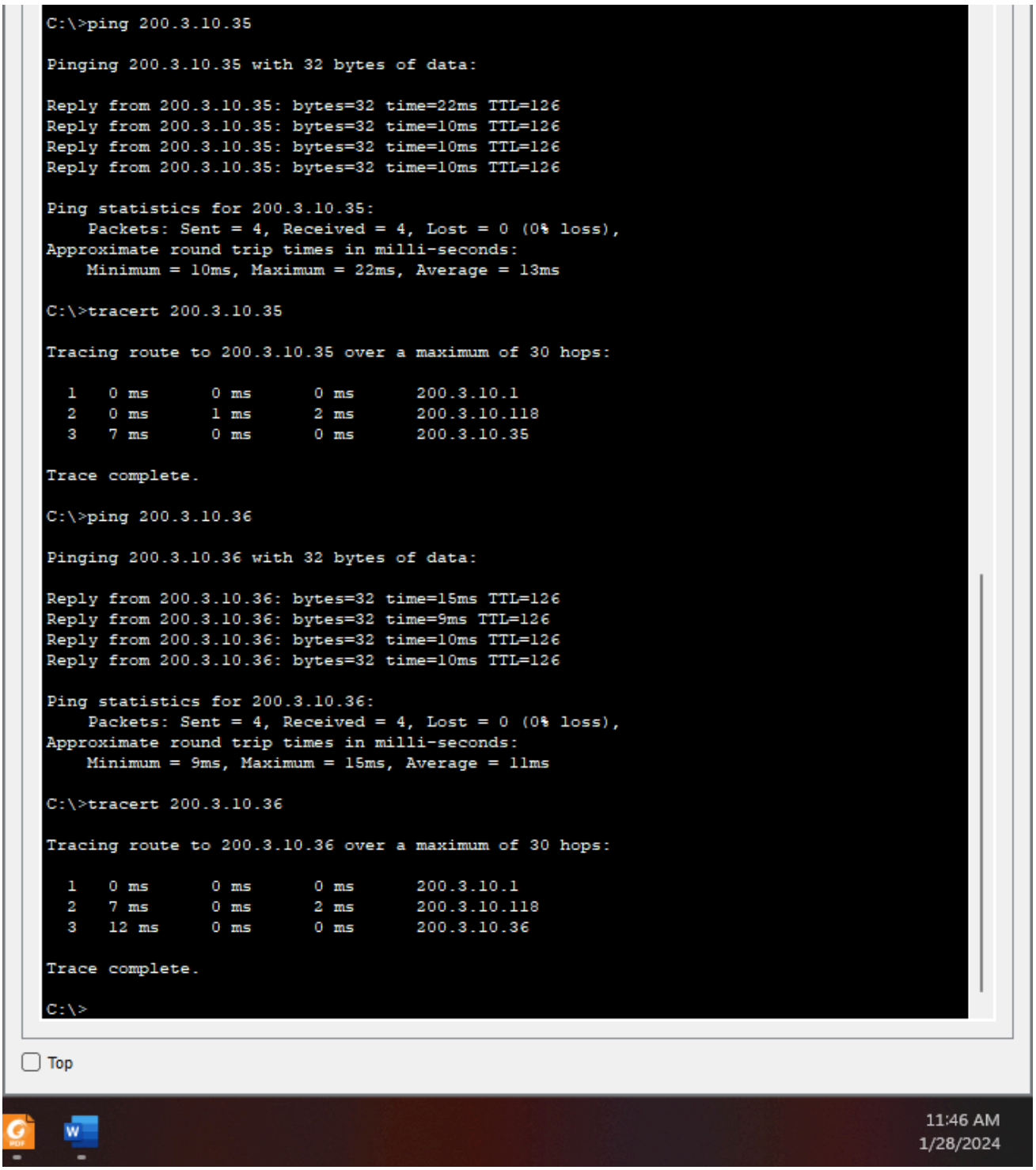
⇒ping and tracert result From PC 2_1 to PC 42_2 :



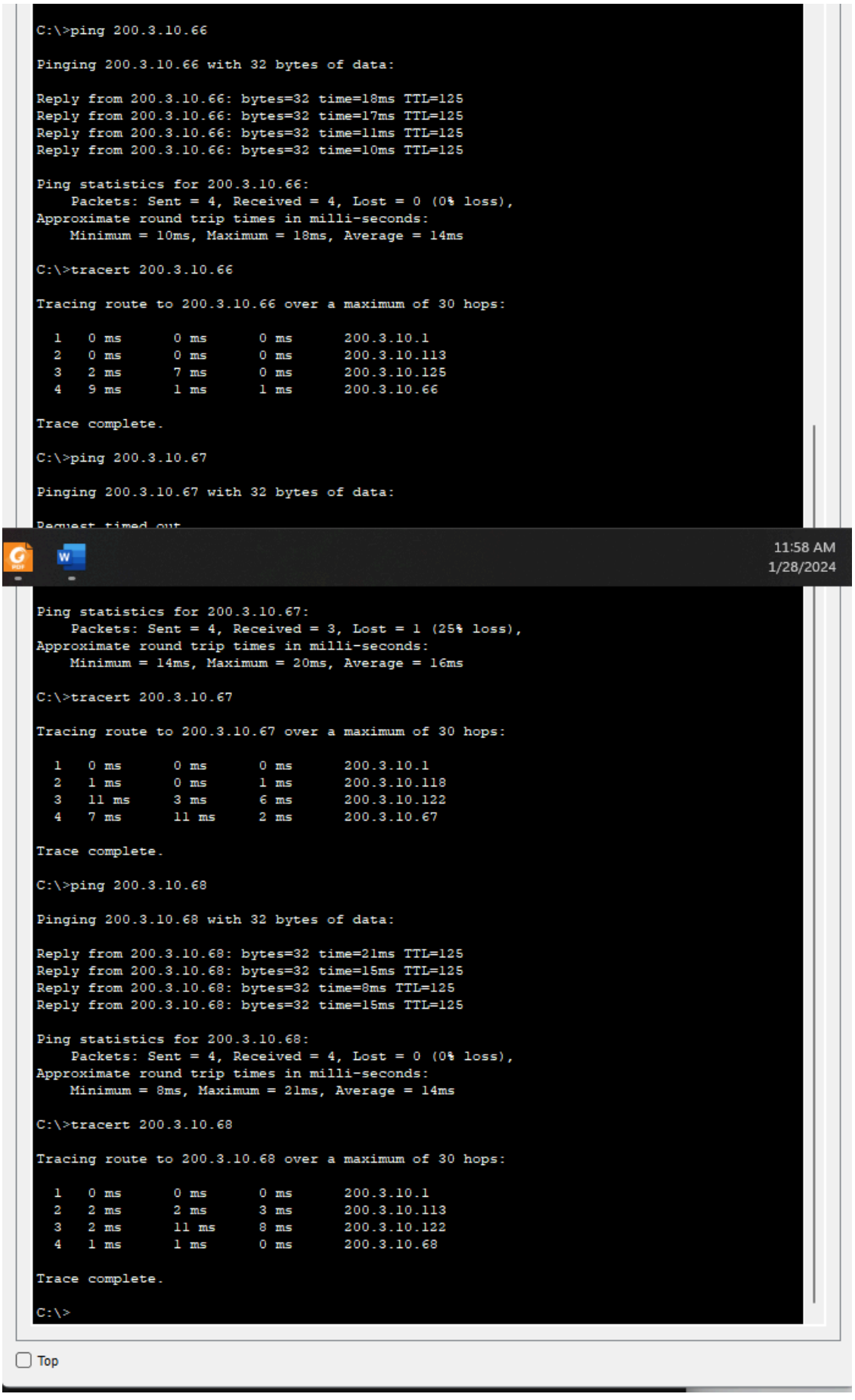
⇒ping and tracert result From PC 2_2 to PC 2_1+2_3:



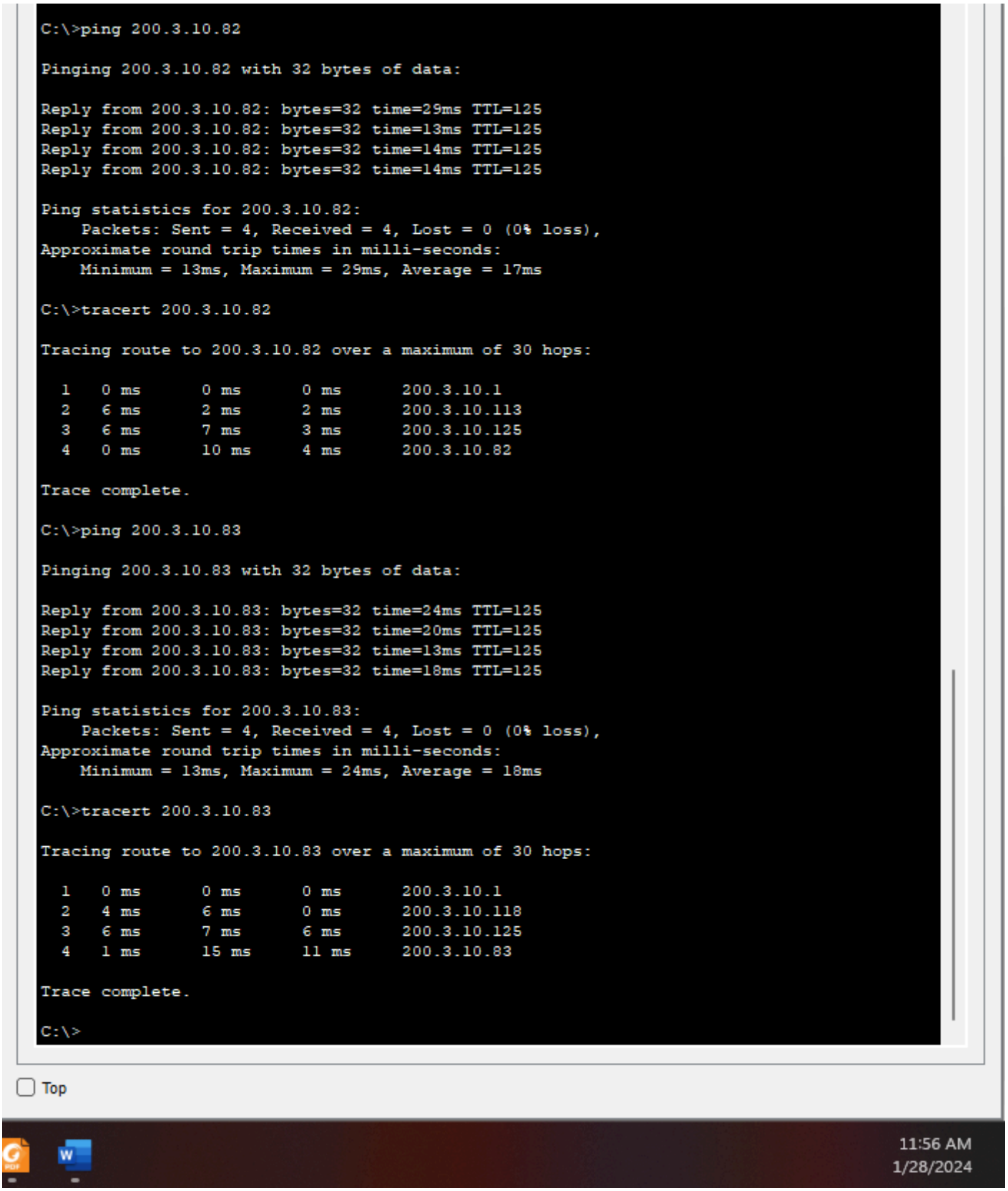
⇒ping and tracert result From PC 2_2 to PC 3_1+3_2:



⇒ping and tracert result From PC 2_2 to PC 41_1+41_2+41_3:

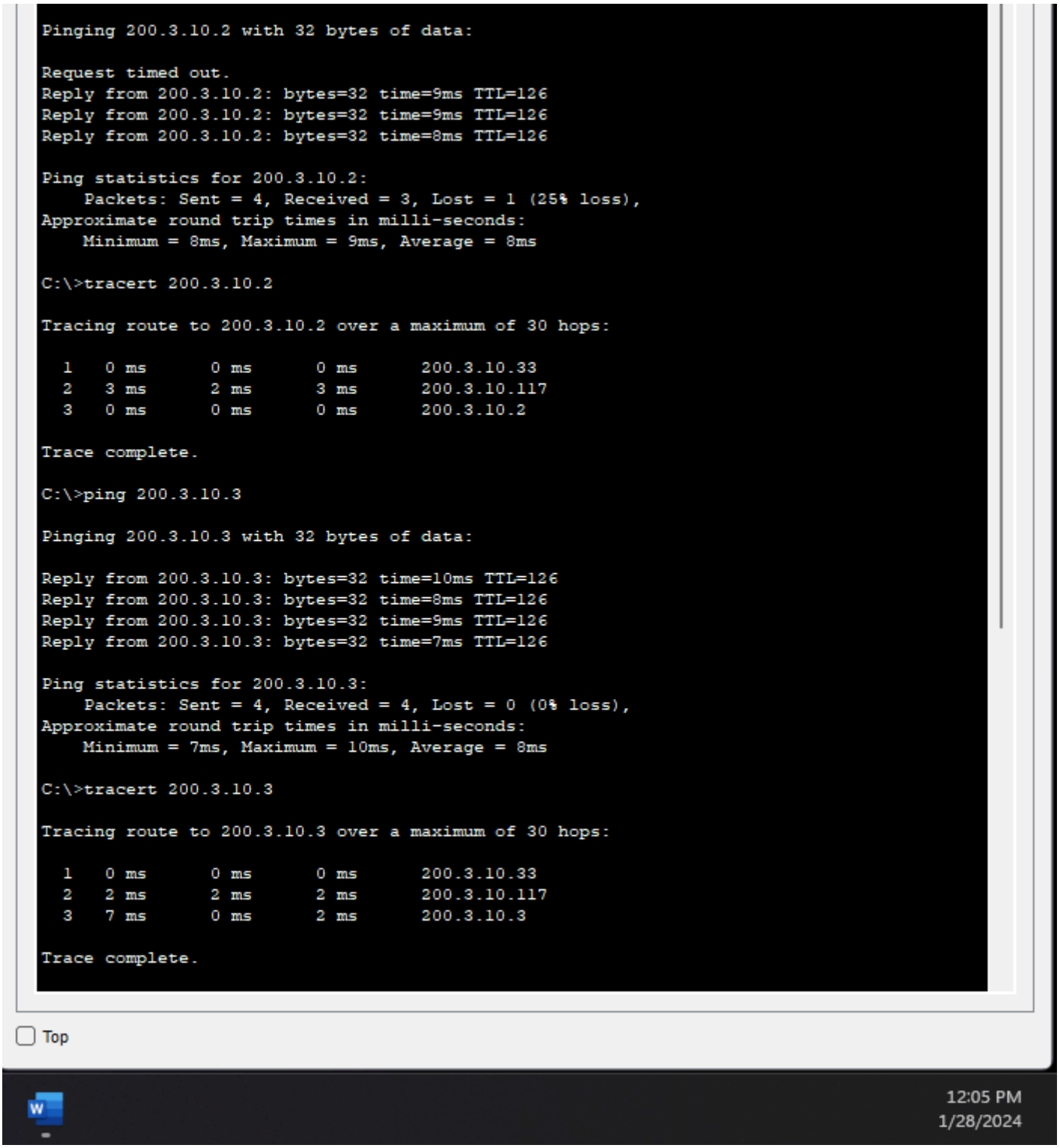


⇒ping and tracert result From PC 2_2 to PC 42_1+42_2:

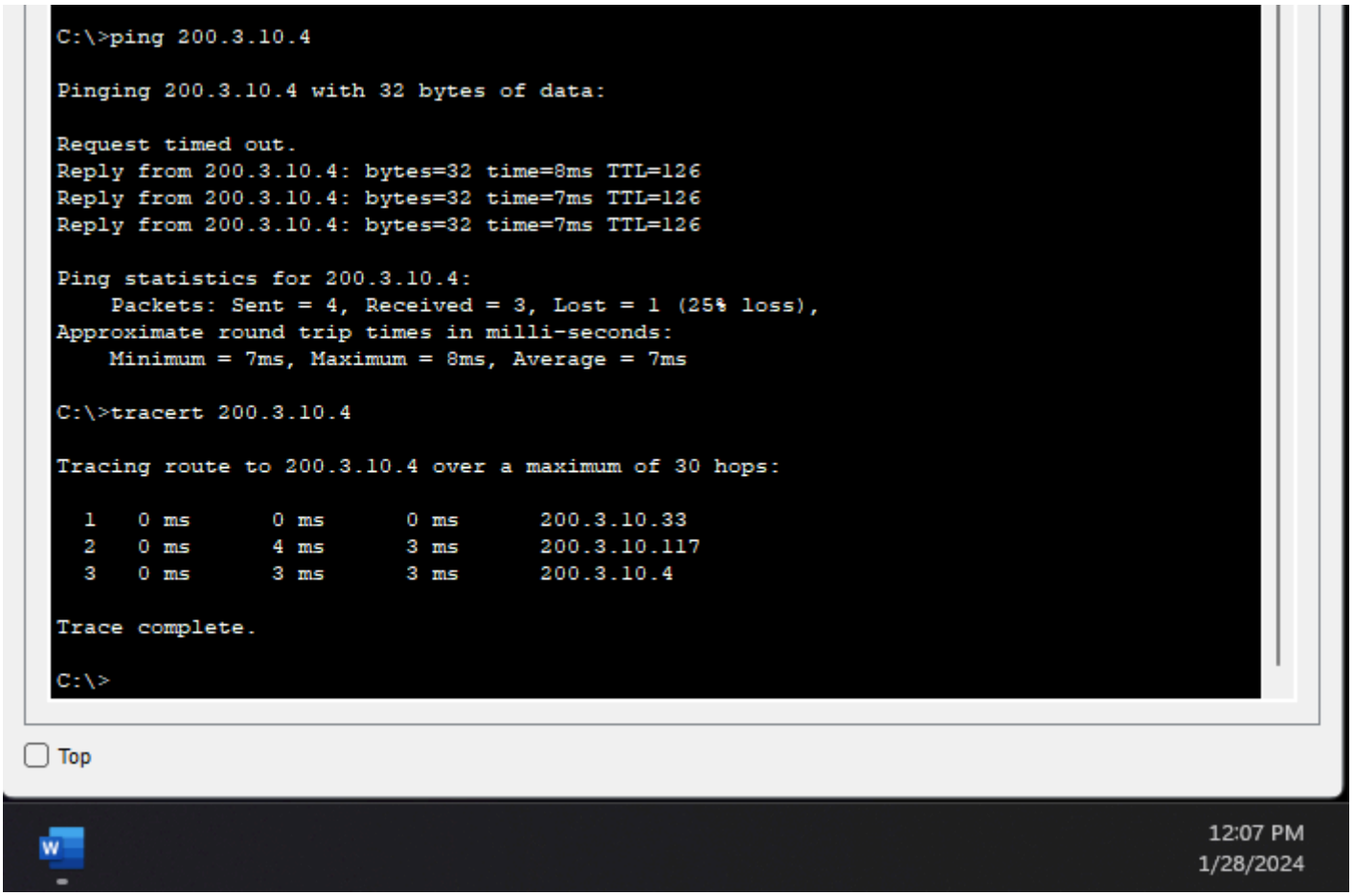


Company B:

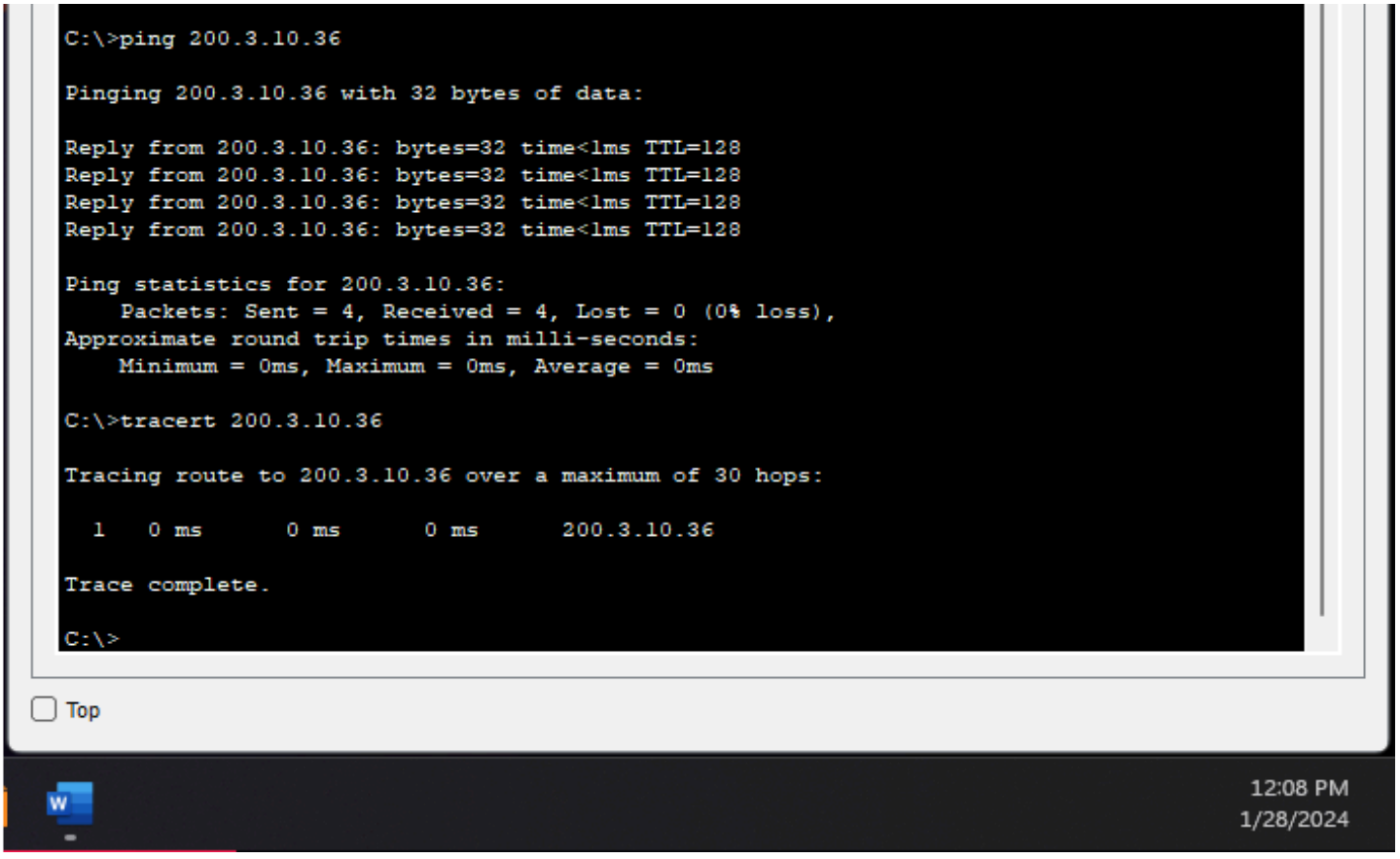
⇒ping and tracert result From PC 3_1 to PC 2_1+2_2:



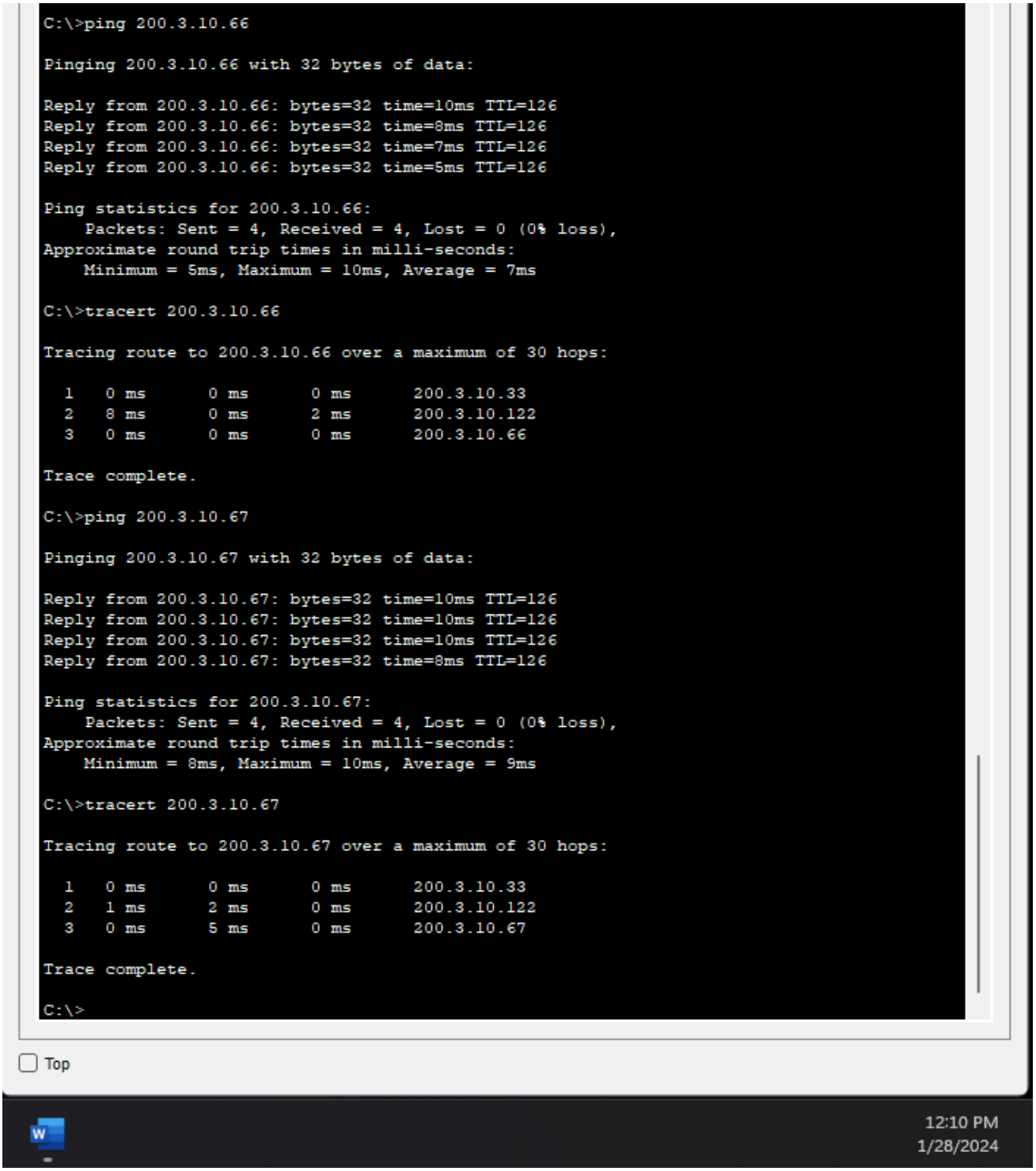
⇒ping and tracert result From PC 3_1 to PC 2_3:



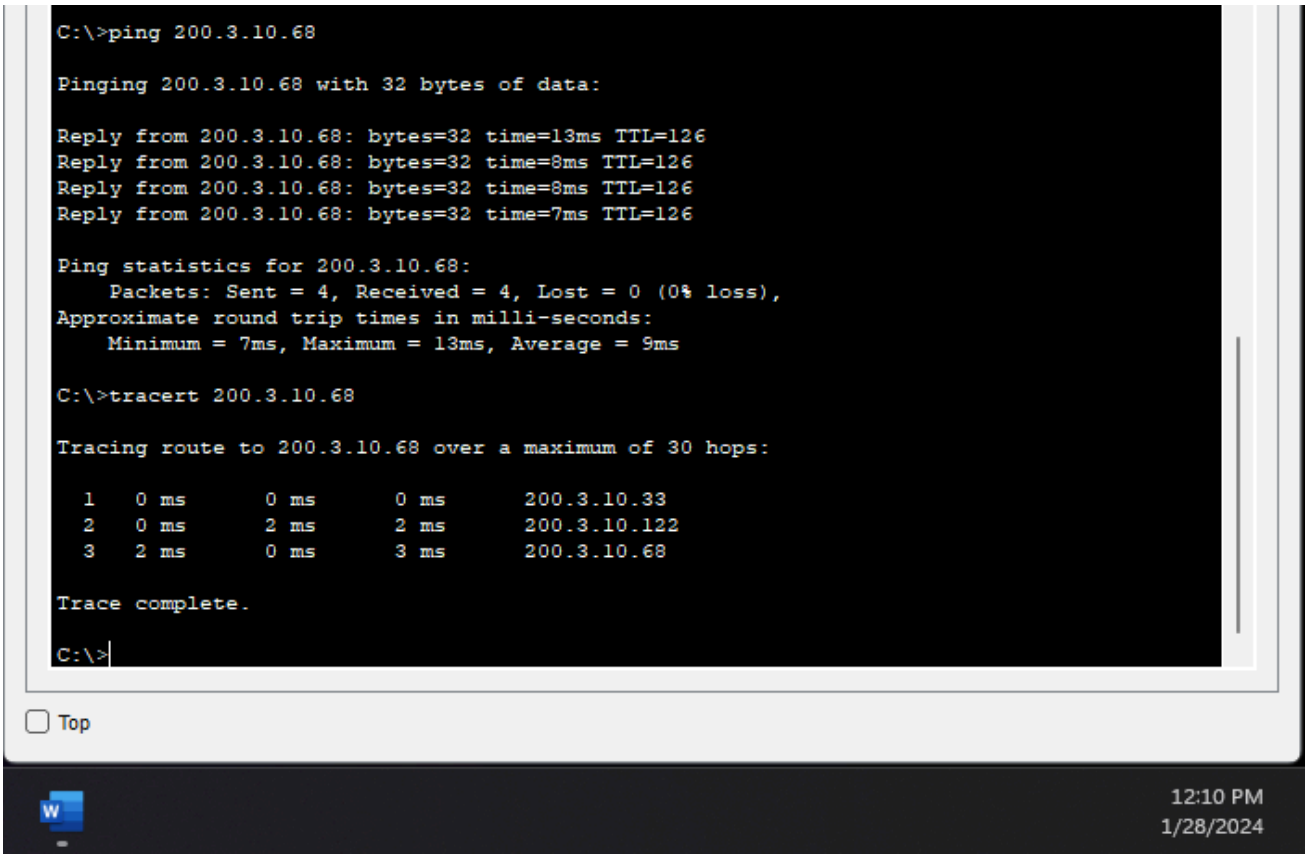
⇒ping and tracert result From PC 3_1 to PC 3_2



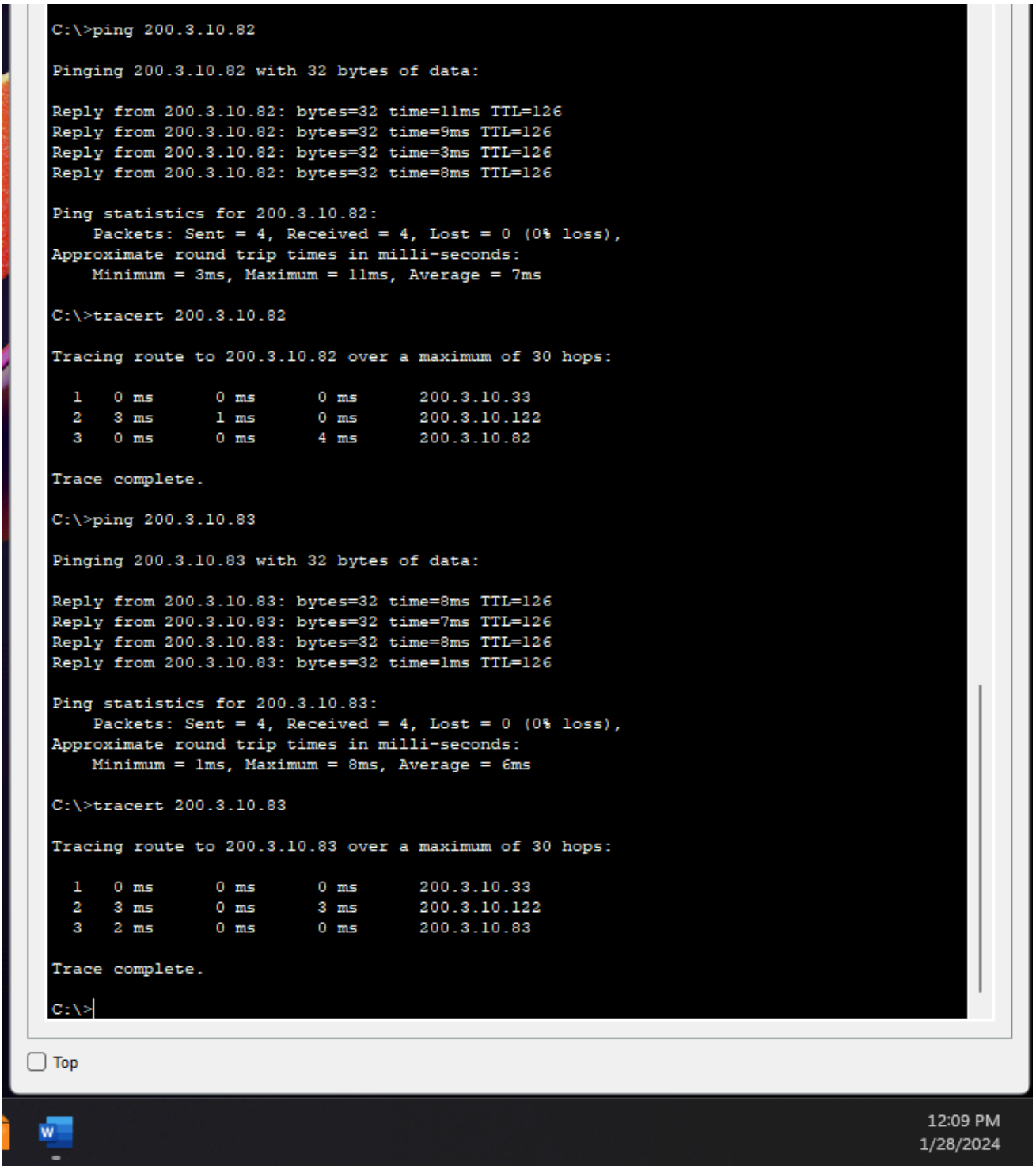
⇒ping and tracert result From PC 3_1 to PC 41_1+41_2:



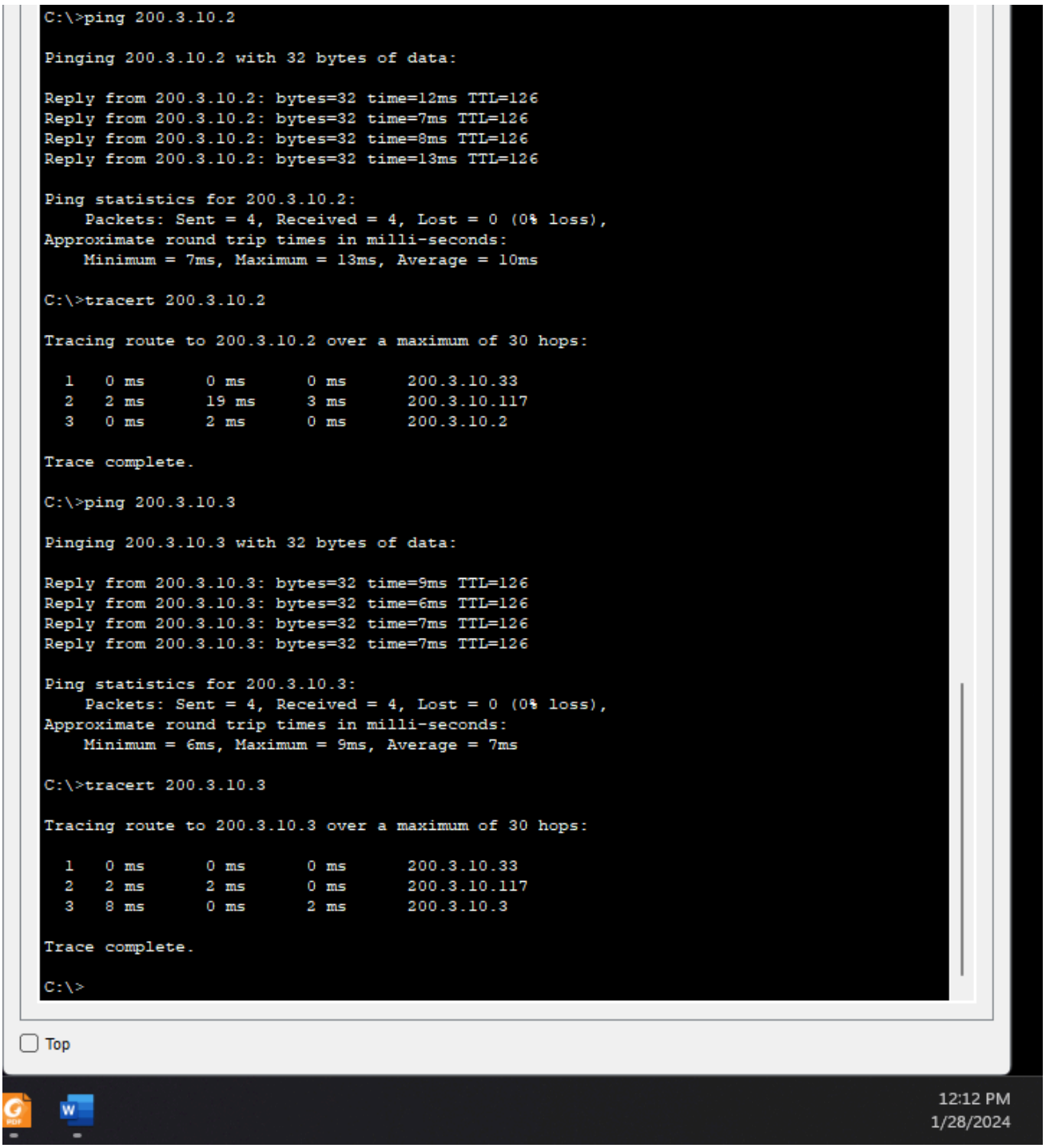
⇒ping and tracert result From PC 3_1 to PC 41_3:



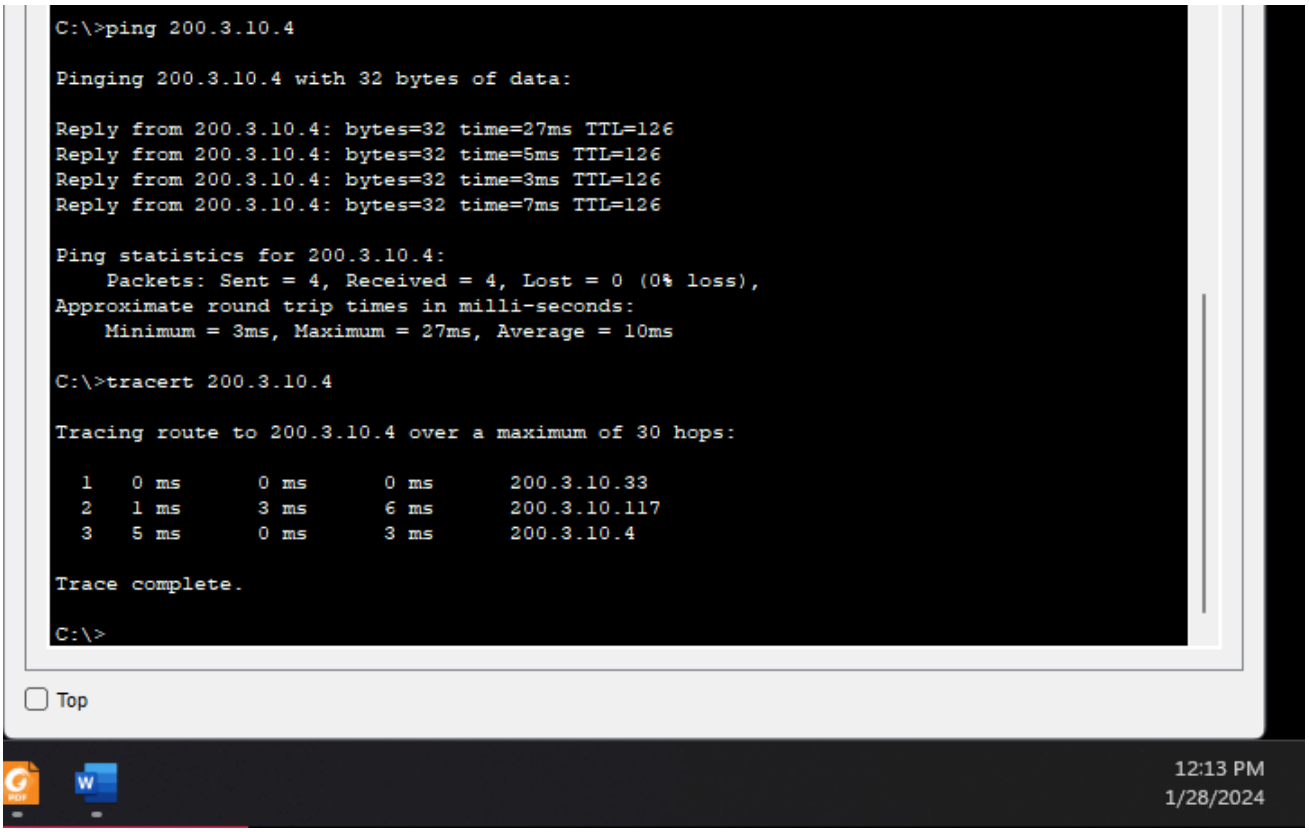
⇒ping and tracert result From PC 3_1 to PC 42_1 +42_2:



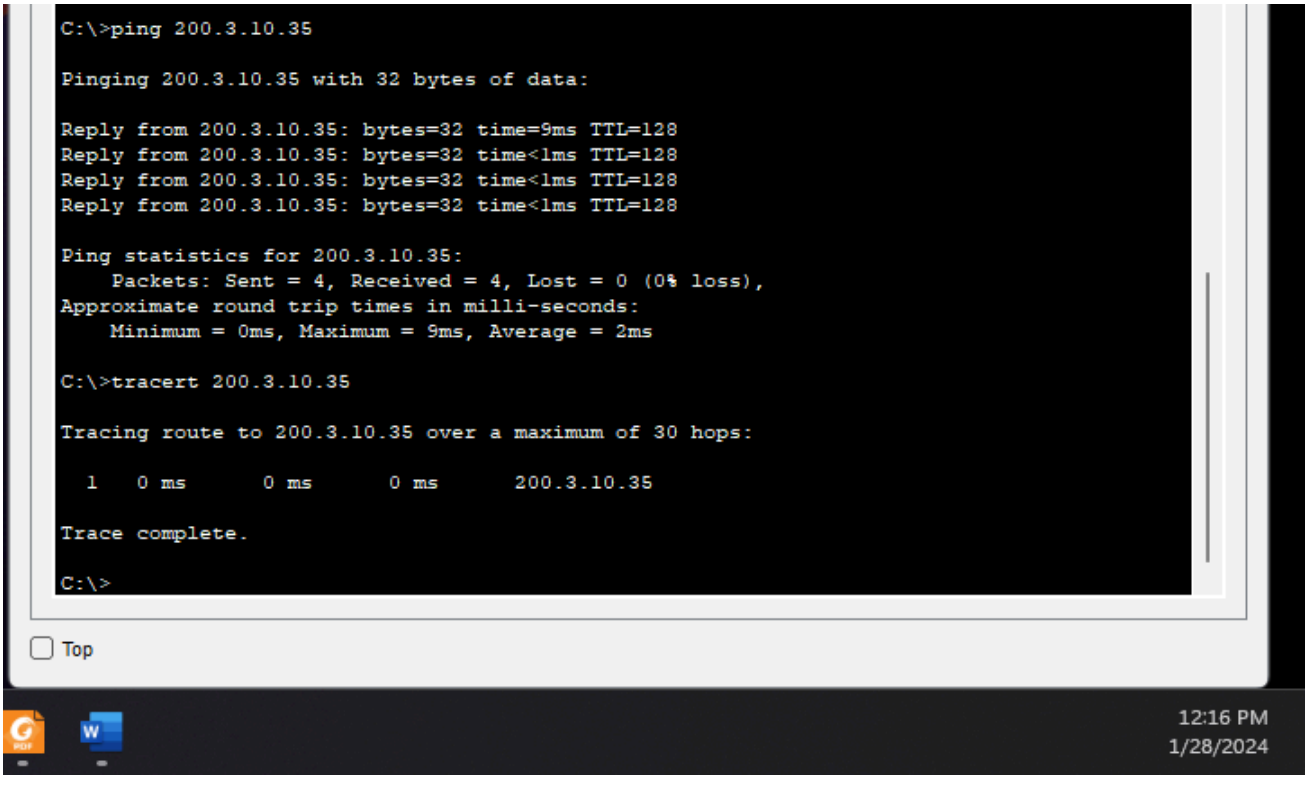
⇒ping and tracert result From PC 3_2 to PC 2_1+2_2:



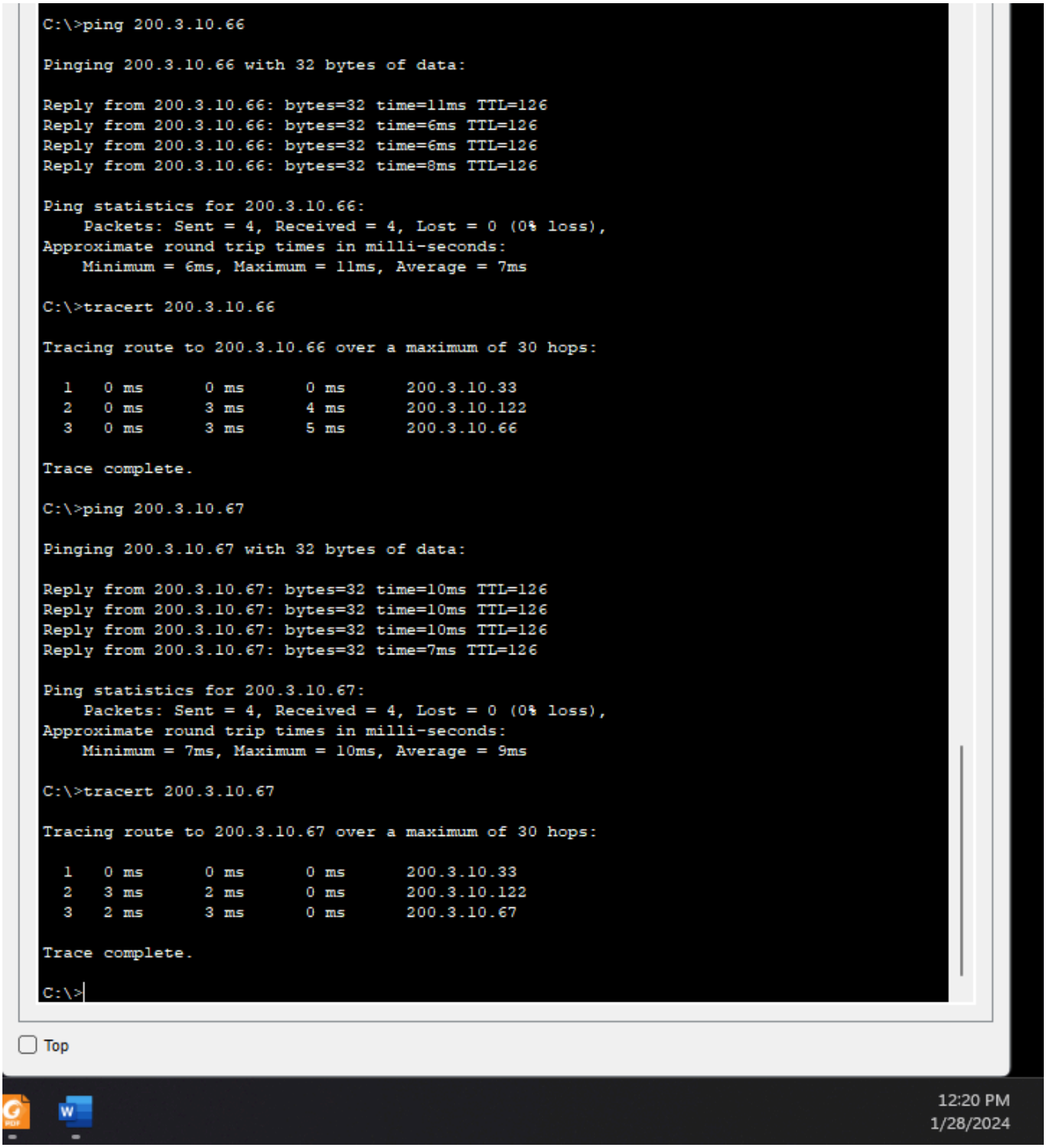
⇒ping and tracert result From PC 3_2 to PC 2_3:



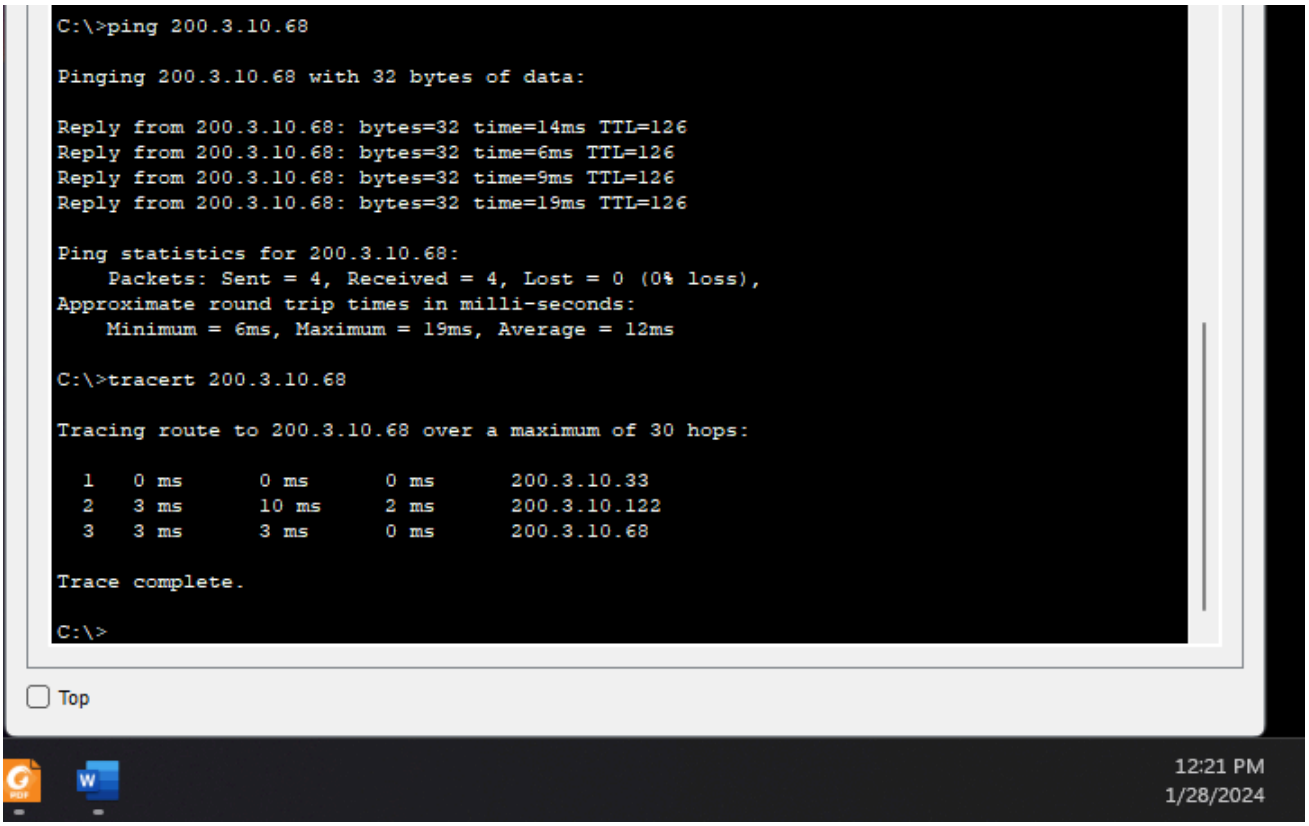
⇒ping and tracert result From PC 3_2 to PC 3_1 :



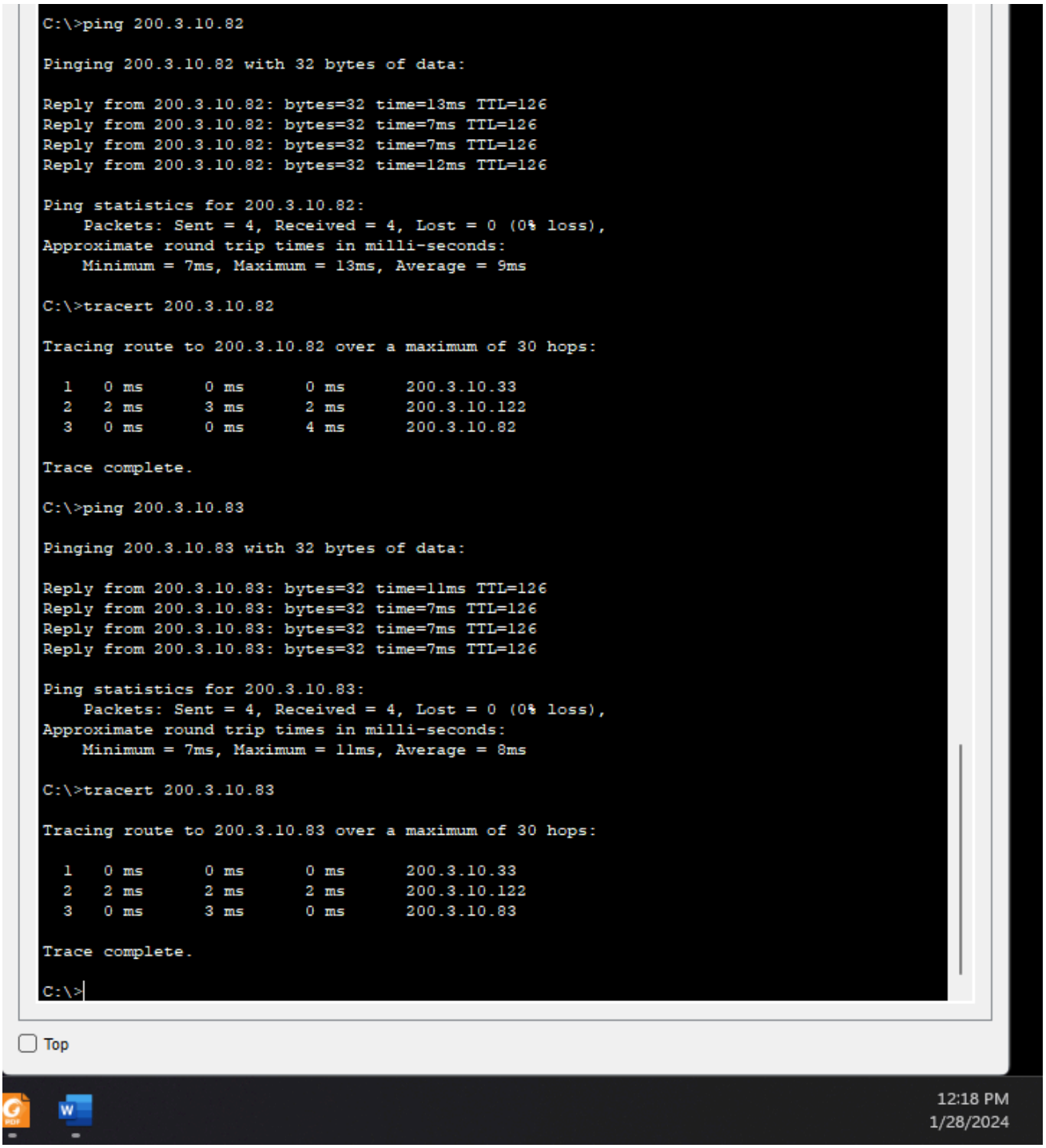
⇒ping and tracert result From PC 3_2 to PC 41_1 +41_2:



⇒ping and tracert result From PC 3_2 to PC 41_3:

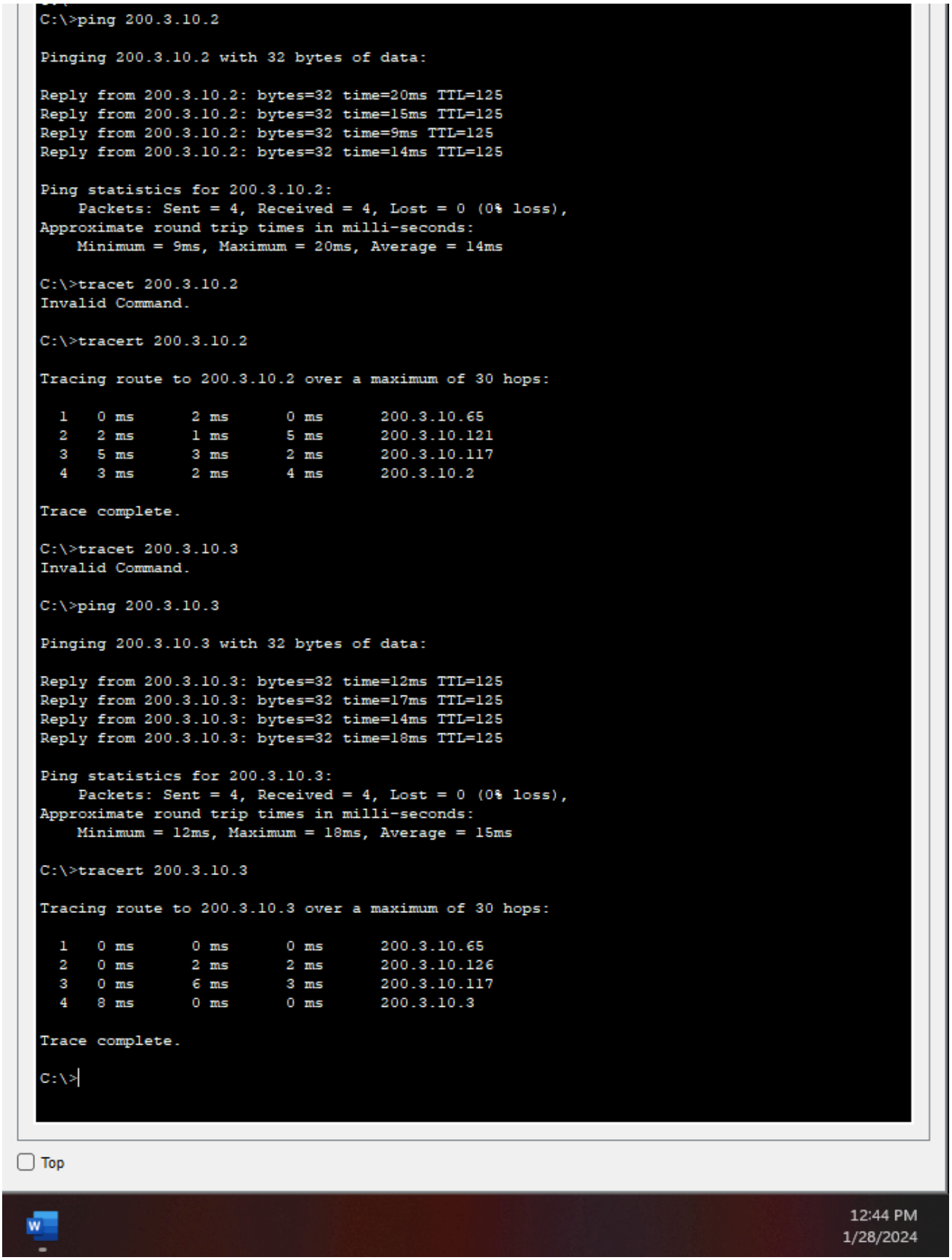


⇒ping and tracert result From PC 3_2 to PC 42_1+42_2:

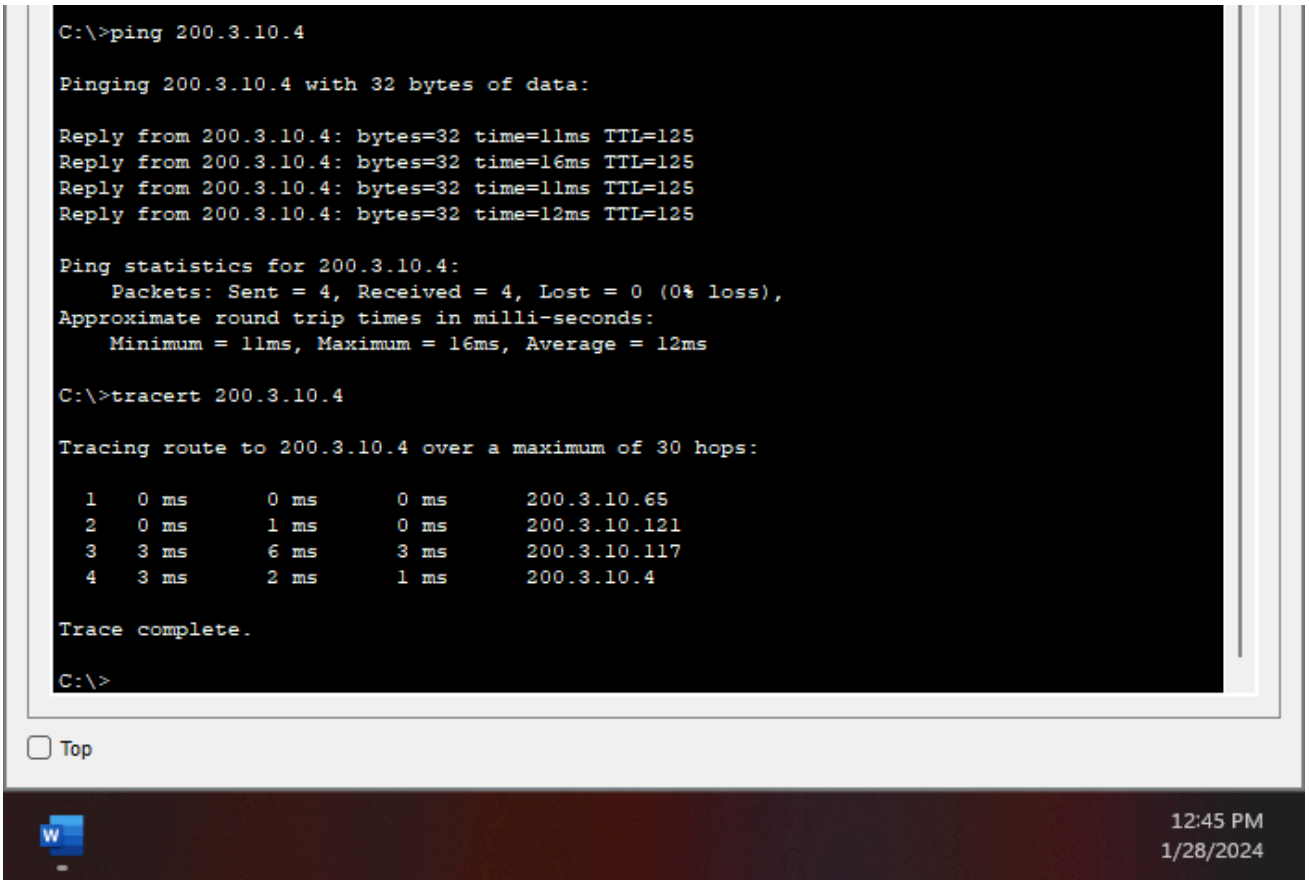


company c office one:

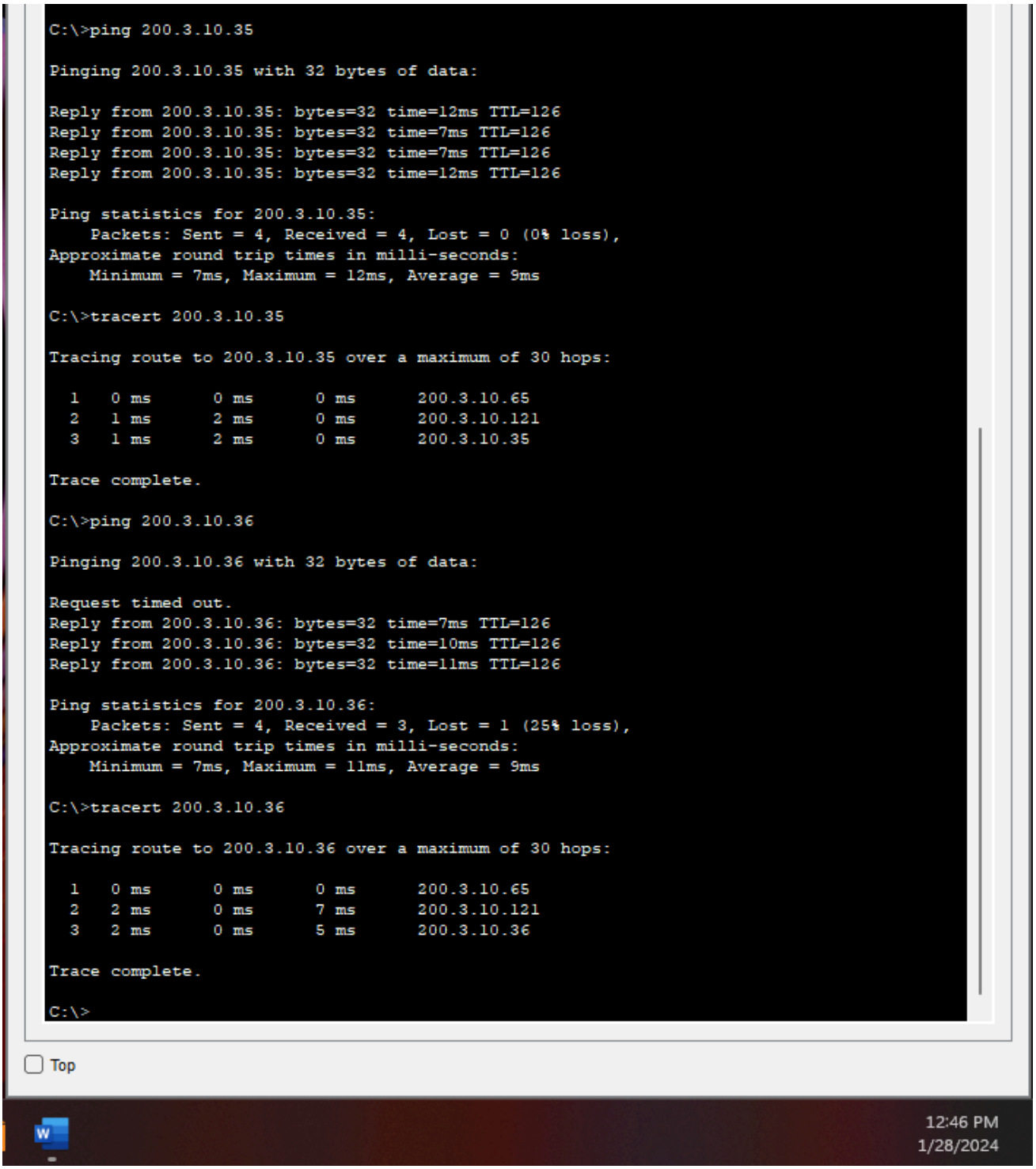
⇒ping and tracert result From PC 41_1 to PC 2_1+2_2:



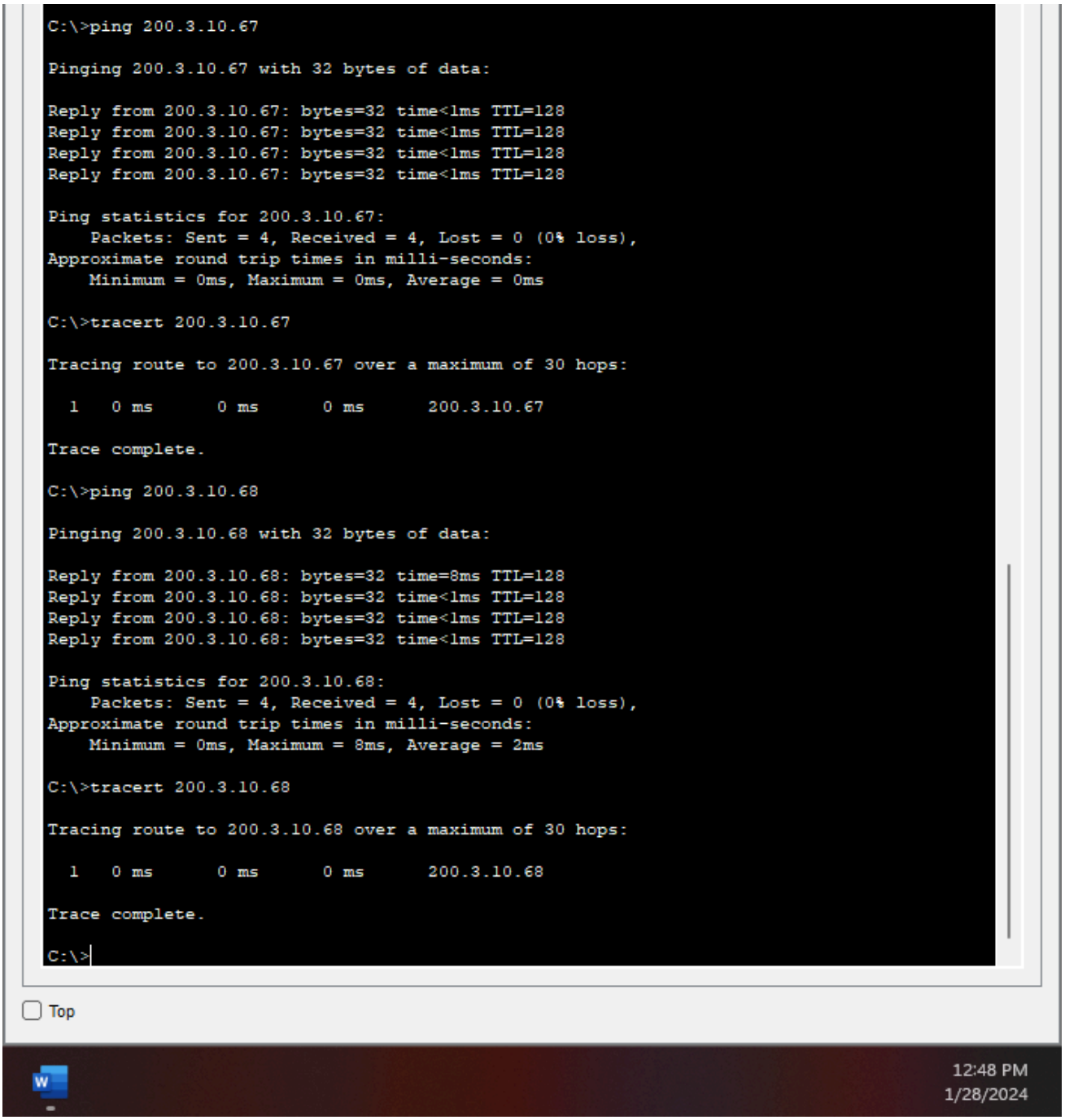
⇒ping and tracert result From PC 41_1 to PC 2_3:



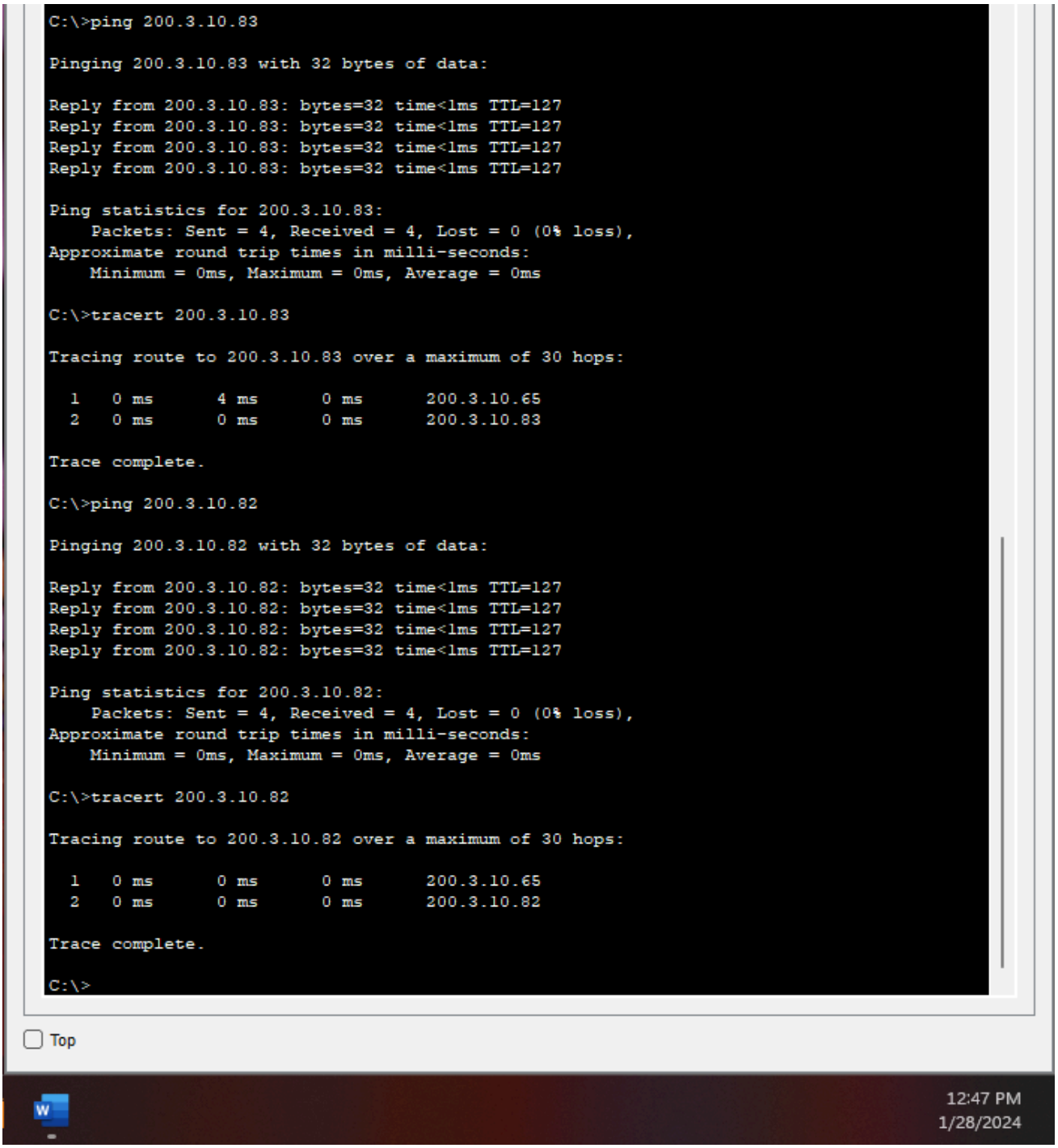
⇒ping and tracert result From PC 41_1 to PC 3_1 +3_2:



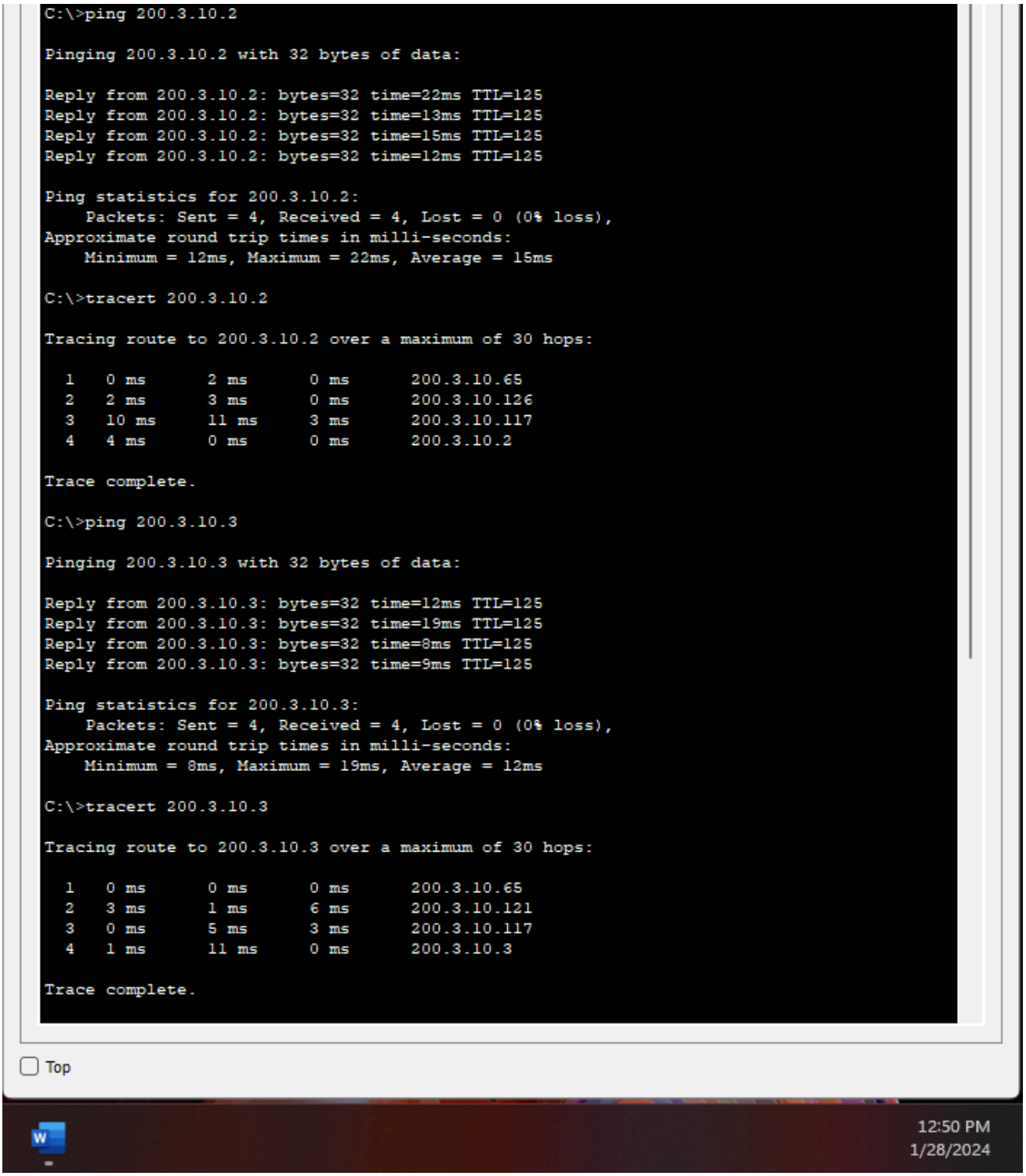
⇒ping and tracert result From PC 41_1 to PC 41_1 +41_2:



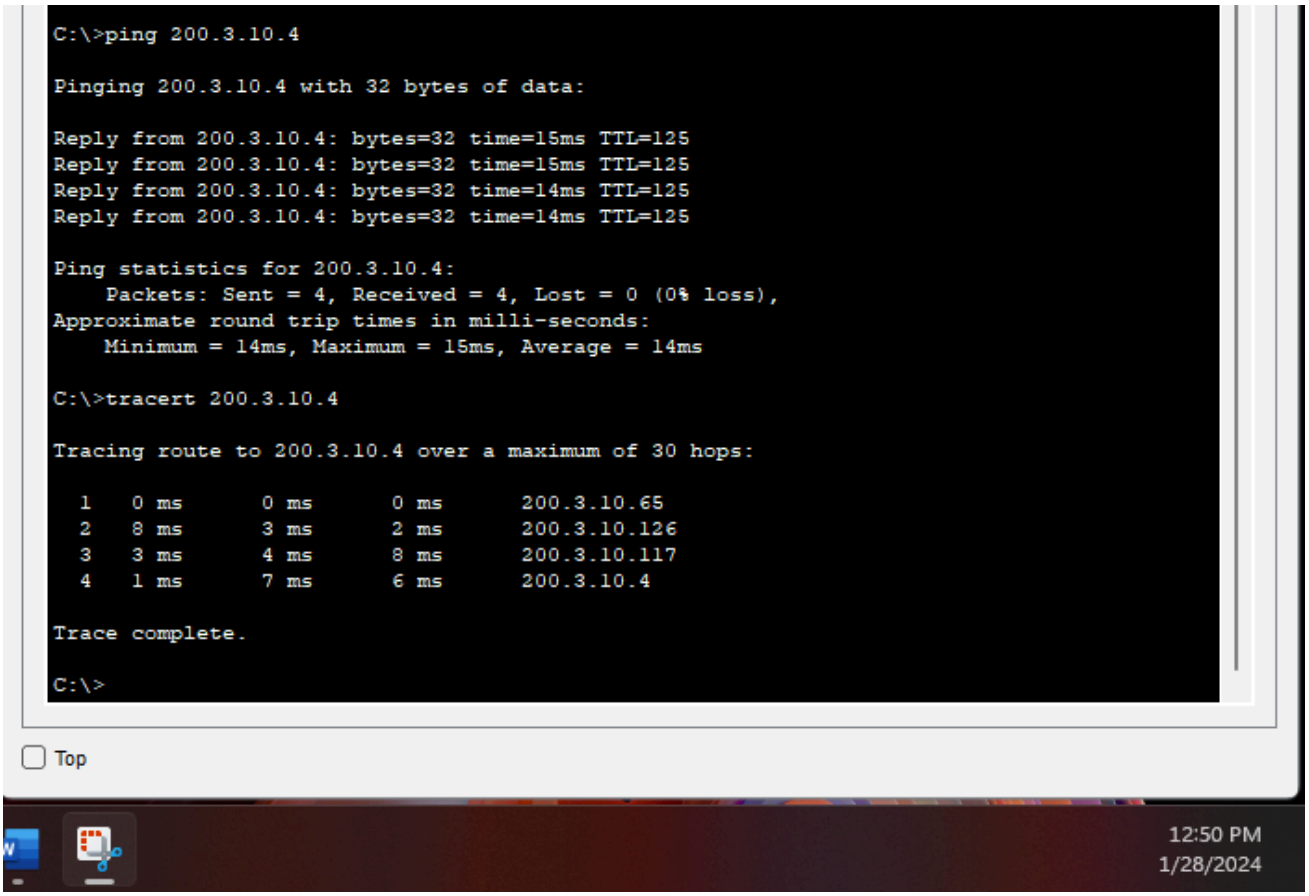
⇒ping and tracert result From PC 41_1 to PC 42_1 +42_2 :



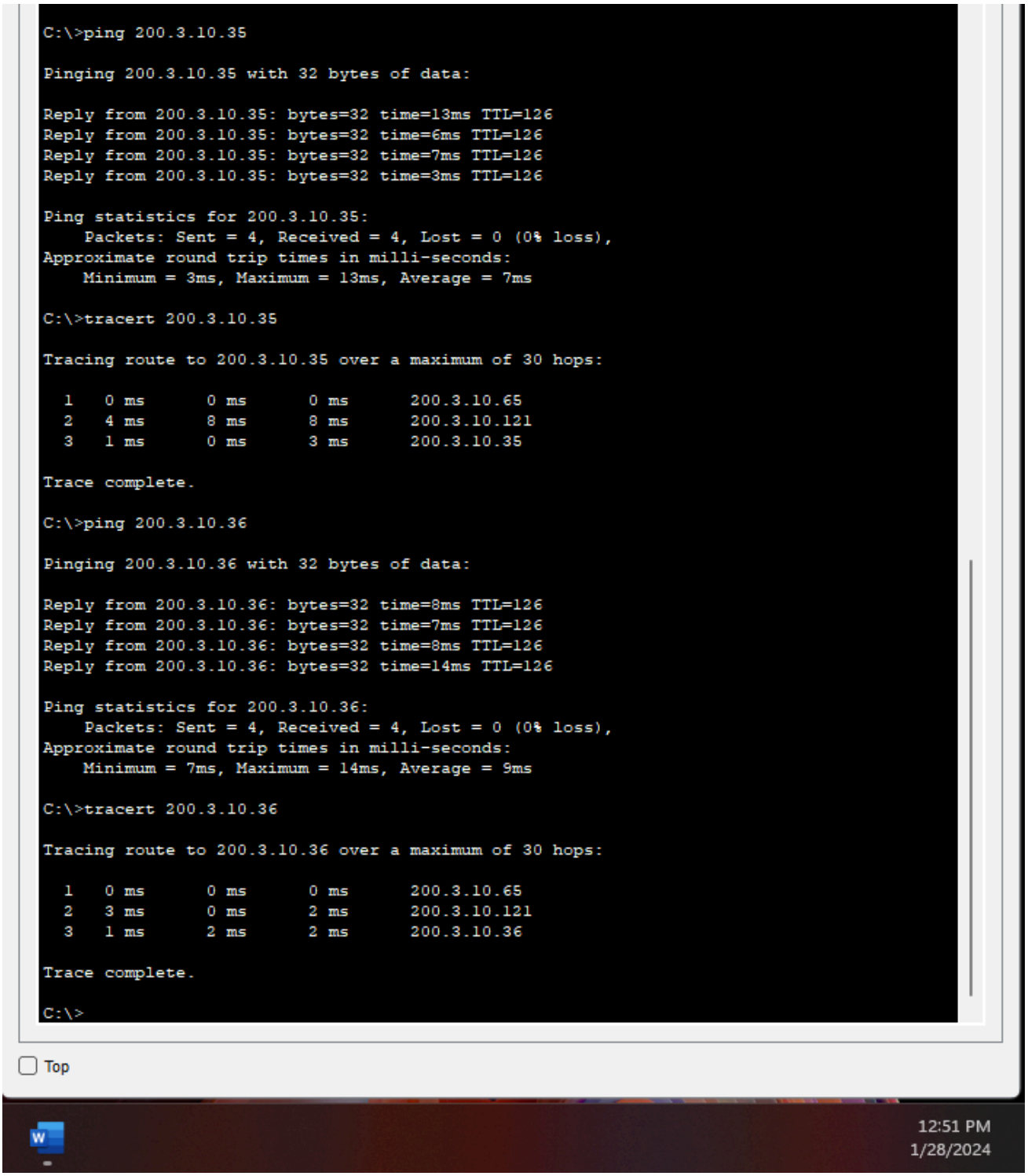
⇒ping and tracert result From PC 41_2 to PC 2_1 +2_2:



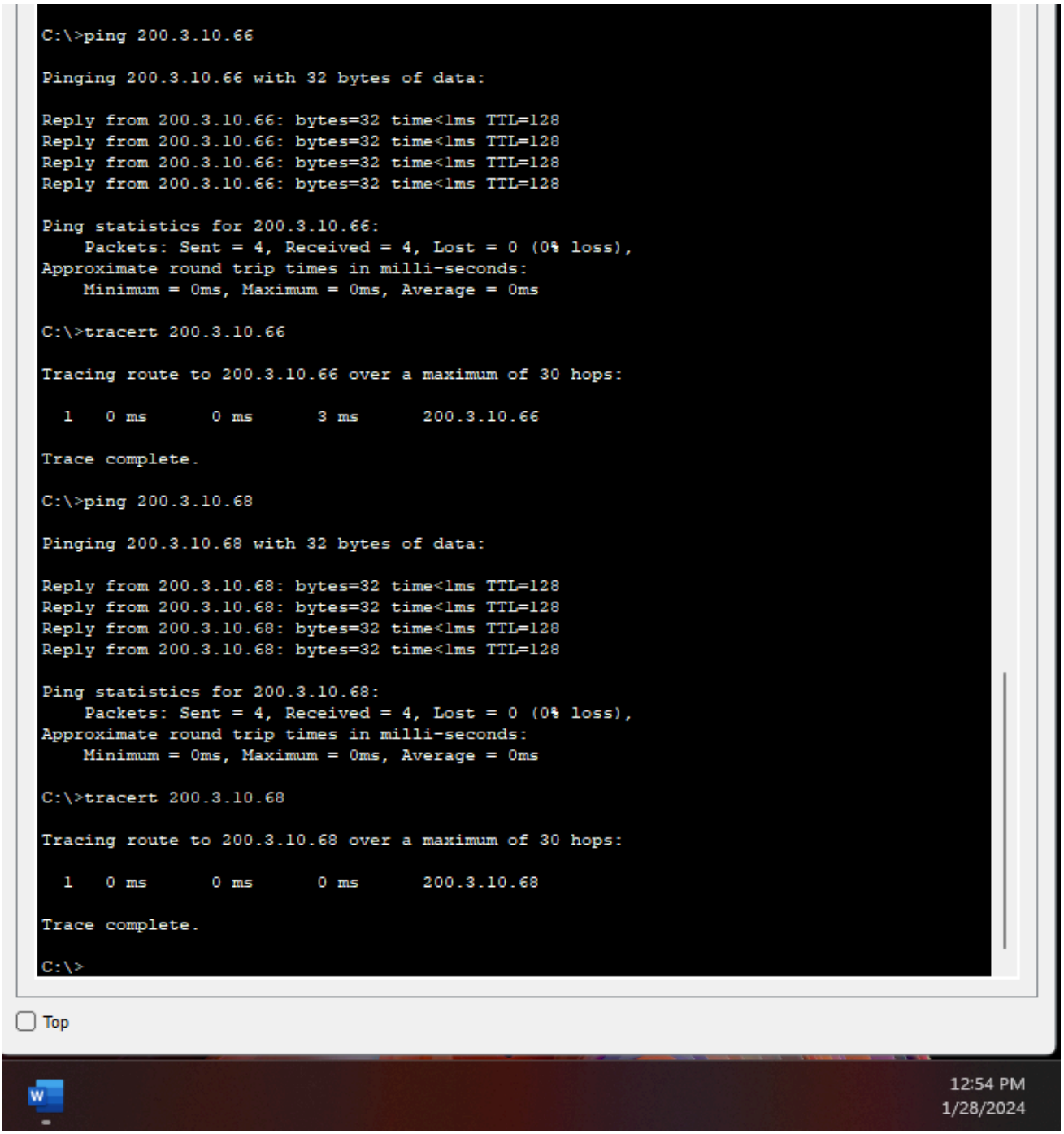
⇒ping and tracert result From PC 41_2 to PC 2_3



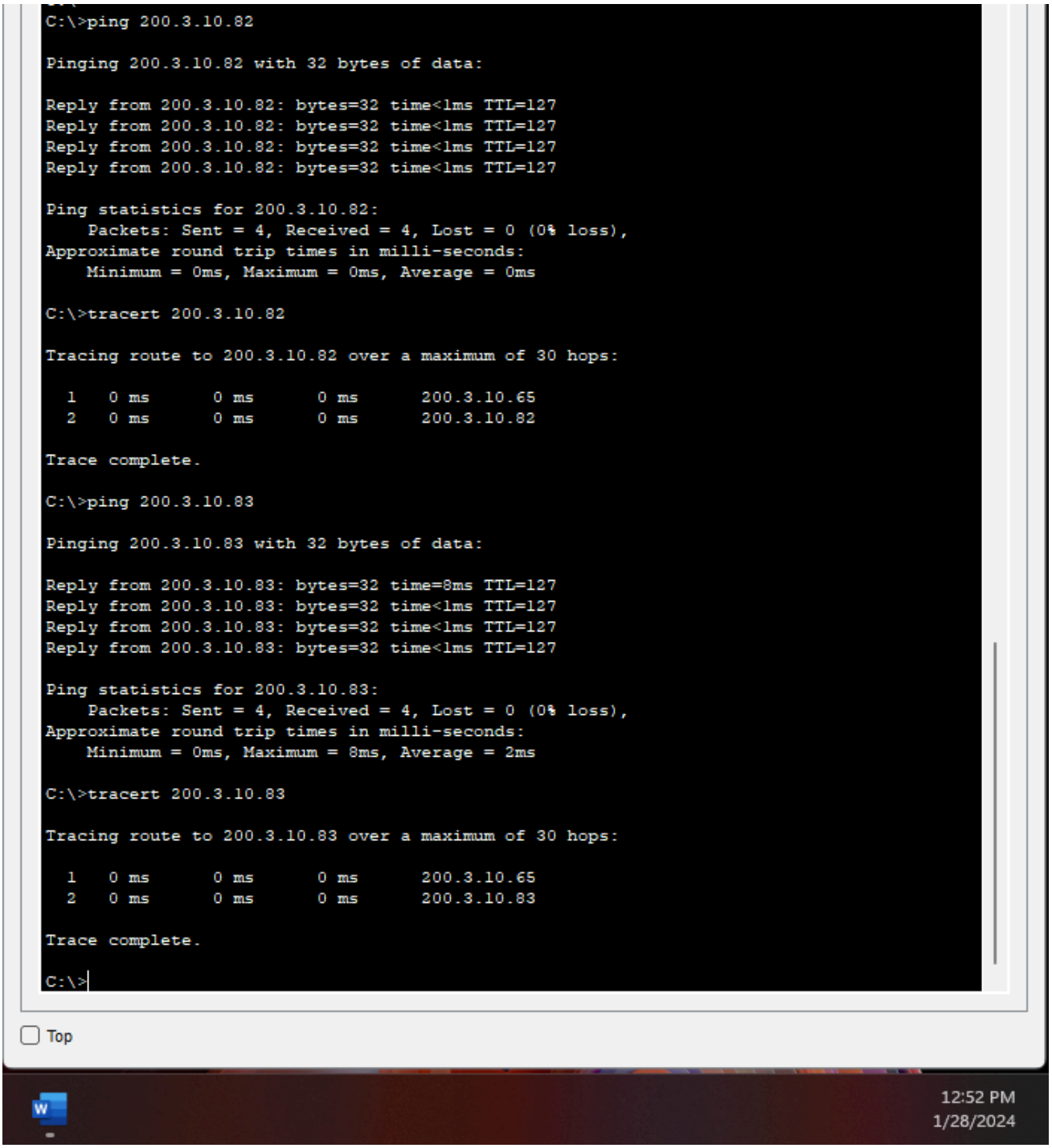
⇒ping and tracert result From PC 41_2 to PC 3_1 +3_2:



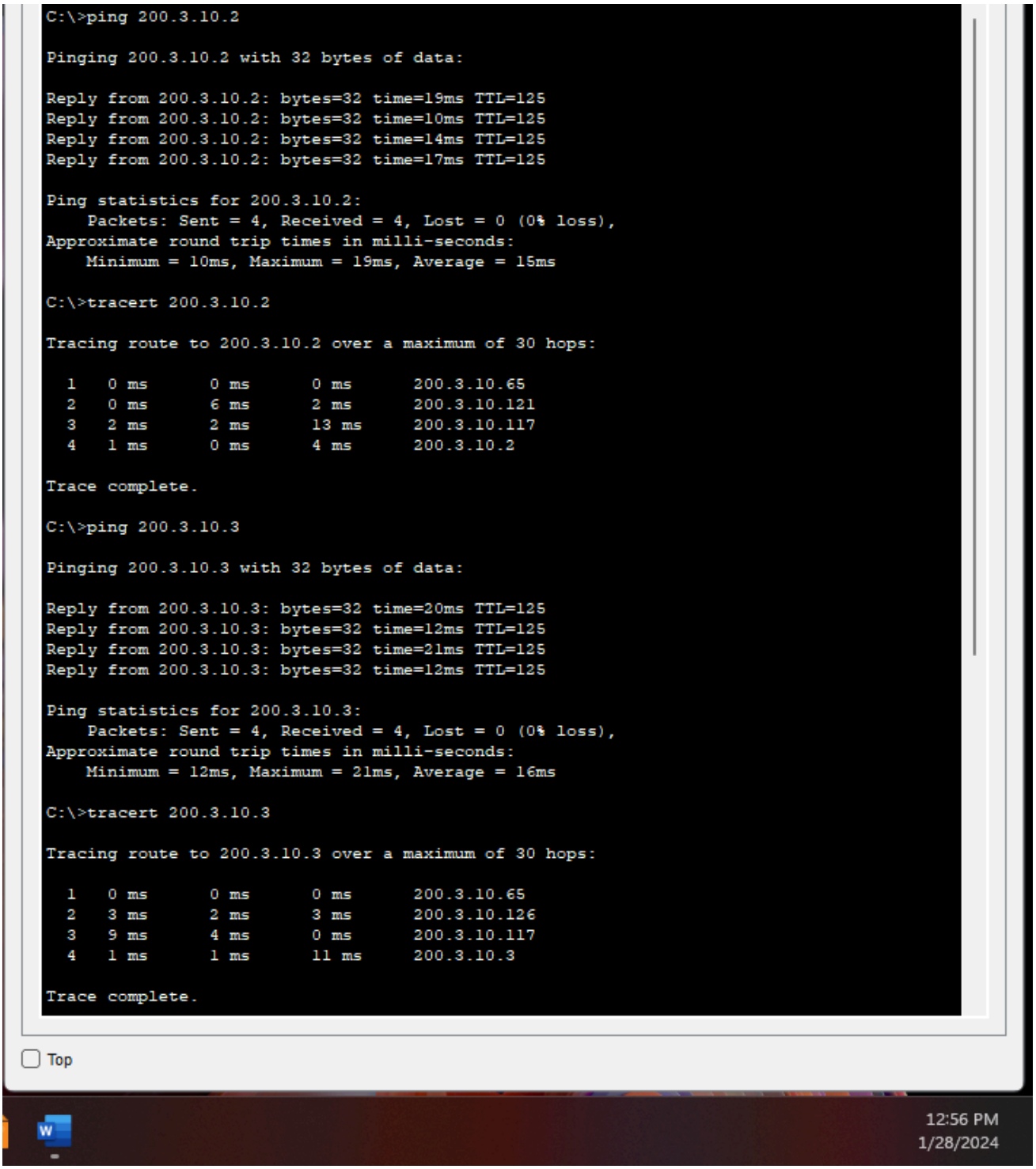
⇒ping and tracert result From PC 41_2 to PC 41_1 +41_2:



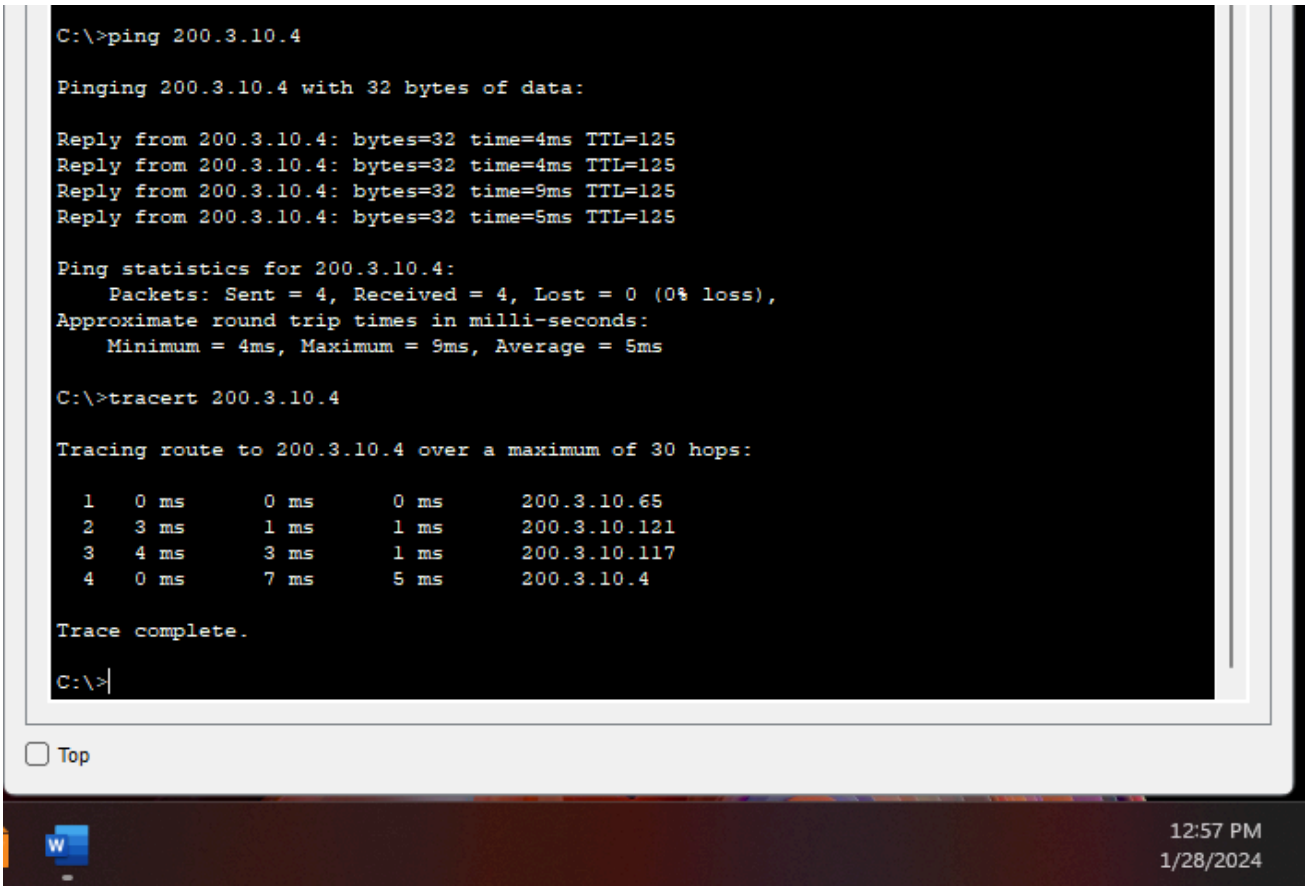
⇒ping and tracert result From PC 41_2 to PC 42_1 +42_2



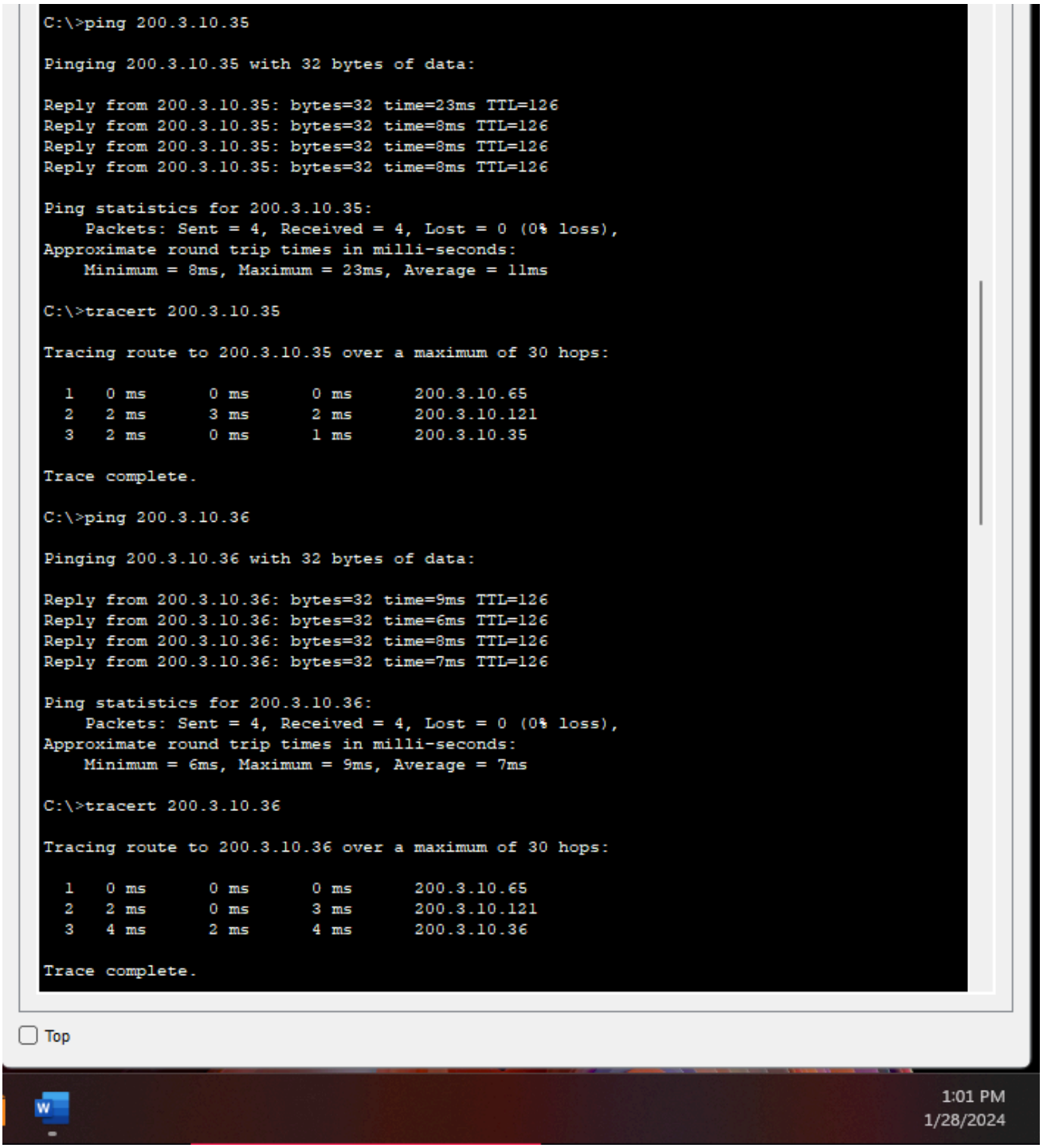
⇒ping and tracert result From PC 41_3 to PC 2_1 +2_2



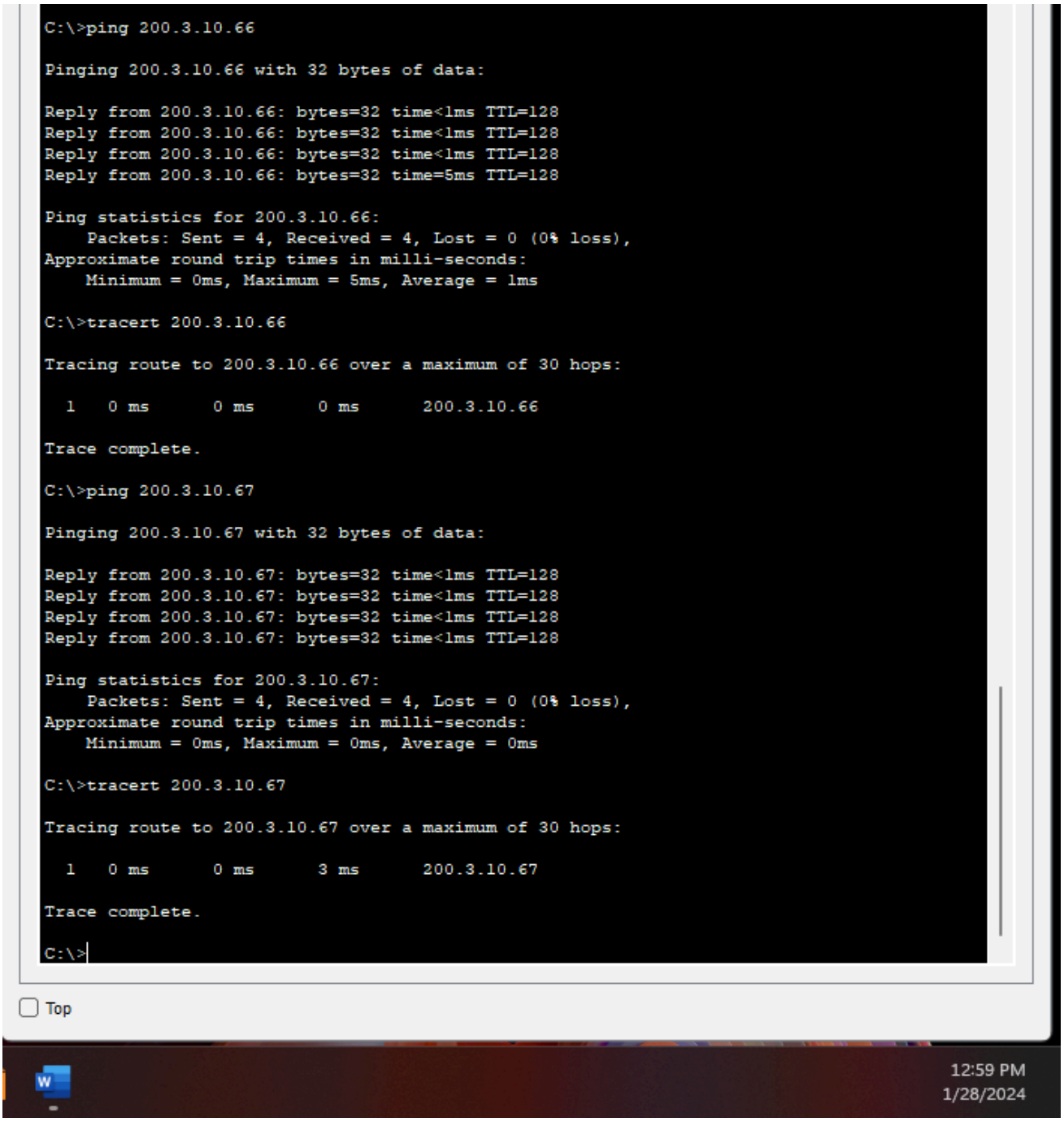
⇒ping and tracert result From PC 41_3 to PC 2_3:



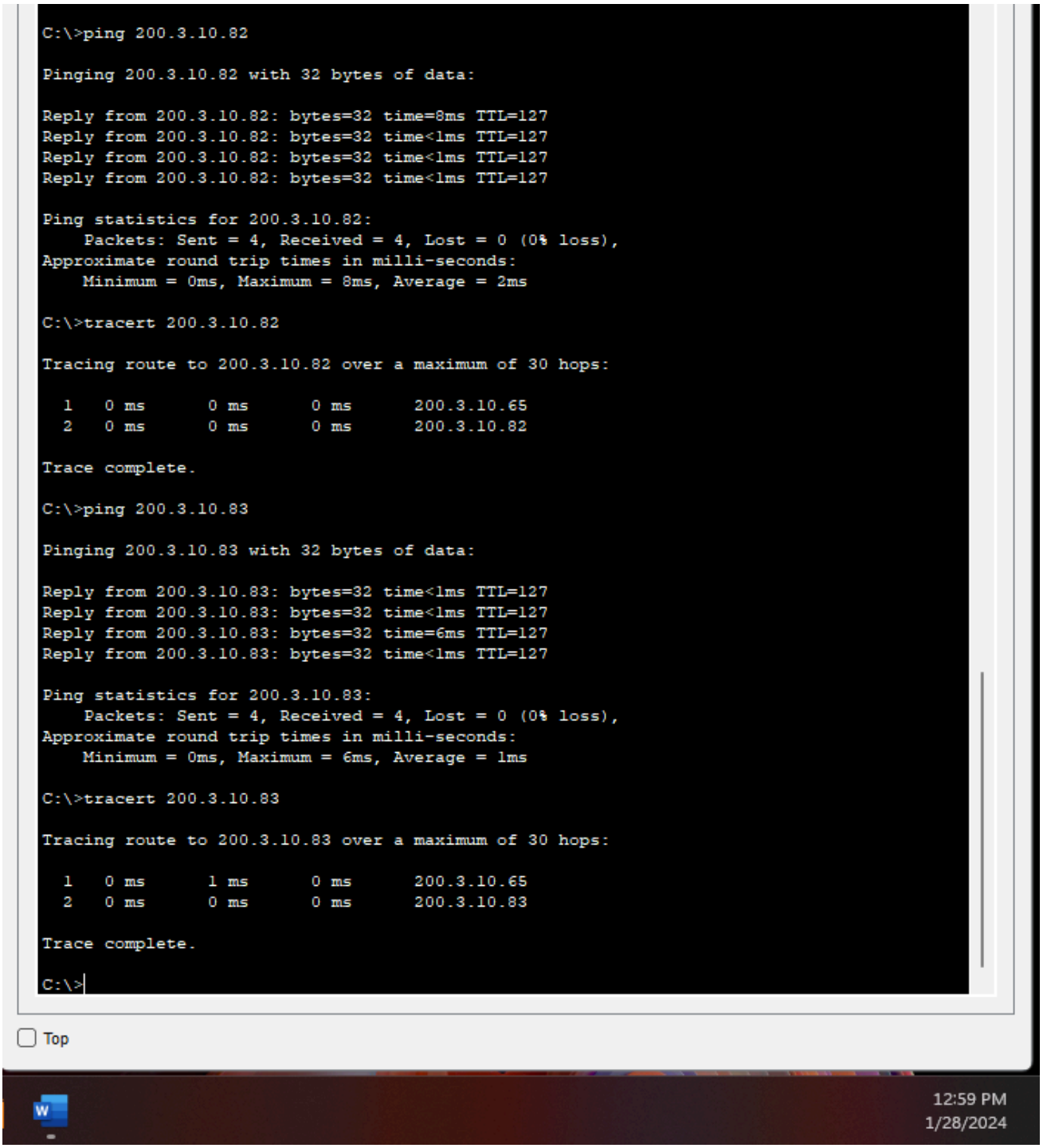
⇒ping and tracert result From PC 41_3 to PC 3_1 +3_2



⇒ping and tracert result From PC 41_3 to PC 41_1 +41_2 :

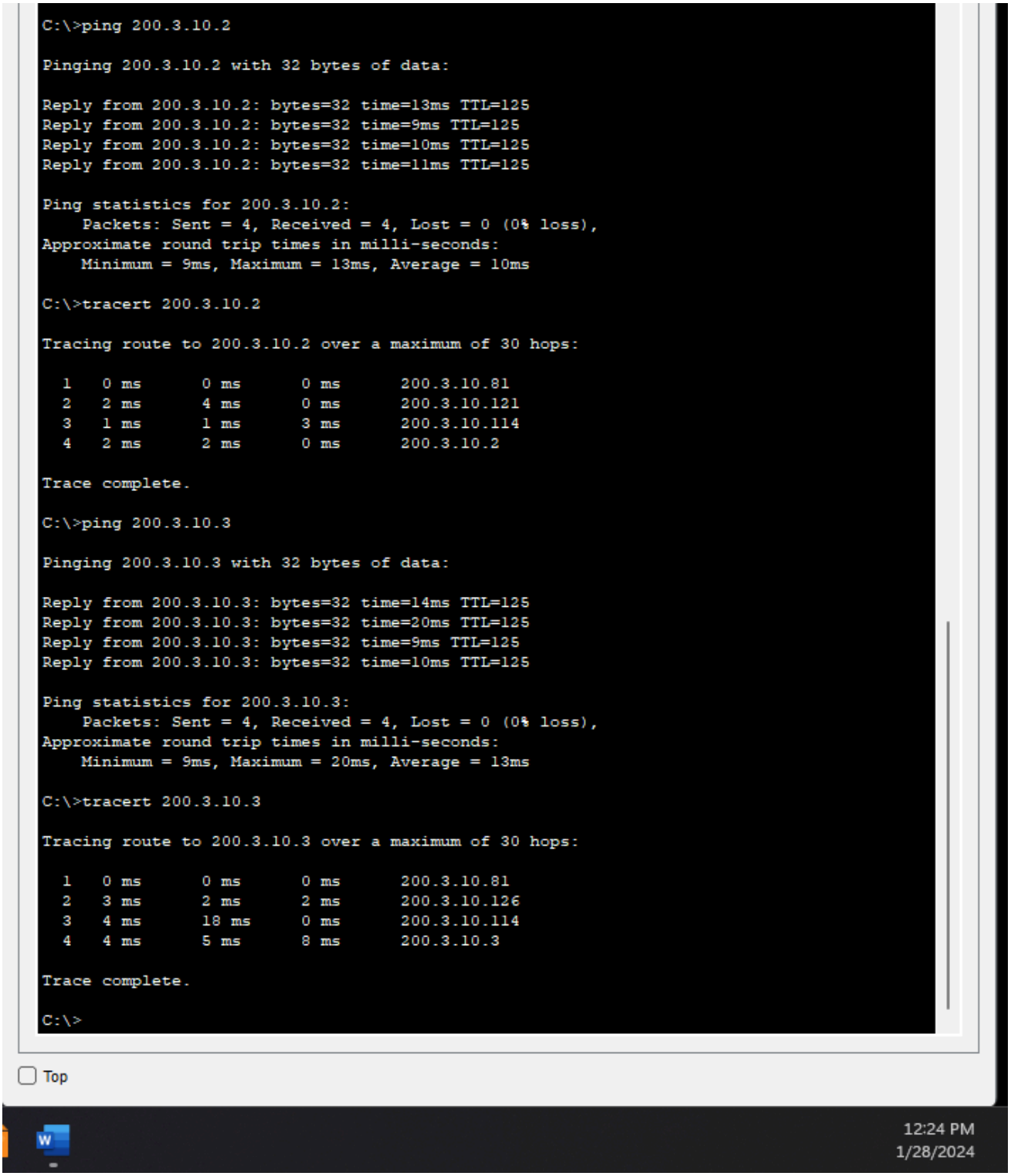


⇒ping and tracert result From PC 41_3 to PC 42_1 +42_2

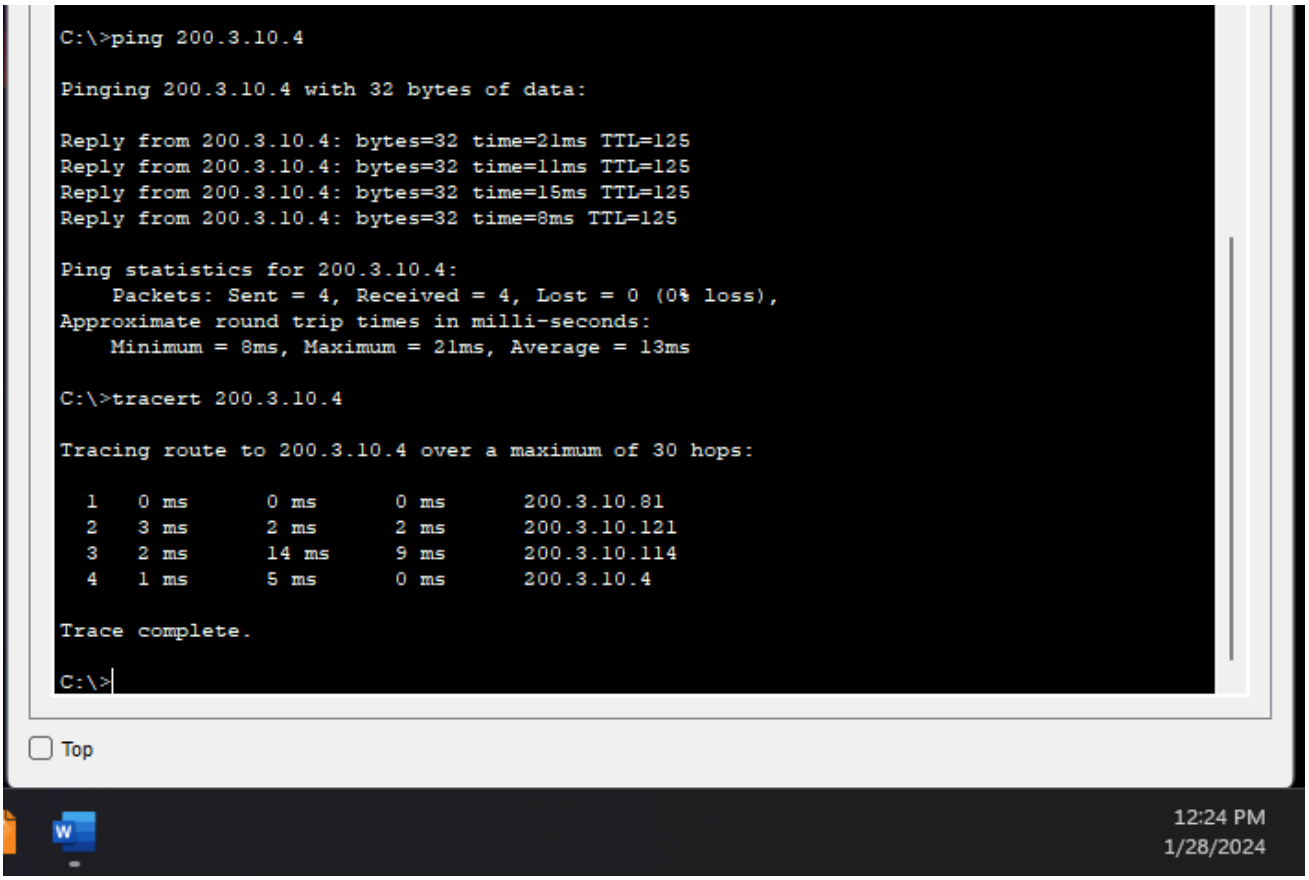


company c office 2:

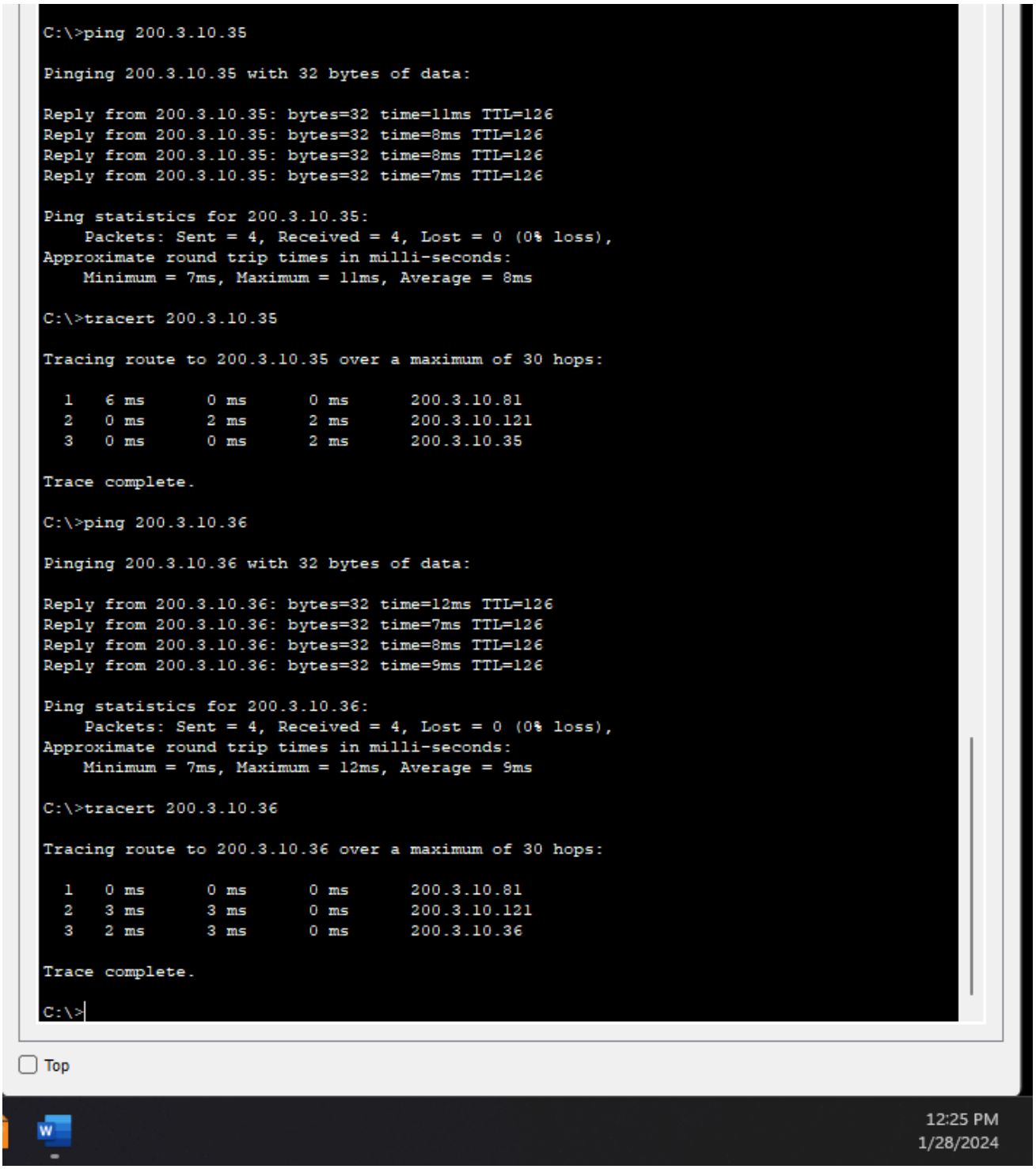
⇒ping and tracert result From PC 42_1 to PC 2_1 +2_2:



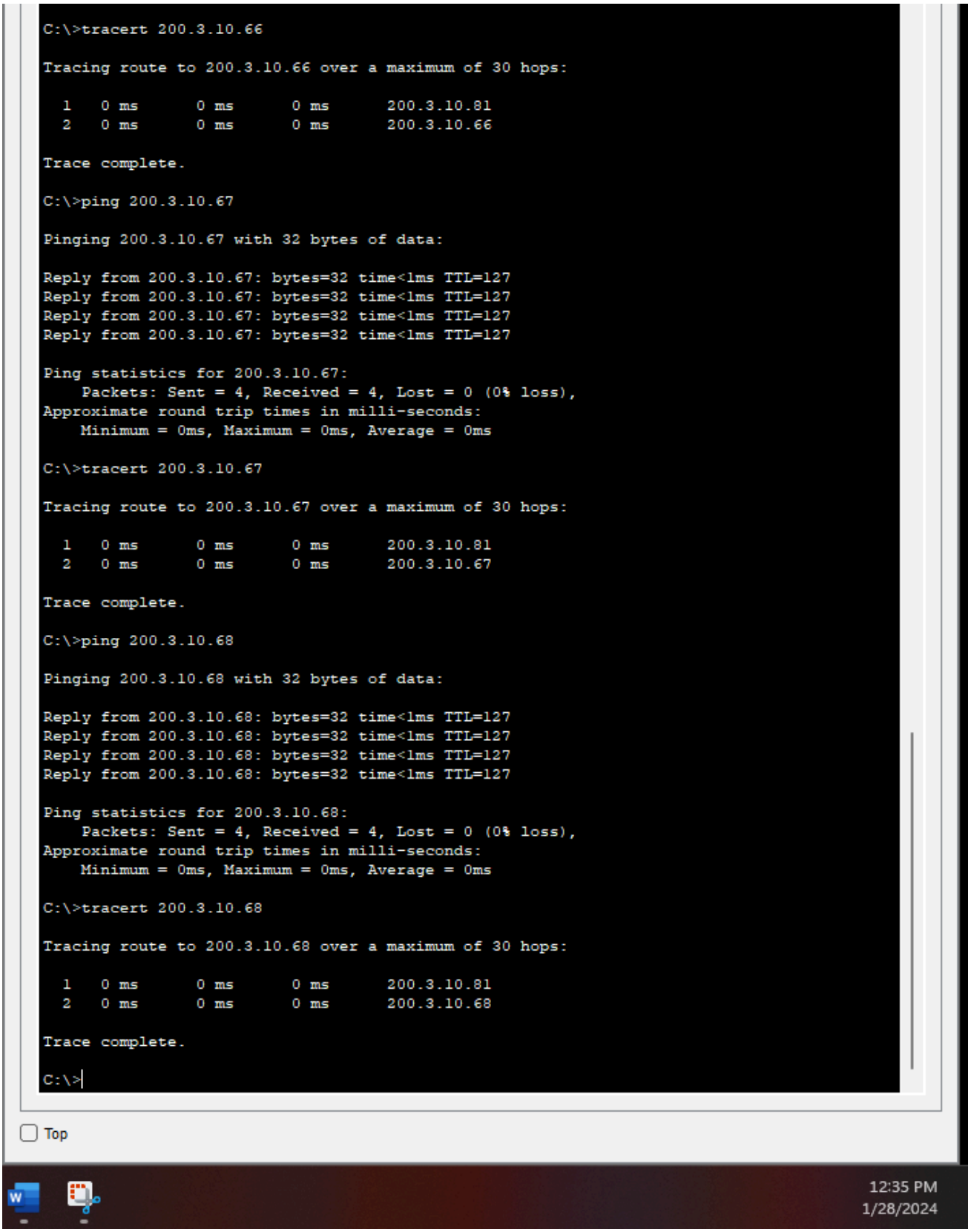
⇒ping and tracert result From PC 42_1 to PC2_3



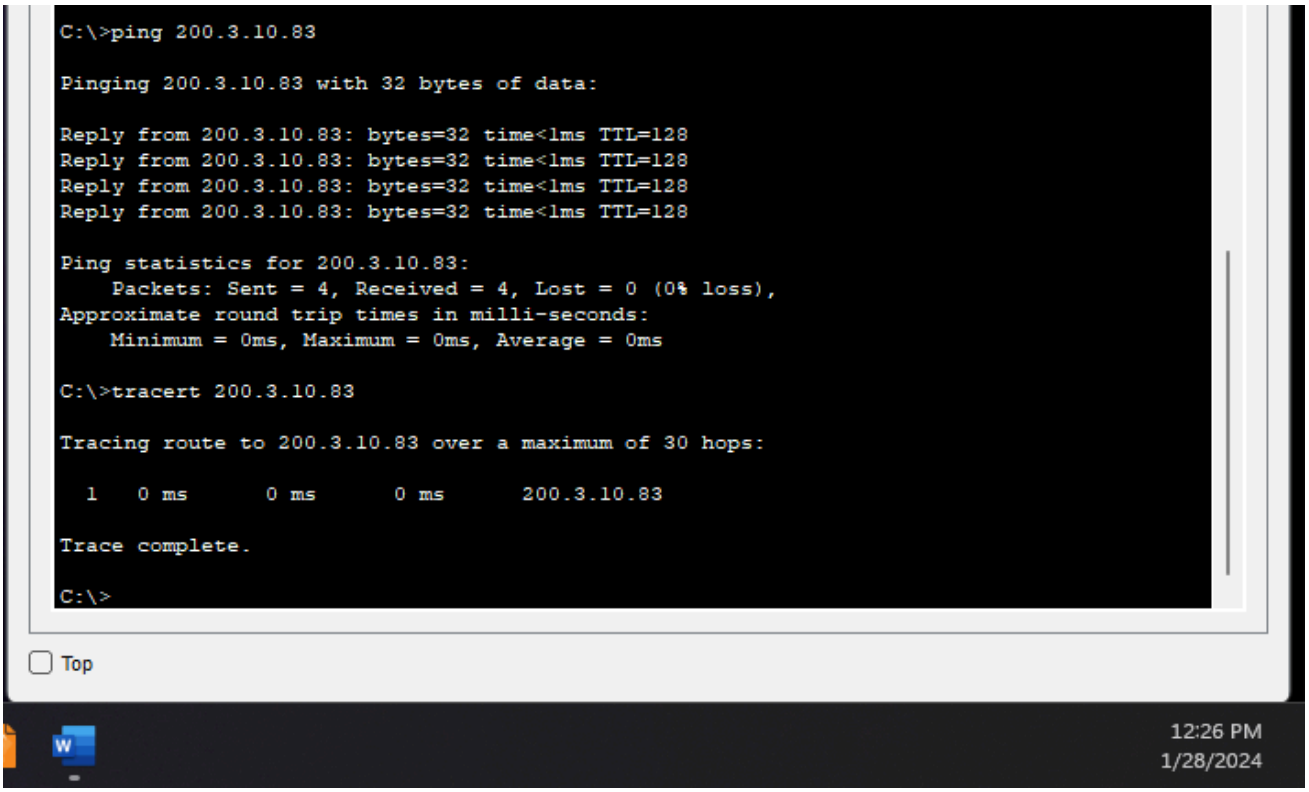
⇒ping and tracert result From PC 42_1 to PC 3_1 +3_2:



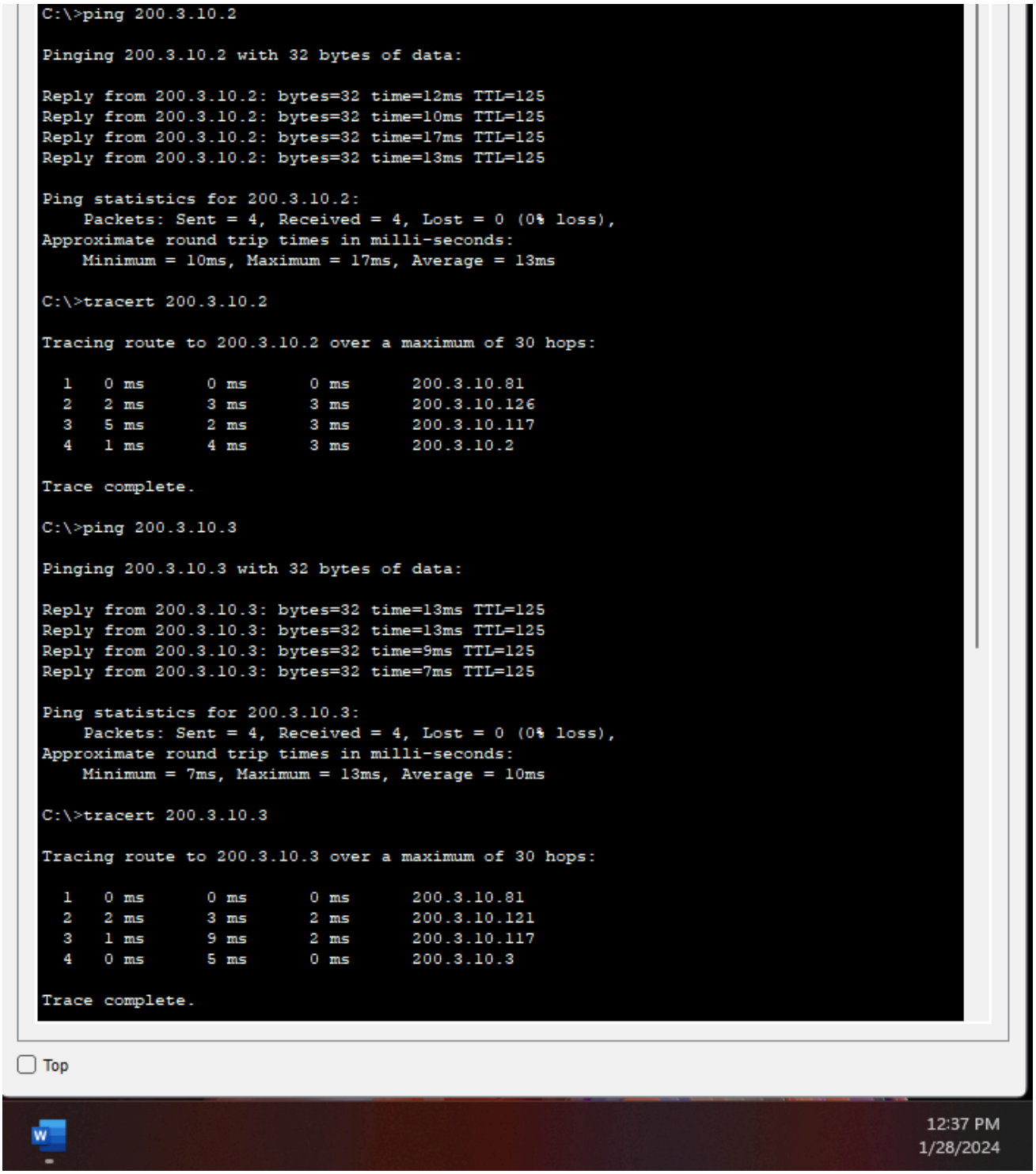
⇒ping and tracert result From PC 42_1 to PC 41_1 +41_2 +41_3:



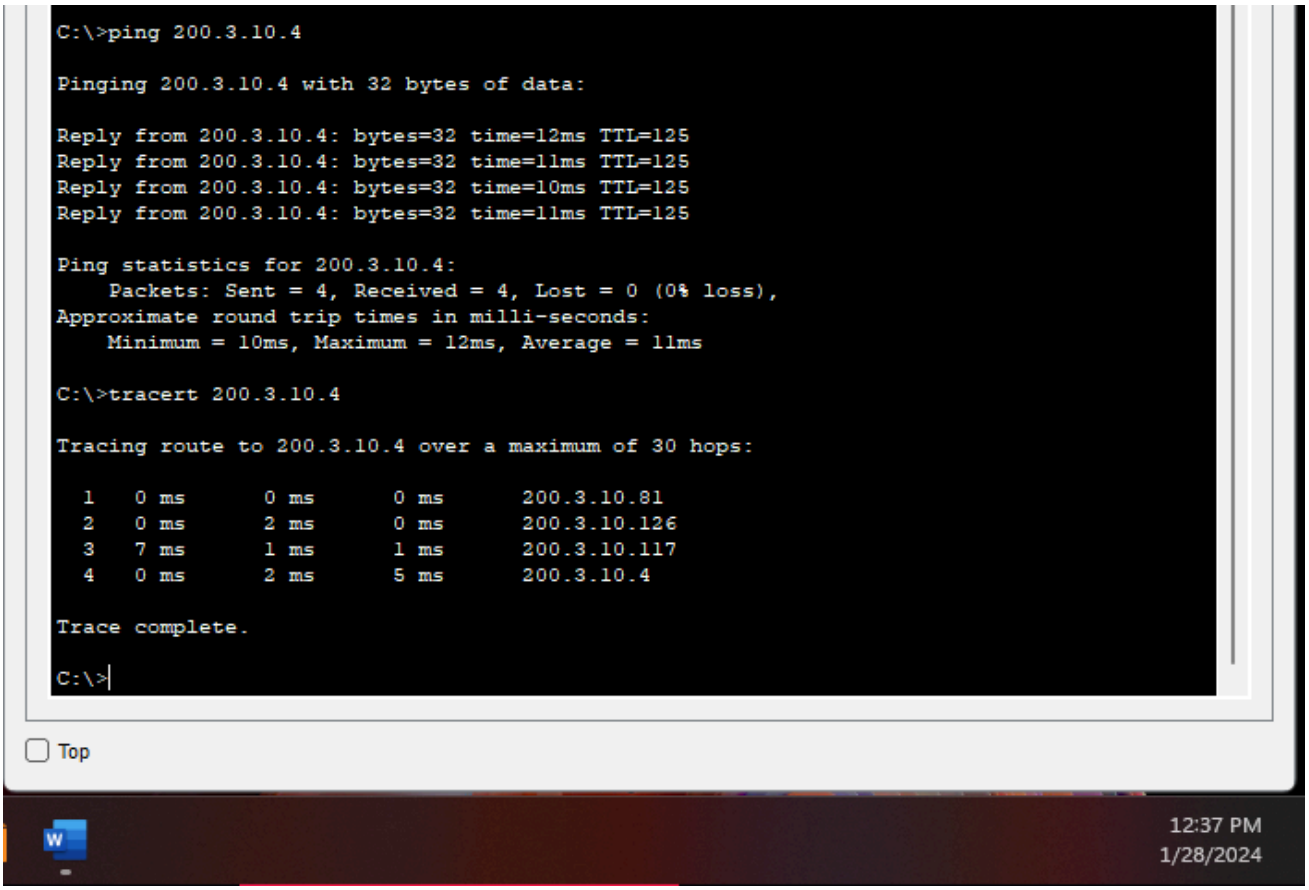
⇒ping and tracert result From PC 42_1 to PC 42_2:



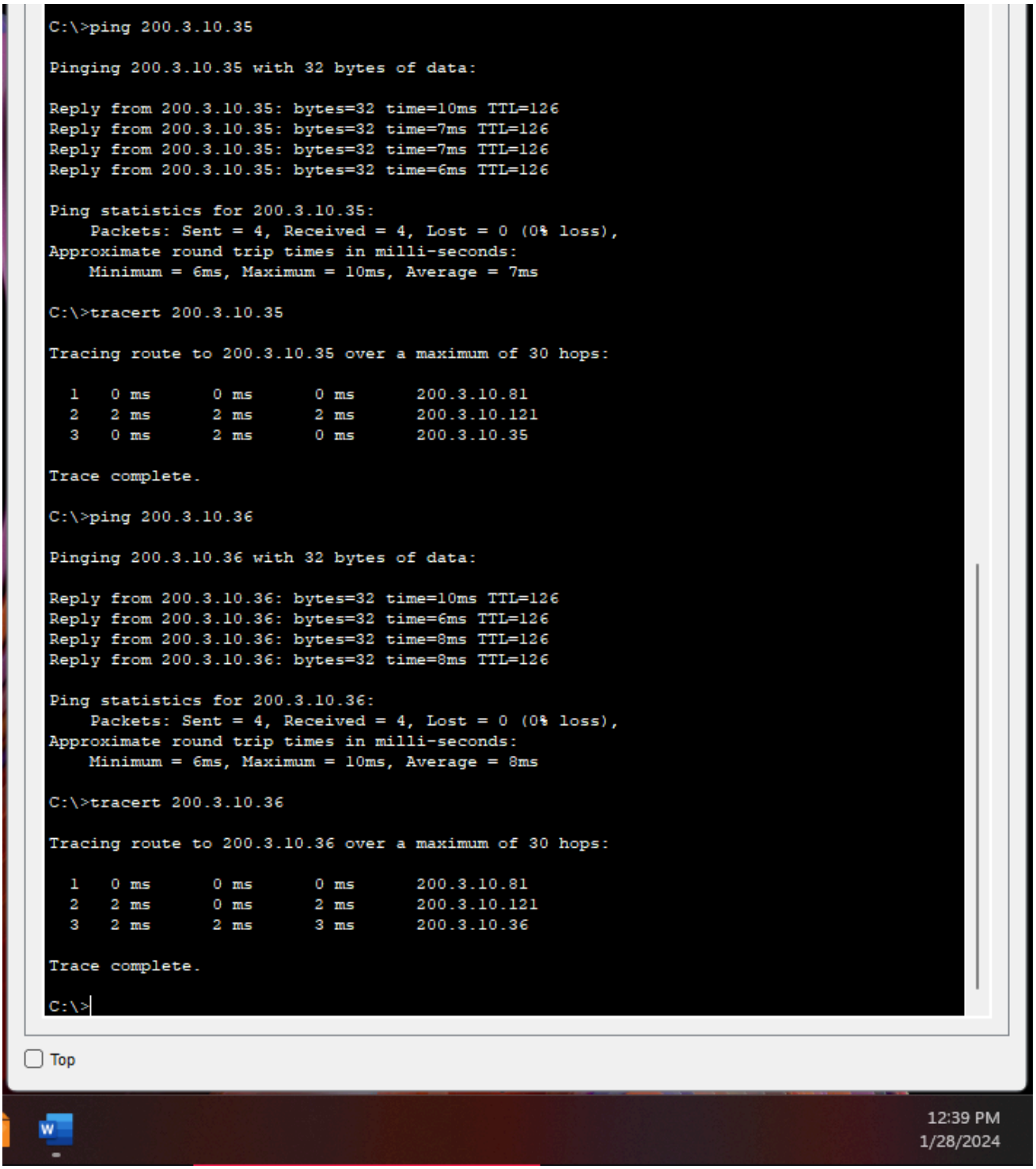
⇒ping and tracert result From PC 42_2 to PC 2_1+2_2:



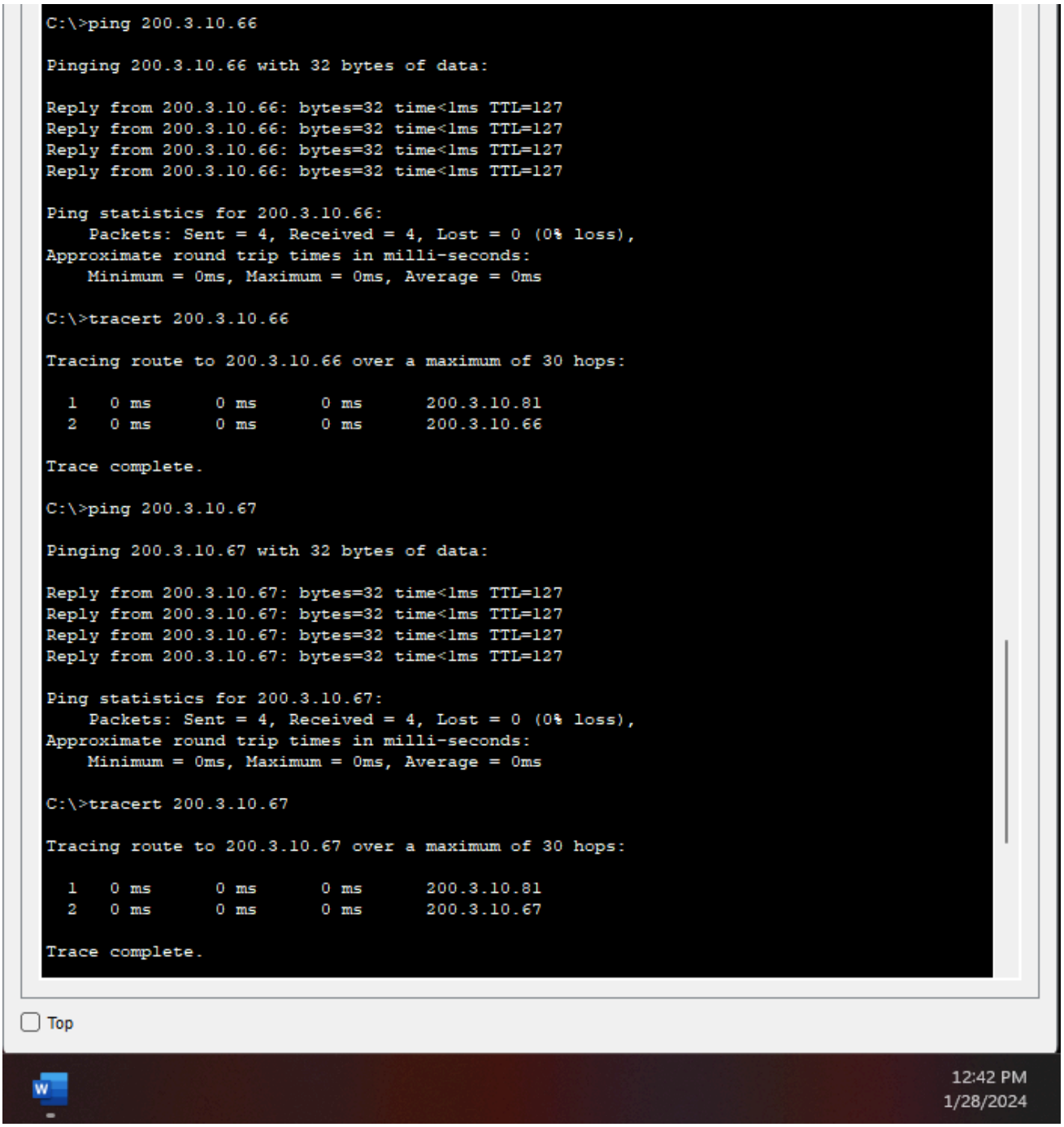
⇒ping and tracert result From PC 42_2 to PC 2_3:



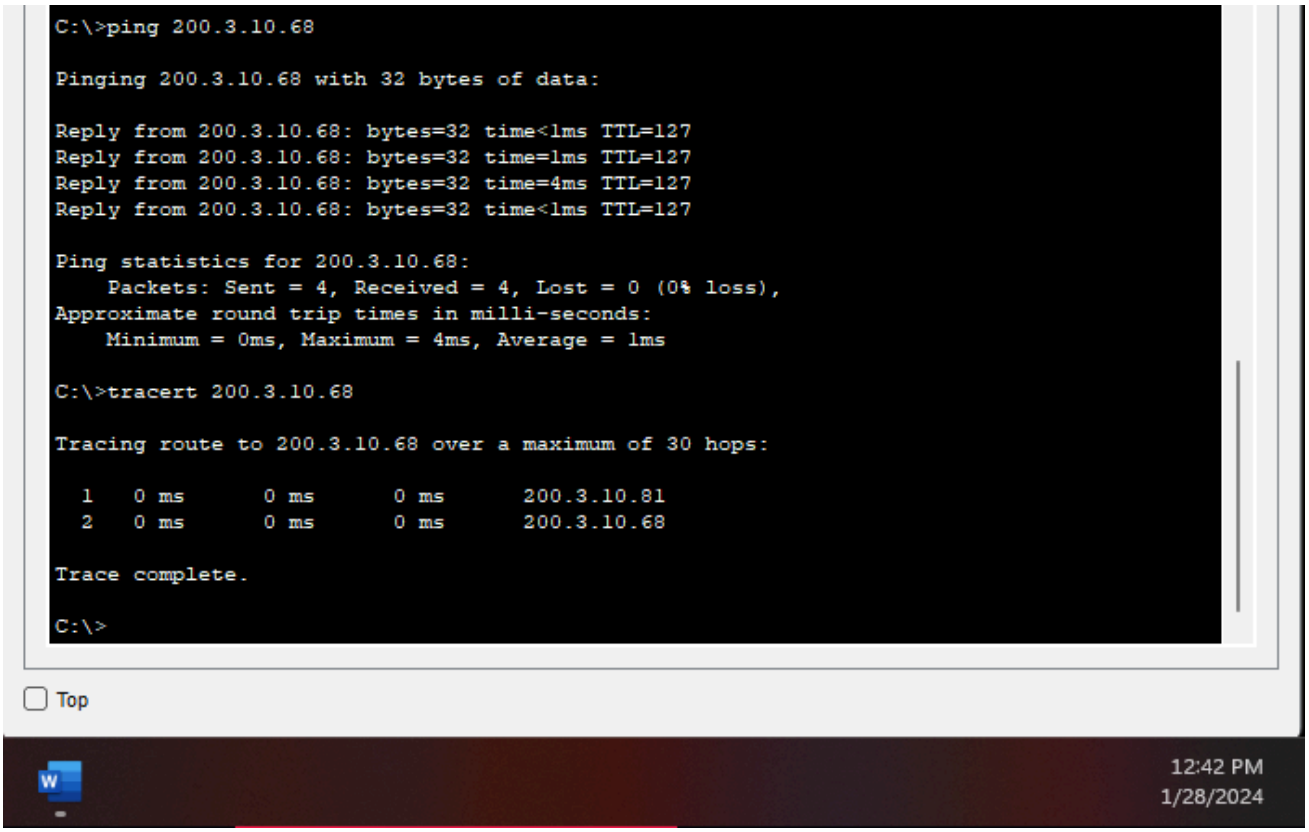
⇒ping and tracert result From PC 42_2 to PC 3_1+3_2:



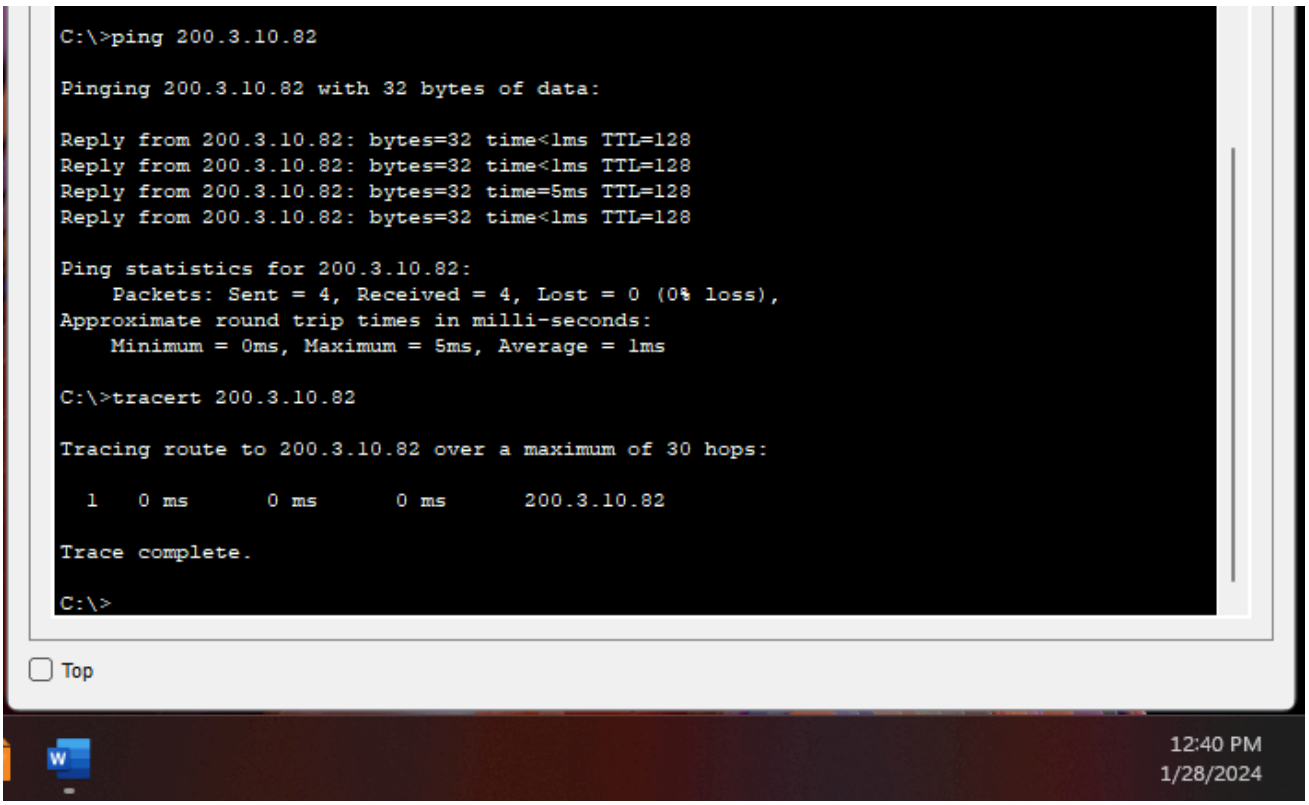
⇒ping and tracert result From PC 42_2 to PC 41_1+41_2:



⇒ping and tracert result From PC 42_2 to PC 41_3:

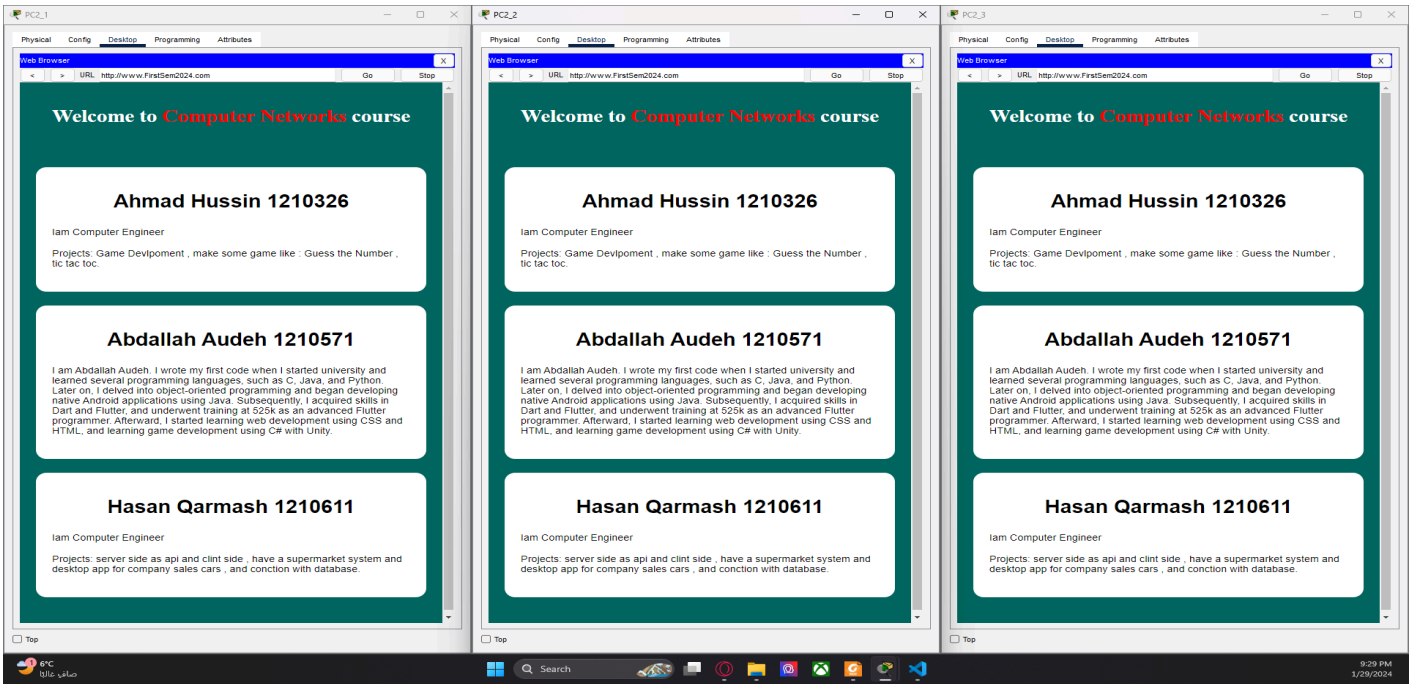


⇒ping and tracert result From PC 42_2 to PC 42_1:

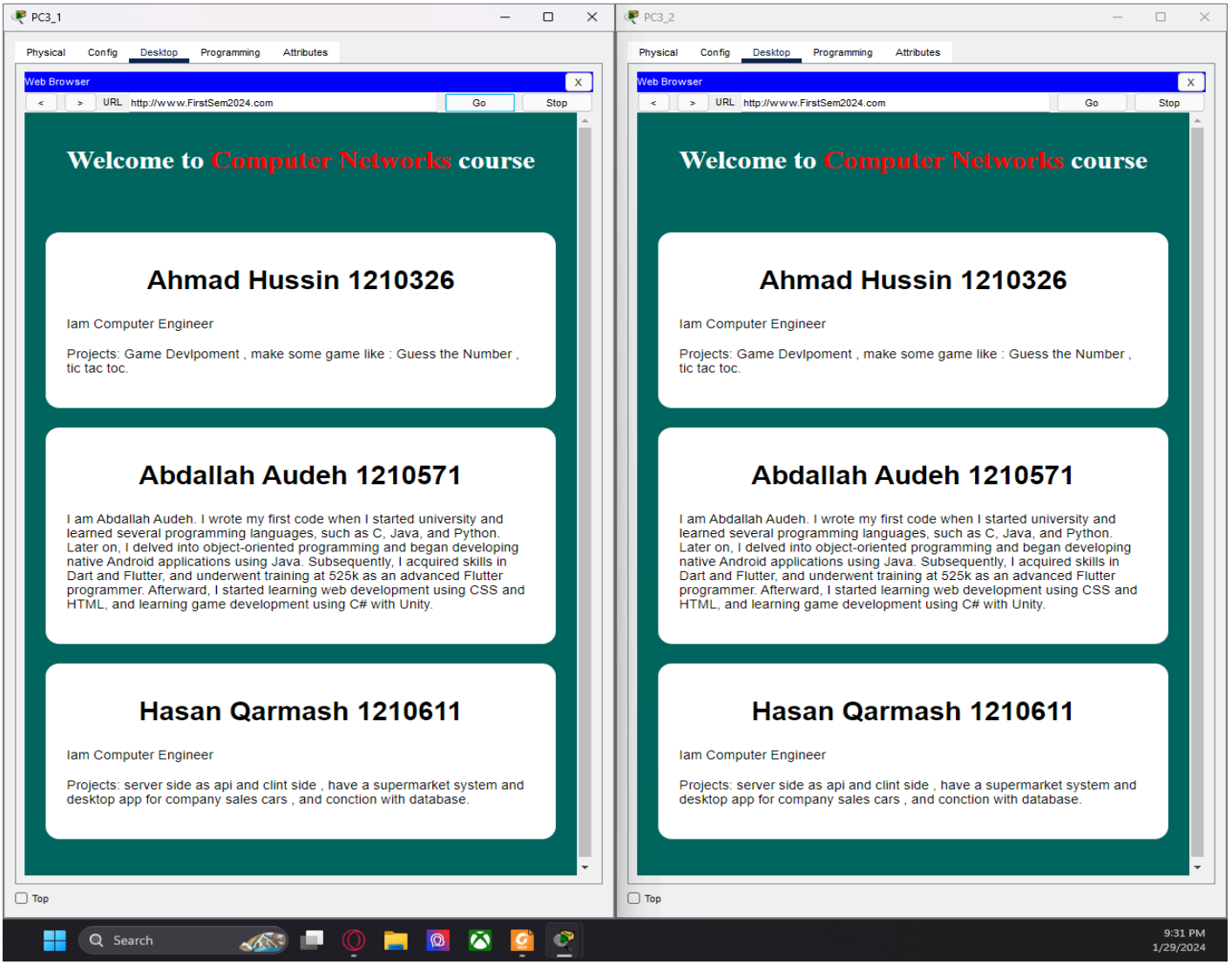


2. Access www. FirstSem2024.com from all PCs, take snapshots for all cases :

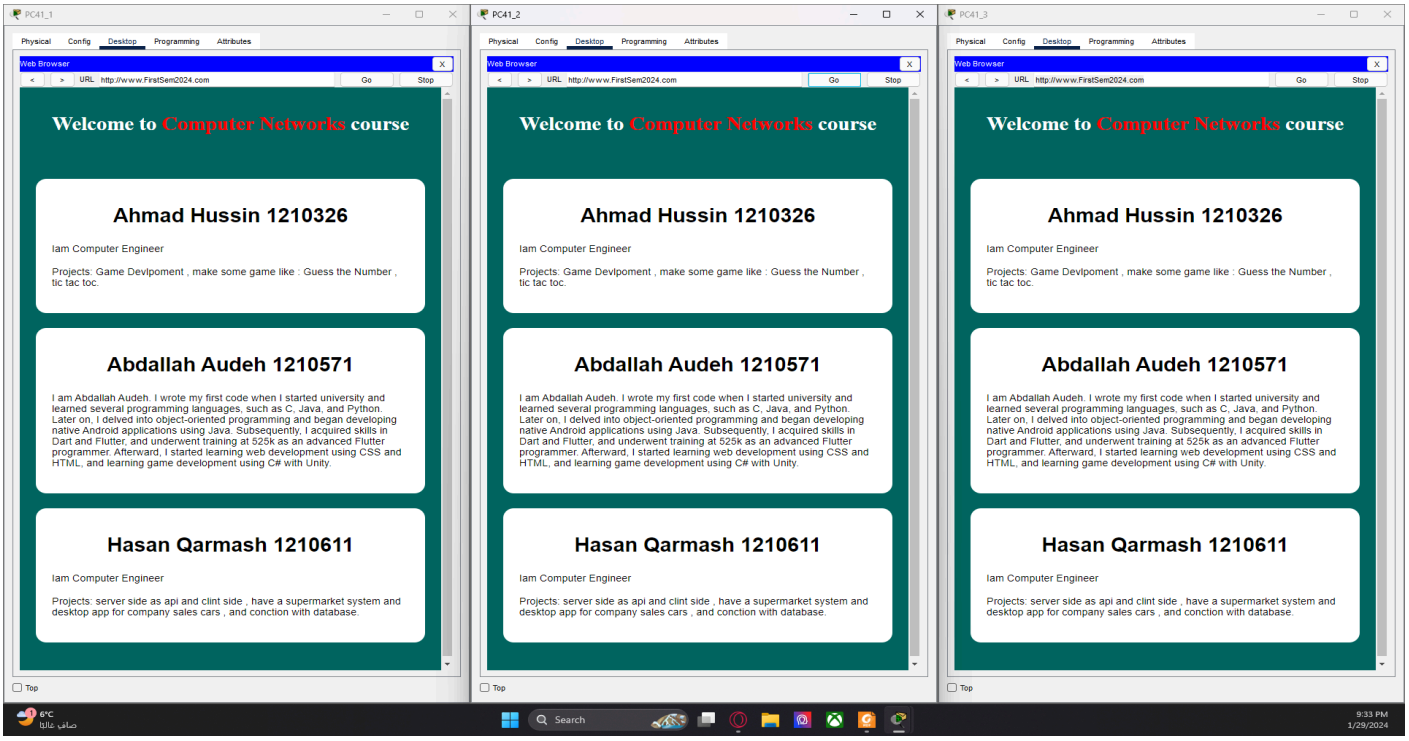
Company A: PC2_1, PC2_2, PC2_3



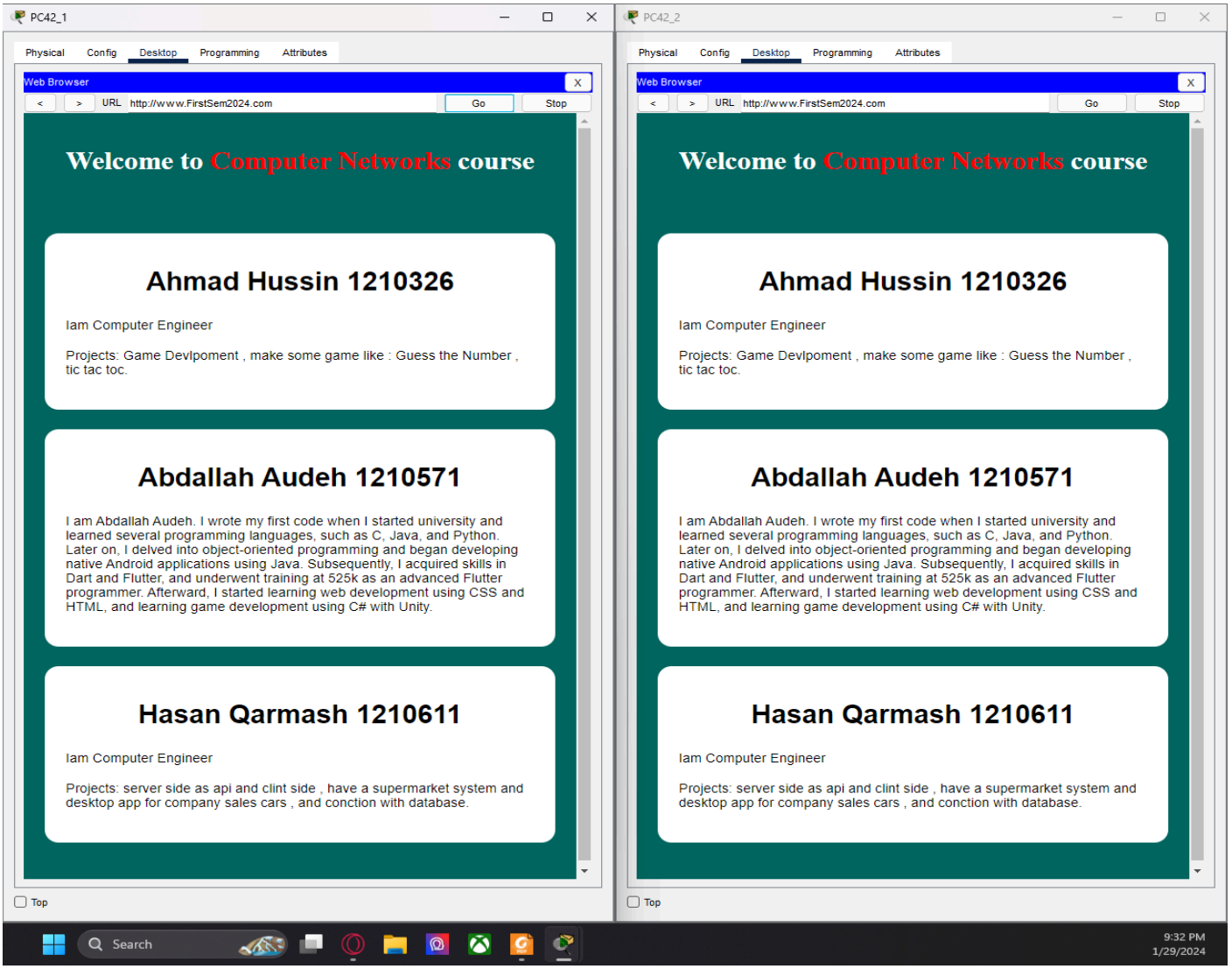
Company B: PC3_1, PC3_2



Company C office 1: PC41_1, PC41_2, PC41_3



Company C office 2: PC42_1, PC42_2



Conclusion:

The completion of this project has successfully achieved the outlined objectives, providing a comprehensive understanding of network design principles and the practical application of OSPF routing. Our team demonstrated proficiency in subnetting a network and configuring end devices with static IP addresses. The routing algorithms were successfully applied to the routers, ensuring seamless connectivity across the simulated enterprise network.

The testing phase validated our network's functionality, as all devices exhibited full connectivity, and the domain www.FirstSem2024.com was accessible from each subnetwork. The successful configuration of email services further emphasized the practical application of the concepts learned.

In conclusion, this project not only served as an essential learning tool for understanding the complexities of network setup and management but also highlighted the importance of teamwork and attention to detail in achieving a fully operational network. The skills acquired from this exercise are invaluable for future endeavors in the field of computer networks.