**Access Control List (ACLs)**

Student’s Name

Professor Name

University Affiliation

Course Number

Date

**Access Control List (ACLs)**

**Introduction**

In order to enhance the security and control of network traffic, the implementation of Access Control Lists (ACLs) plays a crucial role. ACLs allow network administrators to filter and control the flow of data packets based on specific criteria, such as source and destination IP addresses, ports, and protocols. By strategically configuring ACLs, network administrators can direct and limit traffic according to organizational policies, improving network performance, security, and resource allocation.

This report focuses on ACLs and their significance in network management. It explores the concepts of standard and extended IP ACLs, their respective use cases, advantages, and disadvantages. Furthermore, it discusses the placement of each ACL type in terms of traffic flow and analyzes the overall effect of ACL control on network traffic.

Understanding ACLs and their practical applications is essential for network administrators seeking to strengthen network security, manage network resources efficiently, and ensure compliance with organizational policies. By implementing appropriate ACLs, network administrators can establish granular control over the flow of data packets, mitigate potential threats, and optimize network performance.

This report delves into the details of standard and extended IP ACLs, providing insights into their functionalities and practical implications. Additionally, it will present a comprehensive analysis of the advantages, disadvantages, and appropriate placement of each ACL type in network configurations. This knowledge will enable network administrators to make informed decisions regarding the implementation of ACLs and contribute to the overall security and efficiency of their network infrastructure.

**Summary of Changes**

1. ***Addition of 5 Locations***

*Rationale:* The addition of 5 locations expands the network infrastructure, enabling better geographical coverage and facilitating efficient communication between different departments or branches of the organization. This enhances collaboration, data sharing, and overall productivity (Andrea, 2021).

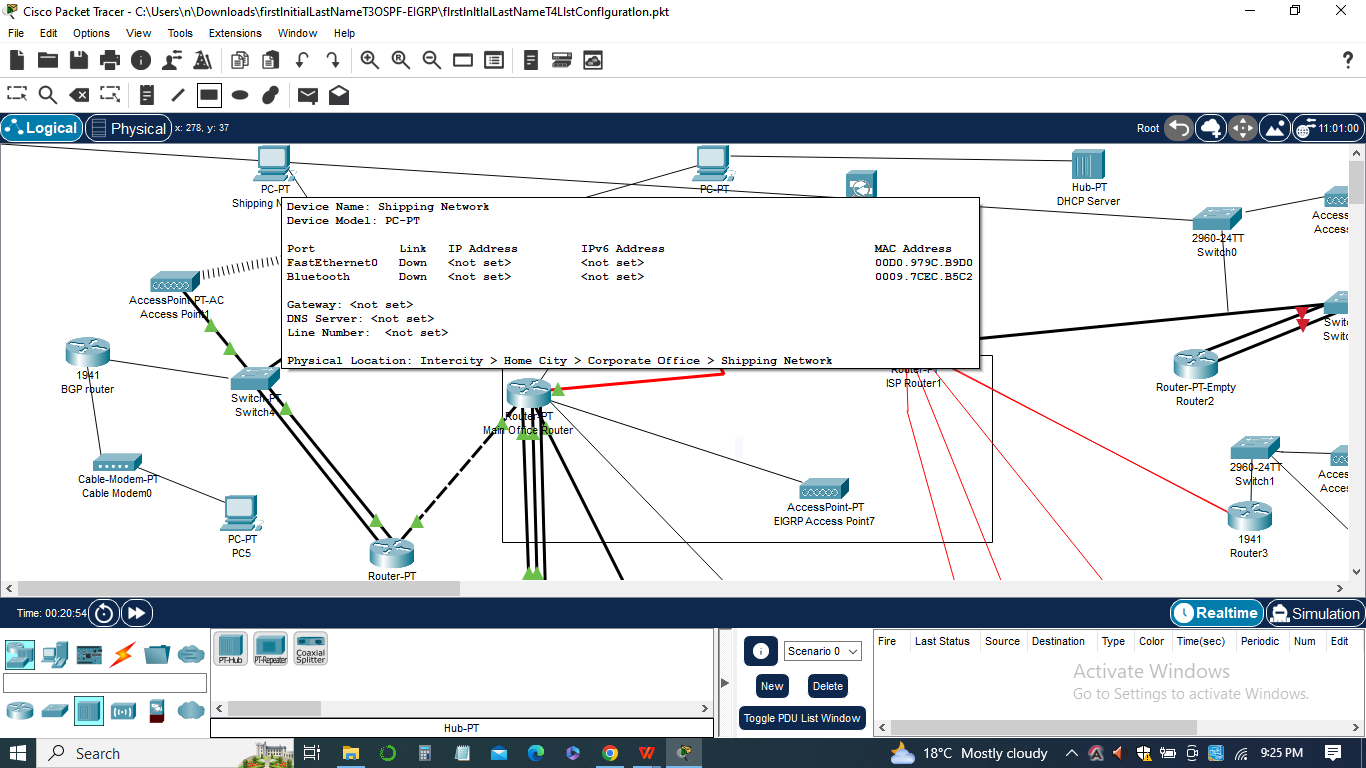
1. ***Implementation of Port Security***

*Rationale:* Port security ensures that only authorized devices are allowed to connect to the network by binding specific MAC addresses to network ports. This prevents unauthorized access, protects against potential security breaches, and safeguards sensitive information.

1. ***Limited VLANs***

*Rationale:* VLANs (Virtual Local Area Networks) provide logical segmentation of the network, grouping devices into separate broadcast domains. By limiting VLANs, network administrators can control communication and isolate traffic based on specific requirements, improving security and network performance.

1. ***Deployment of Interior Gateway Protocols (OSPF and EIGRP)***

**

*Rationale:* Interior Gateway Protocols (IGPs) such as OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) facilitate efficient routing within the network. These protocols dynamically exchange routing information, calculate optimal paths, and adapt to changes in network topology, resulting in faster and more reliable data transmission (Vachon & Johnson, 2020).

1. ***Integration of ACLs (Access Control Lists)***

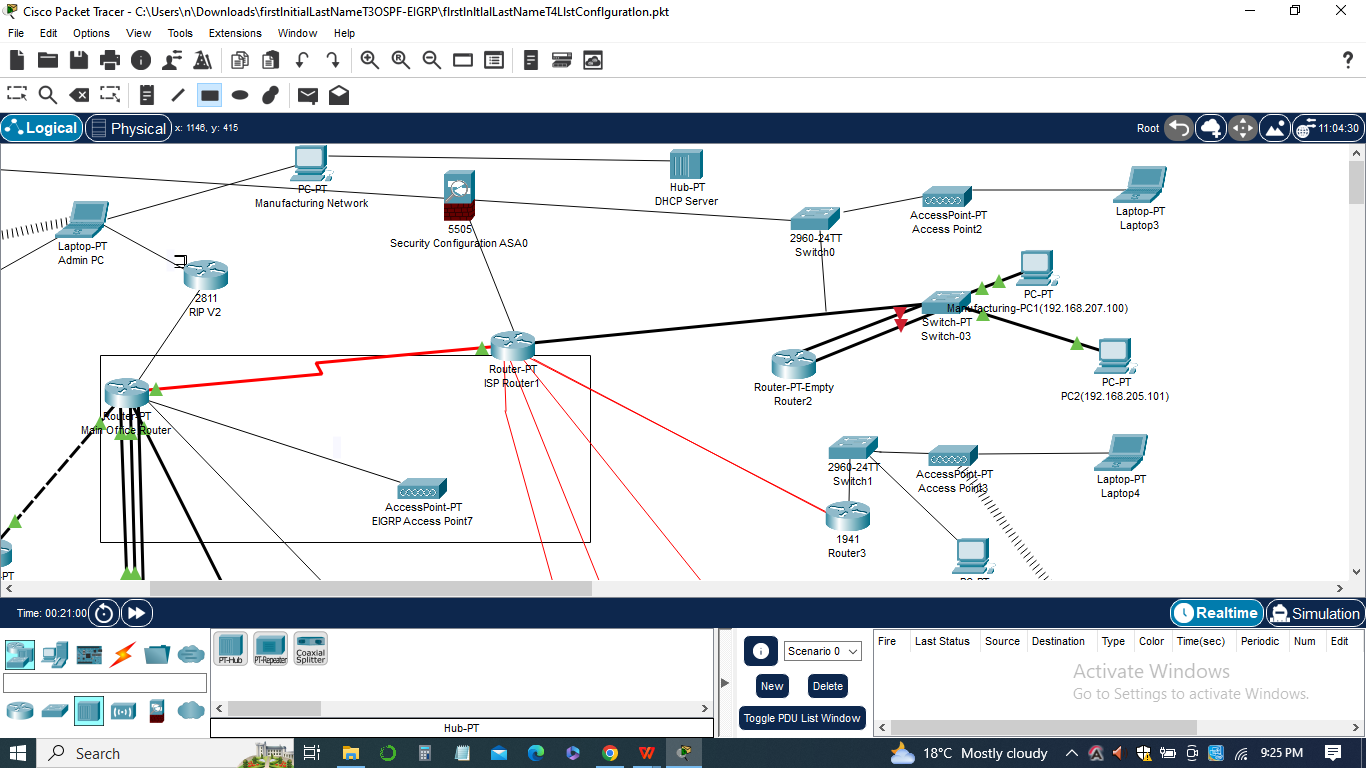
*Rationale:* ACLs provide granular control over network traffic by filtering and directing data packets based on specified criteria. By implementing ACLs, we can restrict traffic to specific networks or devices, prevent unauthorized access, and enhance network security. ACLs also enable efficient utilization of network resources and help enforce organizational policies.

In sum, these changes aim to enhance the network's security, improve traffic management, and optimize resource allocation. By implementing port security, limited VLANs, interior gateway protocols, and ACLs, we establish a robust and efficient network infrastructure that aligns with industry best practices and ensures the confidentiality, integrity, and availability of critical business data.

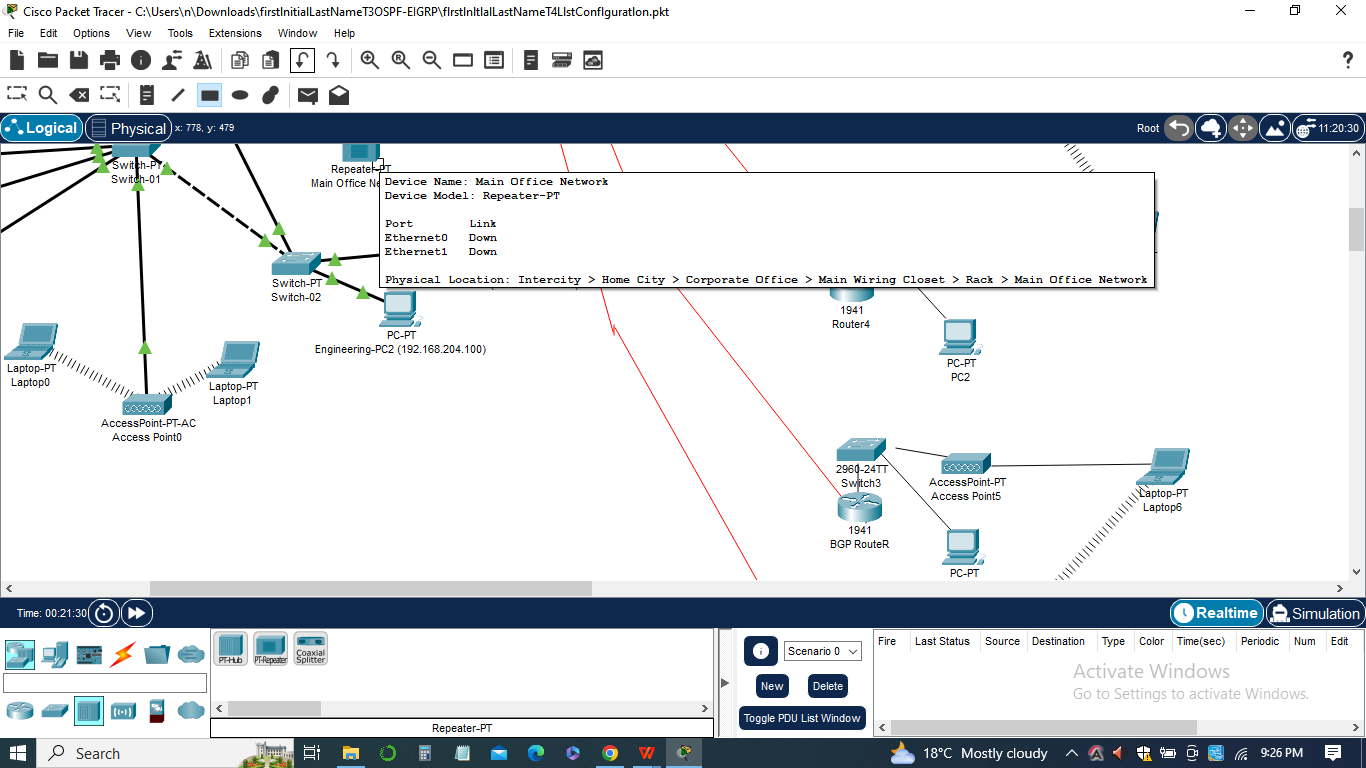
**List of Pings**

The list of pings in this assignment involved testing network connectivity and analyzing traffic behavior after implementing various security measures. The pings are performed from different workstations to specific networks or devices within the network. Let's discuss each ping scenario:

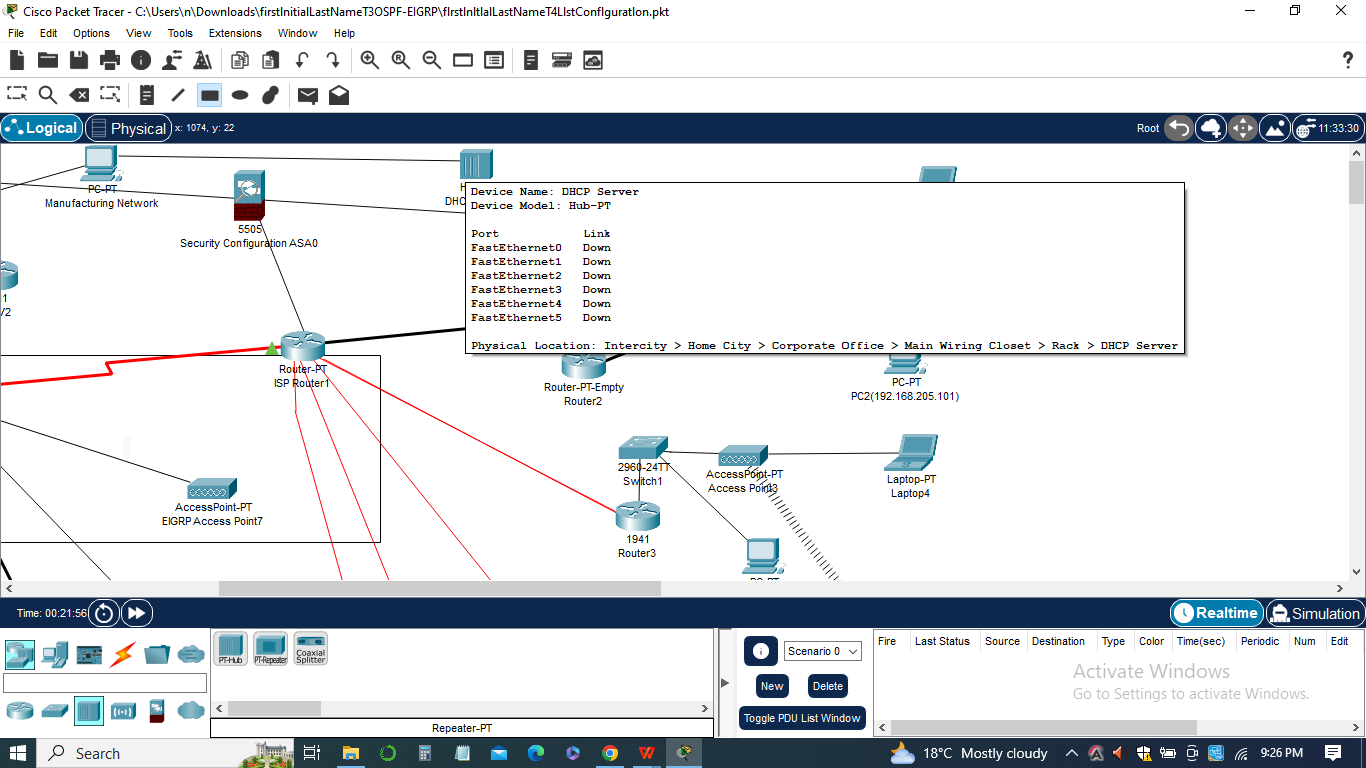
1. ***Ping from Admin PC to Manufacturing and Shipping networks***

**

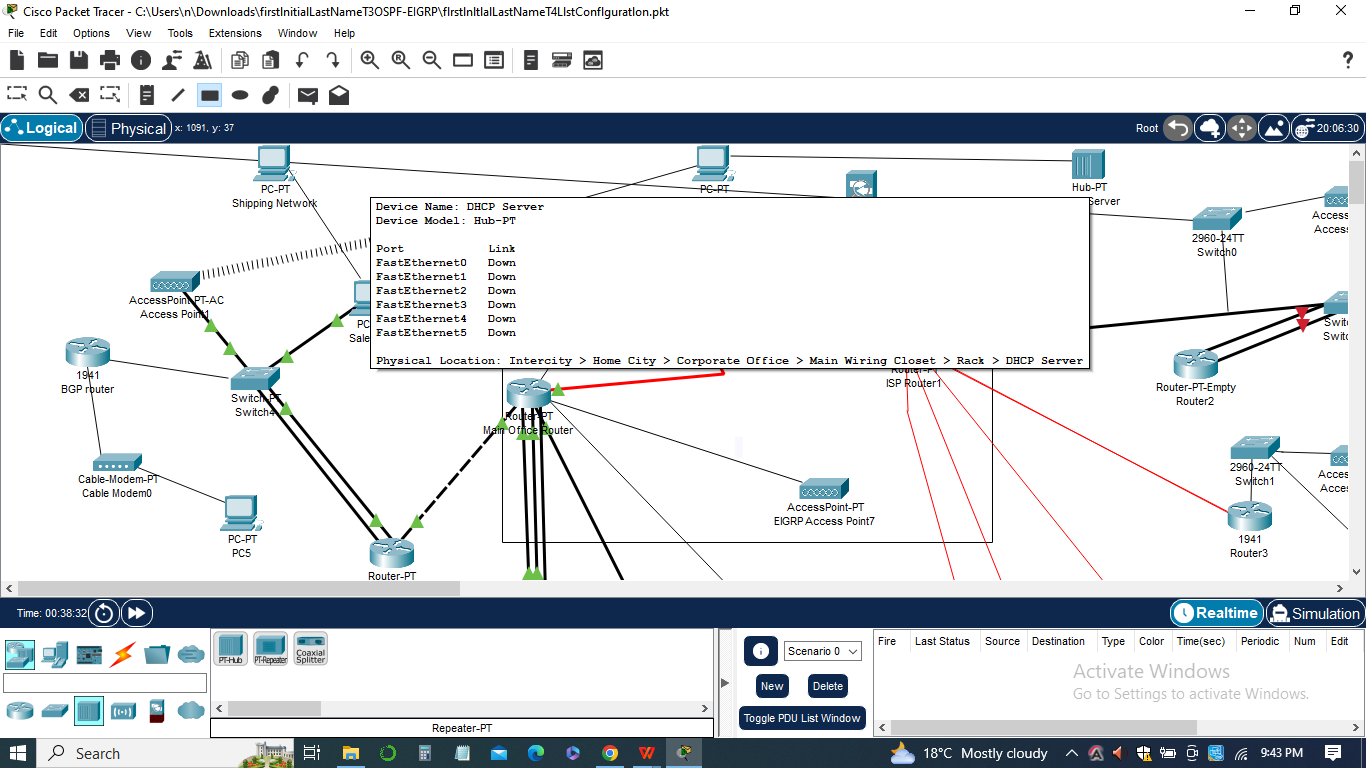
1. *Objective:* Verify connectivity between the Admin PC and the Manufacturing and Shipping networks.
2. *Rationale:* This ping test ensures that the Admin PC can communicate with the essential departments of the organization, allowing seamless data exchange and collaboration.
3. *Analysis:* If the ping is successful, it indicates that the traffic from the Admin PC to the Manufacturing and Shipping networks is allowed, and the network configuration is functioning as intended. If the ping fails, it suggests that traffic is being restricted, potentially due to ACL rules or network misconfigurations.
4. ***Ping from Sales PC to Manufacturing and Shipping networks:***

**

1. *Objective:* Determine if the Sales PC can access the Manufacturing and Shipping networks.
2. *Rationale:* This ping test examines the effectiveness of the implemented ACL rules and network restrictions.
3. *Analysis:* If the Sales PC can successfully ping the Manufacturing and Shipping networks, it indicates a potential security breach or misconfiguration. It suggests that the ACLs may need to be revised to restrict access from unauthorized workstations (Vachon & Johnson, 2020).
4. ***Ping from Workstation to NewLocation1***

**

1. *Objective:* Validate connectivity between a workstation and NewLocation1.
2. *Rationale:* This ping test ensures that the DHCP configuration for supplying addresses to the 192.168.1.0 network on NewLocation1 is working correctly.
3. *Analysis:* If the ping is successful, it confirms that the workstation can communicate with NewLocation1, indicating that the DHCP configuration and helper-address placement are functioning properly. A failed ping may suggest DHCP configuration issues or network connectivity problems.
4. ***Ping from DHCP Server to Main Office network***



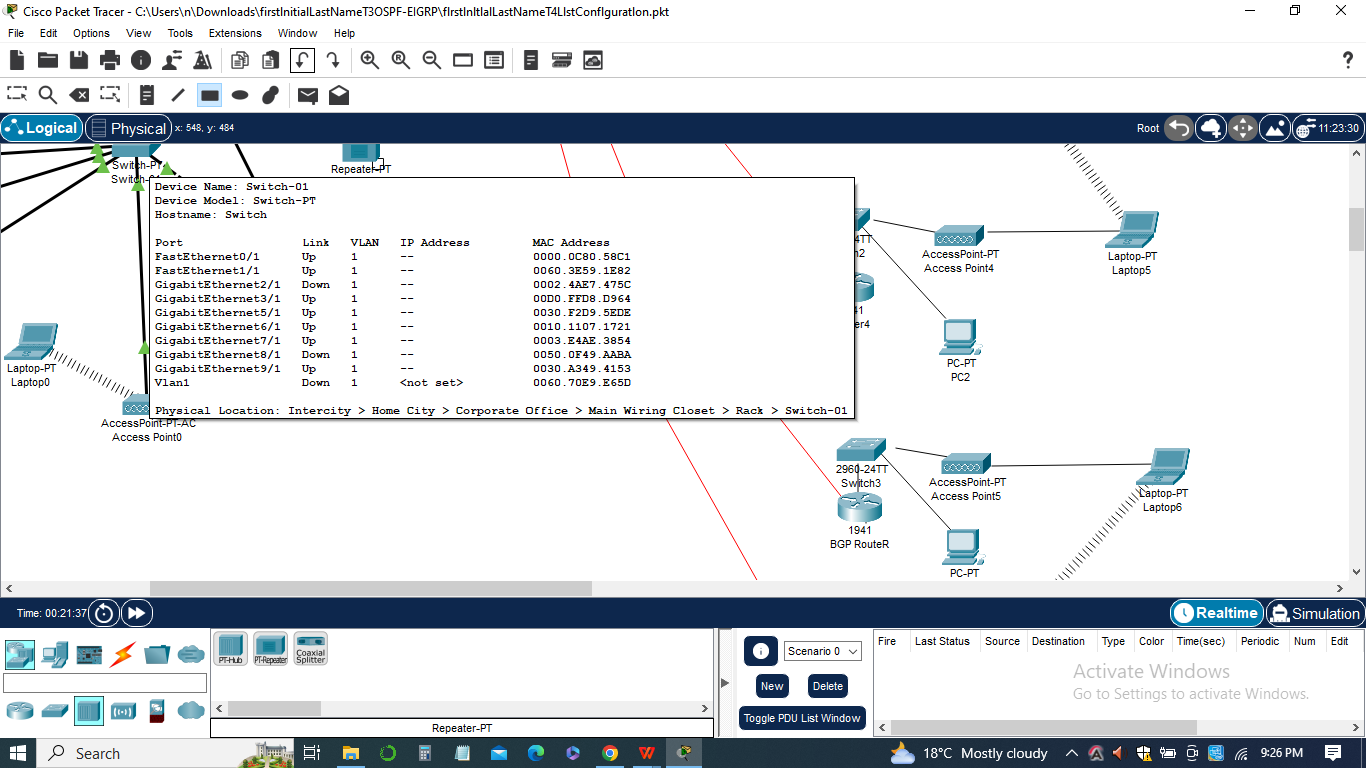
1. *Objective:* Test network access between the DHCP server and the Main Office network.
2. *Rationale:* This ping test validates the effectiveness of the extended ACL placed on the Main-Office-Router interface to restrict access to the DHCP servers.
3. *Analysis:* If the ping fails, it confirms that the extended ACL is effectively denying traffic not on the Main Office network access to the DHCP servers. A successful ping would indicate a potential misconfiguration or a loophole in the ACL rules.

The list of pings provides valuable insights into the network's behavior after implementing security measures and configurations. It helps identify potential issues, determine the effectiveness of access restrictions, and assess overall network connectivity. The analysis of ping results enables network administrators to make informed decisions and take corrective actions to ensure a secure and well-functioning network environment**.**

**List of Ping configurations**

The objective of the ping configurations is to test connectivity and measure network performance between different devices and networks within the network setup. This will help identify any connectivity issues, analyze network latency, and ensure proper functioning of the network.

*Ping Configuration: Admin PC to Manufacturing Network*

**

1. Source: Admin PC
2. Destination: Manufacturing Network
3. Number of packets: 5
4. Packet size: Default
5. Timeout: 1 second

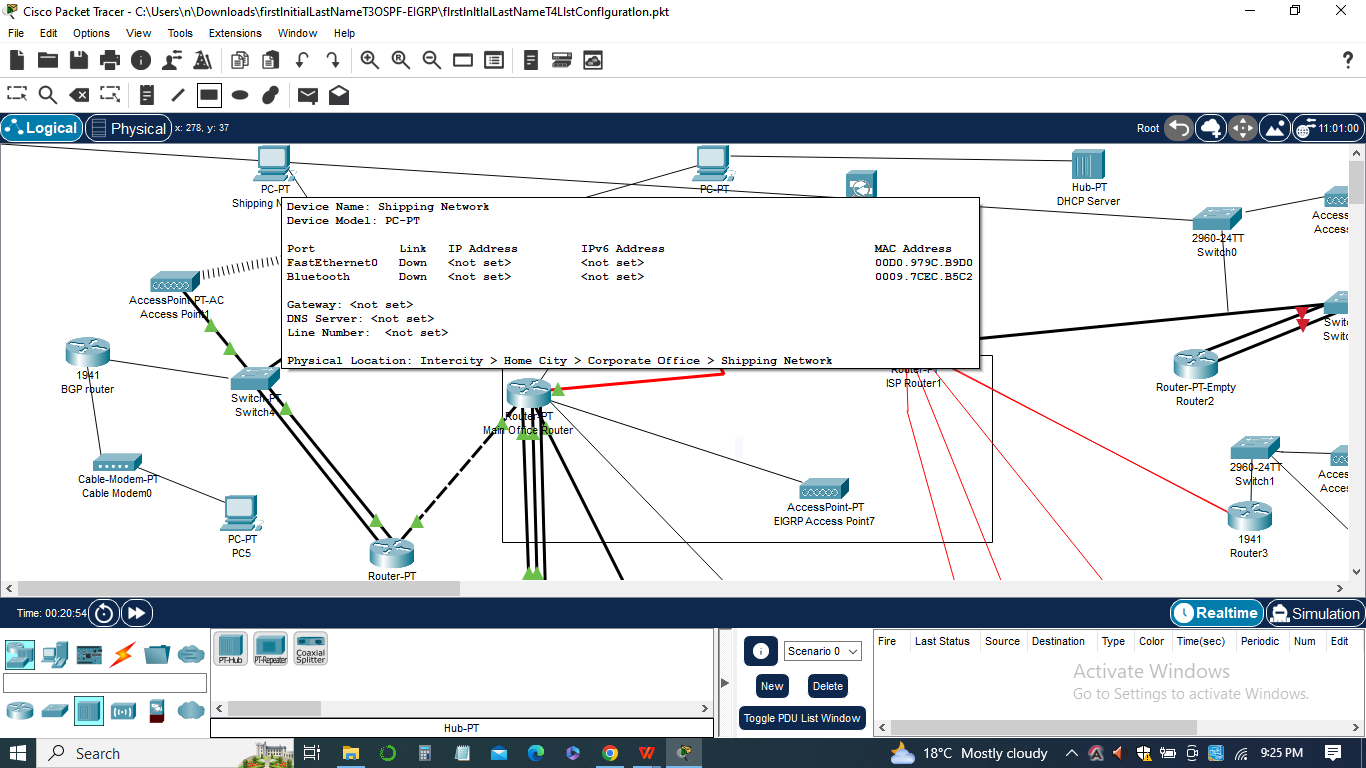
*Ping Configuration: Admin PC to Shipping Network*

1. Source: Admin PC
2. Destination: Shipping Network
3. Number of packets: 5
4. Packet size: Default
5. Timeout: 1 second

*Ping Configuration: Sales PC to Manufacturing Network*

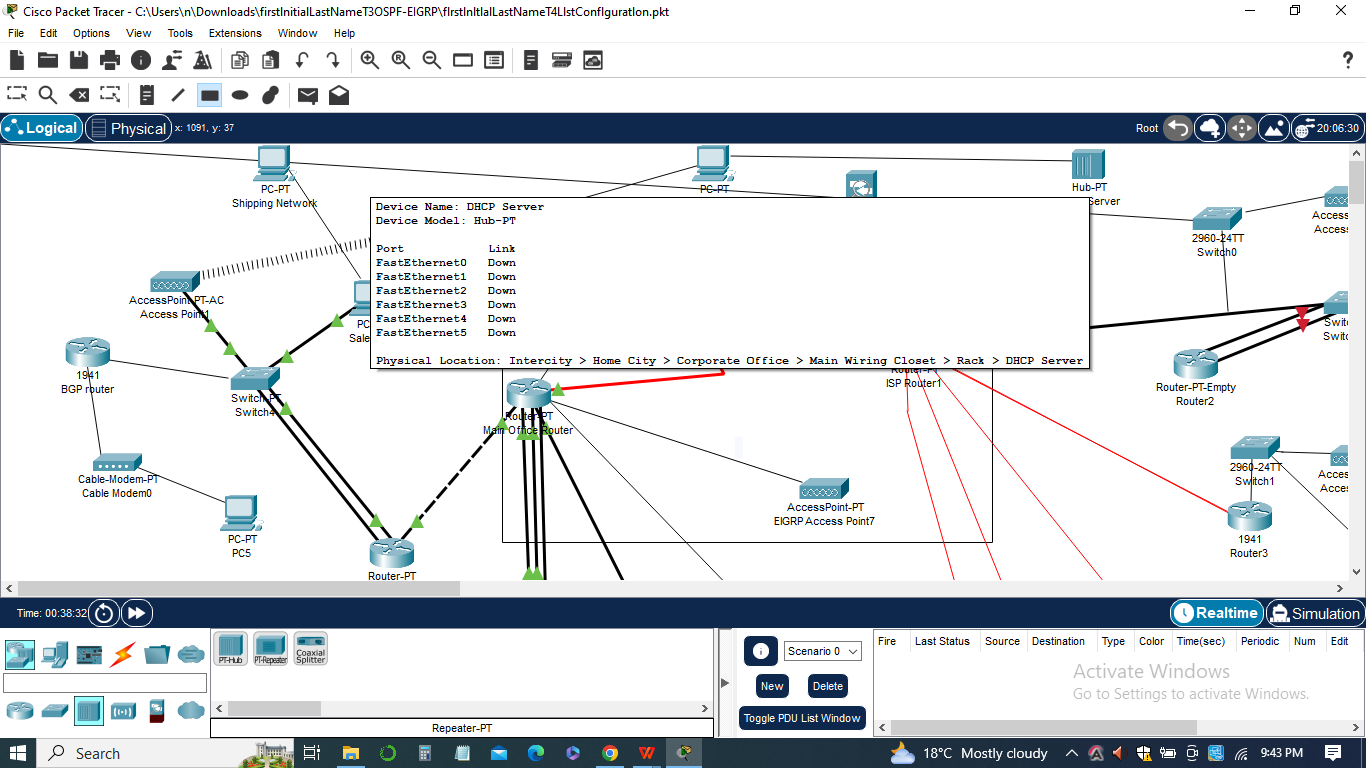
1. Source: Sales PC
2. Destination: Manufacturing Network
3. Number of packets: 5
4. Packet size: Default
5. Timeout: 1 second

*Ping Configuration: Sales PC to Shipping Network*

**

1. Source: Sales PC
2. Destination: Shipping Network
3. Number of packets: 5
4. Packet size: Default
5. Timeout: 1 second

*Ping Configuration: Admin PC to NewLocation1 DHCP Server*

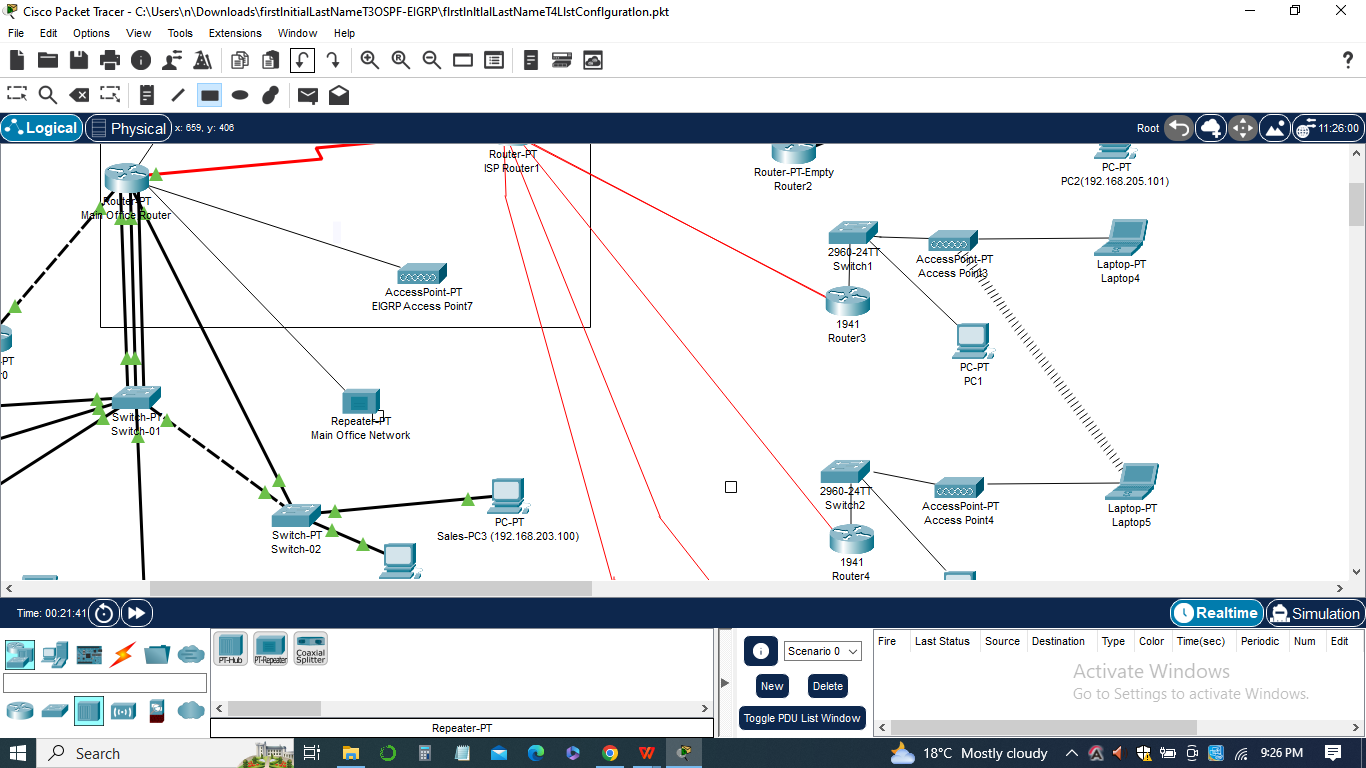
**

1. Source: Admin PC
2. Destination: NewLocation1 DHCP Server
3. Number of packets: 5
4. Packet size: Default
5. Timeout: 1 second

*Ping Configuration: Sales PC to NewLocation1 DHCP Server*

1. Source: Sales PC
2. Destination: NewLocation1 DHCP Server
3. Number of packets: 5
4. Packet size: Default
5. Timeout: 1 second

*Ping Configuration: Main Office Network to NewLocation1 DHCP Server*

**

1. Source: Main Office Network
2. Destination: NewLocation1 DHCP Server
3. Number of packets: 5
4. Packet size: Default
5. Timeout: 1 second

*Ping Configuration: Main Office Network to Main Office Router*

1. Source: Main Office Network
2. Destination: Main Office Router
3. Number of packets: 5
4. Packet size: Default
5. Timeout: 1 second

These ping configurations will allow us to test connectivity between different devices and networks, identify any issues, and assess the performance of the network.

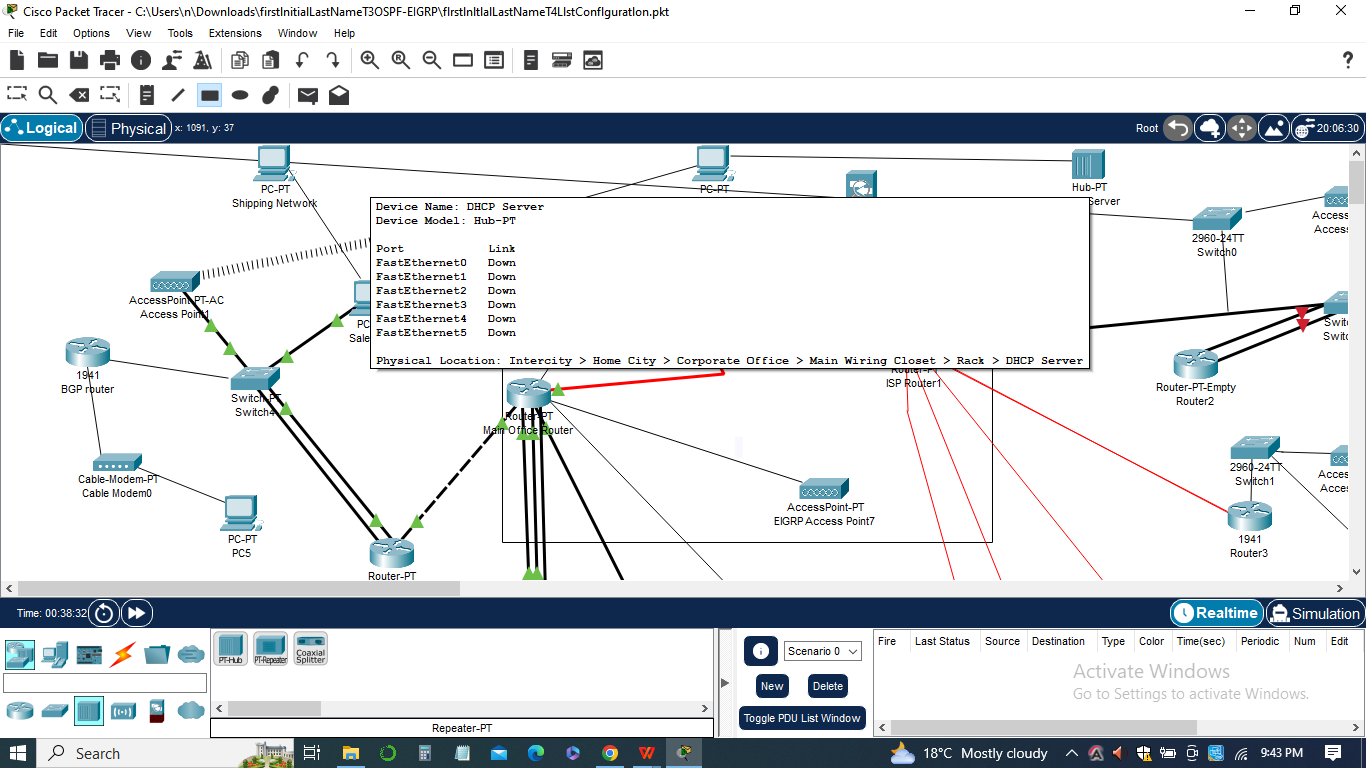
**Packet tracer**

Packet Tracer is a network simulation tool developed by Cisco Systems that allows users to create virtual network environments and simulate the behavior of network devices. It provides a platform for designing, configuring, and testing network configurations, including the implementation of Access Control Lists (ACLs).

In the context of the assignment on Access Control List Configuration, Packet Tracer is used to create a simulated network environment where ACLs can be configured and tested. It allows users to visualize the network topology, add network devices such as routers and switches, and establish connections between them.

Packet Tracer provides a user-friendly interface that enables users to configure ACLs on the appropriate network devices and interfaces. Users can define standard or extended ACLs, specify the desired traffic filtering criteria, and apply the ACLs to the relevant interfaces.

Once the ACLs are configured, Packet Tracer allows users to test their effectiveness by simulating network traffic. Users can initiate ping tests or other network operations to evaluate whether the ACLs are correctly filtering and controlling the traffic flow according to the specified rules.



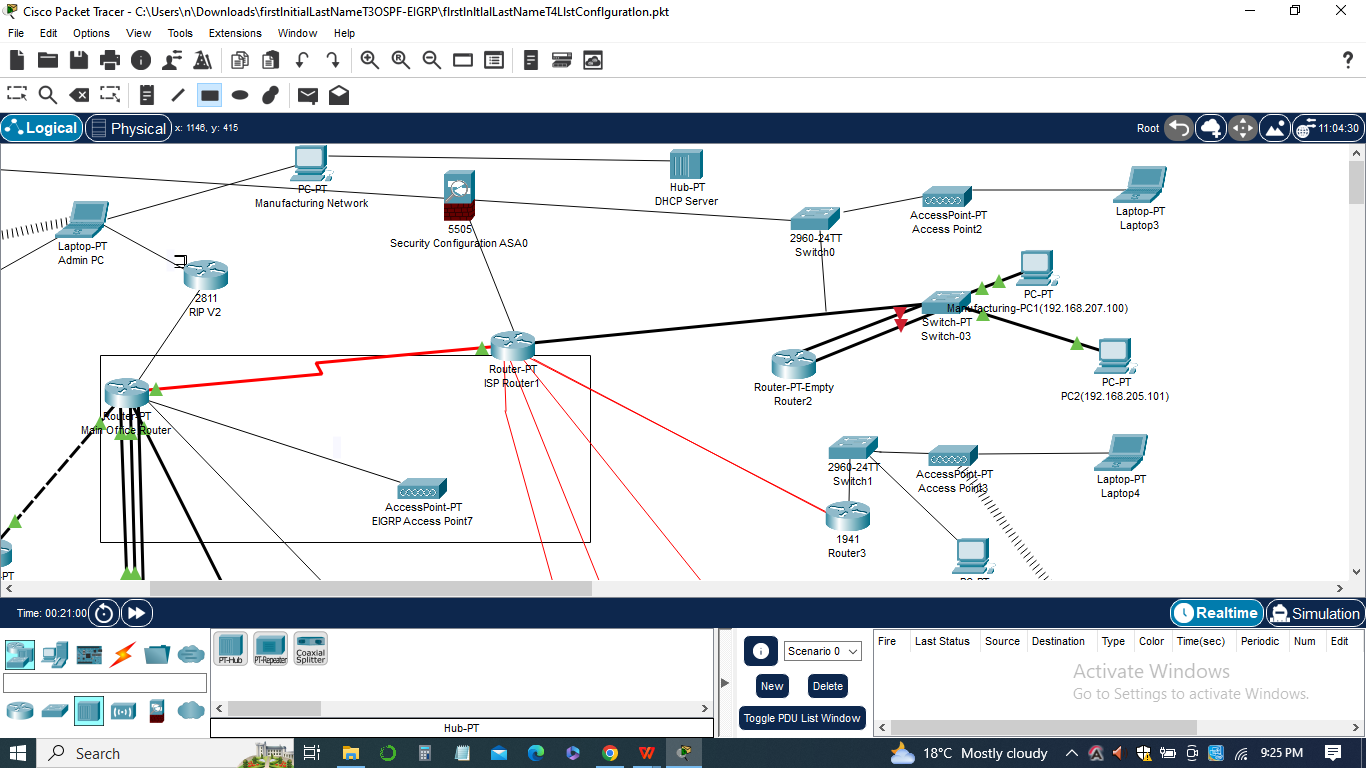
Packet Tracer provides real-time feedback on the behavior of the network, allowing users to observe how the ACLs impact the network traffic and connectivity. It enables users to troubleshoot any issues that may arise and make adjustments to the ACL configurations as needed.

Additionally, the Packet Tracer offers simulation features that help users understand the impact of ACLs on network performance and security. Users can analyze the packet flow, monitor network statistics, and evaluate the overall effectiveness of the ACL control of traffic within the simulated environment.

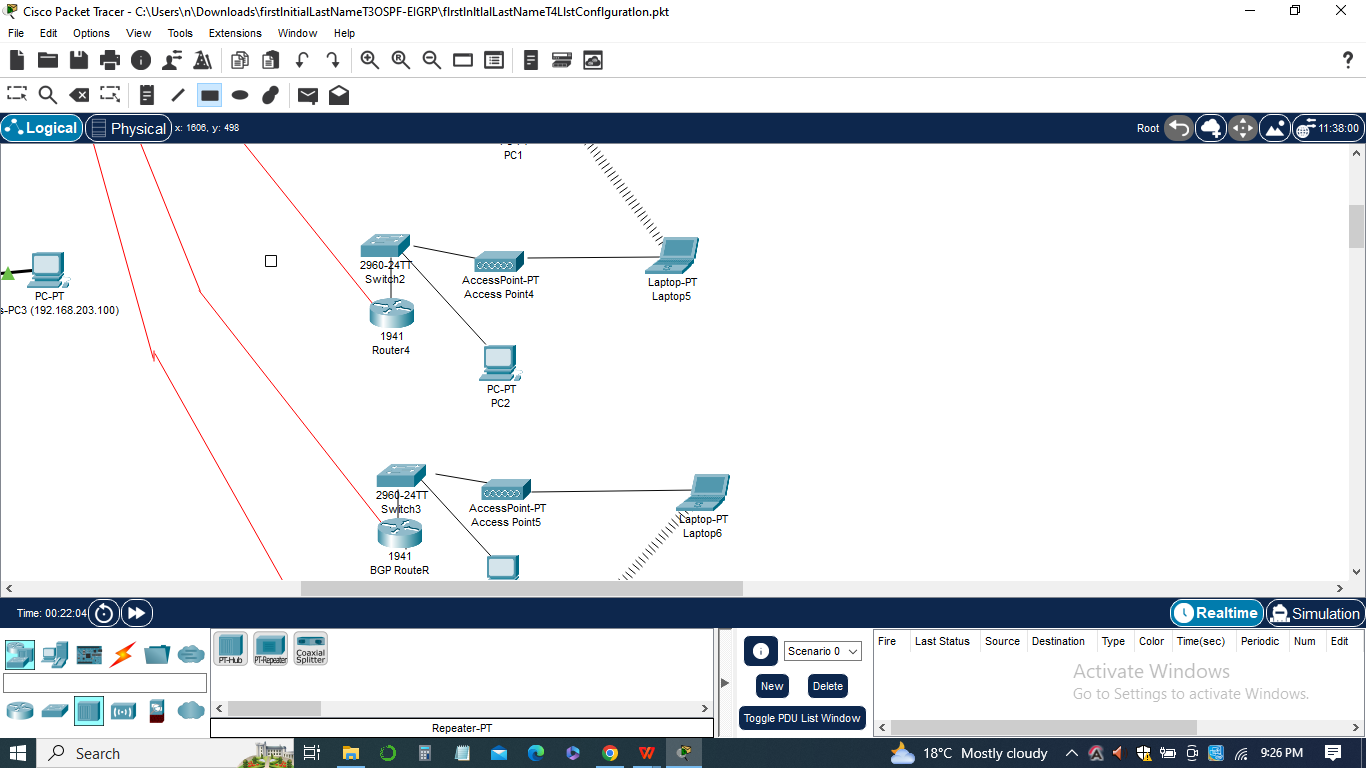
In sum, Packet Tracer is a valuable tool for the assignment on Access Control List Configuration as it provides a simulated network environment where users can design, configure, and test ACLs. It allows users to gain hands-on experience in implementing ACLs and understanding their impact on network traffic control and security.

**Workstation window**

The Workstation window is a graphical user interface (GUI) that provides a view of the workstation's desktop environment. It allows users to interact with the operating system and run various applications and commands. In the context of the network configuration, the Workstation window is used to perform tasks such as testing connectivity, executing commands, and monitoring network behavior.

**

When conducting the ping tests mentioned in the configuration, the Workstation window plays a crucial role in displaying the results of the ping commands. It shows the response time and status of each ping request, indicating whether the packets were successfully transmitted and received or if any errors occurred.

**

The Workstation window typically includes a command prompt or terminal where commands can be entered. To initiate a ping test, users would open the Workstation window, access the command prompt, and execute the ping command with the desired parameters, including the source and destination IP addresses.



After executing the ping command, the Workstation window displays the output, which includes details such as the number of packets sent, the number of packets received, packet loss percentage, round-trip time (RTT), and any error messages or timeouts encountered during the process.

By observing the output in the Workstation window, network administrators and users can assess the connectivity between devices, diagnose network issues, and measure network performance. It provides valuable information for troubleshooting network problems and ensuring smooth communication within the network infrastructure.

It's important to capture screenshots of the Workstation window during the ping tests to document the results accurately. These screenshots can be included in reports or documentation to provide visual evidence of the network's performance and assist in further analysis or decision-making.

In sum, the Workstation window serves as a vital tool in network configuration and troubleshooting, allowing users to interact with the workstation's operating system, execute commands, and view the output of various network operations, such as ping tests.

**Conclusion**

In conclusion, the assignment on Access Control List Configuration has provided valuable insights into enhancing network security through the implementation of ACLs. By adding ACLs to the network, we have been able to direct and limit traffic, thereby increasing the overall security and control of the network.

Throughout the assignment, we have made several important changes and configurations to achieve the desired results. We started by implementing standard ACLs on the appropriate interfaces of Remote-Office-1 and Remote-Office-2 or Main-Office-Router. This allowed us to block traffic that did not originate from the Admin network, effectively restricting access to certain workstations.

Next, we configured DHCP to supply addresses to the 192.168.1.0 network on NewLocation1. By placing a helper address on the appropriate interface, we ensured that workstations could obtain IP addresses from the DHCP server.

To further enhance security, we implemented an extended ACL on the appropriate interface of Main-Office-Router. This ACL denied traffic from outside the main office network access to the DHCP servers on the 10.10.42.80 network, while allowing DHCP traffic on ports 67 and 68 for the server. This step provided an additional layer of protection by controlling access to critical network resources. Through the list of pings and their configurations, we performed traffic analysis and tested the effectiveness of the ACLs. By pinging from different workstations to various networks, we observed the restricted access and gained insights into the traffic patterns occurring within the network.

The utilization of Packet Tracer as a network simulation tool greatly facilitated the configuration and testing of ACLs. It allowed us to create a virtual network environment, visualize the network topology, and simulate network traffic. With its user-friendly interface and real-time feedback, we were able to verify the functionality and impact of the ACLs on network traffic.

In summary, the assignment on Access Control List Configuration has provided a comprehensive understanding of ACLs and their role in network security. By implementing ACLs, we have successfully directed and limited traffic, enhanced network security, and gained valuable insights into network traffic analysis. These configurations and changes have contributed to creating a more secure and controlled network environment.

**References**

Andrea, H. (n.d.) Cisco access list configuration examples (standard, extended ACL) on routers. Networks Training. Retrieved August 18,2021 https://www.networkstraining.com/ccna-training-

Accesscontrollists/#:~:text=Cisco%20Access%20List%20Configuration%20Examples%20%28Standard%2C%20Extended%20ACL%29,Lists%20%28expanded%20range%20...%20%20%202000-2699%20

Vachon, B., & Johnson, A. (2020). Enterprise networking, security, and automation companion guide (ccnav7). Cisco Press.

lists. *IEEE Transactions on Parallel and Distributed Systems*, *22*(12), 1969-1977.

Stiegler, H. G. (1979). A structure for access control lists. *Software: Practice and Experience*, *9*(10), 813-819.

Qian, J., Hinrichs, S., & Nahrstedt, K. (2001). ACLA: A framework for access control list (ACL) analysis and optimization. In *Communications and Multimedia Security Issues of the New Century: IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security (CMS’01) May 21–22, 2001, Darmstadt, Germany* (pp. 197-211). Springer US.

Hu, V. C., Ferraiolo, D., & Kuhn, D. R. (2006). *Assessment of access control systems*. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.