**Limiting VLANs**

Student’s Name

Professor Name

University Affiliation

Course Number

Date

**Limiting VLANs**

**Introduction**

This assignment focuses on strengthening network security by implementing VLAN restrictions and reorganizing workstations for improved protection. With the addition of five new locations to the network infrastructure, security becomes a crucial concern. This assignment builds upon the previous assignment, "Adding New Locations to Network," and introduces additional security measures to ensure data integrity and prevent unauthorized access.

In this assignment, we will review the existing VLANs and trunking configurations to modify them according to the new security requirements. The goal is to restrict the transmission of VLANs across trunks and allow only specific VLANs to communicate with designated switches. By implementing these VLAN restrictions, we can isolate network segments and enhance network security.

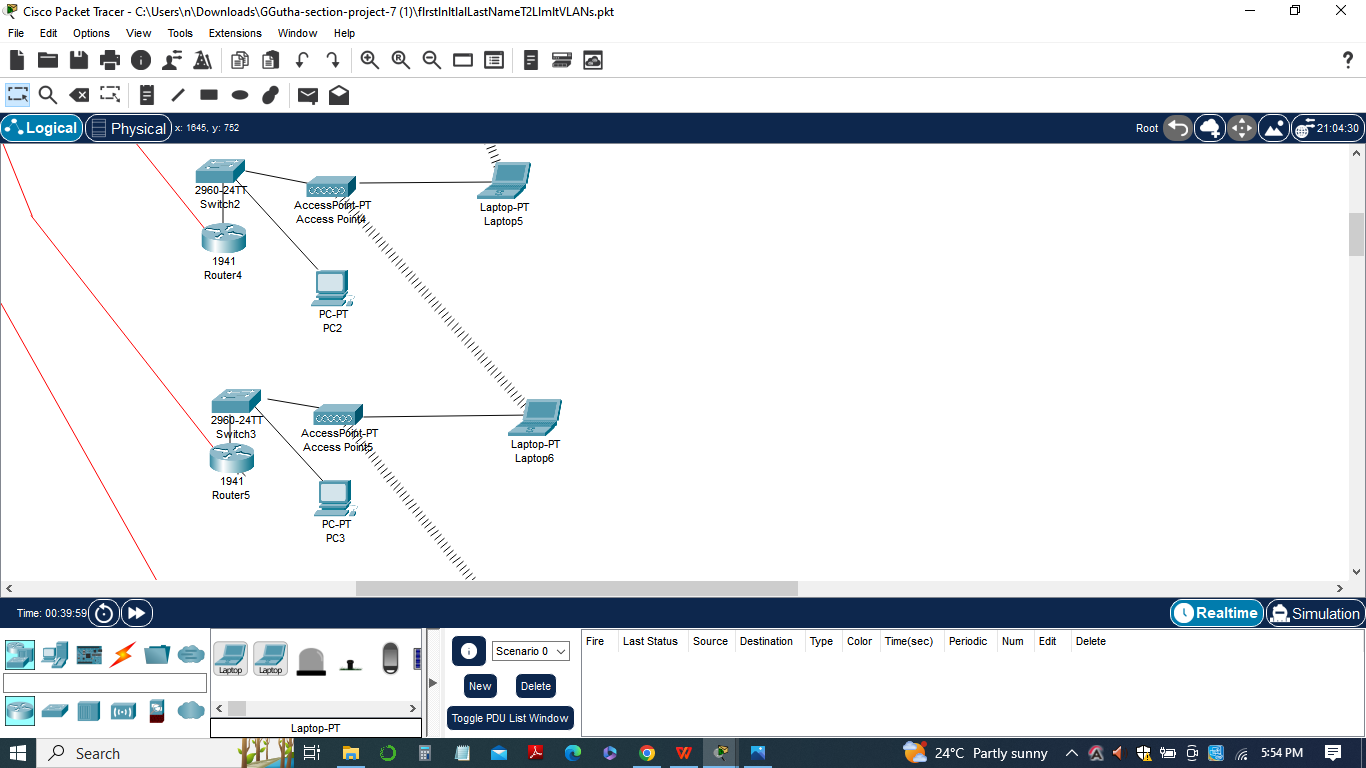
Additionally, the assignment requires us to reorganize workstations to enhance security further. Specific workstations may need to be moved or grouped together to enforce tighter control over access and communication. This reorganization will contribute to the overall security posture of the network and mitigate potential vulnerabilities.

To ensure the effectiveness of the security measures implemented, thorough testing and documentation are essential. We will conduct comprehensive tests, including ping tests from designated workstations, to verify the successful implementation of VLAN restrictions and workstation reorganization. The results of these tests will be documented and presented along with the network configurations in a Word document.

By completing the assignment, we will gain practical experience in securing network infrastructure through VLAN restrictions and workstation reorganization. This will contribute to our understanding of network security principles and best practices in a real-world scenario.

**List of Pings**

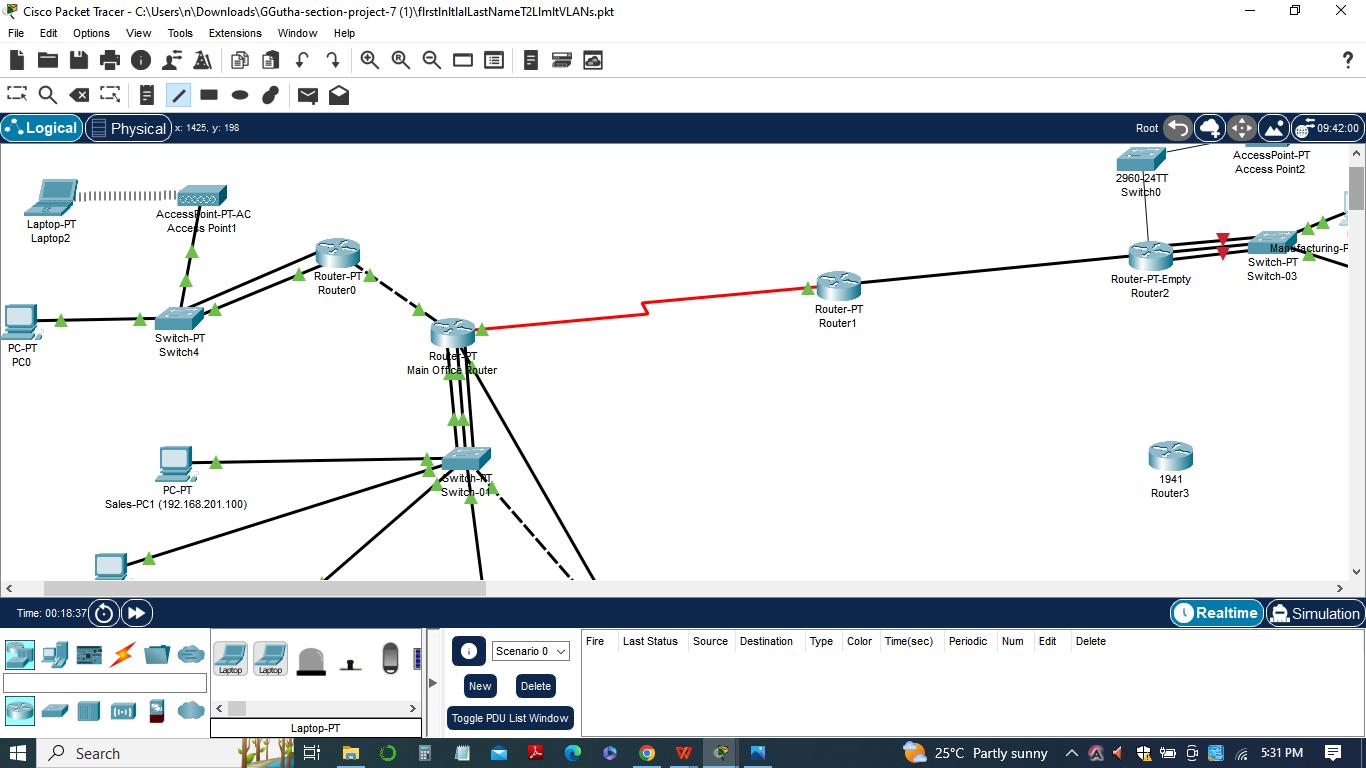
The list of pings in this assignment serves as a critical part of the testing process to validate the effectiveness of VLAN restrictions and network segmentation. By conducting pings from designated workstations to various ports across the network, we can assess whether the VLAN restrictions are functioning as intended and if the network segments are properly isolated.



The pings should be performed from the Sales workstation on Switch-01 in the main location to each port of the new locations, including remote locations 1 and 2. The objective is to determine if the pings are successful or if there are any failures, which may indicate that the VLAN restrictions are working as expected. The list of ping configurations for the assignment, is considered by the network topology and the specific ports and VLANs involved. Here is the list of ping configurations:

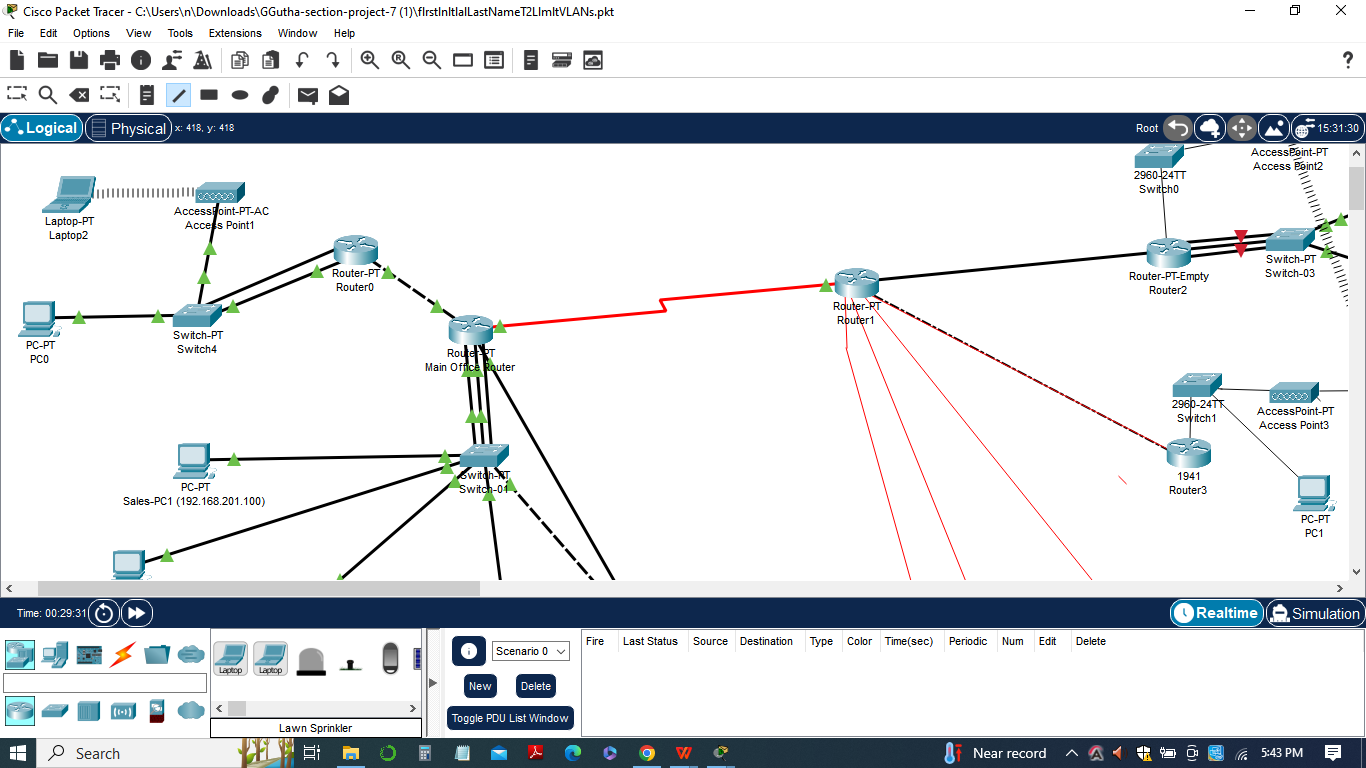
*Ping from Sales workstation on Switch-01 to each port of the new locations:*

1. Sales workstation on Switch-01 -> Port 0/1 on Switch-02
2. Sales workstation on Switch-01 -> Port 0/2 on Switch-02
3. Sales workstation on Switch-01 -> Port 0/3 on Switch-02
4. Sales workstation on Switch-01 -> Port 0/1 on Switch-04
5. Sales workstation on Switch-01 -> Port 0/2 on Switch-04



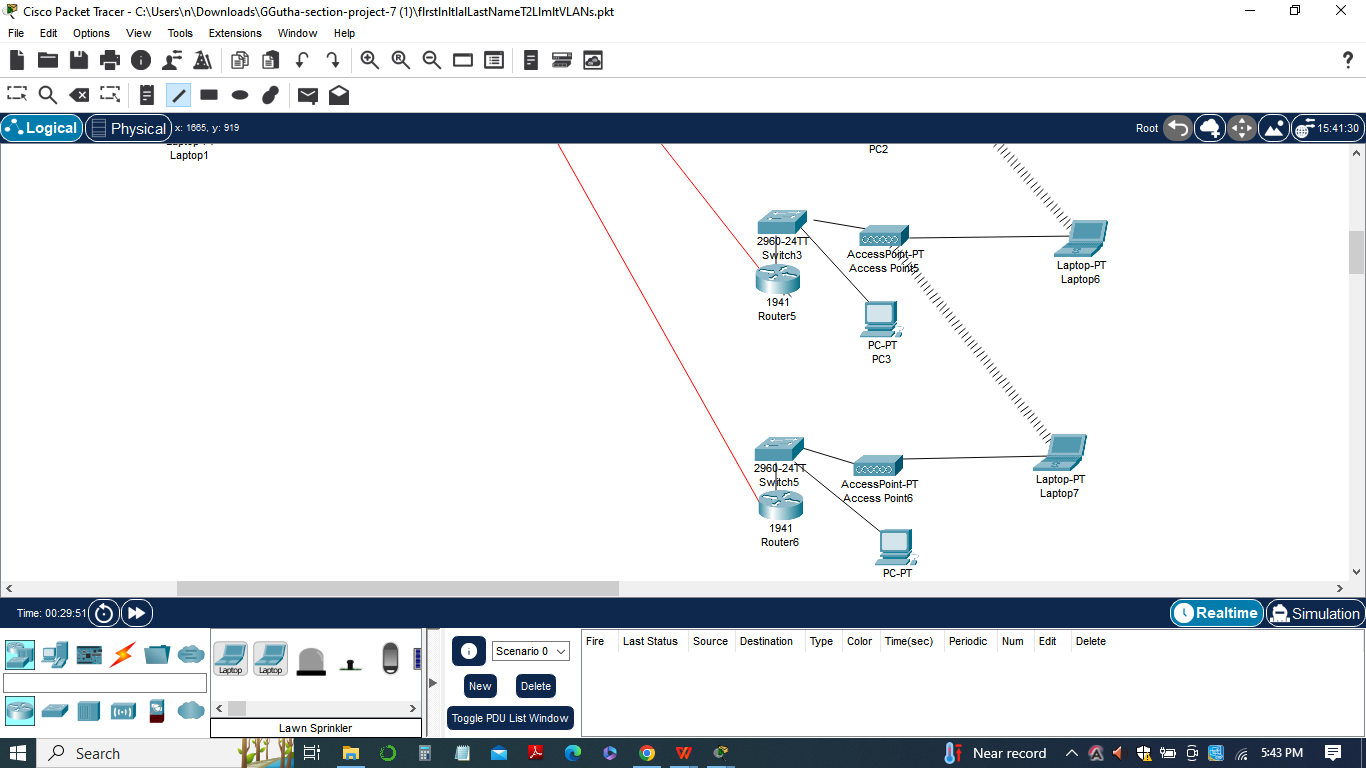
*Ping from Sales workstation on Switch-01 to remote location 1:*

1. Sales workstation on Switch-01 -> Port 0/0 on Router 1



*Ping from Sales workstation on Switch-01 to remote location 2:*

1. Sales workstation on Switch-01 -> Port 0/0 on Router 2



During the pinging process, it was important to note that not all pings are expected to succeed. The intentional failures indicate that VLANs are properly secured and isolated from each other, ensuring data confidentiality and network segmentation.

Additionally, it was important to note that not all pings are expected to succeed. Some pings may intentionally fail as part of the VLAN restrictions and network segmentation. By following the list of ping configurations and documenting the results, we had comprehensive overview of the connectivity and security of the network segments in the assignment.

By documenting the results of the pings, including both successful and failed responses, we can provide evidence of the successful implementation of VLAN restrictions and network segmentation. This documentation helps validate the security measures implemented and provides valuable insights into the network's overall security posture.

**Configurations**

In the assignment, the configurations revolve around implementing VLAN restrictions and reorganizing workstations to enhance network security. Here is an overview of the configurations involved:

***Review VLANs and trunking configurations:***

1. Assess the existing VLANs and trunking configurations in the network.
2. Identify the changes required to restrict VLAN transmission and improve security.

***Restrict VLAN 20 access to Switch-03:***

1. Modify the trunk port configuration connected to Switch-03.
2. Allow only VLAN 20 (server farm VLAN) to be transmitted on that trunk.
3. This restricts access to Switch-03 only to devices in VLAN 20, enhancing security.

***Allow only VLAN 1 on Switch-02:***

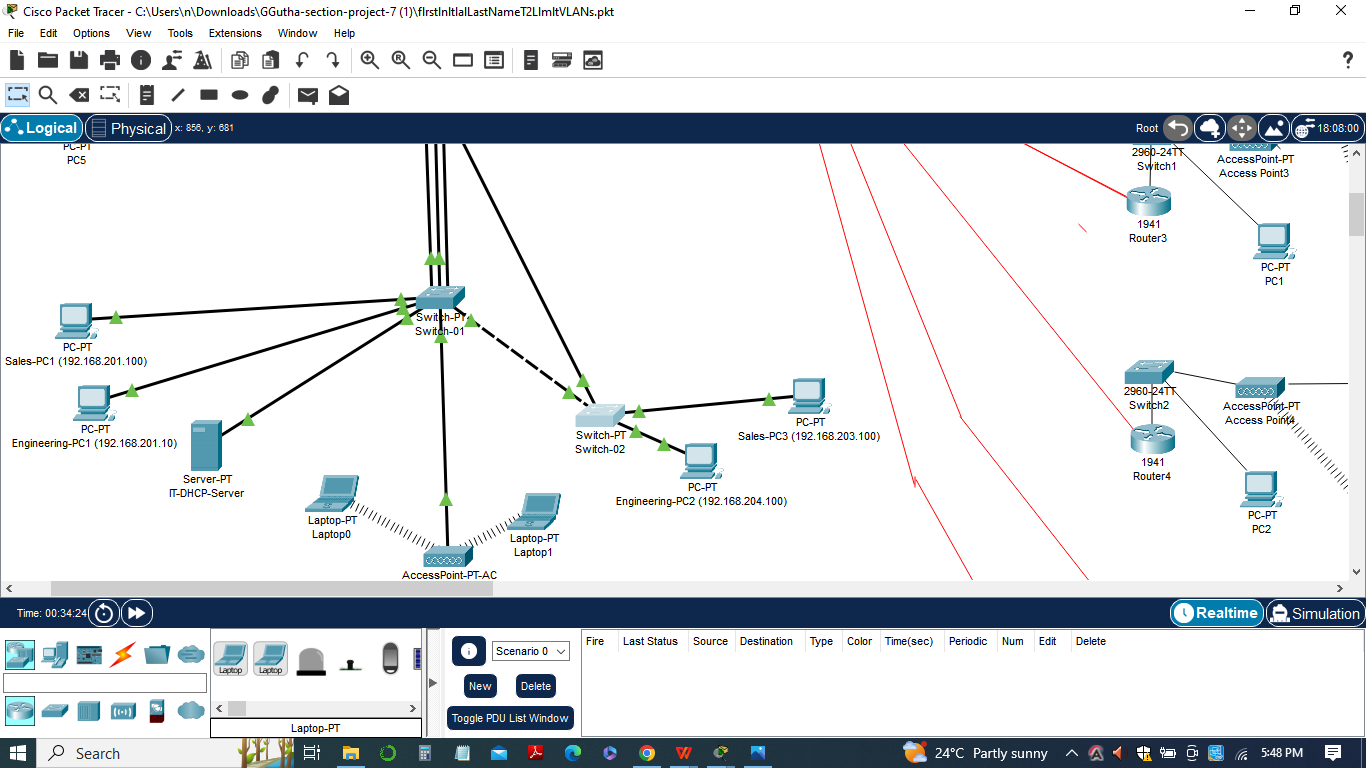
1. Modify the trunk port configuration connected to Switch-02.
2. Configure it to allow only VLAN 1 (Admin VLAN) to be transmitted on that trunk.
3. This isolates Switch-02 to communicate only with devices in VLAN 1, enforcing stricter security measures.

***Move workstations from Switch-02 to Switch-01:***

1. Reorganize the workstations on Switch-02 by moving them to Switch-01.
2. Configure the necessary ports on Switch-01 to accommodate the relocated workstations.
3. Ensure that all workstations on Switch-01, except for the Engineering VLAN, are allowed to communicate.

***Move Engineering VLAN to Switch-04:***

1. Create a new switch, Switch-04, to house the Engineering VLAN.



1. Configure the necessary ports on Switch-04 to connect the Engineering workstations.
2. Restrict access to Switch-04 to only devices in the Engineering VLAN, enhancing security.

***Restrict remote locations to respective VLANs:***

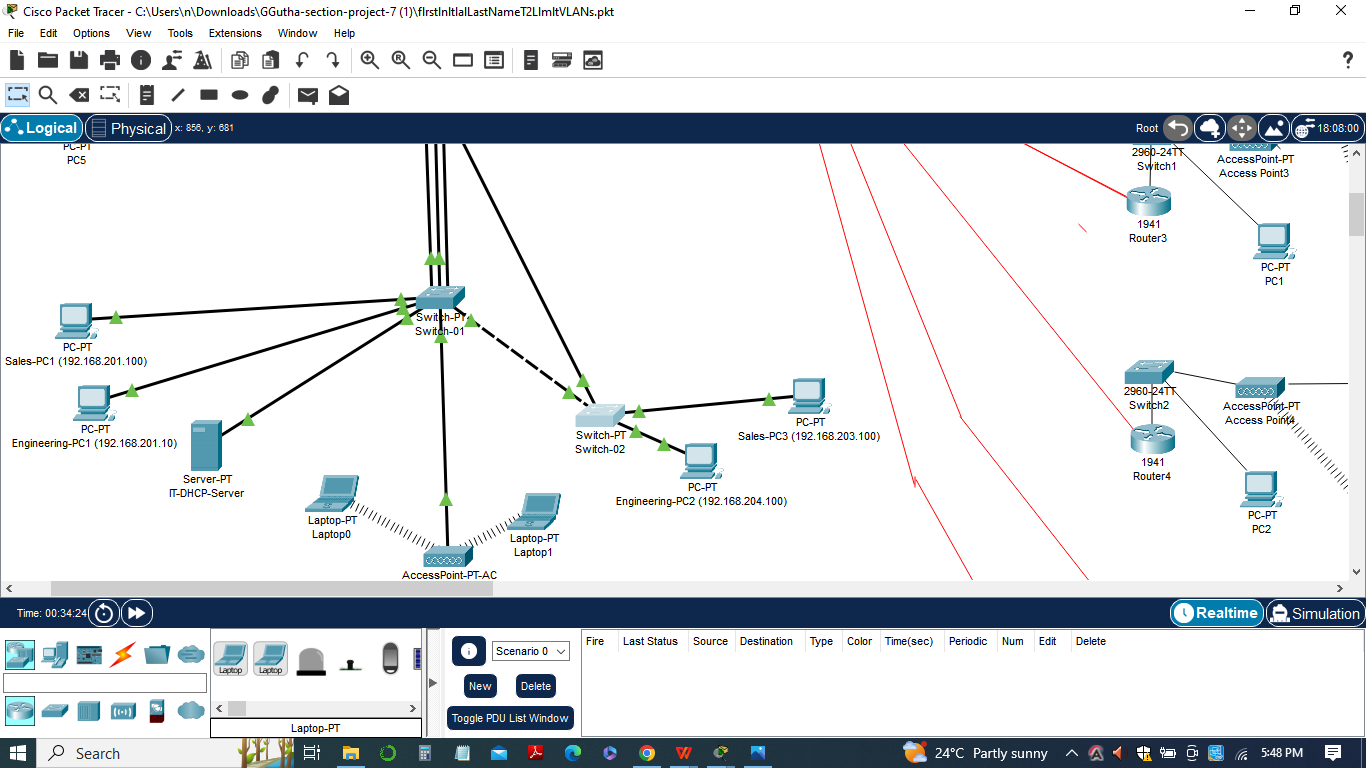
1. Configure the remote locations' routers (Router 1 and Router 2) to restrict access to their respective VLANs.
2. Ensure that each remote location can only communicate within its designated VLAN, preventing unauthorized access.

By implementing these configurations, the network's security posture is significantly enhanced. VLAN restrictions limit communication between VLANs, preventing unauthorized access and data leakage. Workstation reorganization ensures that devices are grouped based on security requirements, further isolating sensitive data and reducing potential vulnerabilities.

Documenting all the configuration changes made, including the specific commands and modifications to each device (switches, routers). Including these configurations in the Word document along with an explanation of the rationale behind each change to provided a comprehensive overview for management.

**Workstation pings**

The workstation window pings play a crucial role in verifying the connectivity and effectiveness of the network configurations implemented in the flrstlnltlalLastNameT2LlmltVLANs assignment. These pings help determine if the VLAN restrictions and network segmentation are functioning as intended and if the security measures are successfully enforced.



During the assignment, the pings are performed from the Sales workstation on Switch-01 to various ports and locations within the network. The purpose of these pings is to test the reachability and accessibility of different network segments and to observe the expected behavior based on the implemented VLAN restrictions.

The results of the pings can be categorized into two outcomes: successful pings and intentional failures.

***1)Successful Pings:***

These are pings that successfully reach their destination within the network.

Successful pings indicate that the VLAN restrictions and network configurations allow communication between the appropriate devices and VLANs.

They validate that the necessary access and connectivity are maintained within the designated network segments.

1. ***Intentional Failures:***

These are pings that intentionally fail as part of the VLAN restrictions and network segmentation.

Intentional failures demonstrate the effectiveness of the implemented security measures.

They show that the VLAN restrictions prevent unauthorized access and communication between different network segments.

Intentional failures confirm that the network is properly segmented and that devices in one VLAN cannot reach devices in other restricted VLANs.

By documenting the results of the workstation window pings and capturing screenshots of the ping outputs, you can provide visual evidence of the network's connectivity and security. These ping results, along with explanations of successful pings and intentional failures, should be included in the Word document as part of the documentation and test report.

The workstation window pings help validate the success of the VLAN restrictions and provide assurance to management that the network is secure, with restricted communication between different VLANs as intended.

**Conclusion**

In conclusion, the flrstlnltlalLastNameT2LlmltVLANs assignment focused on enhancing network security through VLAN restrictions and workstation reorganization. By implementing these configurations, the network's security posture has been significantly strengthened, ensuring that communication is limited to authorized devices and VLANs.

Throughout the assignment, various configurations were made to restrict VLAN transmission, isolate VLANs to specific switches, and enforce security measures at remote locations. These changes were thoroughly tested using workstation window pings, which verified the success of the implemented VLAN restrictions and network segmentation.

The workstation window pings demonstrated that communication was only allowed between the appropriate VLANs and devices, validating the effectiveness of the security measures. Successful pings confirmed that devices within a VLAN could communicate as intended, while intentional failures highlighted the restricted access and prevention of unauthorized communication between VLANs.

By documenting all the configuration changes, including the rationale behind each change, and providing a comprehensive test report with the list of pings, ping results, and network screenshots, a clear overview of the implemented security enhancements has been presented to management.

The successful completion of the flrstlnltlalLastNameT2LlmltVLANs assignment showcases the ability to implement VLAN restrictions, improve network segmentation, and enhance network security. These measures are vital in safeguarding sensitive data, preventing unauthorized access, and reducing potential vulnerabilities within the network infrastructure.In sum, the assignment demonstrates the commitment to network security and the ability to implement effective measures to protect the organization's assets and maintain the integrity of the network. The documented changes and test report provide valuable insights for management to assess the network's security posture and make informed decisions regarding future network improvements.