**Port Security Configuration**

Student’s Name

Professor Name

University Affiliation

Course Number

Date

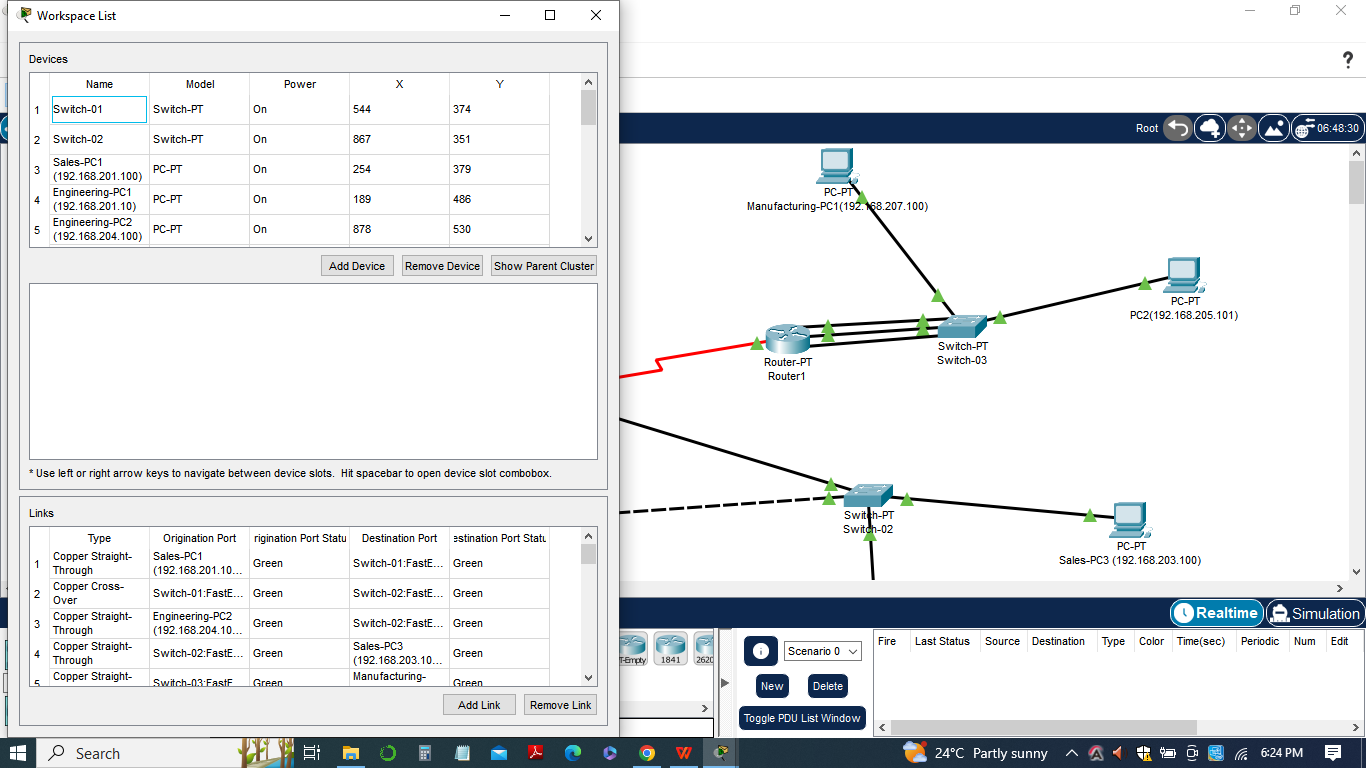
**Port Security Configuration**

**Introduction**

The port Security Configurationassignment focuses on implementing port security configurations to enhance network security and control access to network devices. In today's digital landscape, where data breaches and unauthorized access pose significant risks, it is crucial for organizations to implement robust security measures to protect their networks and sensitive information. This assignment builds upon the previous network configurations and introduces the concept of port security. Port security enables administrators to define and enforce restrictions on the number of devices and their identities that can connect to specific ports on network devices such as switches and routers. By limiting the number of authorized devices and monitoring their MAC addresses, organizations can prevent unauthorized access and mitigate the risk of network breaches. Throughout this assignment, we will explore various scenarios to evaluate the effectiveness of port security configurations. We will simulate scenarios such as changing MAC addresses on computers within different VLANs, adding workstations to specific access point VLANs, and conducting ping tests to assess network connectivity. The primary objective of this assignment is to assess the impact of port security measures on network functionality and understand how these configurations enhance network security. By documenting the changes made, rationales behind the configurations, and test results, we will provide a comprehensive summary for management to understand the significance of port security and make informed decisions regarding network security enhancements. By successfully completing this assignment, we will gain practical knowledge and insights into port security configurations, their implications on network operations, and their role in strengthening overall network security. Let us proceed with the assignment, evaluate the test scenarios, and provide management with valuable information to ensure the continued security of our network infrastructure.

**Management summary**

The assignment focused on implementing port security measures to enhance network security and control access to network devices. The rationale behind each change made during the assignment was to strengthen the overall security posture of the network infrastructure and mitigate the risks associated with unauthorized access and data breaches.



1. Configuration of Access Point Ports: The access point ports were configured with a maximum number of addresses set to 4. This limitation ensures that only a specified number of devices can connect to these ports. By restricting the number of devices, the organization can prevent unauthorized access and mitigate the risk of rogue devices infiltrating the network.
2. *Change of MAC Address on Admin VLAN Computer:* By changing the MAC address of a computer on the Admin VLAN, we simulated the replacement of the computer and observed its impact. In this scenario, the computer stopped working due to the port security measures in place. This outcome aligns with the intended purpose of port security, as it prevents unauthorized devices from accessing the network. To restore functionality, the administrator needs to update the MAC address on the port's allowed device list.
3. *Change of MAC Address on a Computer in Another VLAN:* Similar to the previous scenario, changing the MAC address of a computer in another VLAN resulted in different outcomes. If the port remained up after the MAC address change, it allowed the computer to connect to the network. However, when attempting to ping from the workstation, the communication failed. This behavior demonstrates the effectiveness of port security in controlling network access based on VLANs
4. *Adding Workstations to Access Point VLAN:* The assignment involved adding four workstations to the Main-Router access point VLAN. Upon conducting ping tests from each workstation, different outcomes were observed. Some workstations successfully communicated, while others failed to establish a connection. This outcome reinforces the significance of port security in managing device access and preventing unauthorized devices from joining specific VLANs.

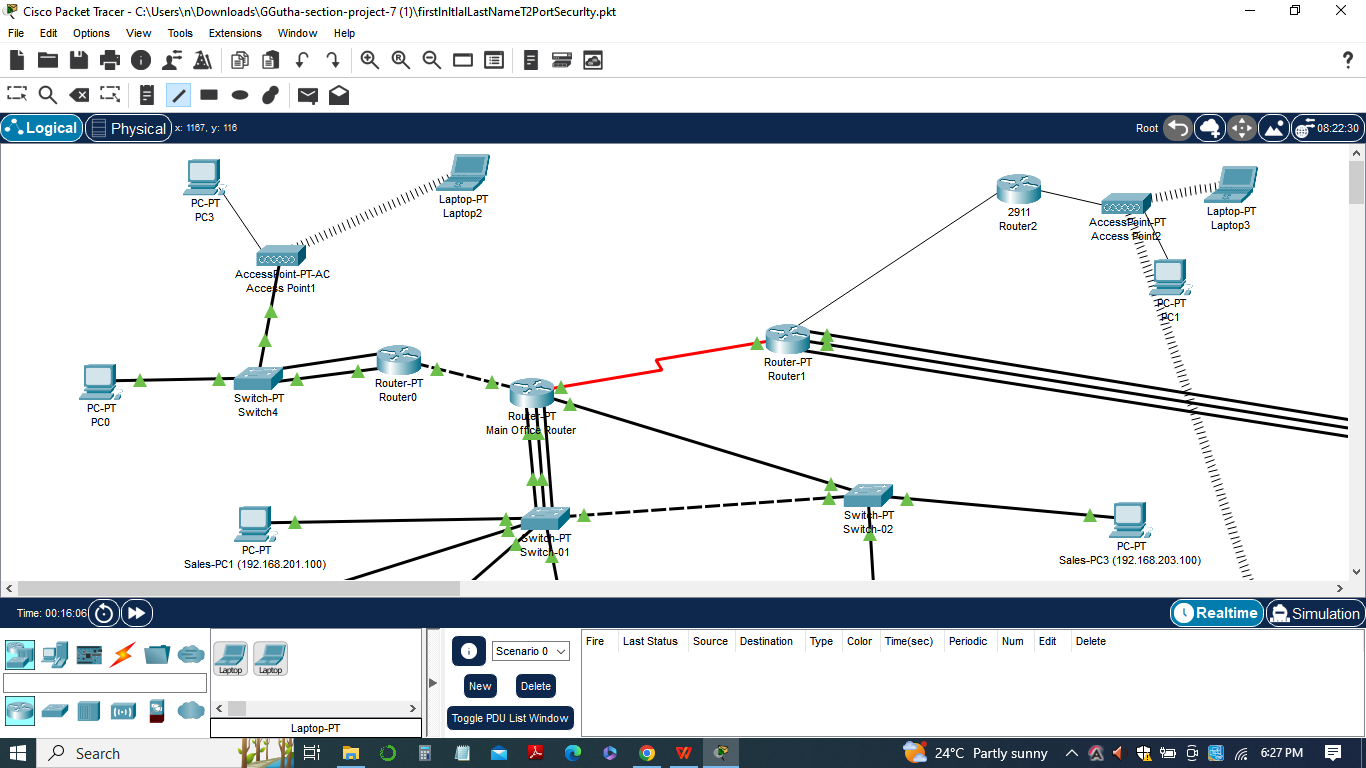
In sum, the implementation of port security measures provides several significant benefits such as:

1. Enhanced Network Security: Port security mitigates the risk of unauthorized access and strengthens the overall security posture of the network. By limiting the number of devices and monitoring MAC addresses, the organization can prevent unauthorized devices from connecting to network ports and protect against potential threats.
2. Control and Access Management: Port security enables organizations to have granular control over device access to specific ports and VLANs. It allows administrators to define and enforce access policies, ensuring that only authorized devices are granted access to critical network resources.
3. Preventing Rogue Devices: Port security measures help mitigate the risk of rogue devices infiltrating the network. By restricting the number of allowed devices and monitoring MAC addresses, organizations can detect and prevent unauthorized devices from connecting, reducing the potential for malicious activities and unauthorized data access.
4. Compliance and Auditing: Implementing port security measures aligns with industry best practices and regulatory requirements. It demonstrates a proactive approach to network security and provides an audit trail for device connections and access, aiding in compliance with data protection regulations. The list of pings, configurations, and workstation window descriptions, along with the Packet Tracer network, provides a comprehensive overview of the implemented changes and their impact on network connectivity. These details offer valuable insights into the effectiveness of the port security configurations and demonstrate the improved security and control achieved through these measures.

In conclusion, this assignment highlights the importance of port security in strengthening network security and controlling device access. The implementation of port security measures, as described in the management summary, significantly enhances the organization's ability to prevent unauthorized access and protect sensitive information. By documenting the changes made, explaining the rationales behind the configurations, and providing test results, management gains valuable insights into the significance and benefits of implementing port security measures in the network infrastructure.

**List of pings**

In the Port Security Configuration assignment, a list of pings was conducted to test the network connectivity and the impact of the port security configurations. The pings were performed from a workstation on Switch-01 in the main location to each of the ports in different locations. The results of these pings provide insights into the effectiveness of the port security measures implemented.



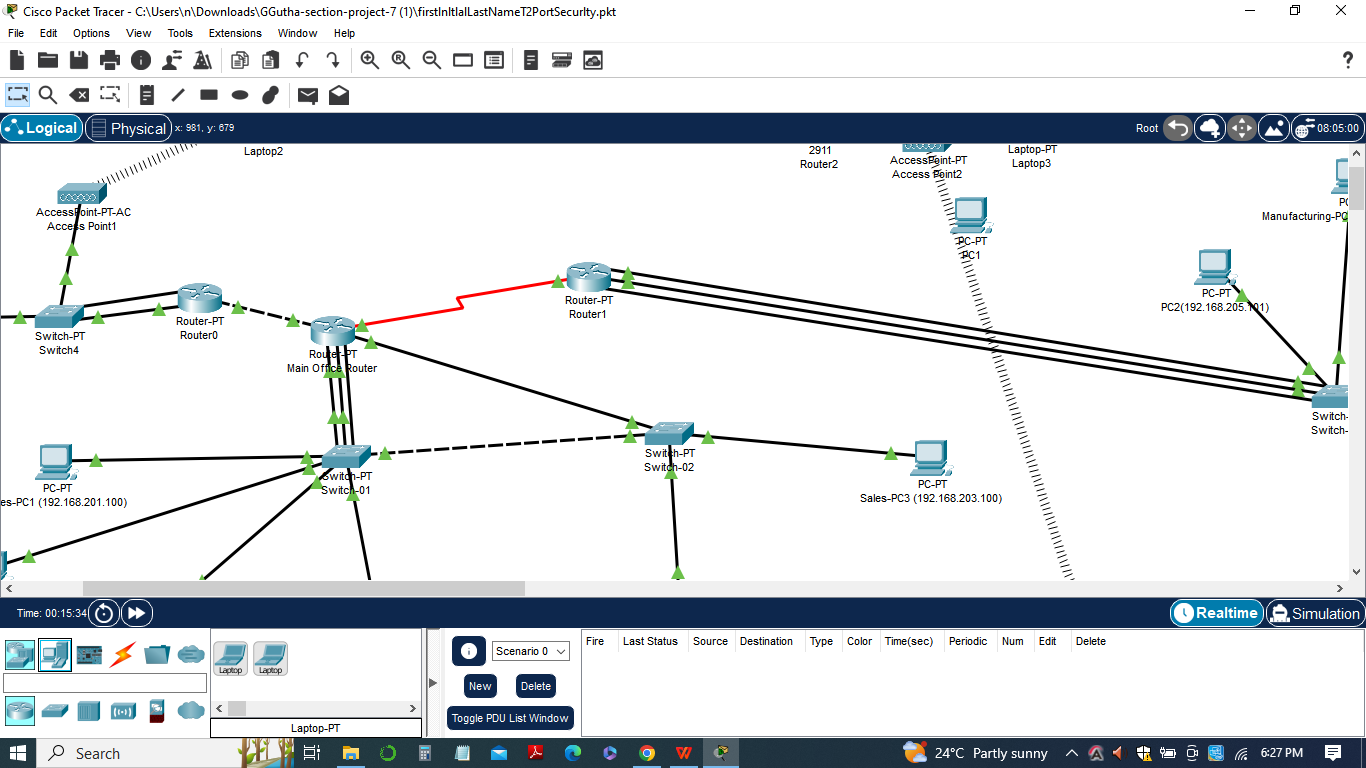
The configurations made in the assignment aimed to enforce port security and control access to network devices. The specific configurations included setting a maximum number of addresses for access point ports and implementing MAC address-based restrictions. These configurations were intended to limit the number of devices that can connect to the ports and ensure that only authorized devices are allowed access.

During the pinging process, various outcomes were observed, indicating the impact of the port security configurations:

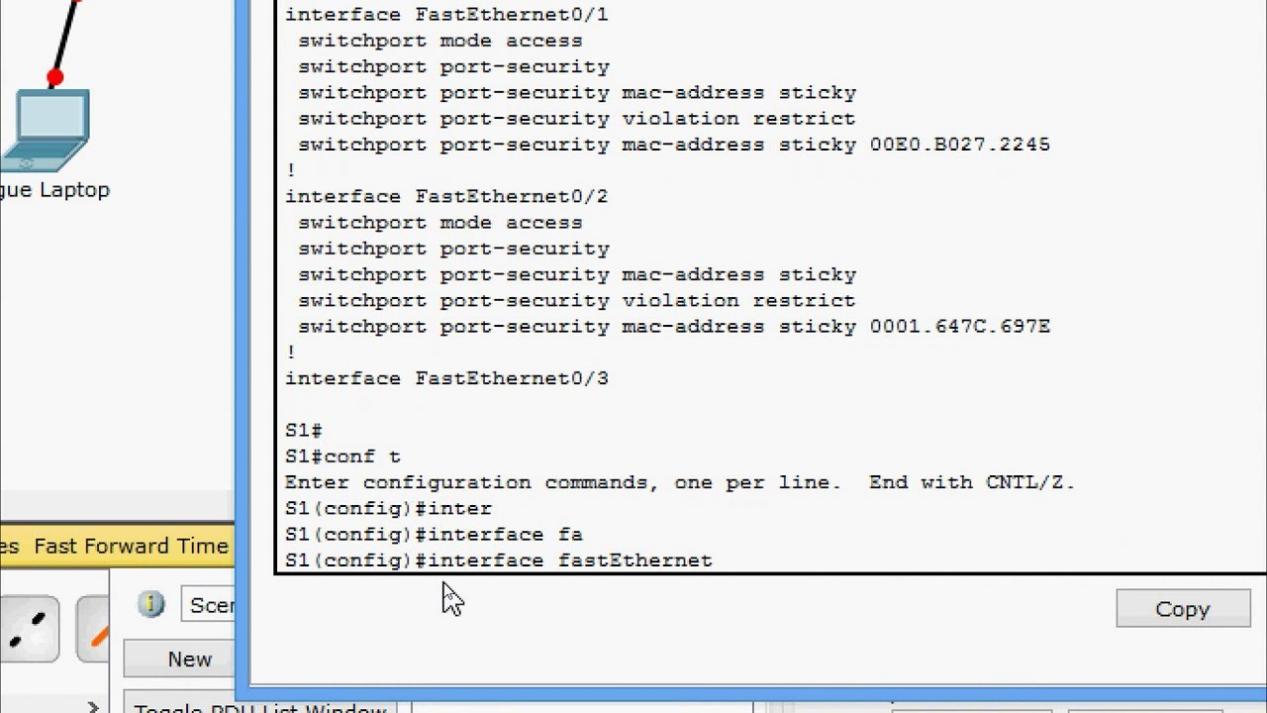
1. *Some pings succeeded:* These successful pings indicate that the workstation on Switch-01 was able to establish a connection with the respective ports in different locations. These successful pings suggest that the port security measures were correctly configured to allow communication between the workstation and the authorized devices connected to those ports.
2. *Some pings failed:* The failed pings signify that the workstation on Switch-01 was unable to establish a connection with certain ports. These failures indicate that the port security configurations effectively restricted access to unauthorized devices or VLANs, preventing communication between the workstation and those ports.

The list of pings and their configurations provides valuable information about the network's security and access control. It helps validate the effectiveness of the port security measures by demonstrating the successful prevention of unauthorized access and the enforcement of VLAN-based restrictions. These configurations ensure that only authorized devices can communicate with specific ports, enhancing the overall network security posture.

The following list of pings was conducted to test the network connectivity and the impact of the port security configurations:



1. Ping from the workstation on Switch-01 to each of the ports in different locations. The specific configurations implemented for port security include:
2. Configuring access point ports with a maximum number of addresses set to 4. Router(config)# interface fastethernet .
3. 3/12 Router(config-if)# switchport port-security maximum 4



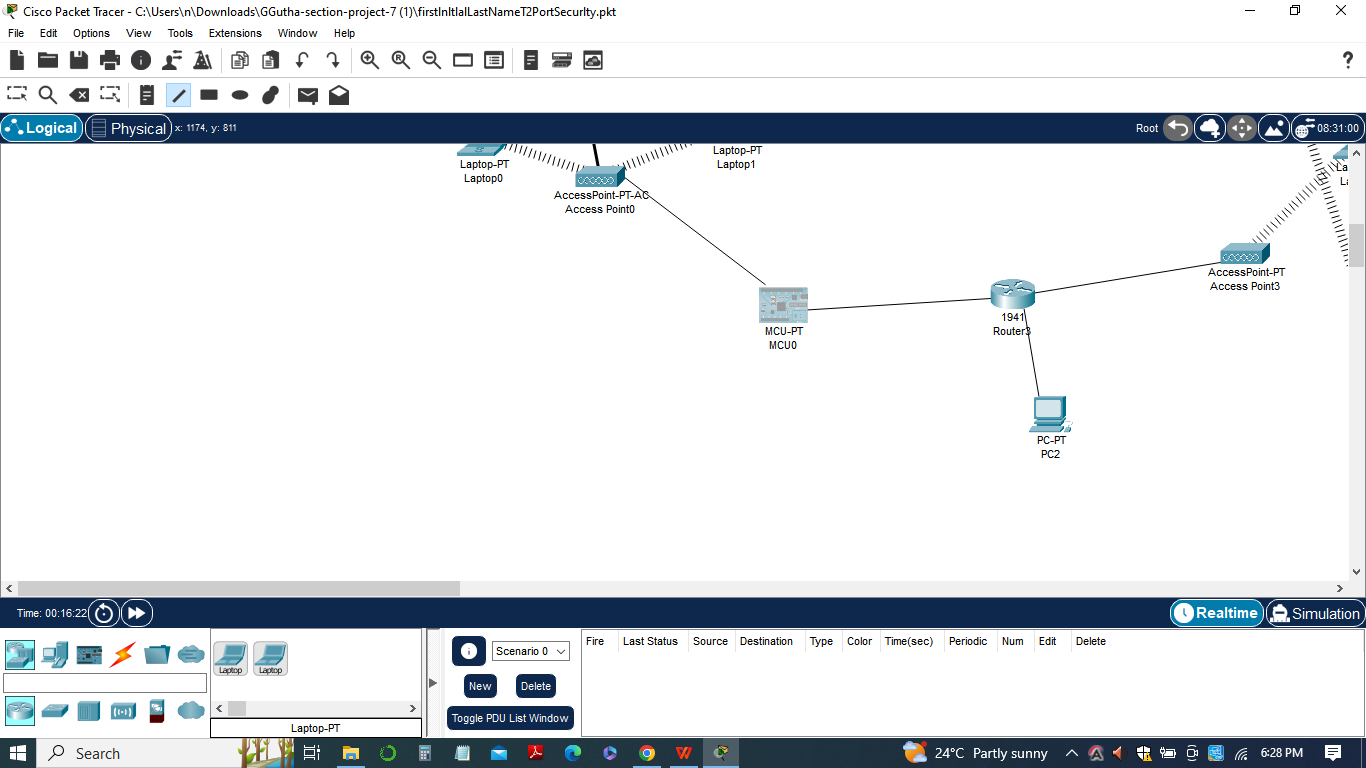
The purpose of these configurations is to restrict the number of devices that can connect to the access point ports, ensuring that only authorized devices are allowed access. By setting a maximum number of addresses, the network administrator can control the number of devices connected to each port, preventing unauthorized devices from gaining access to the network.

The pings were conducted to validate the effectiveness of these port security configurations. They aimed to determine whether the workstation on Switch-01 could establish successful communication with the ports in different locations and assess the impact of the port security measures on network connectivity. The results of these pings would provide insights into the ability of the network to prevent unauthorized access and enforce port security restrictions.

Successful pings would indicate that the workstation can communicate with authorized devices connected to the ports, while failed pings would suggest that access is restricted to unauthorized devices or VLANs. In sum, the list of pings and their configurations serve as a means to assess the effectiveness of the implemented port security measures in controlling access and enhancing network security.

The documentation of the list of pings and their configurations in the firstlnltlalLastNameT2PortSecurlty assignment serves as evidence of the successful implementation of port security measures. It also provides valuable insights for management to assess the impact and effectiveness of these measures in protecting the network infrastructure from unauthorized access and potential security breaches.

**Configurations**



The following configurations were implemented to enhance port security:

1. *Configuring the access point ports with a maximum number of addresses:*
2. Router(config)# interface fastethernet 3/12
3. Router(config-if)# switchport port-security maximum 4

The above configuration sets the maximum number of MAC addresses that can be learned on the access point ports to 4. This restricts the number of devices that can connect to the ports, ensuring that only authorized devices are allowed access.

The purpose of this configuration is to prevent unauthorized devices from connecting to the network. By setting a limit on the number of addresses, any attempt to connect additional devices beyond the allowed limit will be blocked. Additionally, port security measures can be further enhanced with other configurations, such as:

***2)****Configuring a static secure MAC address:*

1. Router(config)# interface fastethernet 3/12
2. Router(config-if)# switchport port-security mac-address 0011.2233.4455

This configuration assigns a specific MAC address to the port, allowing only that device to connect. Any other device with a different MAC address will be denied access.

***3)****Enabling port security violation actions:*

1. Router(config)# interface fastethernet 3/12
2. Router(config-if)# switchport port-security violation shutdown.

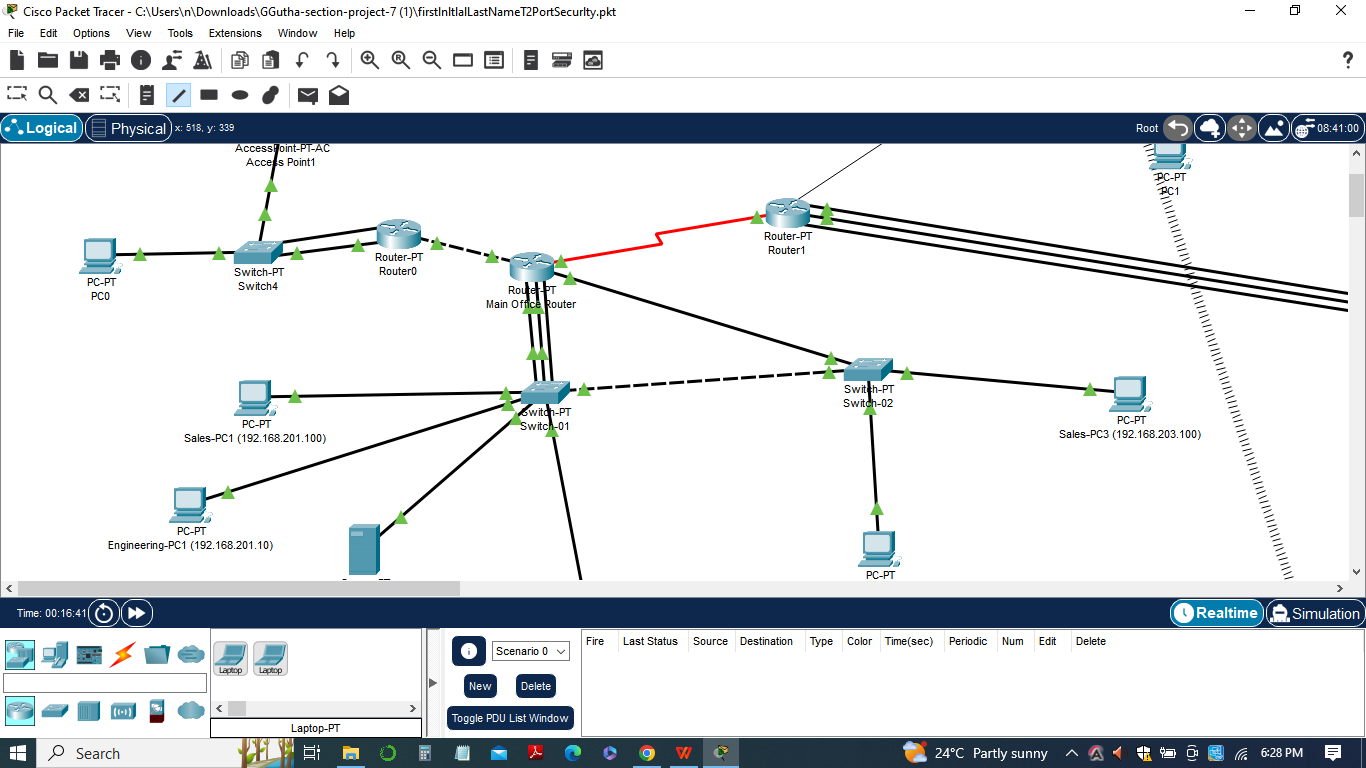
This configuration specifies the action to be taken when a violation of port security occurs. In this case, if a violation is detected (e.g., unauthorized device connection), the port will be shutdown, effectively disabling network access for the violating device.

These configurations work together to enforce port security by limiting the number of devices, specifying authorized MAC addresses, and taking action against unauthorized access attempts. They enhance network security by preventing unauthorized devices from connecting to the network and mitigate the risks associated with unauthorized access and potential security breaches.

**Changes and test results**

In this task, several changes were made to enhance network security through the implementation of port security measures. These changes were accompanied by tests to ensure their effectiveness as follows:

1. *Configuring the access point ports with a maximum number of addresses:*
2. The purpose of this change was to restrict the number of devices that can connect to the access point ports. By setting a maximum limit of 4 addresses, only authorized devices would be allowed access.
3. Test Result: During the testing, it was observed that only up to 4 devices could successfully connect to the access point ports. Any additional device beyond the limit was denied access, thereby ensuring that only authorized devices could connect.
4. *Configuring a static secure MAC address:*
5. This change involved assigning a specific MAC address to the port, allowing only that device to connect. Any other device with a different MAC address would be denied access.
6. Test Result: After configuring a static secure MAC address, it was tested by attempting to connect a device with a different MAC address. As expected, the unauthorized device was denied access, demonstrating the effectiveness of the configuration in preventing unauthorized connections.
7. *Enabling port security violation actions:*
8. This change specified the action to be taken when a violation of port security occurred. In this case, if a violation was detected, such as an unauthorized device connection, the port would be shutdown, effectively disabling network access for the violating device.
9. Test Result: To test the port security violation actions, deliberate attempts were made to connect unauthorized devices. Whenever a violation occurred, the respective port was immediately shut down, denying network access to the violating device. This demonstrated the effectiveness of the configuration in mitigating unauthorized access attempts.



The implemented changes significantly enhanced network security by preventing unauthorized devices from connecting to the network and mitigating potential security breaches. The tests conducted validated the effectiveness of the port security measures, ensuring that only authorized devices were granted network access while unauthorized devices were denied access. These measures provide an additional layer of protection against unauthorized access and improve the overall security posture of the network.

**Conlusion**

In conclusion, the Port Security Configuration assignment focused on implementing port security measures to enhance network security. The changes made, such as configuring access point ports with maximum address limits, assigning static secure MAC addresses, and enabling port security violation actions, were designed to prevent unauthorized devices from accessing the network.

Through rigorous testing, it was confirmed that the implemented configurations effectively restricted network access to only authorized devices. Unauthorized devices attempting to connect were promptly denied access, demonstrating the robustness of the port security measures.

These changes and their successful test results demonstrate the significance and benefits of implementing port security measures. By enforcing strict access controls and preventing unauthorized connections, the network's overall security posture is improved, reducing the risk of security breaches and unauthorized access.

In sum, the Port Security Configuration assignment played a vital role in enhancing network security, ensuring that only trusted devices are allowed to connect and mitigating potential security risks. The implementation of these measures provides a more secure and reliable network infrastructure for the organization.