**Part 1:**

In order to for me to design a secured network, I had to implement a specific requirements to make the network secured. However, I started implementing all the PC’s, switches and routers using star topology due to its advantages where it is easy to install and configure, easy to troubleshoot, and it has a high security. Even though it has a high cost but at the same time it meets the business requirements that I need to implement from all the hardware and the software requirements in order to make it secured enough.

I implemented the main router called Amman R in the middle and four routers around it, Aqaba, Irbid, Turkey, and Saudi Arabia routers with Amman switch connected with Amman R router. Amman switch that is connected to Amman R router has eight PC’s connected with Amman switch, Aqaba router has two switches where every switch is connected with a single PC, Irbid router has one switch which is connected to a single PC, Turkey and Saudi Arabia has the same as turkey has.

I initially focused on implementing VLANs in the network as per the requirements of the company I work for. VLANs provide several benefits such as flexibility, security, efficient management, and quality of service. By logically segmenting the network into virtual networks, VLANs allow administrators to group devices based on different criteria, enhancing network organization and control.After successfully implementing VLANs, my attention shifted to selecting an appropriate routing protocol for exchanging network information and determining the best paths for packet forwarding. Considering the goals of simplicity, coverage time, and compatibility among the implemented routers, I opted for the Routing Information Protocol (RIP).RIP, known for its simplicity, acceptable convergence time, and widespread compatibility, was a suitable choice to establish a reliable routing protocol across the network. With RIP implemented, the routers were able to dynamically learn about network topologies and make informed decisions on how to forward data.By first implementing VLANs and then integrating the RIP routing protocol, I ensured a well-structured network that benefited from both the advantages of VLANs and the efficient routing provided by RIP. The VLANs allowed for logical grouping of devices, enhancing security and network management, while RIP facilitated dynamic routing and optimal path selection. This combined approach resulted in a network that was both secure and efficient in its communication and resource utilization.

After implementing the RIP routing protocol and VLANs, I took the necessary steps to further on network security. This involved shutting down all unused ports, using the native VLANs, and implementing port security. By leveraging port security, which controls and monitors access to network ports based on MAC addresses, I added an additional layer of protection. Unauthorized devices attempting to connect to the network were effectively prevented from doing so, mitigating potential security breaches. Port security also helped counter MAC address spoofing attacks and provided greater visibility into network activity. By combining the RIP protocol, VLANs, and port security measures, I established a robust and secure network environment.

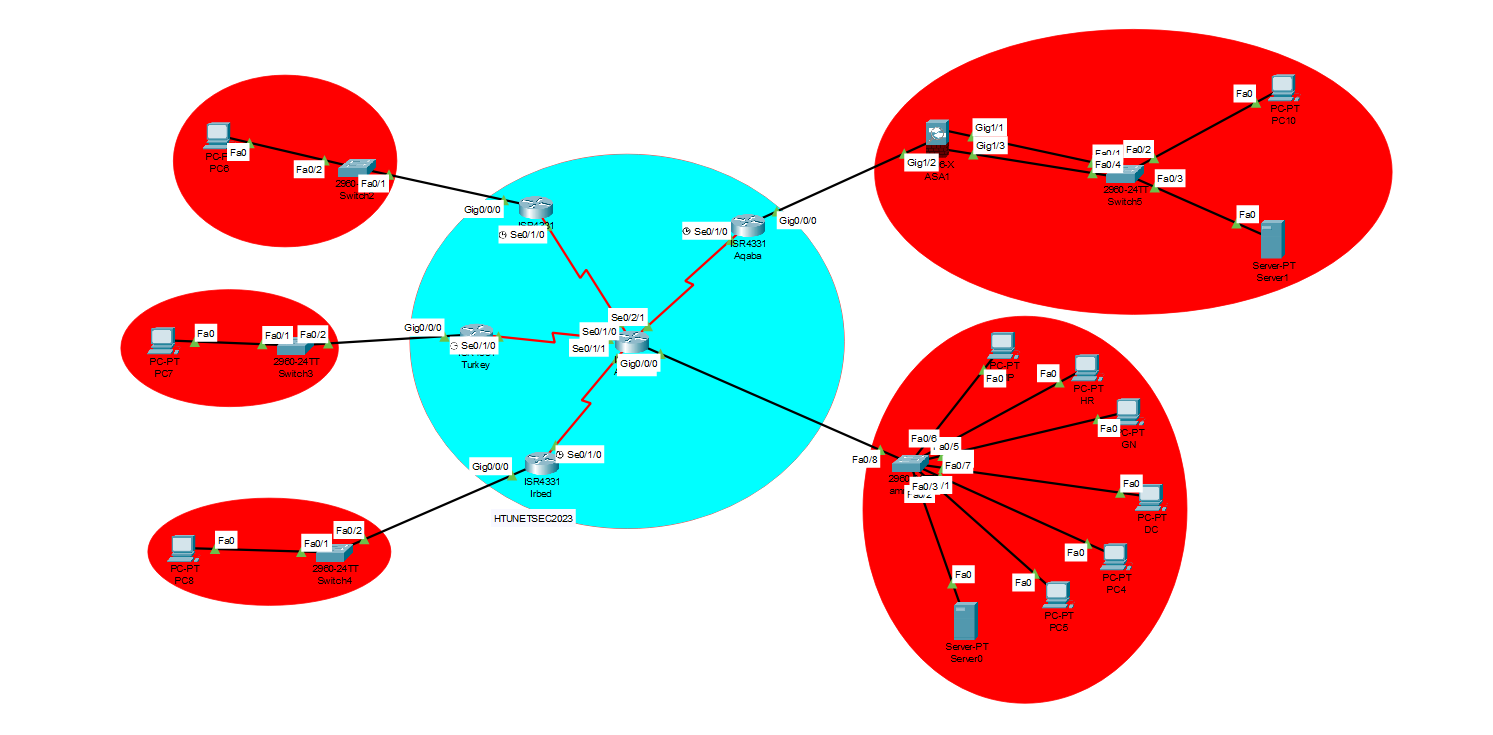
Additionally, I wanted to ensure that only authorized used can access network resources, so I used AAA (Authentication, Authorization, and Accounting) protocol is used to manage access control and user management in a comprehensive and centralized manner. By implementing AAA, authorized access to network resources is ensured through user authentication and verification of credentials. Authorization determines user privileges based on roles and policies, while accounting logs user activities for security audits and troubleshooting. AAA offers centralized management, integrates with other security systems, and enhances network security.

Thinking of the countries that are outside Amman which are Turkey and Saudi Arabia, I had to make a VPN (virtual private network) and it is especially used when accessing networks or resources from countries outside the country Amman. VPN enhance security, privacy, and accessibility when accessing network or resources from the countries outside of our own, so it gives the implemented network security and privacy, accessing local resources, and source remote access.

I started thinking that in Aqaba I implemented an ASA (adaptive security appliance) inside the Aqaba network where it is between the router and the two switches where every switch has one PC each. Inside the ASA there are some features and functionality that makes it popular choice for network security where one of the features firewall protection. It provides a security by inspecting the incoming and the outgoing network traffic where it also protect Aqaba network against unauthorized access, threats, and attacks that may happen to Aqaba network.

After implementing all the necessary components in the network, I realized the missing piece: Access Control Lists (ACLs). ACLs are crucial for network devices like switches and routers as they allow for the control and filtering of network traffic based on predefined rules. To ensure proper network security, each PC within the network should have its own set of rules outlining what is permitted and what is not. By organizing these do's and don'ts, ACLs help administrators enforce access control policies, restrict unauthorized access attempts, and maintain a secure network environment. With ACLs in place, the network gains an additional layer of protection, ensuring that traffic flows according to specified guidelines and preventing potential security breaches. Must add the DMZ

Finally, to enhance the security of remote access to network devices, I implemented SSH (Secure Shell), a cryptographic network protocol. SSH provides a secure method for accessing network devices remotely. By encrypting the entire communication session, including authentication and data transfer, SSH protects against unauthorized access and interception of sensitive information. With SSH in place, remote administrators can securely manage and configure network devices, ensuring that confidential data remains protected during remote access sessions.

****

**Question 2:**

The purpose of the secure network in the given scenario is to establish a reliable and protected communication infrastructure, ensuring secure data transfer and preventing unauthorized access. The network implementation includes a star topology connecting multiple routers to a central router for easy installation, configuration, and troubleshooting. VLANs have been implemented to provide flexibility, security, efficient management, and quality of service benefits. The Routing Information Protocol (RIP) has been chosen for dynamic routing, and VPN connections have been established between the main router in Amman and routers in Turkey and Saudi Arabia for secure remote access. The integration of AAA enhances access control and user management. An Adaptive Security Appliance (ASA) and Access Control Lists (ACLs) have been implemented for firewall protection and traffic filtering. To further strengthen security, it is recommended to incorporate a DMZ between the Amman switch and router. Regular security audits, vulnerability assessments, and penetration testing should be conducted. Network monitoring capabilities, including intrusion detection and prevention systems, should be improved. Timely updates of firmware and security patches are essential, along with user education on best security practices. By implementing these improvements, the network will have a robust security framework that aligns with the purpose and requirements of the given scenario.

**Question 3:**

The network uses a combination of hardware and software to ensure strong security. It has a powerful firewall device (hardware) that can detect and prevent advanced threats. Additionally, there is a special device called a VPN gateway (hardware) that is built into the router/firewall. This gateway allows for secure remote access using IPsec and VPN protocols.

The network is built on high-quality switches and routers (hardware) that provide advanced security features. Software components play a crucial role as well, such as the firewall (software) that configures and controls the firewall.

Remote devices have VPN client software (software) installed, while the network gateway runs VPN server software (software). Access Control Lists (ACLs) are set up and managed through software interfaces on switches, routers, or firewall devices (software).

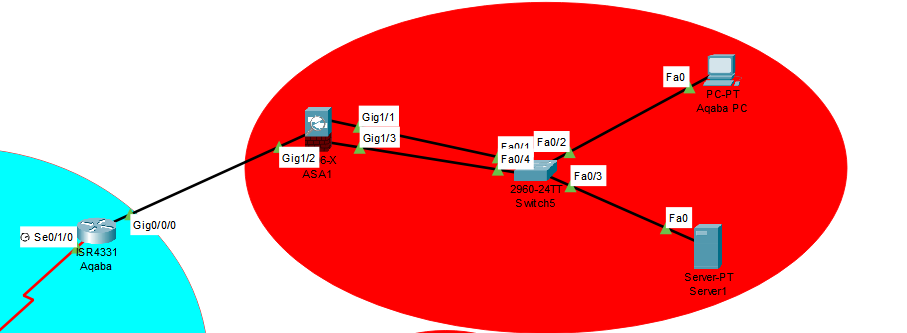
The DMZ architecture, which creates an isolated area for public-facing services, is controlled through similar interfaces (software). To ensure proper authentication, authorization, and accounting, the network utilizes AAA protocols (software).

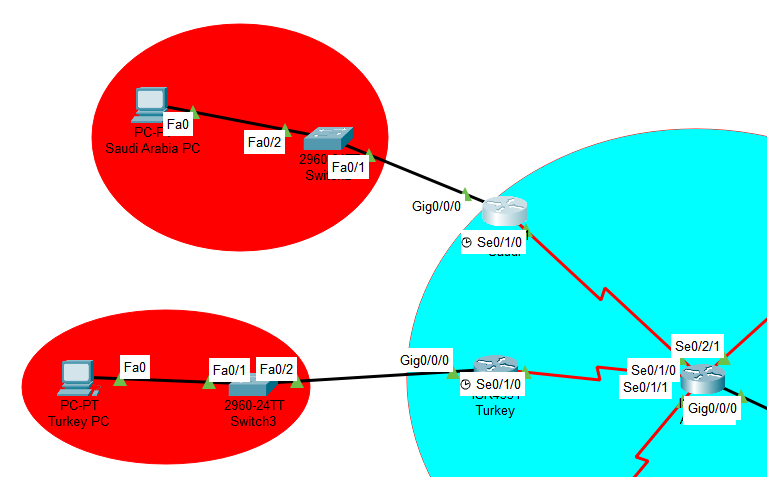
To enable secure remote administration, remote devices use SSH client software (software), while network devices use SSH server software (software). Finally, software-based SSL/TLS libraries and protocols ensure secure communication through protected ports.

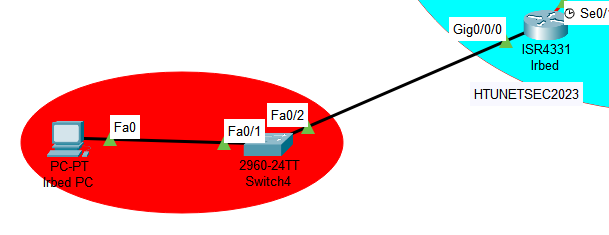
Must add server as a hardware

**Question 4:**

In this picture I implemented the ASA protocol in Aqaba network.



In this picture I implemented the VPN protocol in the main router, turkey and Saudi Arabia  


In this picture, I implemented the AAA protocol in Irbid network  


**Question 5:**

**Justification for the chosen network security configuration:**The chosen network security measures provide a comprehensive approach to protect the network from various security threats. Firewalls effectively monitor and control traffic, routers and switches enforce security policies, and gateways enable secure remote access. Strong passwords, along with SSH and SSL, ensure secure authentication and data transmission. IPsec and VPN protocols establish encrypted connections, while HTTPS and FTPS secure web and file transfers. Properly configuring DHCP and DNS services ensures efficient network operations. Collectively, these measures offer layered security, mitigating risks and safeguarding against unauthorized access, data breaches, and malicious attacks.

**Firewalls** act as a protective barrier that shields your network from external threats by monitoring and controlling incoming and outgoing network traffic according to predefined security rules. Their purpose is to prevent unauthorized access and malicious attacks. Routers play a crucial role in directing network traffic between different networks.

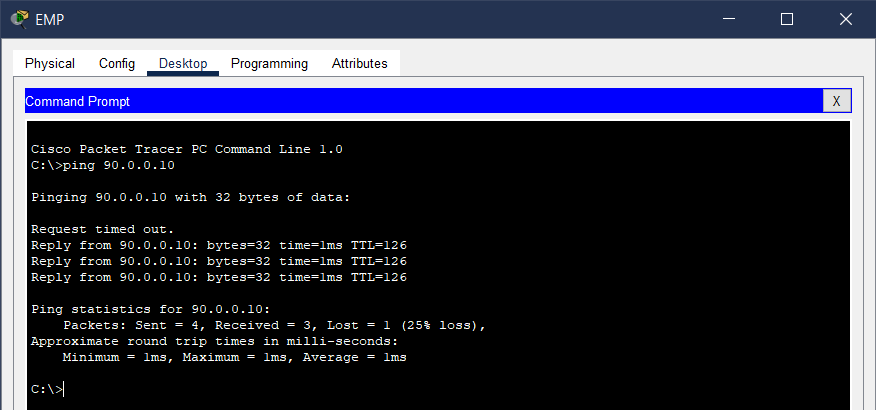
They can be configured to enforce security policies, such as filtering specific types of traffic or blocking particular IP addresses, thus offering protection against potential threats. Switches, on the other hand, provide connectivity to devices within a local network. Utilizing enterprise-grade switches ensures the incorporation of robust security features like **VLANs** (Virtual Local Area Networks) and port-level security, which help segregate and secure network traffic.Gateways, including **VPN** gateways, serve as entry points into your network. They facilitate secure remote access using protocols like IPsec and VPN, establishing encrypted communication channels that allow authorized users to connect to your network from external locations. Implementing strong passwords is crucial for network security. It is highly recommended to enforce rules for password complexity and regularly update passwords to prevent unauthorized access.**SSH** (Secure Shell) provides secure remote administration by encrypting remote connections and authenticating users. SSL (Secure Sockets Layer), on the other hand, ensures secure communication between web browsers and web servers, safeguarding data transmitted over HTTP.**IPsec and VPN** protocols enable secure communication over public networks, such as the internet. By encrypting data transmitted between devices, these protocols ensure confidentiality and integrity, making them vital for secure remote access and private network connections.

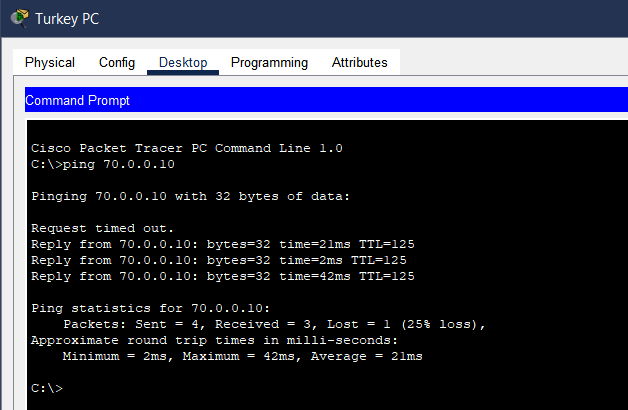
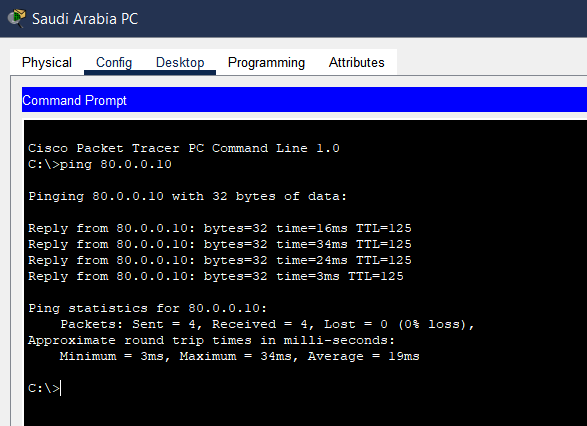
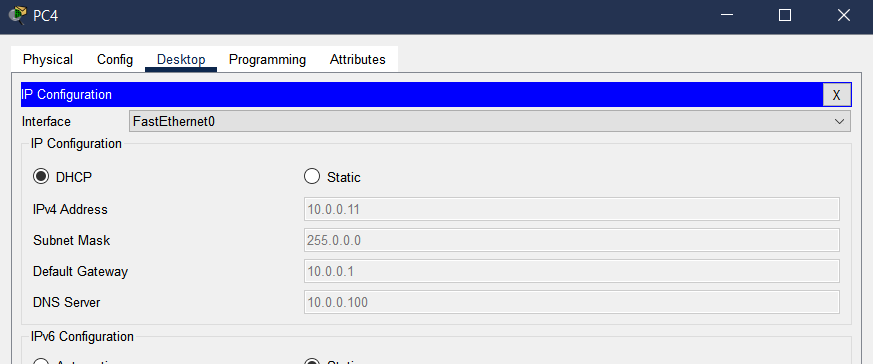
**HTTPS and FTPS** are secure versions of the HTTP and FTP protocols, respectively. They utilize encryption mechanisms (SSL/TLS) to secure data transmission, thereby ensuring confidentiality and preventing unauthorized access to sensitive information.

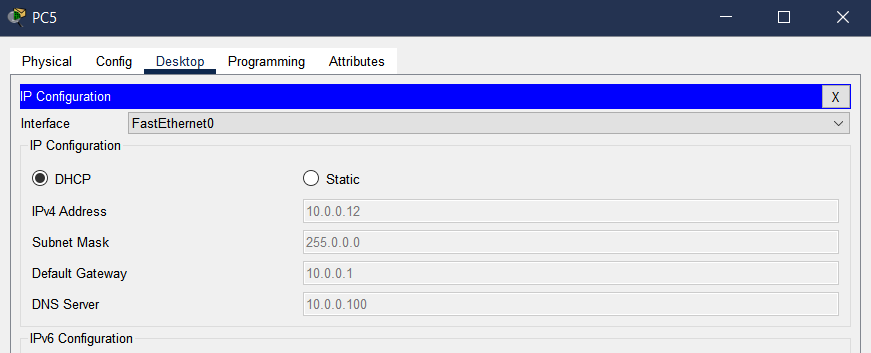
**DHCP (Dynamic Host Configuration Protocol)** automatically assigns IP addresses to devices on the network, simplifying network management. **DNS (Domain Name System),** on the other hand, translates domain names into IP addresses, facilitating communication between devices. Proper configuration of DHCP and DNS services is crucial to maintain network integrity and efficiency.

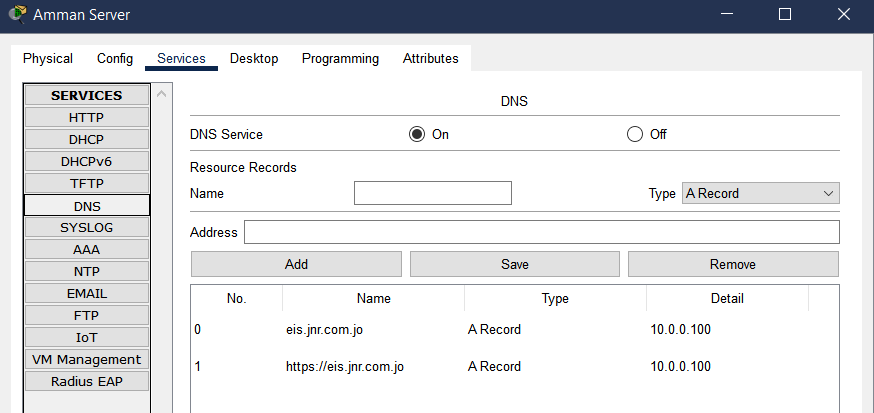
**Part 2 (question 1 and 2):**

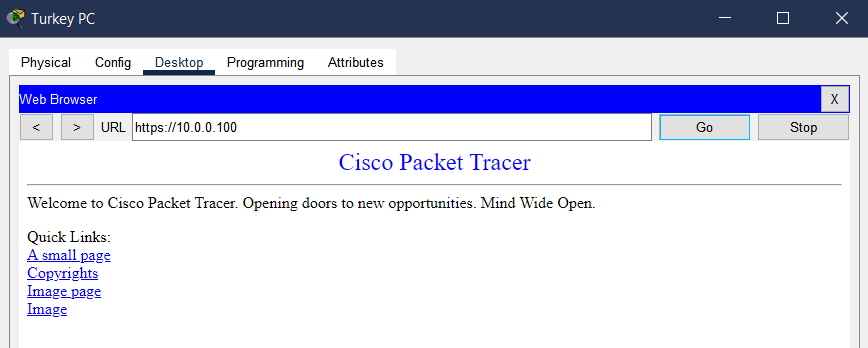
1. Testing the RIP routing configuration : I started by pinging from between whats is connected with Amman switch, and Irbid Pc (vlan 20)

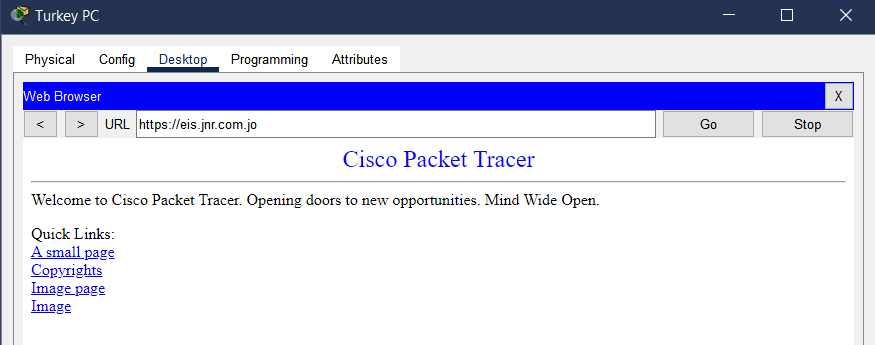


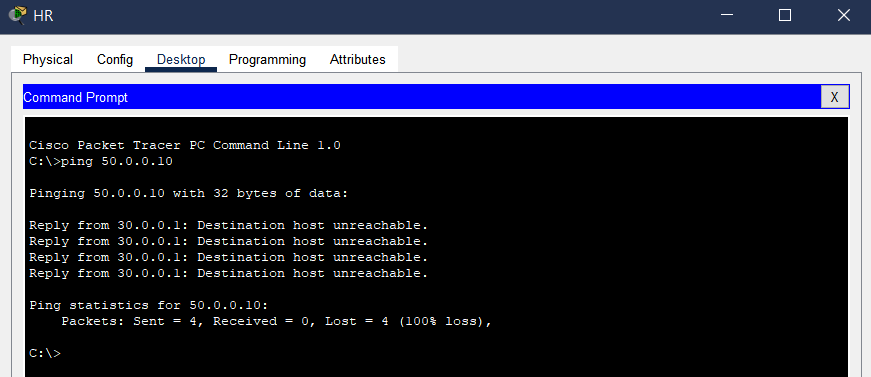
1. Testing VPN: I will start pinging between whats outside Amman, which is Turkey and Saudi Arabia.  
   
2. Ping testing VPN between Turkey and Saudi Arabia  
   
3. Checking and testing DHCP on two PC’S   
    

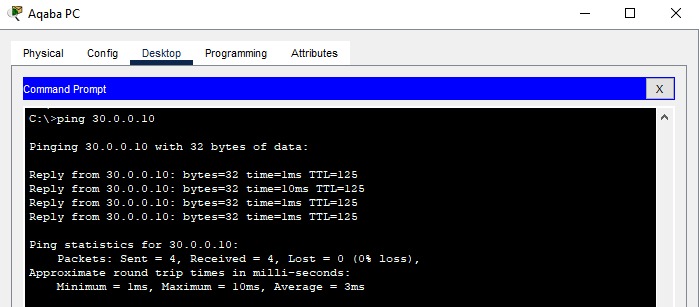


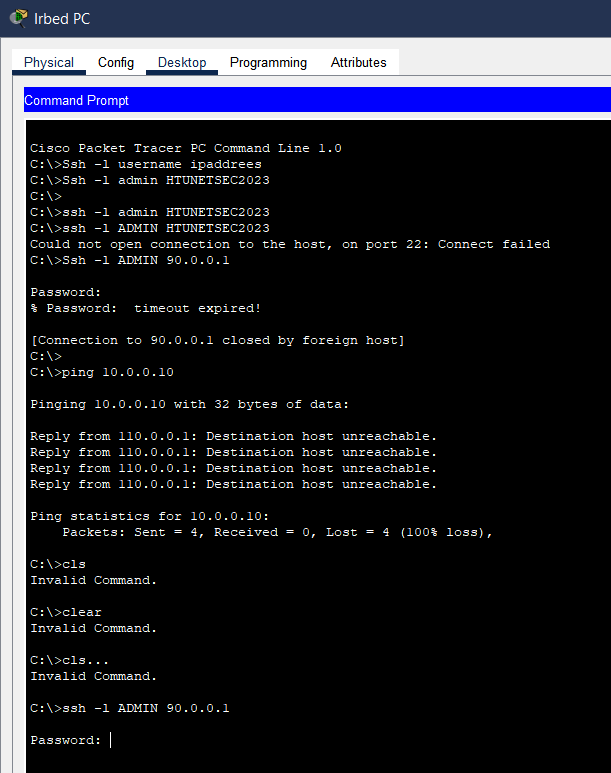
1. Testing the DNS and the HHTPS :  
   



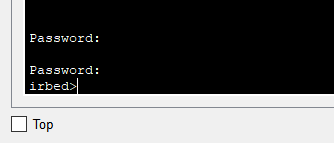


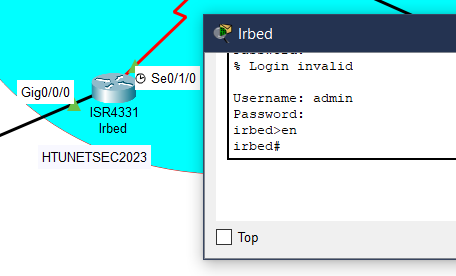
1. Testing the ASA for Aqaba network. What outside the ASA cannot contact what inside of Aqaba network cause of the firewall.  
   

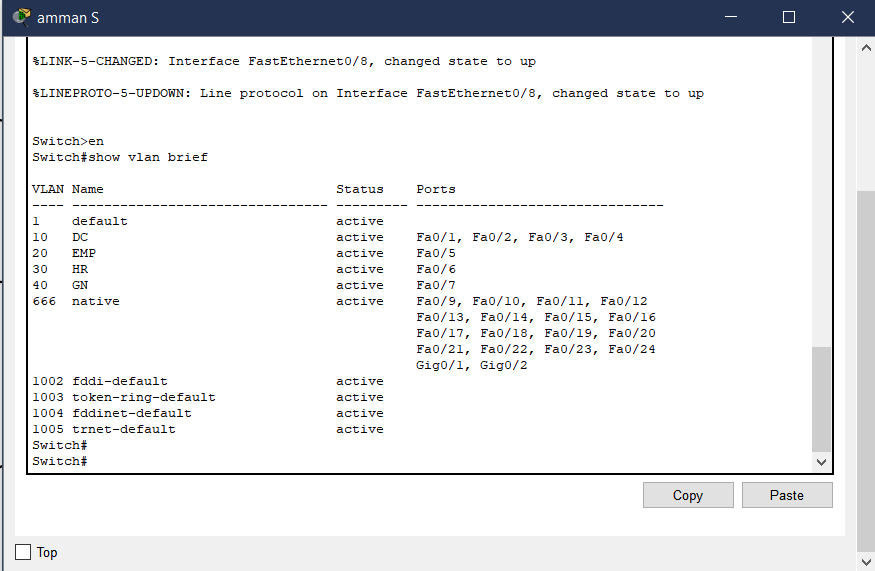
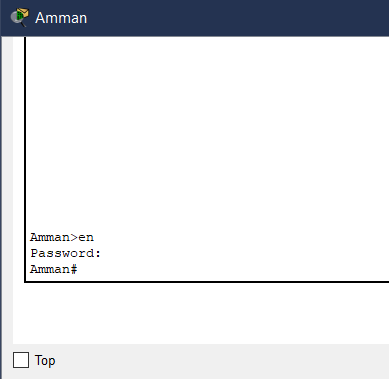


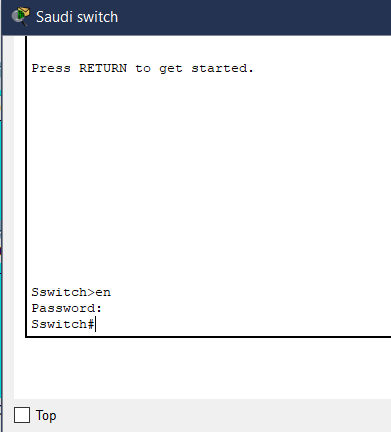
1. Testing the AAA on Irbid PC  
   

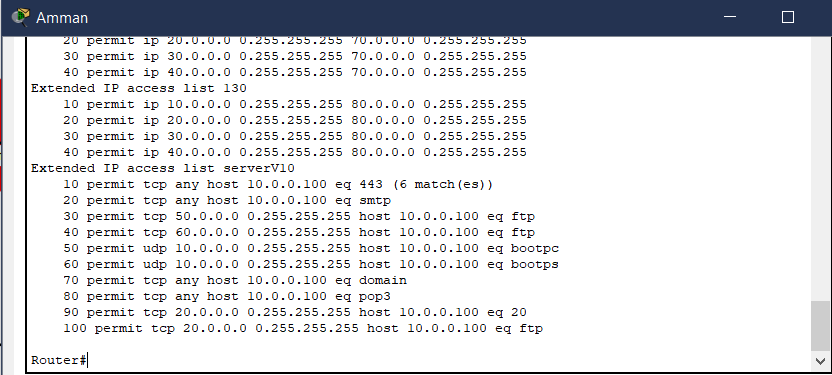
You can see that it is in the bottom of the command prompt

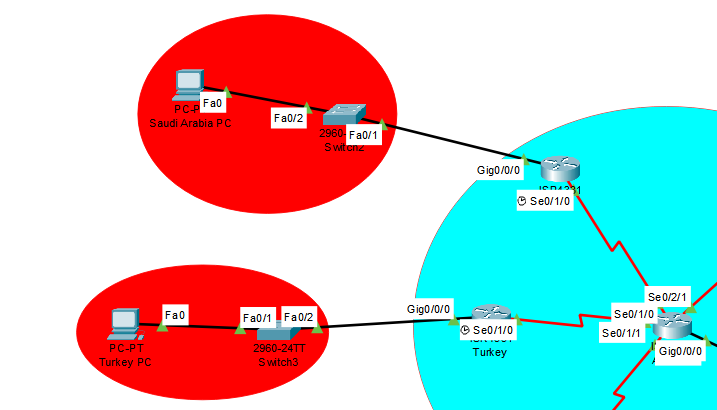
  
A screen shot shows that the password HTUNETSEC2023 worked in command prompt.

On Irbid router, to enter it  


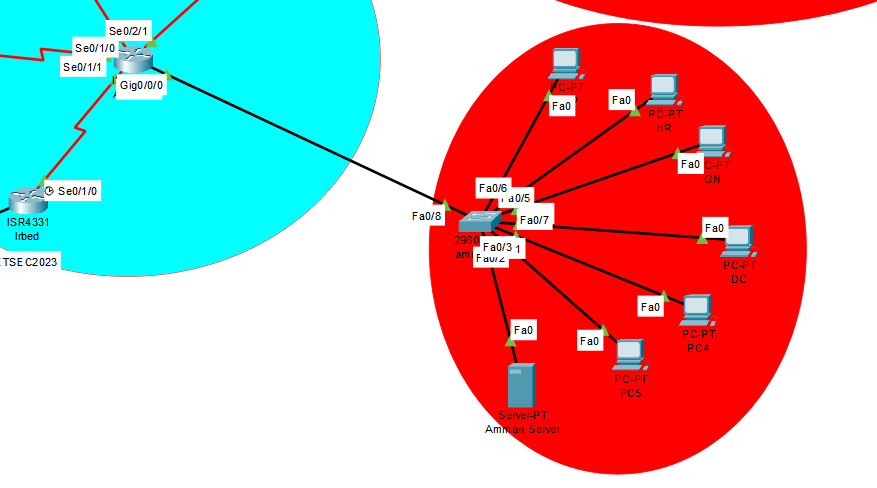
1. Port security testing, closing all the unused ports in VLANS, and testing when connecting another PC to the LAN  
   
2. testing routers and switches to see if they ask for a password when enabling them  
   



1. I already tested the ACL in the above testing commands. And here is the ACL I did in Amman router   
   
2. Testing that HTTP works in VLAN 20  
   
3. Testing that HTTP does not work in VLAN 30, and only accessible by VLAN 20  
   

**Testing vulnerabilities inside the network.  
**

Between these two routers, there is a VPN connection between the main router Amman, and the others Turkey and Saudi Arabia. There must be a regularly update firmware and security patches that keeps the routers' firmware up to date to address any known vulnerabilities. Promptly apply security patches released by the router manufacturers. Additionally, we can also add an Intrusion detection and prevention (IDPS), that Deploys intrusion detection and prevention systems (IDPS) to monitor network traffic for any suspicious activities or signs of MITM (man in the middle) attacks.



If we do not add DMZ between Amman switch, and Amman router, the vulnerability might be is weakened Defense-in-Depth: A DMZ serves as an additional layer of defense, separating your internal network from the external network. Without this segmentation, your defense-in-depth strategy may be weakened, as there are fewer barriers for attackers to overcome. However, Without a DMZ, all devices within the internal network are potentially exposed to the external network. This expands the attack surface, making it easier for attackers to target and compromise devices within your network.

**Conclusively:**

To ensure network security, I conducted various tests to identify potential vulnerabilities. I start by verifying the proper configuration of the RIP protocol and testing its functionality. Next, I focused on testing the VPN connection between Turkey and Saudi Arabia, checking for stability, encryption, and proper traffic flow. My assessment also included DHCP with DNS testing to validate IP address allocation and domain name resolution. Additionally, I examined the implementation of HTTPS for secure web communication and perform web application security tests. On the Aqaba network, we will review the Adaptive Security Appliance (ASA) configurations and conduct penetration testing and to check if the inside network can ping with the outside, and to alos check if the outside can or cannot reach the inside of the network. In Irbid, I (AAA) mechanisms. Finally, an overall network security assessment I performed, including vulnerability scanning, compliance review, and evaluation of monitoring capabilities.

**Question 3:  
  
Evaluating the design, planning, configuration and testing of your network security**

Upon evaluating the design, planning, and configuration of the network, several strengths stand out. The implementation of a star topology provides ease of installation, configuration, and troubleshooting, along with high security. VLANs offer flexibility, security, efficient management, and quality of service. The choice of RIP for dynamic routing is suitable due to its simplicity, convergence time, and compatibility. The integration of AAA enhances access control and user management. VPNs ensure secure remote access, while the ASA in Aqaba strengthens security with firewall protection. ACLs contribute to traffic filtering and control. However, to further enhance network security, it is recommended to incorporate a DMZ, conduct regular security audits and testing, improve monitoring capabilities, ensure timely updates, and focus on user education.

The selection of the Routing Information Protocol (RIP) as the dynamic routing protocol exhibits careful consideration. RIP is known for its simplicity, acceptable convergence time, and compatibility, making it a suitable choice for establishing reliable routing across the network. By leveraging RIP, the network routers can dynamically learn about network topologies and make informed decisions regarding the best paths for data forwarding. This facilitates efficient and optimized communication within the network.The integration of AAA (Authentication, Authorization, and Accounting) into the network architecture highlights the commitment to access control, user management, and centralized management of network resources. AAA protocol offers comprehensive authentication and verification of user credentials, determining user privileges based on predefined roles and policies, and logging user activities for security audits and troubleshooting purposes. This centralized approach enhances network security by ensuring that only authorized users can access network resources, preventing unauthorized access attempts, and maintaining control over user privileges.

The implementation of VPNs (Virtual Private Networks) to establish secure connections between locations outside the main network hub demonstrates a proactive approach to network security. VPNs enhance security, privacy, and accessibility when accessing network resources from external locations, ensuring encrypted and protected communication between different geographical sites. This feature is particularly crucial for countries such as Turkey and Saudi Arabia, enabling secure remote access and maintaining the privacy of data transmitted over the network.The inclusion of an Adaptive Security Appliance (ASA) in the Aqaba network showcases a well-rounded security strategy. The ASA provides firewall protection, inspecting incoming and outgoing network traffic, and safeguarding the Aqaba network against unauthorized access attempts, threats, and potential attacks. By implementing the ASA, an additional layer of protection is added to the network, enhancing its overall security posture.

The utilization of Access Control Lists (ACLs) for traffic filtering and control further fortifies network security. ACLs allow administrators to define rules that determine which types of network traffic are permitted or denied, based on various criteria such as source IP address, destination IP address, protocol, and port numbers. By enforcing these rules, administrators can restrict unauthorized access attempts, mitigate network threats, and maintain a secure network environment.While the design, planning, and configuration of the network demonstrate thoughtful consideration for security, there are areas that can be improved to enhance overall network protection. Firstly, incorporating a DMZ (Demilitarized Zone) into the network architecture would provide an additional layer of security by isolating publicly accessible services from the internal network in Aqaba. This separation reduces the risk of unauthorized access to critical resources and helps mitigate potential threats. The evaluation of the network design, planning, and configuration reveals several positive aspects, such as the effective utilization of the star topology, VLAN implementation, RIP routing protocol, AAA integration, VPNs, ASA, and ACLs. However, to further strengthen network security, it is recommended to incorporate a DMZ, conduct regular security audits and testing, improve network monitoring capabilities, ensure timely updates for network devices, and focus on user education and awareness. By implementing these improvements, the network's overall security posture can be significantly enhanced, reducing the risk of potential breaches and ensuring a resilient and secure network infrastructure.Testing the VPN connection between Turkey and Saudi Arabia for stability, encryption, and traffic flow is crucial in establishing secure and reliable communication across different geographical locations. Assessing the functionality of DHCP with DNS ensures correct IP address allocation and domain name resolution, contributing to the smooth operation of the network. Testing the implementation of HTTPS for secure web communication and performing web application security tests demonstrate a proactive approach to identifying and mitigating potential vulnerabilities in web services.The review of Adaptive Security Appliance (ASA) configurations and conducting penetration testing in the Aqaba network reveal a focus on evaluating the effectiveness of firewall protection and assessing the network's resistance to potential breaches. Additionally, conducting AAA testing in Irbid emphasizes the importance of access control, authentication, and user management.

Moreover, it is important to ensure that the testing methodology covers all relevant aspects of network security, including network device hardening, and secure configuration. Regular updates of network devices, including routers, switches, firewalls, and servers, should be part of the testing process to address any known vulnerabilities promptly.

**Some improvements recommendation on the network I have:**   
  
as I mentioned before we have to implement a DMZ because if we do not add DMZ between Amman switch, and Amman router, the vulnerability might be is weakened Defense-in-Depth: A DMZ serves as an additional layer of defense, separating your internal network from the external network. Without this segmentation, the defense-in-depth strategy may be weakened, as there are fewer barriers for attackers to overcome. However, Without adding a DMZ, all devices within the internal network are potentially exposed to the external network. This expands the attack surface, making it easier for attackers to target and compromise devices within your network. However, Failure to implement a DMZ between the Amman switch and Amman router could weaken the Defense-in-Depth strategy. A DMZ provides an extra layer of protection by segregating the internal network from the external network. Without this separation, there are fewer obstacles for attackers to overcome, potentially compromising the overall security measures. It is crucial to establish a DMZ as it prevents direct exposure of internal devices to the external network, reducing the attack surface and enhancing network security.

Another suggested improvement is to connect all five routers together using a Virtual Private Network (VPN). This setup would establish an encrypted gateway, ensuring secure communication between the routers. By leveraging the internet, we can effectively interact with the countries without the need for expensive physical cables. This approach not only enhances security through encryption but also offers cost savings by utilizing internet connectivity for seamless communication with the countries involved.

Implementing AAA (Authentication, Authorization, and Accounting) in the network improves security by ensuring that only authorized individuals can access the network. With AAA, users are required to authenticate themselves using secure credentials, such as usernames and passwords, to verify their identities. This prevents unauthorized access and protects sensitive data and resources. AAA also allows you to control access by granting appropriate permissions to authorized users. Additionally. By implementing AAA, i can enhance network security and ensure trusted access to network resources.