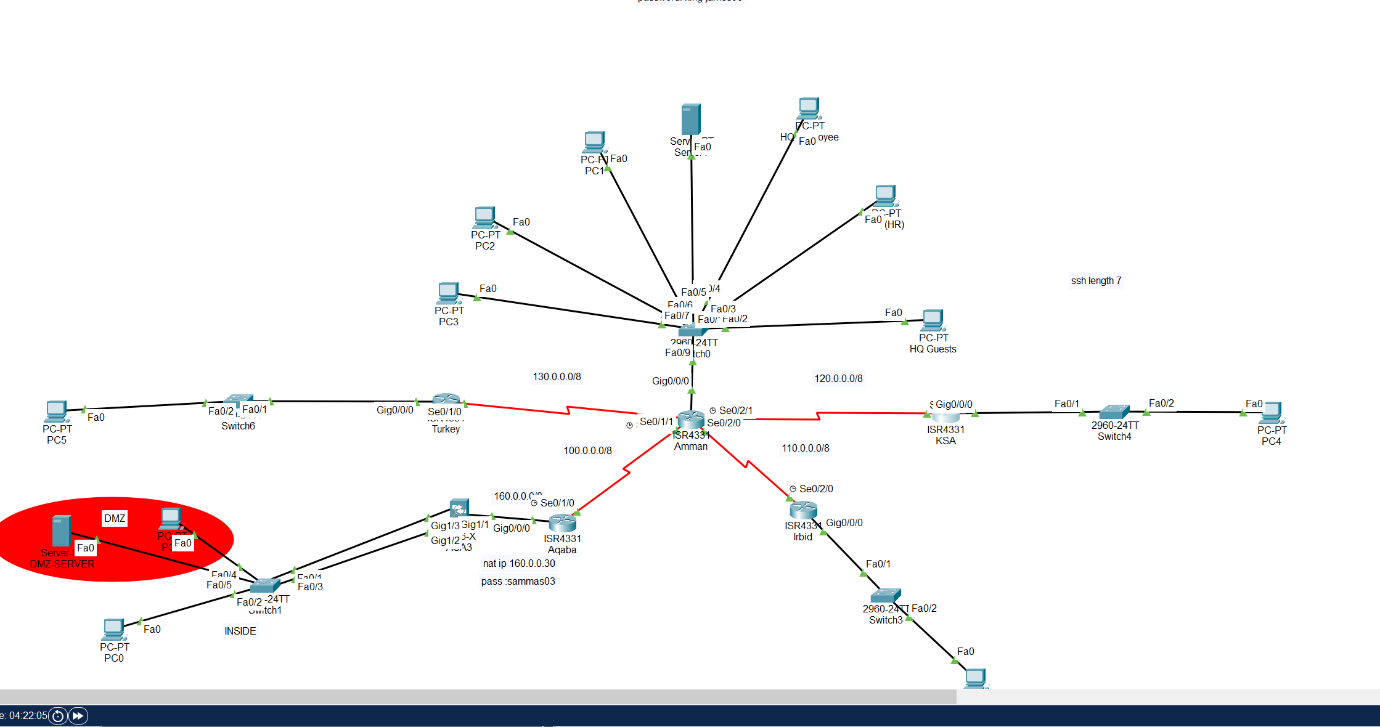
System design:

Topology of a network: the first thing that I would think about is the general topology. \_1

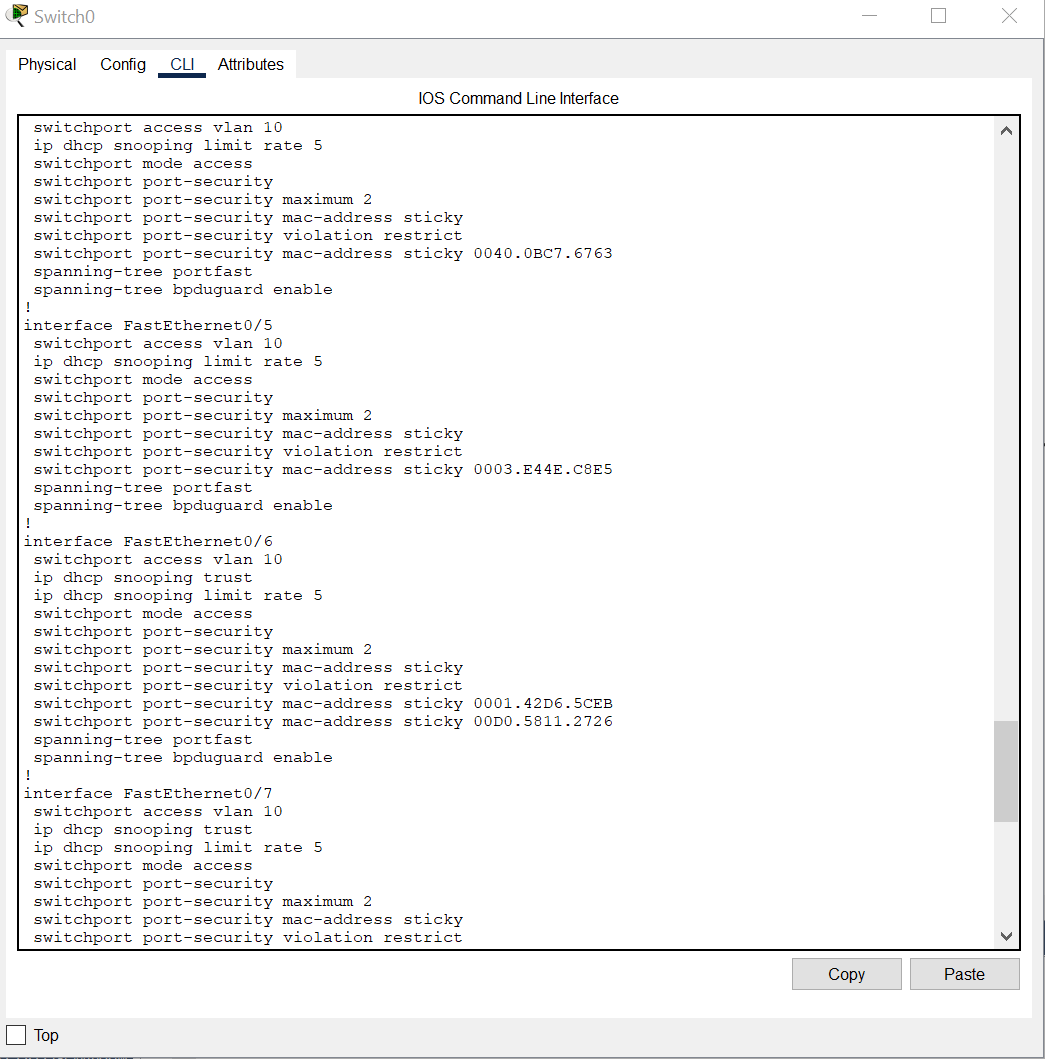
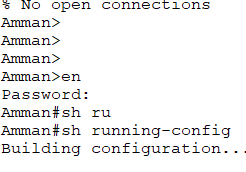


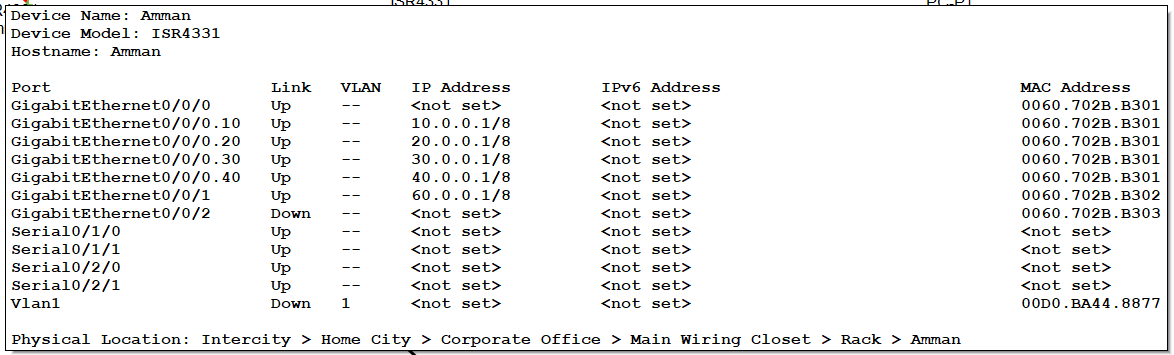
Create a network topology that includes the necessary locations, such as the office in Aqaba, the

data center in Amman, as well as outlying sites in Saudi Arabia, Turkey, and Irbid.

To connect the distant sites to the Amman data center, use VPN/IPsec site-to-site connections

2\_ the second thing that I would think about is the routers and switches, switch and router security measures:





1\_For administrative access to switches and routers, use secure passwords.

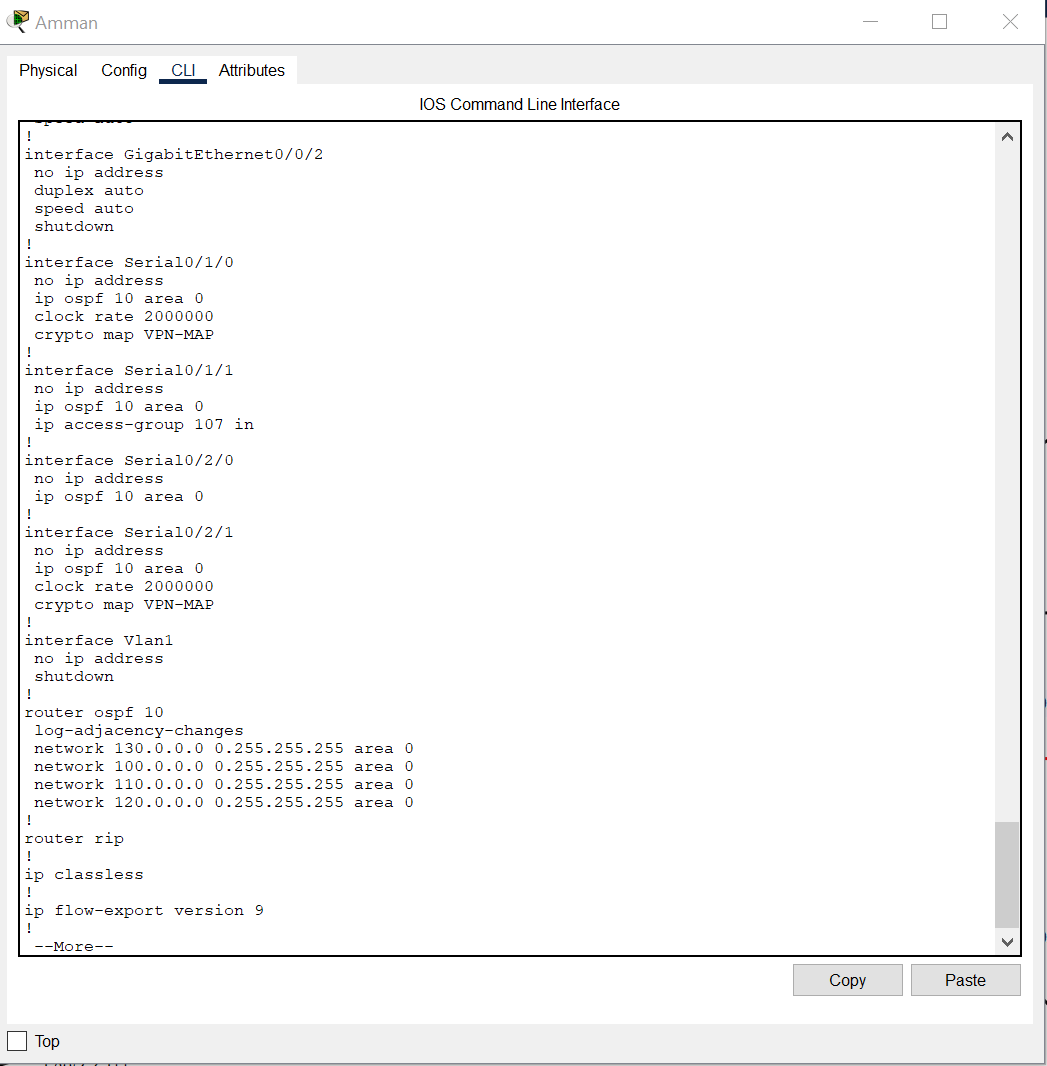
When managing remotely, use SSH rather than Telnet. \_2

3\_To reduce potential attack points, disable unused ports.

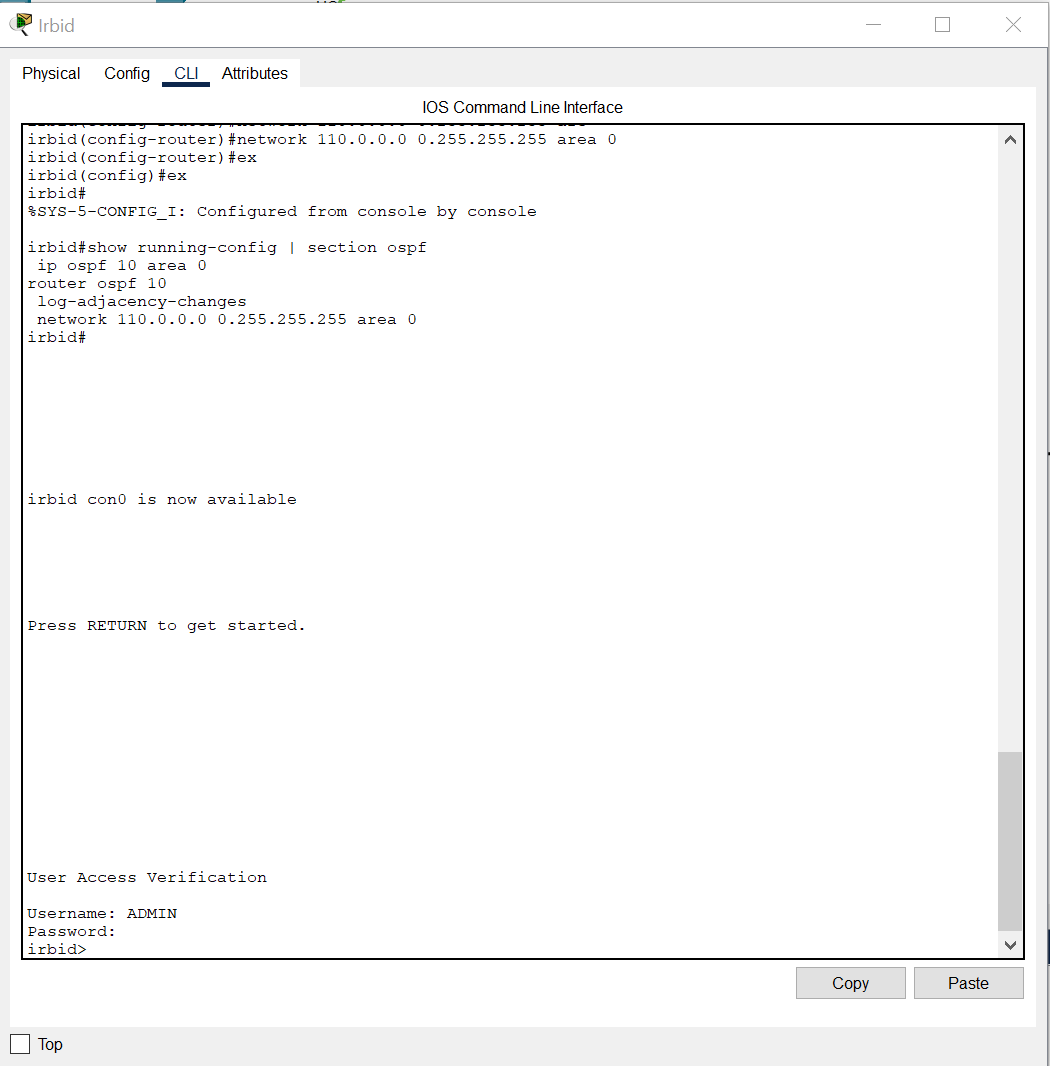
Put in place port security with a two-MAC-address restriction per port. \_4

Apply DHCP security measures with a rate limit of 5 to guard against spoofing and hunger. \_5

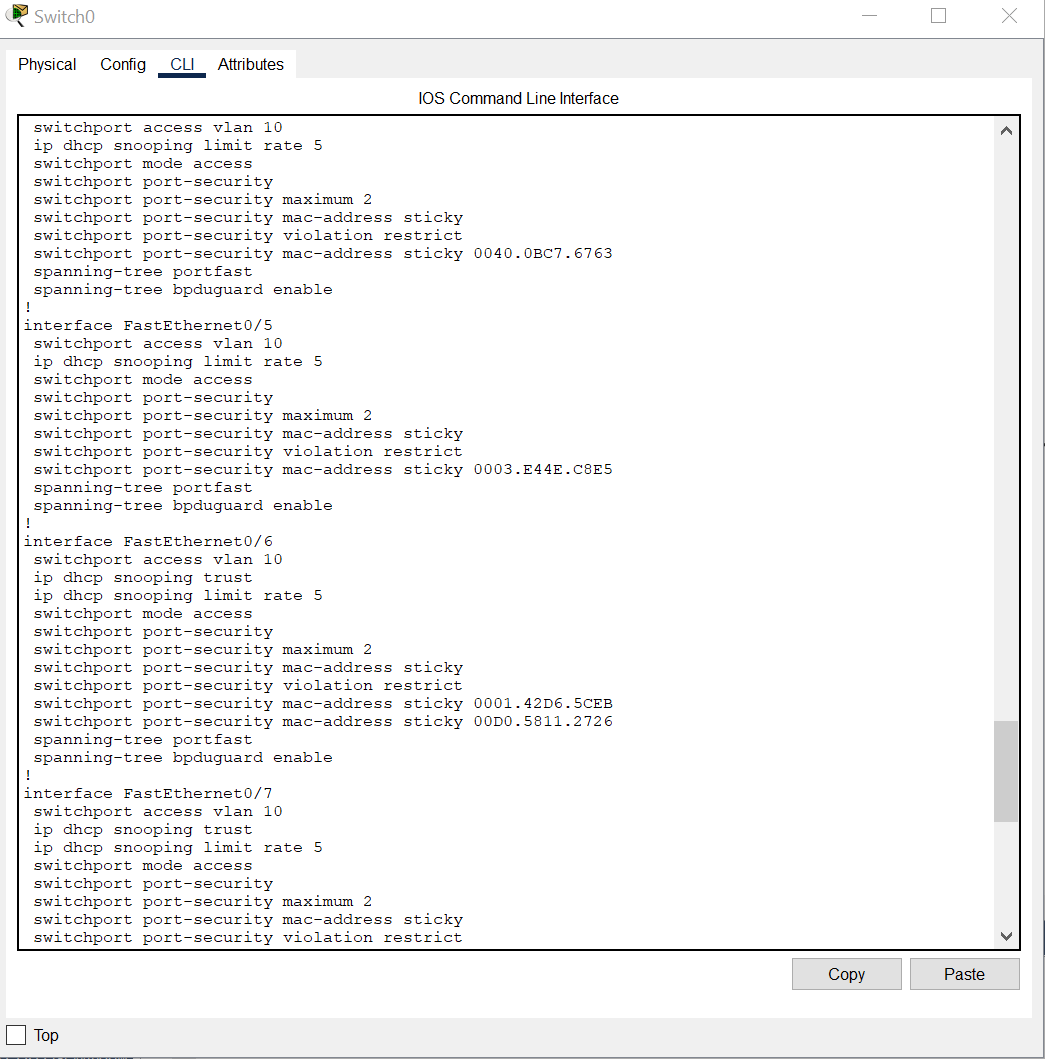
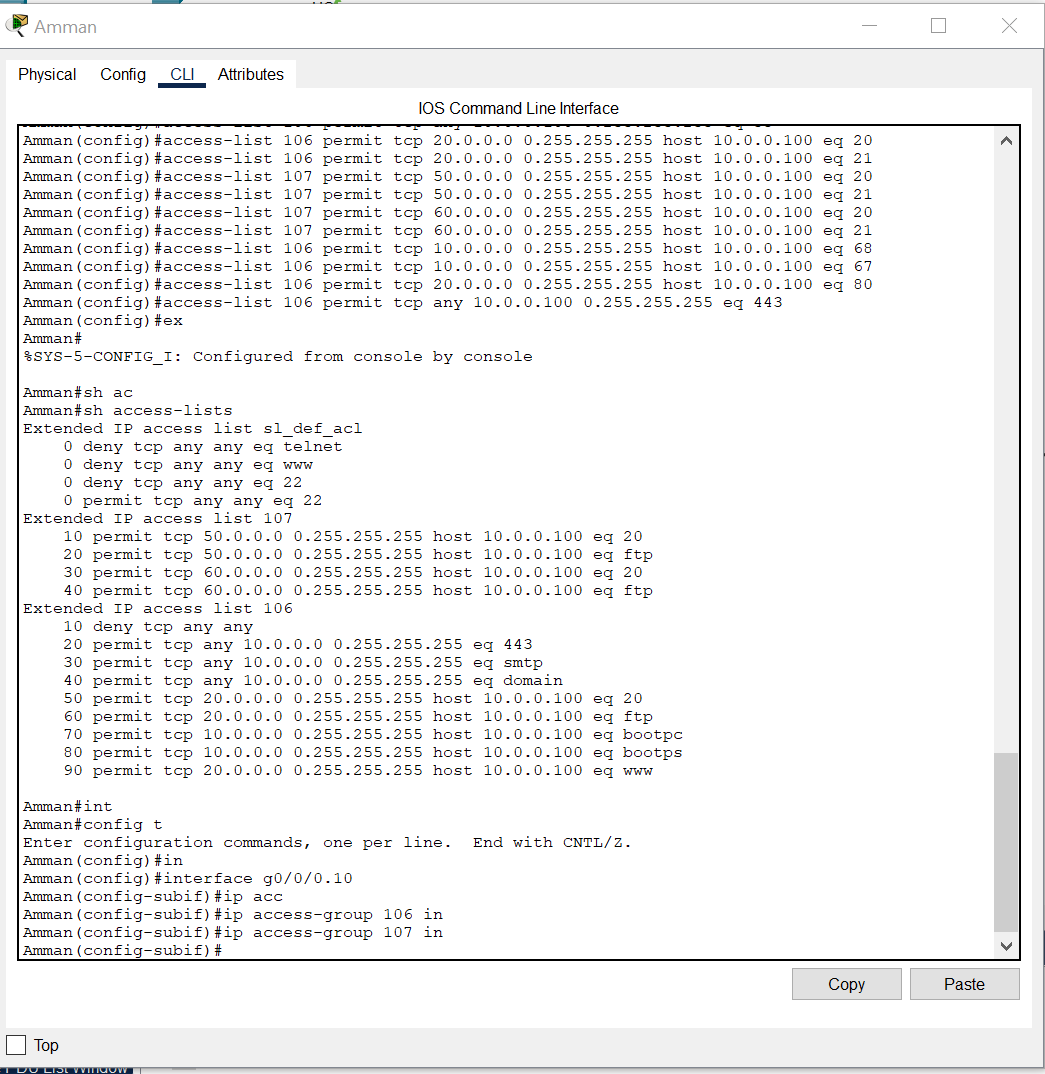
3\_Routing: to pick the routing protocol and the protocol that transfer the traffic throw the routers and from them:

Instead of static routing, use dynamic protocols like OSPF or EIGRP, to provide proper routing between network segments, configure OSPF or EIGRP.

4\_AAA local authentication: that connected with the vty line to have username and password in local database and that's done in IRBID router, configure local AAA authentication for VTY lines. For SSH access, create a username (ADMIN) and strong password (HTUNETSEC2023).



5\_Server accessibility: and its control by something called ACL but let's talk about it, it's restriction of accessing and basic level of security, to control server access based on the rules provided. Also Create a VLANs for network segmentation and assign appropriate IP subnets to each VLAN. That make the VLANs can have multi sup interfaces with one physical cable. Let's take a look of these in topology



Allow HTTP server access from all VLANs and LANs. \_

Allow mail server access from all VLANs and LANs. \_

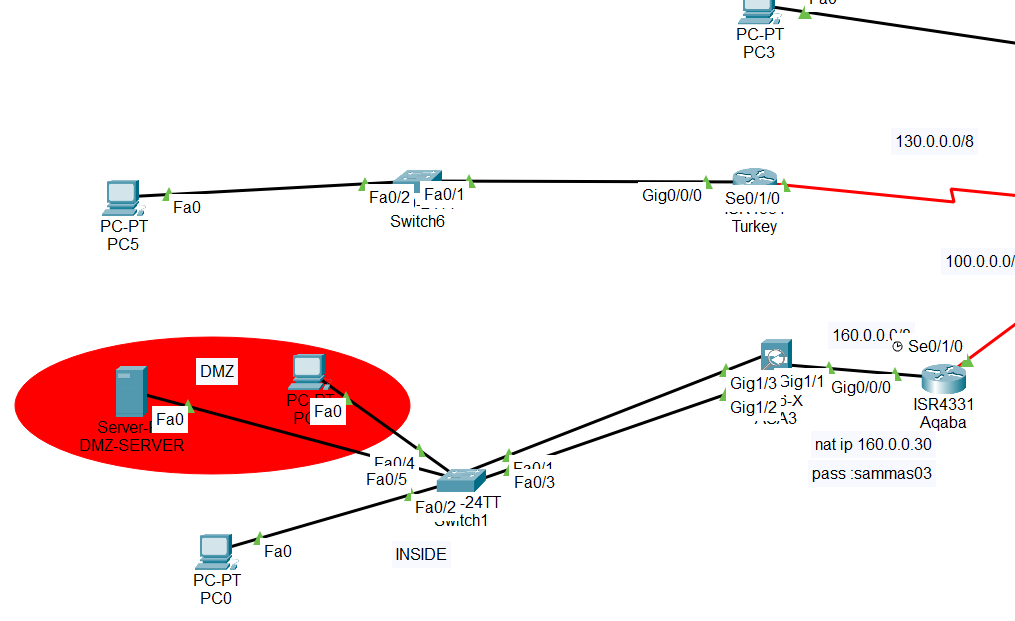
\_Allow DNS server access from all VLANs and LANs.

Allow access to the FTP server only from his EMP headquarters and office in Aqaba. \_

Allow access to the DHCP server only from the HQ data center VLAN. \_

Allow access to the HTTP server only from the HQ EMP LAN. \_

6\_DMZand ASA firewall: the DMZ is isolated area that has sensitive assets with a firewall to protect the network, Aqaba office disaster recovery location:



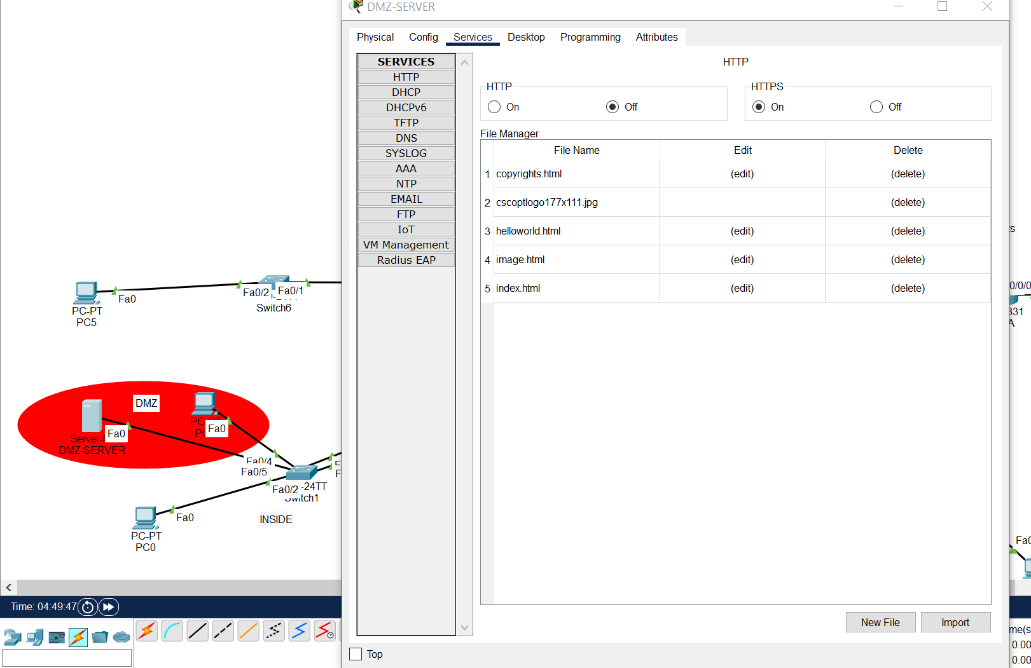
Configure the ASA firewall instead of the Aqaba office router.

Set up two separate VLANs.

One for the Aqaba office and one for the redundant HTTPS server.

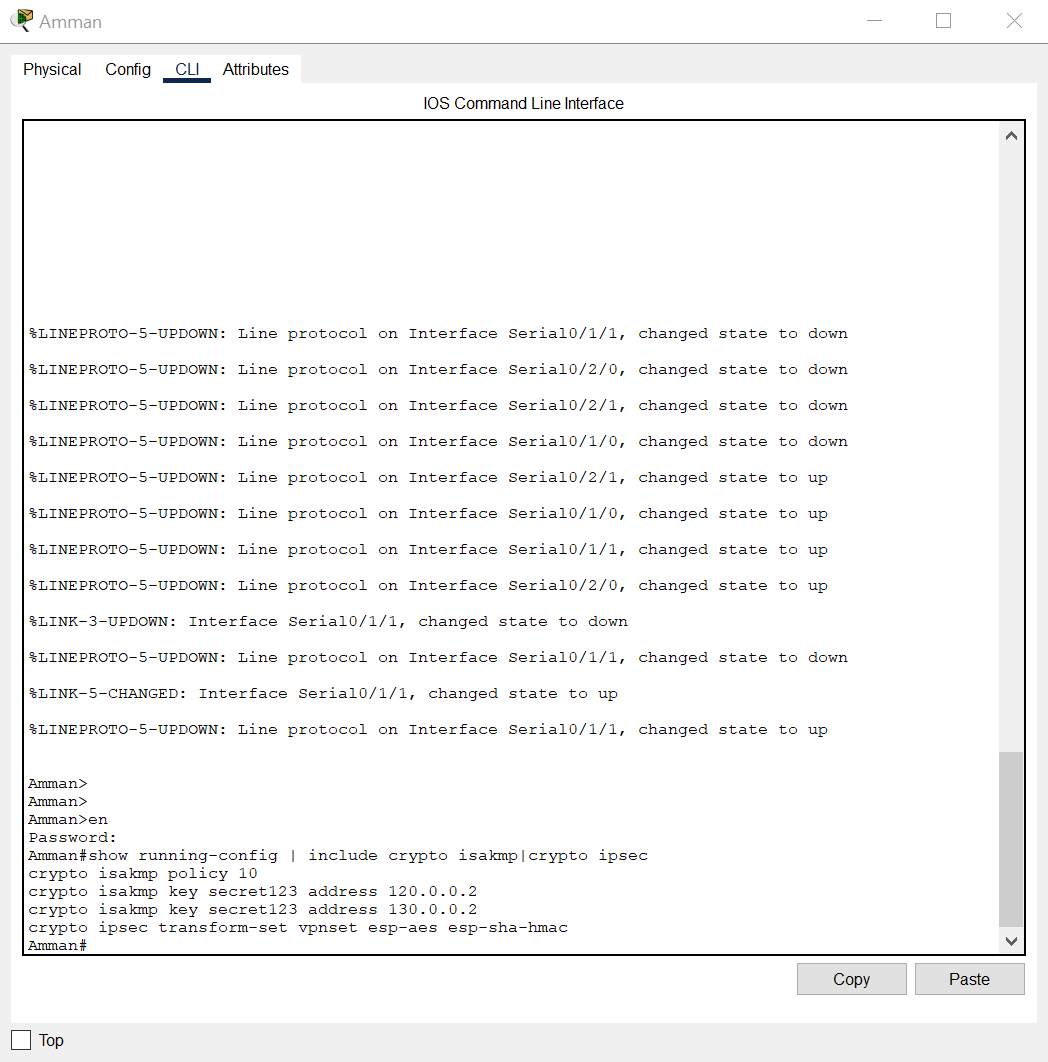
Configure an access rule on the ASA firewall to allow SSH access to the Aqaba ASA router only from HQ data center PC1 (10.0.0.10).

Configure DMZ for VLANs (VLAN 50 for private and VLAN 60 for public) on the ASA firewall.



7\_ VPN protocol:

Implement a VPN/IPsec site-to-site connection between a network outside Jordan and a data center in Amman. Choose a VPN protocol that supports secure and encrypted communication.



certification:

Configure strong authentication mechanisms such as digital certificates and pre-shared keys to ensure only authorized devices can establish her VPN connection.

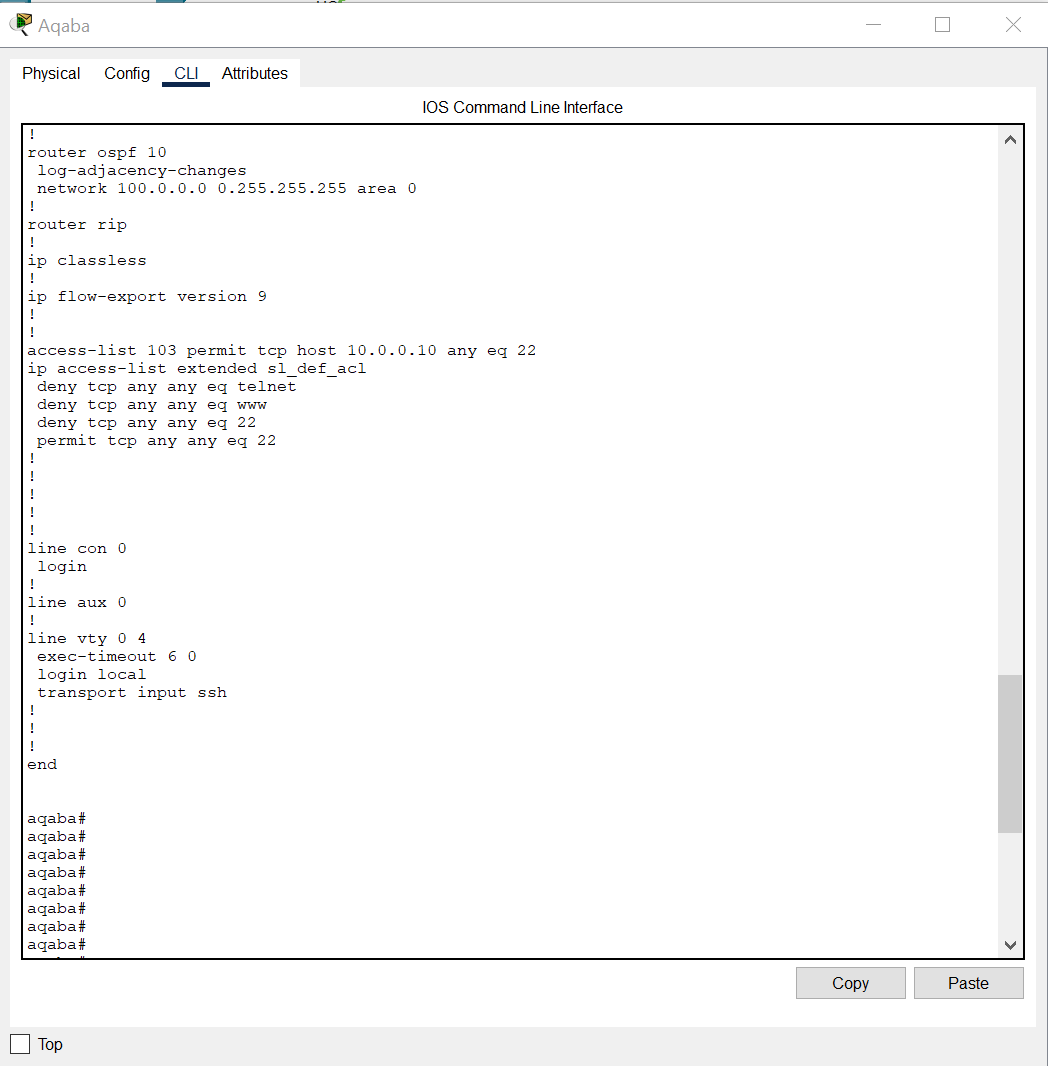
encryption:

It uses strong encryption algorithms to protect data sent over VPN tunnels, ensuring confidentiality and integrity.

Hardening the VPN gateway:

Apply security best practices to VPN gateway devices, such as disabling unnecessary services, applying regular patches, and configuring secure administrator access. Access control:

Implement access control policies to restrict access to VPN connections. For example, allow access to his SSH service on Aqaba ASA router only from HQ data center PC1 (10.0.0.10).



Logging and monitoring:

Enable logging and monitoring on your VPN device to track and detect suspicious activity and potential security breaches.

Investigation:

The goal of a secure network in this scenario is to set up a reliable and protected network infrastructure that meets customer needs. The main requirements are:

Establishing a VPN/IPsec site-to-site connection:

Networks outside Jordan must use VPN/IPsec technology to securely connect to the Amman data center. This ensures secure encrypted communication between remote networks and central data centers.

Hardening Switches and Routers:

To mitigate potential security risks, all switches and routers in your network should be hardened. This includes implementing strong passwords, enabling SSH (Secure Shell) instead of Telnet for remote access, disabling unused ports, implementing port security with a maximum MAC address limit of 2, Includes applying DHCP security measures to prevent spoofing and starvation. Proper Directions Support:

To ensure efficient and scalable routing within the network, the network should use a dynamic routing protocol such as OSPF (Open Shortest Path First). This eliminates the need to use static routing and allows automatic and dynamic path selection.

Access control to servers in VLAN 10:

Servers in VLAN 10 have special access requirements. HTTPS, mail, and DNS servers must be accessible to all VLANs and LANs. The FTP server should only be accessible to his EMPs (employees) in the headquarters and Aqaba offices. The DHCP server should only be accessible via his VLAN in the HQ data center. The HTTP server should be accessible only from the headquarters EMP LAN.

Local AAA authentication for SSH:

The IRBID router must implement local AAA (Authentication, Authorization, and Accounting) authentication for the SSH protocol. This requires creating a username (ADMIN) and password (HTUNETSEC2023) for secure access to her VTY line on the router.

Aqaba office as a disaster recovery hub:

The Aqaba office was to act as a disaster recovery site with two separate VLANs. The first VLAN serves the Aqaba office and the second VLAN hosts redundant HTTPS servers. You should use an ASA (Adaptive Security Appliance) firewall instead of a router. Access to the SSH service on the Aqaba ASA router should be restricted to HQ Datacenter PC1 (10.0.0.10). Additionally, the DMZ should be configured to support VLAN 50 (private) and VLAN 60 (public).

By implementing these requirements, your network can ensure secure communications, protect against malicious activity, support efficient routing, and control access to servers based on specific rules and VLAN configuration is designed to.

Hardware:

1\_ router: Series routers are a good choice for your network. It offers advanced security features, support for dynamic routing protocols such as OSPF, and built-in VPN capabilities.

2\_ASA firewall: Firewalls can be used to enhance security and access control. It provides features such as VPN/IPsec, SSH access control, DMZ configuration, and intrusion prevention.

3\_ a server that include the services and well secured to avoid any attack on it. It could include DHCP, DNS, HTTPS, HTTP, FTP, TFTP. All those services to serve the network.

4\_ switches: Series switches are commonly used in corporate networks. Models like the Catalyst 9000 Series offer superior performance, advanced security features, support for VLANs, port security, and dynamic routing protocols.

5\_ end points: and those represent the workstation and the user devices that use the network.

Software:

1\_ VPN: It can be used to establish a secure site-to-site connection between a network outside Jordan and the Amman data center so to make remotely connection. IPsec can be used as the underlying protocol for secure communication.

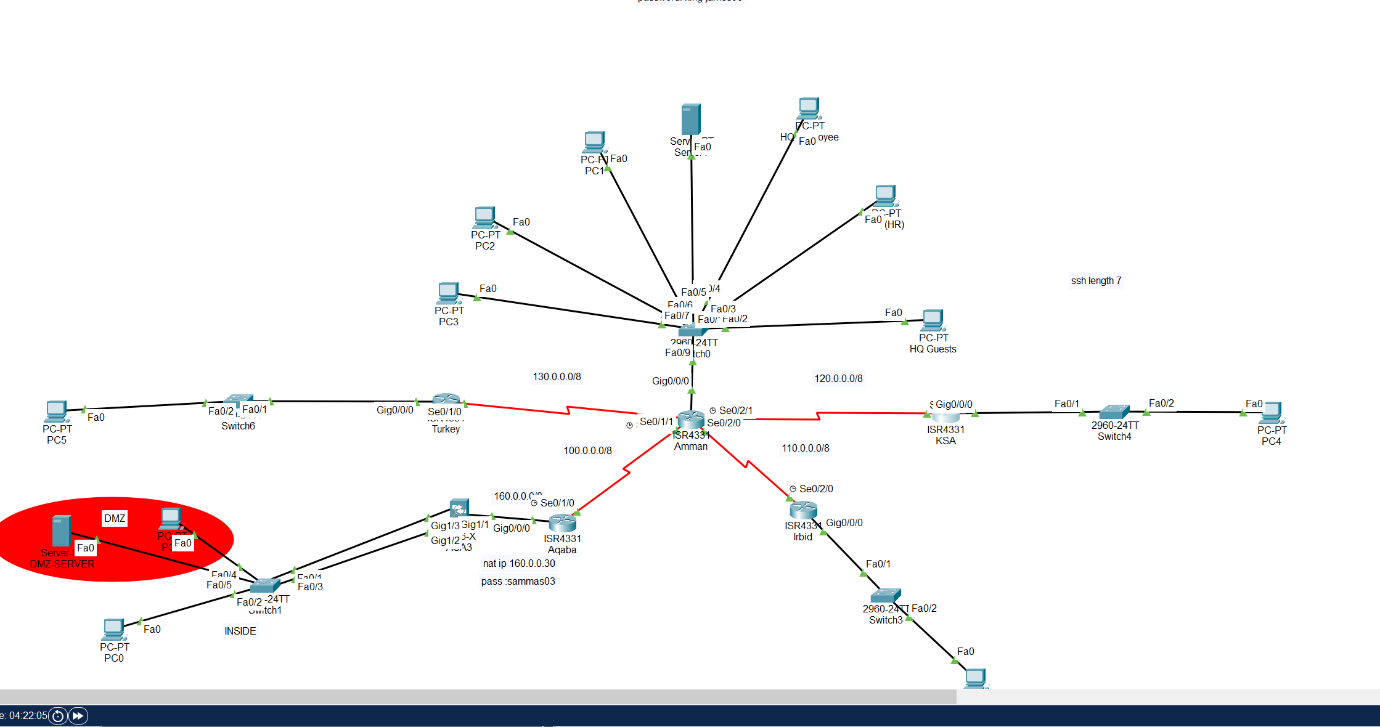
2\_ ssh(secure shell): Encrypt all communication between client and server, including usernames, passwords and transmitted data. This prevents eavesdropping, data interception, and manipulation by malicious users.

3\_AAA: it's a protocol to guarantee the authentication, authorization, accounting and can AAA authentication is implemented by configuring specific software on the router to enable AAA services, defining an authentication method (such as a local username/password or an external authentication server such as RADIUS or TACACS+), and defining an authentication policy. and set rules to allow access.

4\_ipsec: A set of protocols and algorithms used to secure IP communications by providing encryption, authentication, and data integrity.

5\_ Nat: is a network technique used to change IP addresses and port numbers in IP packets as they pass through network devices such as routers and firewalls. NAT is primarily used to conserve IP address space and facilitate communication between different networks with overlapping or private IP address ranges.

The implementation:



Let's justify our choices:

Router: this device is a smart device to transfer the packets around the network it's a perfect device t represent a branch in the scenario.

Firewall: is a network security device that guarantee the filtering of the packets it's the first device against any malicious packets it's wonderful choice for the network and essential in the same time.

Switches: it's a local device to control the LAN so it's better than hub, the switch don't send broadcast massage it's depends on layer to transfer packets locally.

Gateways: play an important role in forwarding network traffic between different networks. It examines the destination IP address of incoming packets and determines the appropriate path to forward the packet to reach its intended destination.

Passwords: it's a way of denying any authorized user to come in and we can make It encrypted.

SSH: this protocol guarantees the confidentiality with encryption connection between the client and server it's essential in for the network security.

SSL: is a cryptographic protocol that allows secure communication over a computer network (usually the Internet). It establishes an encrypted connection between a client and server and ensures the confidentiality and integrity of data sent between the client and server. It's absolutely great choice.

IPsec: it's software to secure the IP address that get the confidentiality, integrity and authentication also accept implement ACL.

VPN: this protocol isn't make a remote connectivity only and it's encrypted and hash so it's perfect protocol for that.

HTTPS: is an encrypted protocol of HTTP that use for the web browsing in the network so it's much better in security.

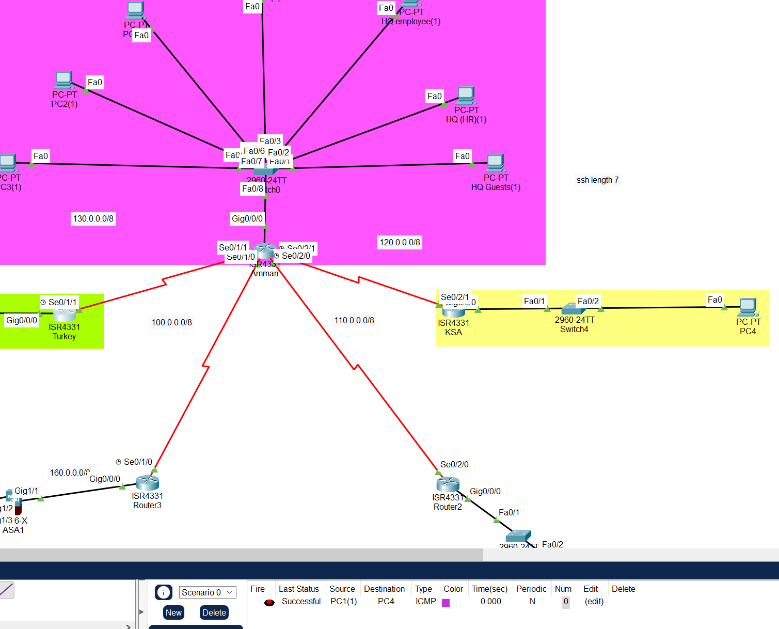
FTP: it's a protocol to transfer the files and it's useful in the network we could make ACL to make It more secure.

DHCP: so the protocol to getting the ip address dynamically depends on specific range.

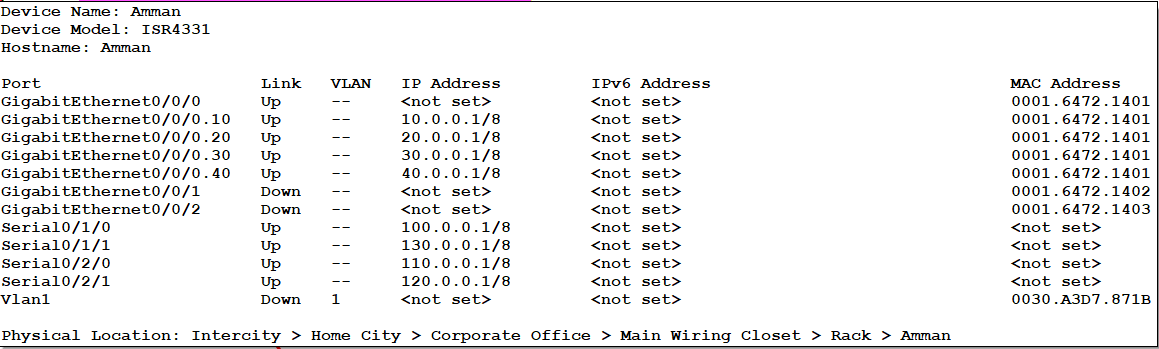
TEST PLAN: A test plan is a vital document that specifies the goals, scope, strategy, and particular actions for testing network infrastructure, protocols, settings, and security measures in the context of networking and network security. It is essential for making sure that testing efforts are well specified and in line with intended results. The test plan aids in methodically evaluating the network's operation, performance, dependability, and security by establishing objectives, scope, and testing procedures. Additionally, it makes it easier to analyze risks, follow rules, collaborate with stakeholders, record testing operations, and ensure overall quality. In the end, a well-executed test strategy aids in vulnerability discovery and mitigation, creating a stable and secure network environment.

|  |  |
| --- | --- |
| The way of testing | The tested part |
| The routing protocol can be tested by the ICMP service between two networks and any device in any network. Check any open unused ports and be careful of misconfiguration and to have the right configuration | Router |
| Check the layer 2 security by accessing the configuration of the switch. Close uneased ports and having the write mode between the switch and the router also the switch and the endpoints. | Switches |
| Check if the firewall have the right ACL to filter the packets then to ensure of the firewall give it right with security level of it you can do this by ICMP between two different area like (DMZ,INSIDE,OUTSIDE) | Firewall |
| It can be test it if it's implement in router and switch is by accessing from a pc from that network. | SSH |
| We should test it by making ICMP packet go throw it and make sure every gateway have the right gateway | Gateway |
| It should be strong to avoid any unauthorized access we can check by go through the level of CLI of those devices. | Password |
| It's can be tested by the ICMP method between two routers that has the VPN connection and that with using IPSEC protocol. | VPN |
| That a basic level of security and can be test it from the command that Benn permitted and denied and see if that correctly implemented | ACL |
| Make sure the connectivity of this server to the desire destination is completed and check every service alone. | Sevier of services |

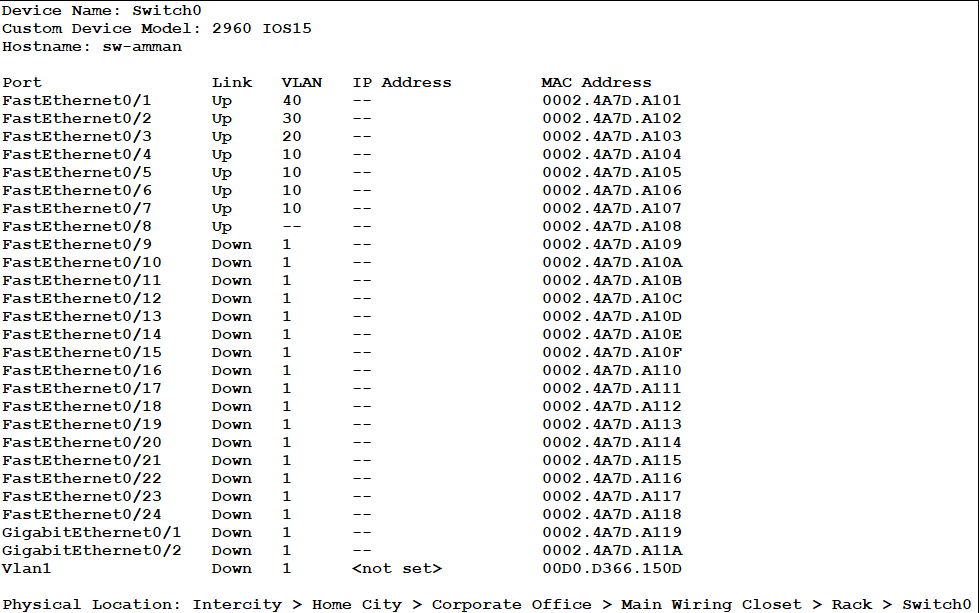
1\_ router:

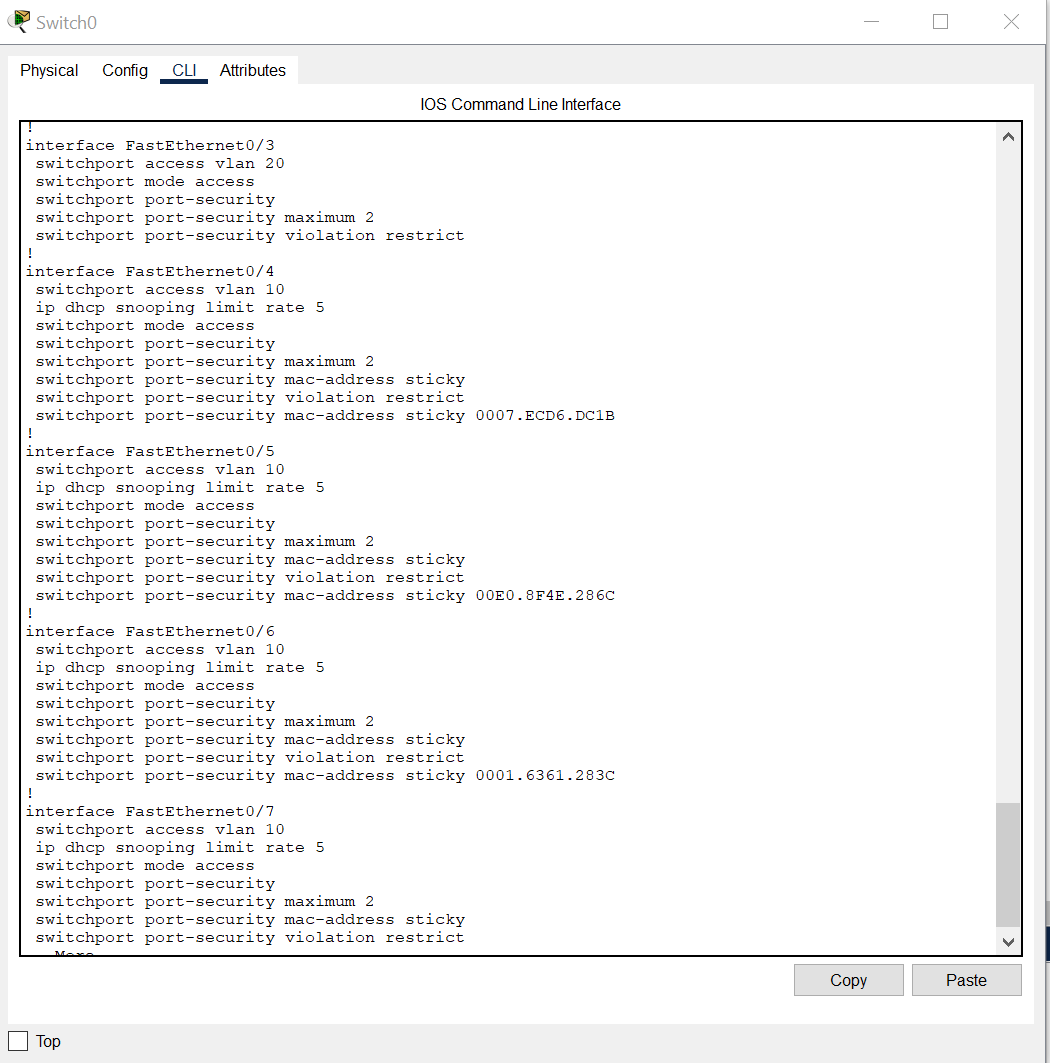


In this case to test ospf which is a routing protocol so the ping from the pc in ksa network to pc in Amman network.

the unused ports in the router

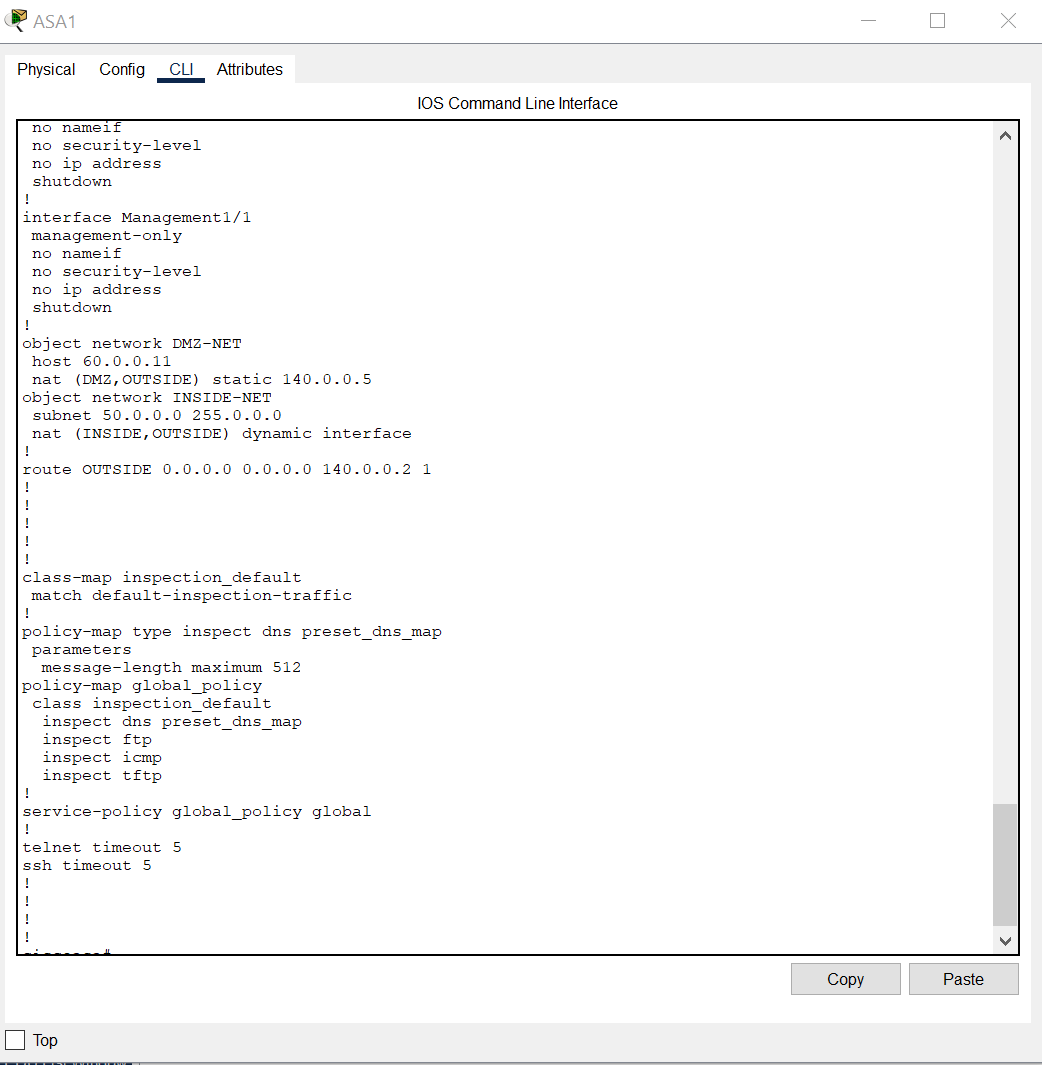
2\_ switch

this is the ports in the Amman switch the unused is closed let's see these ports what it got:



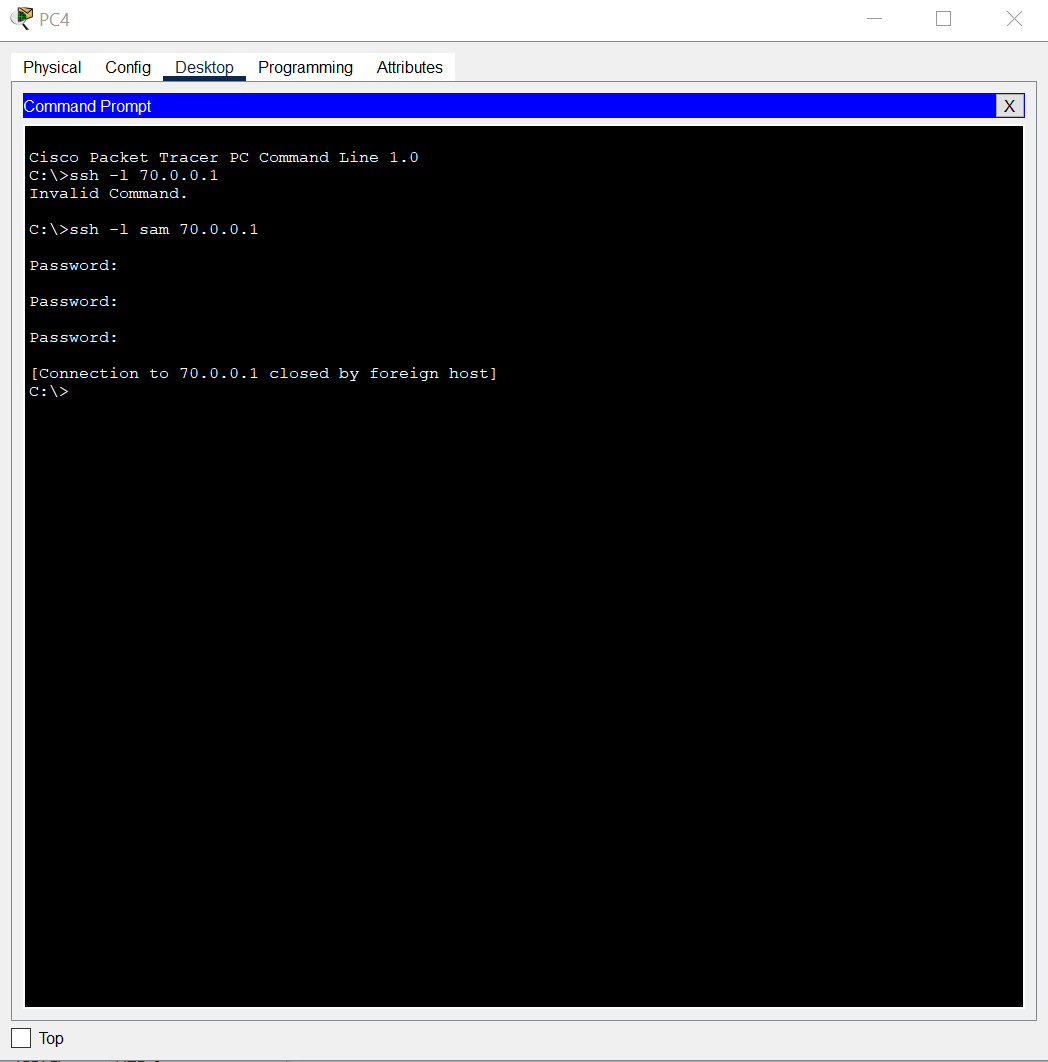
We got port security and dhcp snooping with VLAN configuration in the switch Amman. The others switches have port security.

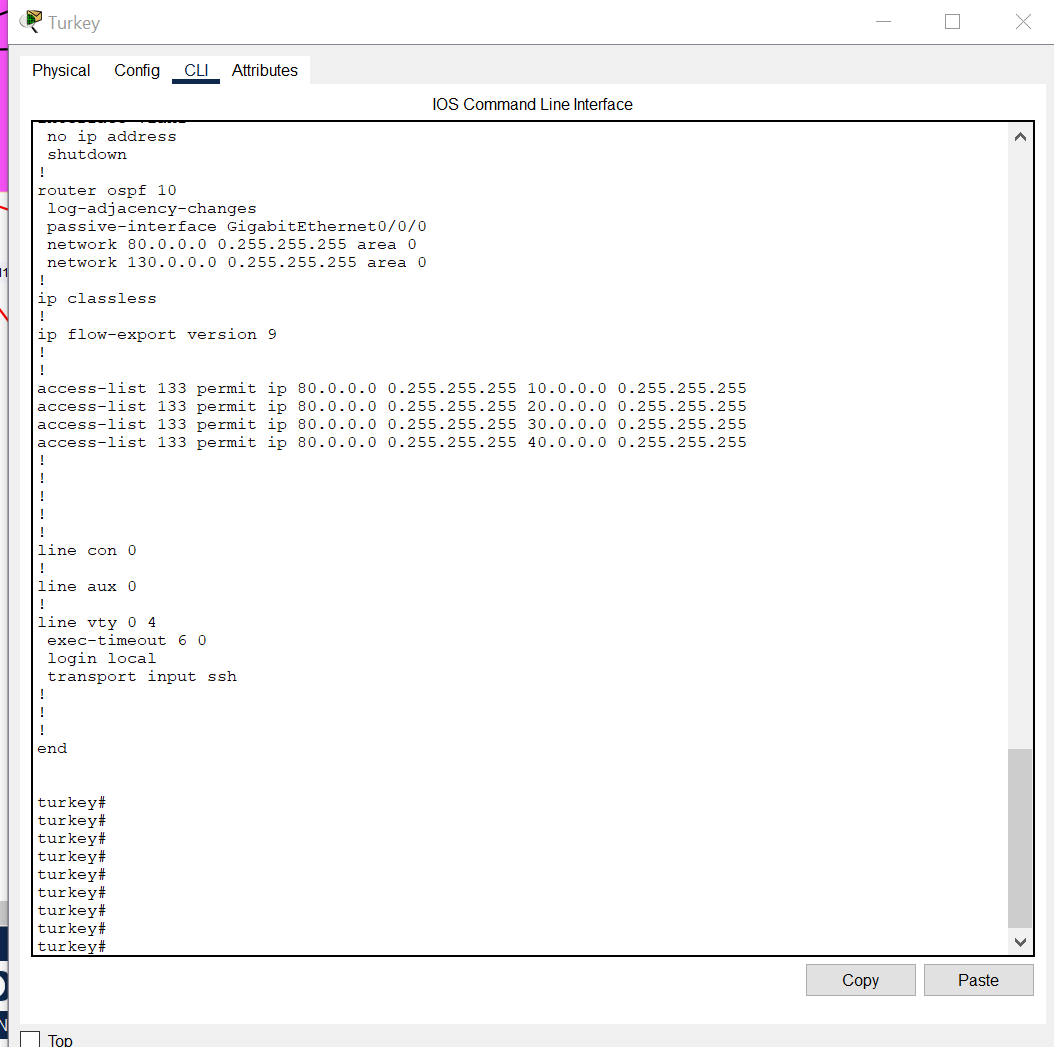
3\_Firewall:

The firewall ASA device have and we going to check of the inside and outside also the DMZ that we have.

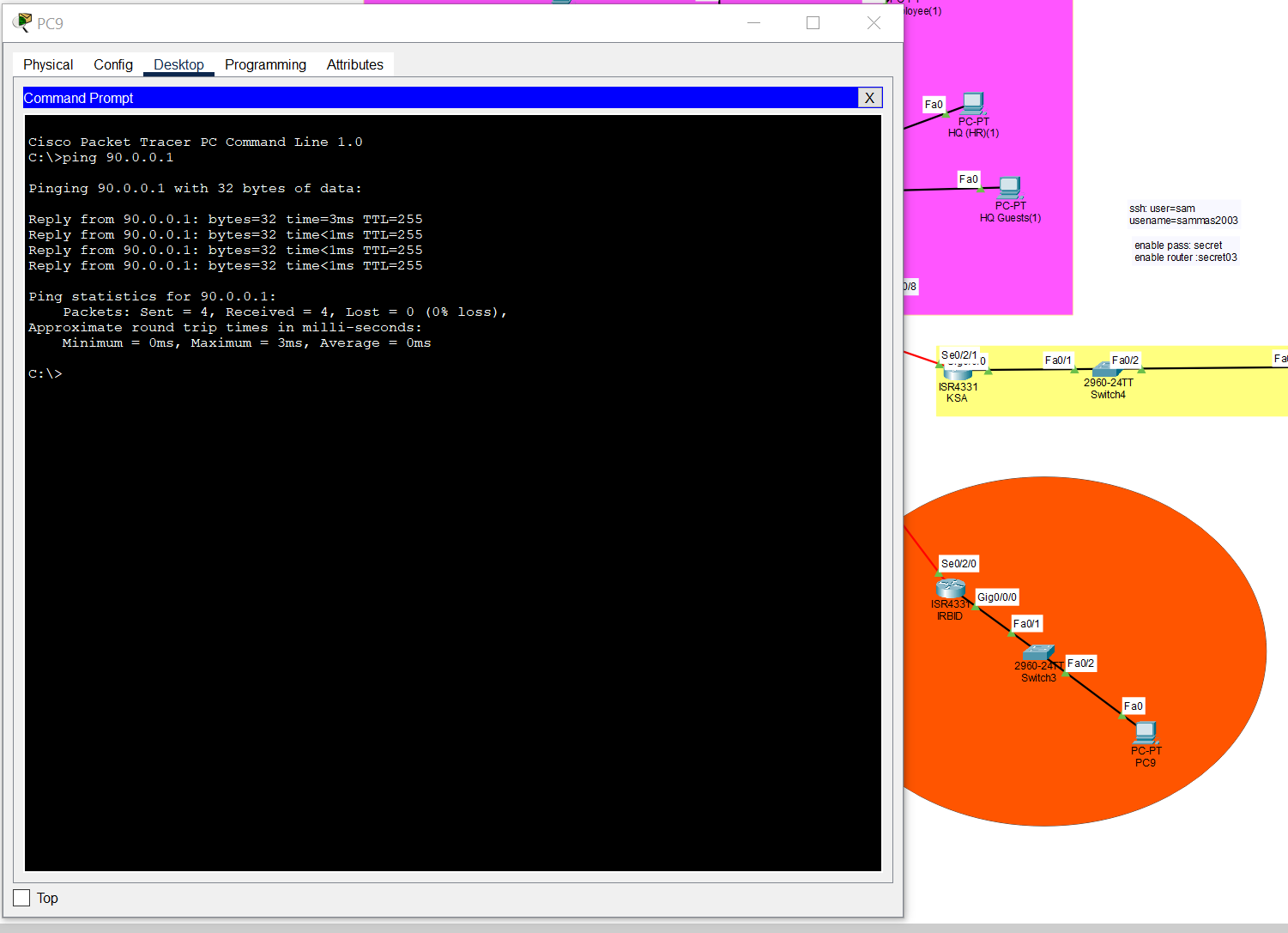
4\_ SSH

I use it for both routers and switches:



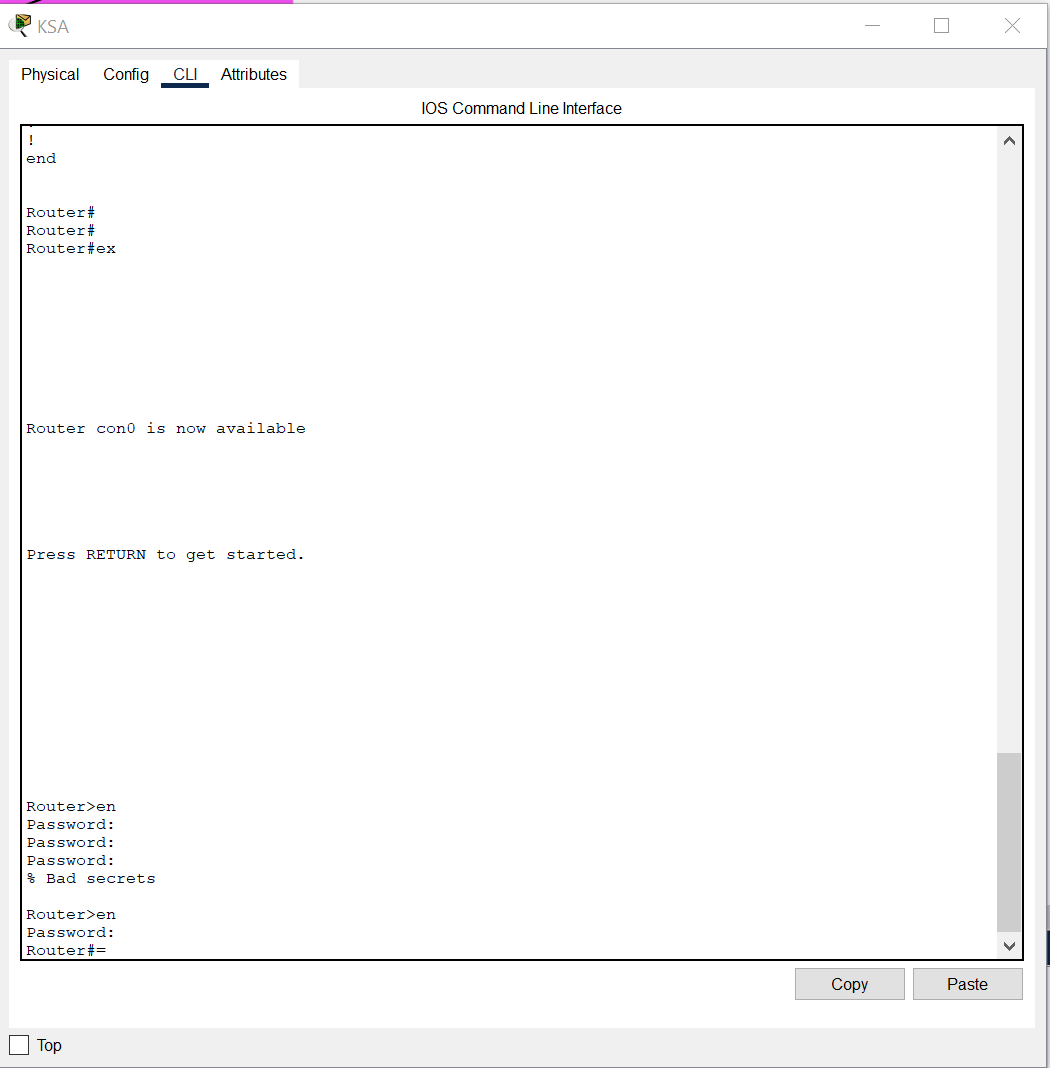
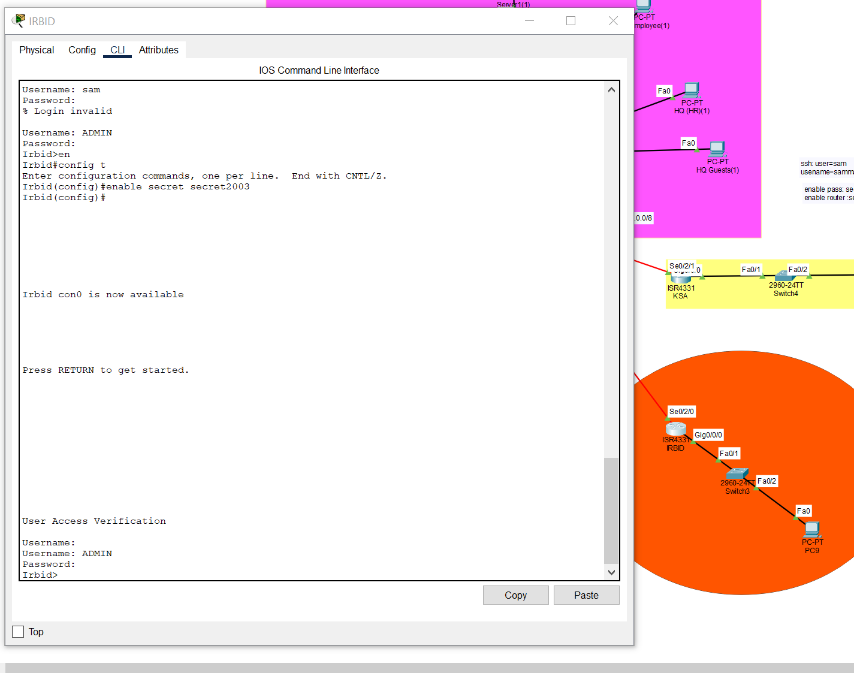


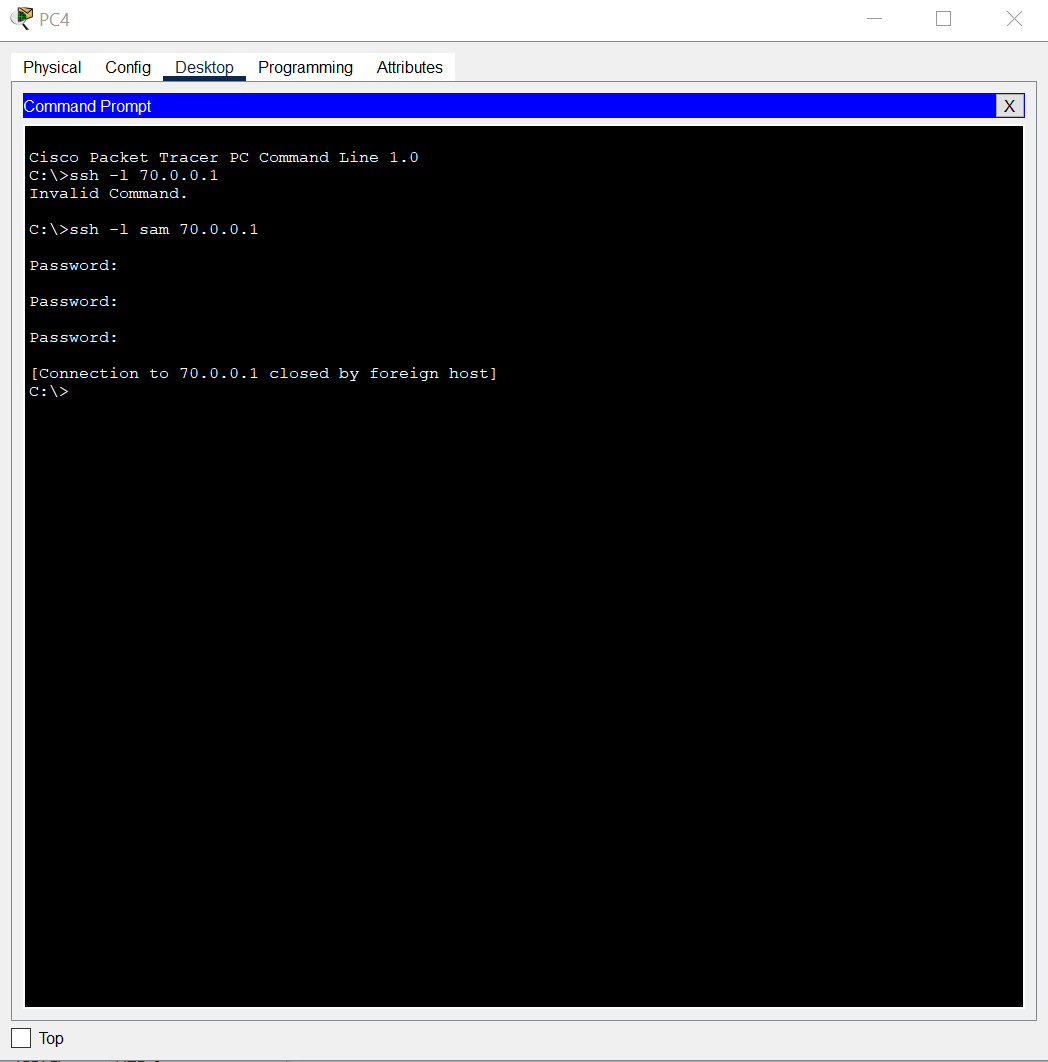
5\_Gateway: ensure that we get the right ip for the gateway so we could check by ping in device inside to the router let's say from pc to gateway directly:



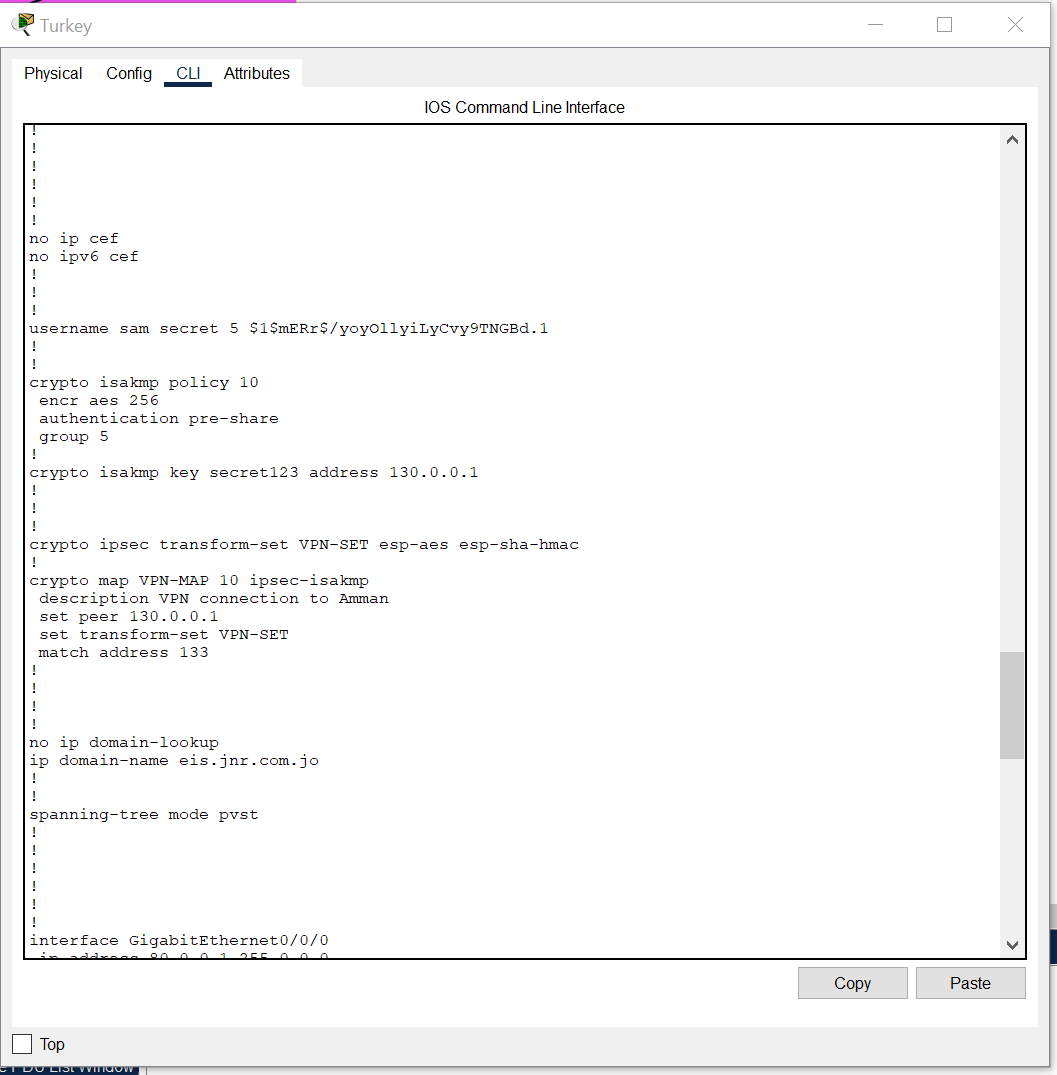
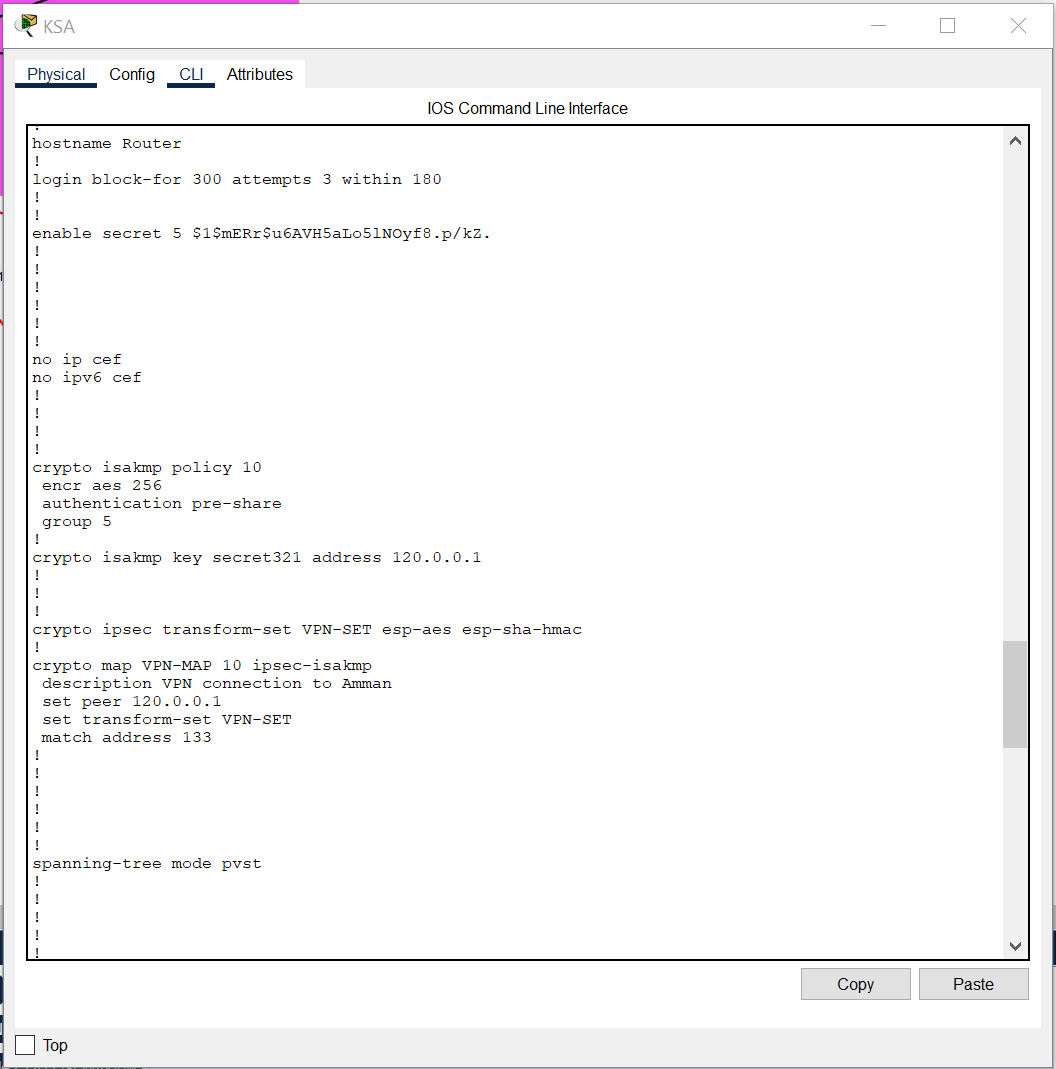
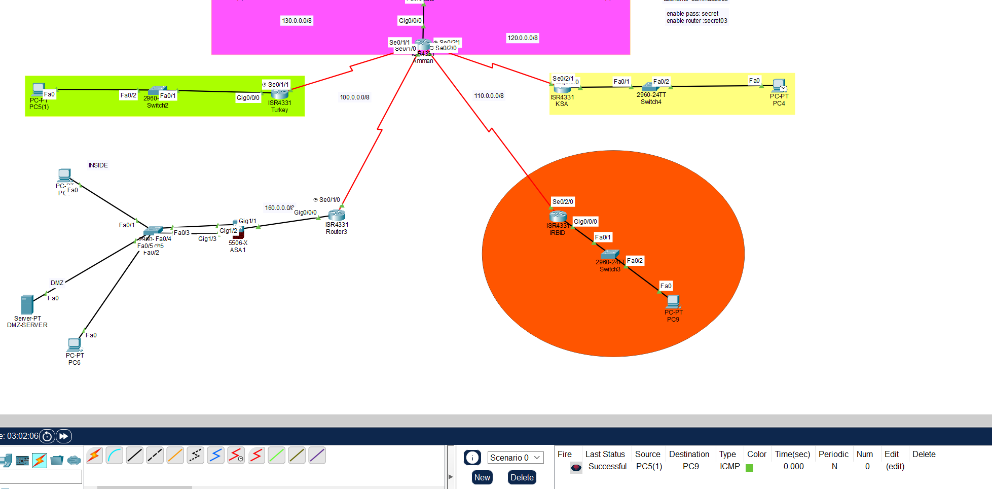
6\_password: it's to use strong password and we have several examples in AAA, SSH and enable password:

The enable in all as SSh but AAA only in IRBID let's a look:



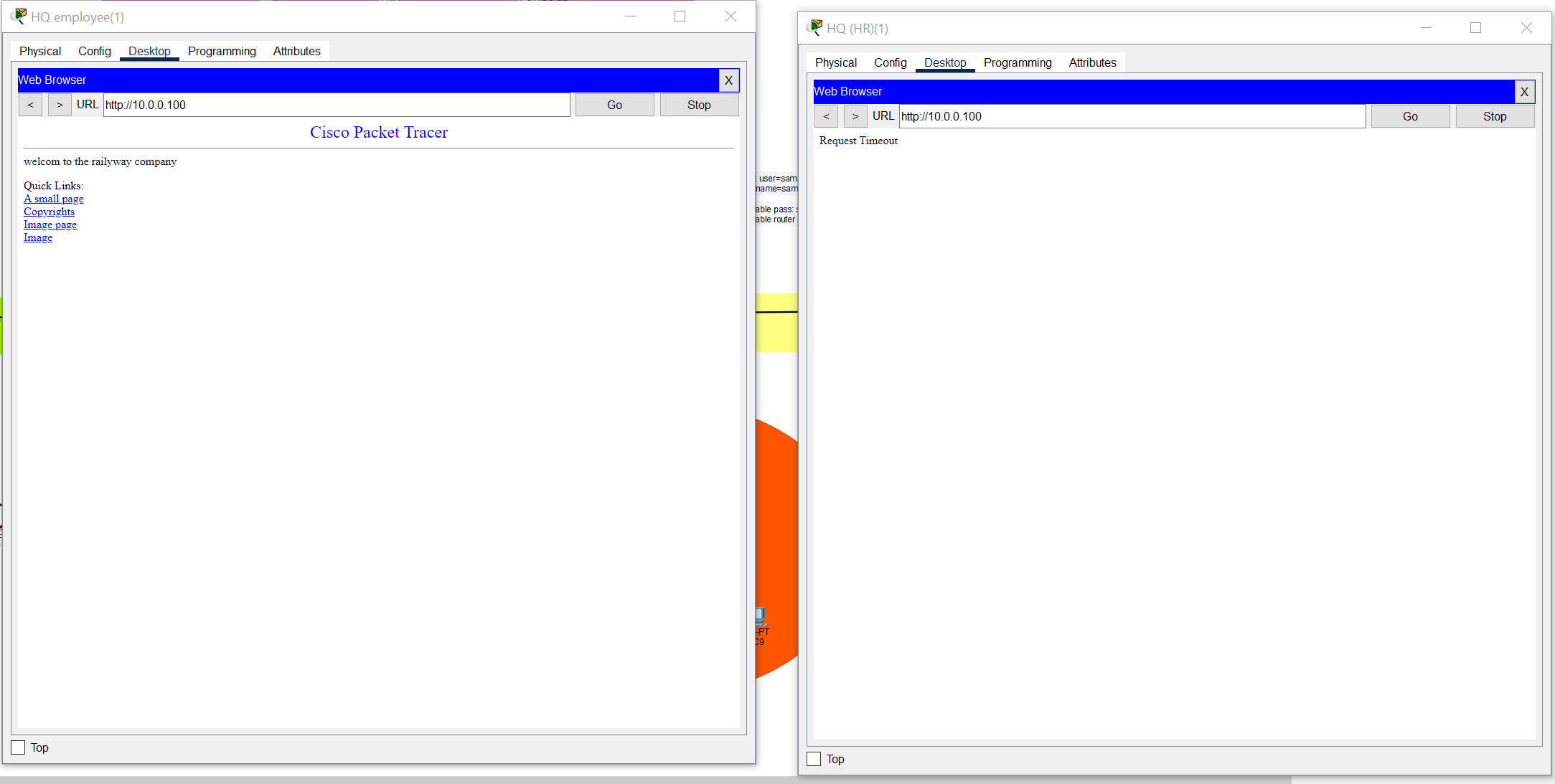


7\_ VPN: it's implemented in the KSA and turkey:

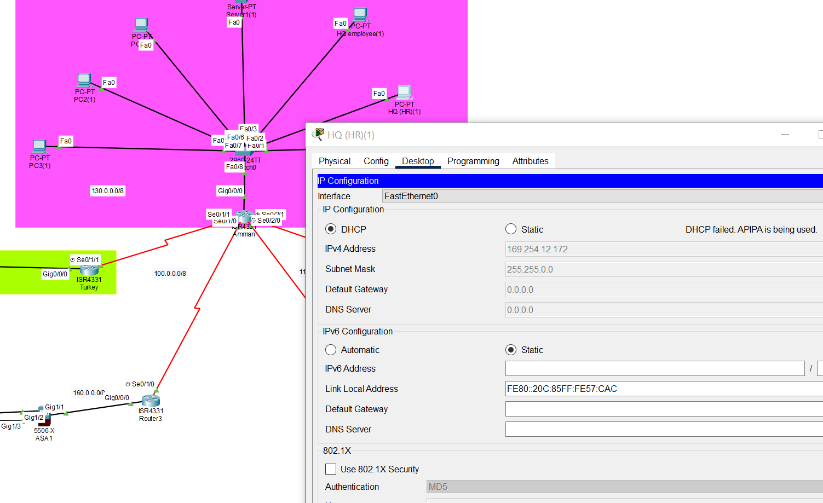


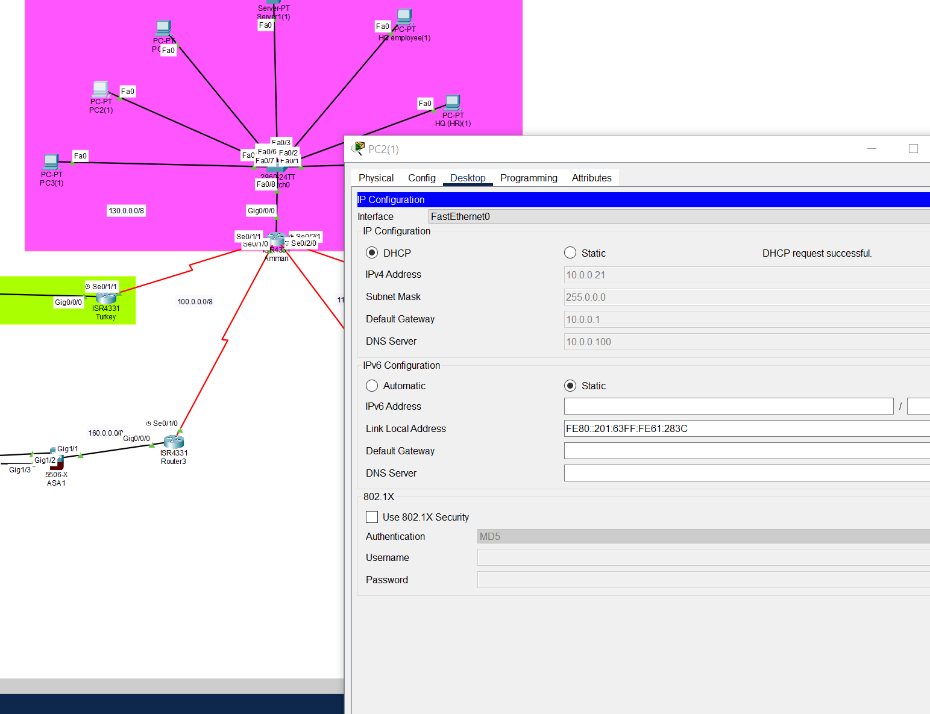
9\_ACL: it's implemented in the outbound Amman router

\_HTTP:



\_DHCP





I think the design is so perfect for the requirements that given. Critically we could add SSL to more secure so the system will be monitored and record logs.

with more obvious procedure to test layer 2 security to have more of one way to check and test part of the network.

Having more than ping massages to check VPN. Using of ftp and implementing an ACL on it not enough use TFTP instead of FTP.

Always make the network easily adopting with the future satiation and scalability for example to have an AAA server instead of AAA database.

To remove all the unencrypted protocol from the network such as HTTP even if it has ACL, still danger.