NAME	HAMZA MUHSEN
COURSE	NETWORK SECURITY
SECTION	ONE
TITLE	TECH GLOBAL

REFERENCES ARE ON THE FINAL PAGE

NETWORK SECURITY REPORT

STEP BY STEP PLAN TO DESIGN A SECURE NETWORK

- First, read and carefully understand the requirements of the network and security:
    - Network requirements needed:
        - Connect HQ (Amman) network with Aqaba, Turkey, Tunisia, Kuwait. Each device in each network should have the ability to connect and communicate with other devices on other networks.
        - Access to certain services (HTTPS, HTTP, FTP, Mail, DNS and DHCP) based on VLANs.
        - Deploy separate subnets to every VLAN as required in the requirements.
        - Configure static IP addresses to certain devices (Gateway, one PC per network, server in HQ datacenter) and the other devices should be given dynamic IP addresses from the DHCP server.
        - Site-to-site VPN/IPsec for linking the remote offices (Turkey, Kuwait, and Tunisia) to the Amman data center.
    - Security requirements needed:
        - Implement security measures on all routers and switch such as : strong passwords, ssh , security ports, DHCP snooping.
        - AAA on Tunisia router.
        - SSH access to ASA from PC with IP address “15.0.0.10” in HQ datacenter VLAN.
        - Configure various access controls lists on all network routers to limit the access of server services that located in HQ datacenter.
    - Define the devices needed to implement the network:
        - Router → for each network (Amman, Aqaba, Turkey, Kuwait, Tunisia) for WAN connectivity.
        - Switch → to create VLANs in each network.
        - ASA firewall → to enhance security in Aqaba network.

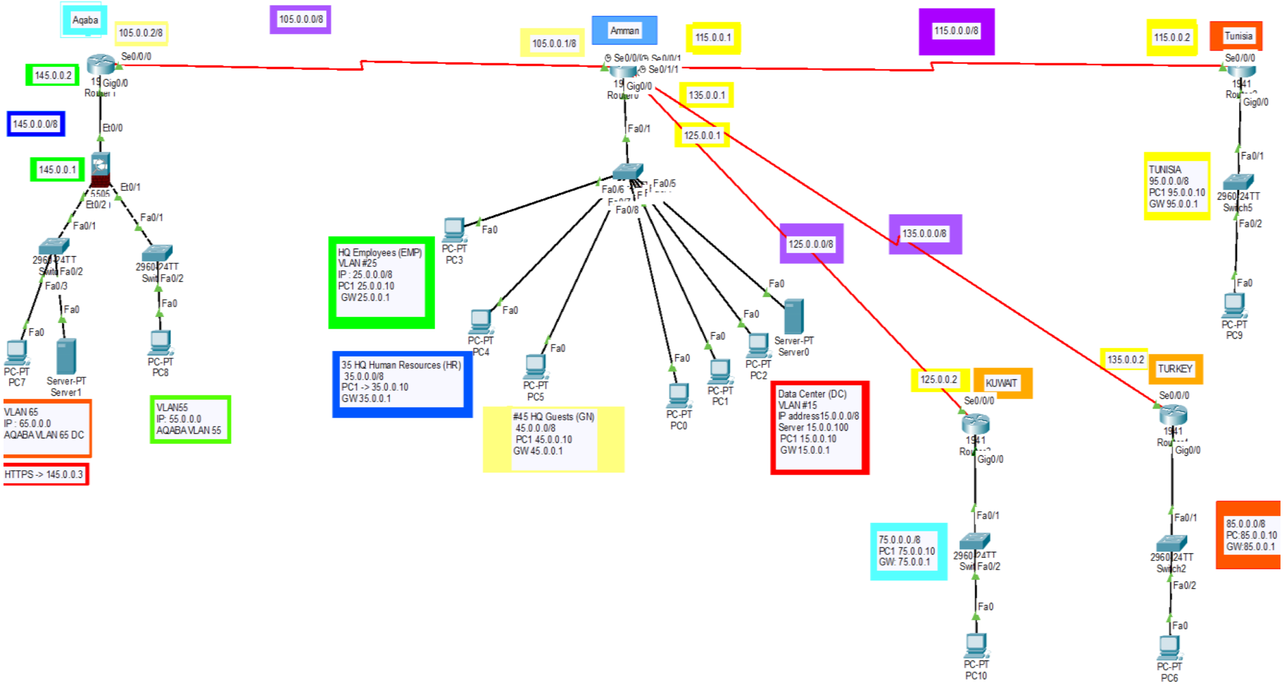
        - Server → to provide services to networks. It is in the Amman router (HQ datacenter).
        - PC → to communicate with each other.
- Design Tech global network topology
    - Amman network contains:
        - One Router and one switch (configured with VLAN 15 “15.0.0.0/8”, 25 “25.0.0.0/8”, 35 “35.0.0.0/8”, and 45 “45.0.0.0/8”).
        - One server with IP address 15.0.0.100 contains all the services required (HTTPS, HTTP, FTP, DNS, DHCP, MAIL)
        - 3 administrators → located in VLAN 15.
        - 3 PCs → one located in VLAN 25 (25.0.0.10/8), one located in VLAN 35 (35.0.0.10/8), and the last one located in VLAN 45 (45.0.0.10/8).
        - Server, One PC from each VLAN and gateway → static IP address.
    - Aqaba network contains:
        - One router and two switches.
        - ASA firewall →configured with VLAN 55 (55.0.0.0 /8),65 (65.0.0.0 /8)
        - 2 PC → each PC located in each VLAN, one for inside network (VLAN 55 “55.0.0.10”) and one for DMZ network (VLAN 65 “65.0.0.10”).
        - One server → located in DMZ network (VLAN 65 “65.0.0.100”) and contains only HTTPS service.
        - Server, One PC from each VLAN and gateway → static IP address.
    - Remote offices, each office contains:
        - One router → with VPN/IPsec tunnels connect each remote office to HQ datacenter and AAA authentication on only Tunisia office.
        - One switch
        - One PC
        - PC and gateway → static IP address.
    - Routing protocol:
        - OSPF routing protocol for offices connectivity.

- After that, use packet tracer to implement all the requirements defined and topology designed:
    - Implement the topology designed in the previous step on packet tracer:
        - Add routers (1941), switches (2960), PCs, ASA 5055 , and servers.
        - Connect devices based on the requirements defined by using cables in packet tracer.
- Apply static IP address to specific devices that are mentioned in the requirement.
- Configure the server in the HQ datacenter and apply all the services required.
- Give dynamic IP addresses to remaining devices.
- Configure VLANs in each network.
    - Create VLANs.
    - Define Port mode (access/trunk).
    - Assign ports to specific VLANs.
    - Transfer the trunk ports from default VLAN to specific VLAN (called native in this project with number 1000)
    - Shutdown and transfer unused ports from default VLAN to specific VLAN (called Parking_Lot with number 999).
- Setup ASA firewall
    - Create VLANs for inside, outside, and DMZ.
    - Give IP addresses for each VLAN.
    - Give security level for each VLAN.
    - Setup routing, address translation, and inspection policy.
    - Implement SSH to access ASA from HQ datacenter with IP address 15.0.0.10.
    - Setup DMZ and static NAT to the server located in DMZ.
- Setup VPN on remote offices
    - Setup all IPsec parameters on the routers such as ISAKMP policy, crypto map, crypto set, etc..
- Implement OSPF routing protocol for dynamic routing between routers.
- Implement ACLs on router based on the requirements defined.
- Configure security measures on all switches and routers:
    - Define hostname.
    - Set password in enable → set password.

- Configure line console 0 → set password.
- Configure line vty → set password.
- Implement ssh.
- Encrypts passwords.
- Implement port security with MAC address and violation.
- Implement “no negotiate” between trunk ports.
- Apply Fast port and BPDU guard.
- Implement DHCP snooping.
- Implement AAA on Tunisia router witch selected username and password.

- Validate and test connectivity between all offices and test:
  - VPN tunnels
  - ACLs
  - Security measure
- Solve any issue that is found during testing.

TOPOLOGY



PURPOSE OF SECURE NETWORK ACCORDING TO TECH GLOBAL

It's important for multi-bran companies like Tech global to have a secure system, especially if the company has international branches. The aim of secure network is to ensure the confidentiality, integrity, and availability CIA of the tech global data.

Examples of implementing CIA:

- VPN: is used in tech global to ensure confidentiality by securing and protecting the data from any unauthorized access during transmission. VPN is very helpful in implementing secure connection between the remote office and datacenter.

- AAA: Also, AAA authentication is used to implement robust authentication to prevent any unauthorized access and making sure that only the authorized people have access to specific data or network.

- Applying security measures such as SSH for protected remote management, passwords that are complex, blocking unneeded ports, and using port security keeps away unauthorized access to the network and prevent tacks that may happened to the network.

- DHCP security: DHCP snooping used to protect the network from unauthorized access and enhance the performance of the network by marking the trusted and untrusted ports because DHCP attacks have various disadvantages on the network such as: denial of service, resource exhaustion and unauthorized network access. So, by using DHCP snooping, it will prevent these threats and enhance network performance.

NETWORK HARDWARE AND SOFTWARE USED

HARDWARE

- 1941 Router → for each network (Amman, Aqaba, Turkey, Kuwait, Tunisia) for WAN connectivity and control traffic, and configure VPN connections.
- 2960 Switch → to create VLANs in each network and connect devices with each other.

- ASA 5505 → defend network perimeters, handle, and track traffic on the network, as well as avoid attacker to access network.
- Server-PT → to provide services such as HTTPS, HTTP,FTP,MAIL,DHCP and DNS to networks.

BENEFITS OF USING HARDWARE FOR ENSURING NETWORK SECURITY

ROUTER

- It can help the security by giving it the ability to manage traffic between two routers (WAN) or between internal networks.
- Through using router, VPN can be configured to enhance the security of the network by making secured and encrypted tunnels between remote offices and datacenter.
- In addition, through using router, access control lists can also be configured to manage traffic between networks and prevent unauthorized access to services or data.
- NAT can also be used in routers to disappear internal IP addresses from internet or outside networks.

All these security measures can enhance the security of the network and make it difficult to be accessed from unauthorized people and defend the network from any cybersecurity attacks that can negatively affect the network resources and users.

SWITCH

- By using a switch, you can create VLANs and distribute one network into smaller LANs which enhances the security by making it difficult for attackers when they access the network to reach and access all the devices in the network.
- By using port security measures, it helps to enhance security by limiting MAC addresses to specific ports and thus avoiding unauthorized access to the network.
- Use spanning tree to avoid network loop because network loop is considered as vulnerability that can be used to perform attacks against networks.

ASA FIREWALL

- Provide an additional security layer on the network by saving the network from any external unauthorized access.

ANALYZE NETWORK SECURITY PROTOCOLS USED AND CRYPTOGRAPHIC METHODOLOGIES/TYPES

NETWORK SECURITY PROTOCOLS USED:

- SSH:

It employs public-key cryptography for authenticating the remote devices and users to access system or devices. It is used by the administrator to make it easier for the administrator to access and control the system and devices remotely.

SSH is used in Tech global network to enhance the security of the network by providing robust authentication, encrypted data transmission and preventing attacks such as eavesdropping, connection hijacking and others.

By using SSH, we (administrators) accessed routers, switches, and ASA firewall remotely by using username and password to access and manage devices in the network.

- IPsec

It contains various protocols for protecting and securing IP communications through encryption and authentication of IP packets of a communications session. In Tech global network, it is very important to implement because it creates secure communication channels over publicly accessible networks, particularly when using Virtual Private Networks (VPNs). In addition, it gives data confidentiality and integrity.

In Tech global network, one of the requirements was to implement VPN connections between remote offices Tukey, Tunisia, and Kuwait with datacenter located in Amman. To secure IP communications and ensure that the data is secured even when transferred between networks, IPsec was implemented to do the work and enhance the security of the network.

- HTTPS

It is an extension of HTTP, but this version is more secure than HTTP. It is more secure because it provides secure communication using encryption standards over computer network within browser. It is important in our case to ensure security between the PCs and the website and prevent any attacks like man in the middle , and other attacks.

It also helps in protecting user's information and transactions and create a reliable network. In Tech global requirements, HTTPS was required to implement in the server with domain name (eis.techglobal.com.jo).

- SSL

It is a security protocol that creates a secure connection among a web server and a web browser. This guarantees that any information exchanged among the web server and the web browser is strictly private. It is very important because it gives encrypts data integrity during communications.

CRYPTOGRAPHIC METHODOLOGIES/TYPES

- SHA

It is considered one of the cryptographic functions and used to generate unique and fixed size hash values from data. It is very important because it is applied for data integrity by making hash value that displays data. In this hash function, if there was any changes to the data, the hash value will be different and this will guarantee that data has not been alerted or modified with while transfer.

In Tech global network, SHA function used in establishing VPN between remote offices and data center located in Amman to create and establish a secure and reliable communication by checking the data transmitted through tunnels for integrity to check if the data modified or not while transmission. This absolutely enhances the network and VPN communication on the network.

- HMAC

HMAC is used in Tech global network for establishing VPN between remote offices and datacenter along with SHA hashing function. HMAC with SHA both provide not only data integrity, but also authentication which means that the data is transferred using authenticated sources which enhances the security of Tech global network.

- AES

It is a symmetric encryption algorithm that helps to ensure confidentiality, it is a very popular encryption due to its efficiency by encrypting data in fixed size blocks and using various key lengths.

It was also used in Tech global network during the VPN setup to transfer encrypted data in the VPN tunnels using AES which enhances the security of Tech global network by protecting the information transferred.

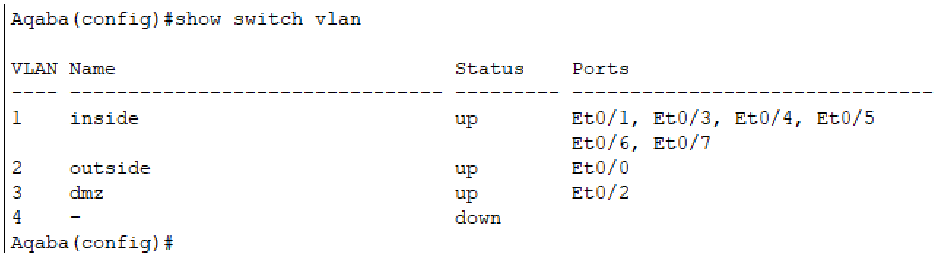
- RSA

It is a key component because of its use of asymmetric cryptography. It establishes a solid foundation for safe transmission of information. The RSA algorithm creates two keys: a public key for encrypted data and a private key for unlocking incoming data. It assures that regardless of whether a cyber attacker captures the data that has been encrypted, the data will be unreadable without the secret key.

RSA is used because it supports and protects all communications such as SSL, and SSH for remote access from unauthorized access so this is why it implemented in Tech global network.

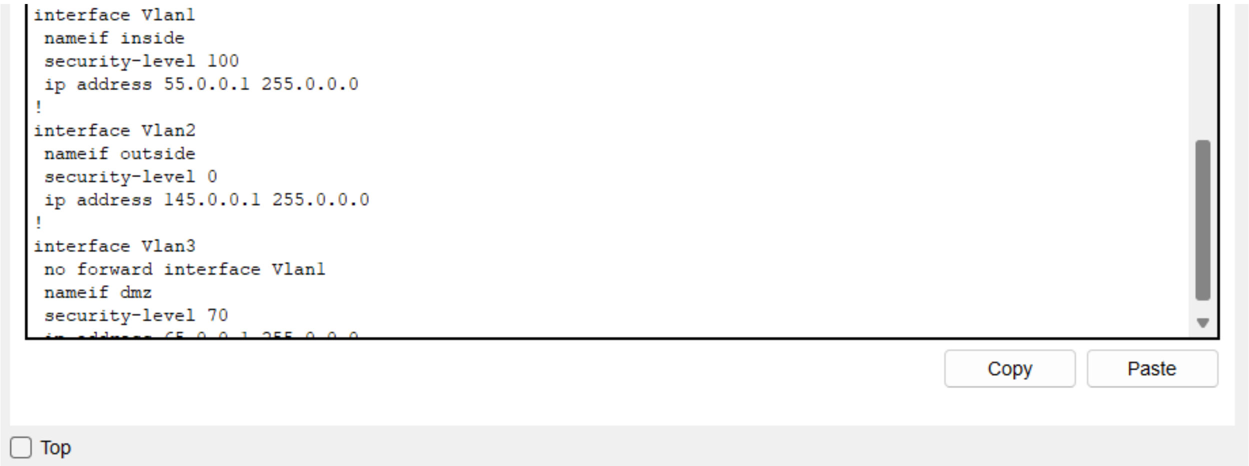
CONFIGURATION AND JUSTIFICATION FOR THE CHOICES MADE IN THE NETWORK SECURITY CONFIGURATION

ASA 5505CONFIGURATION



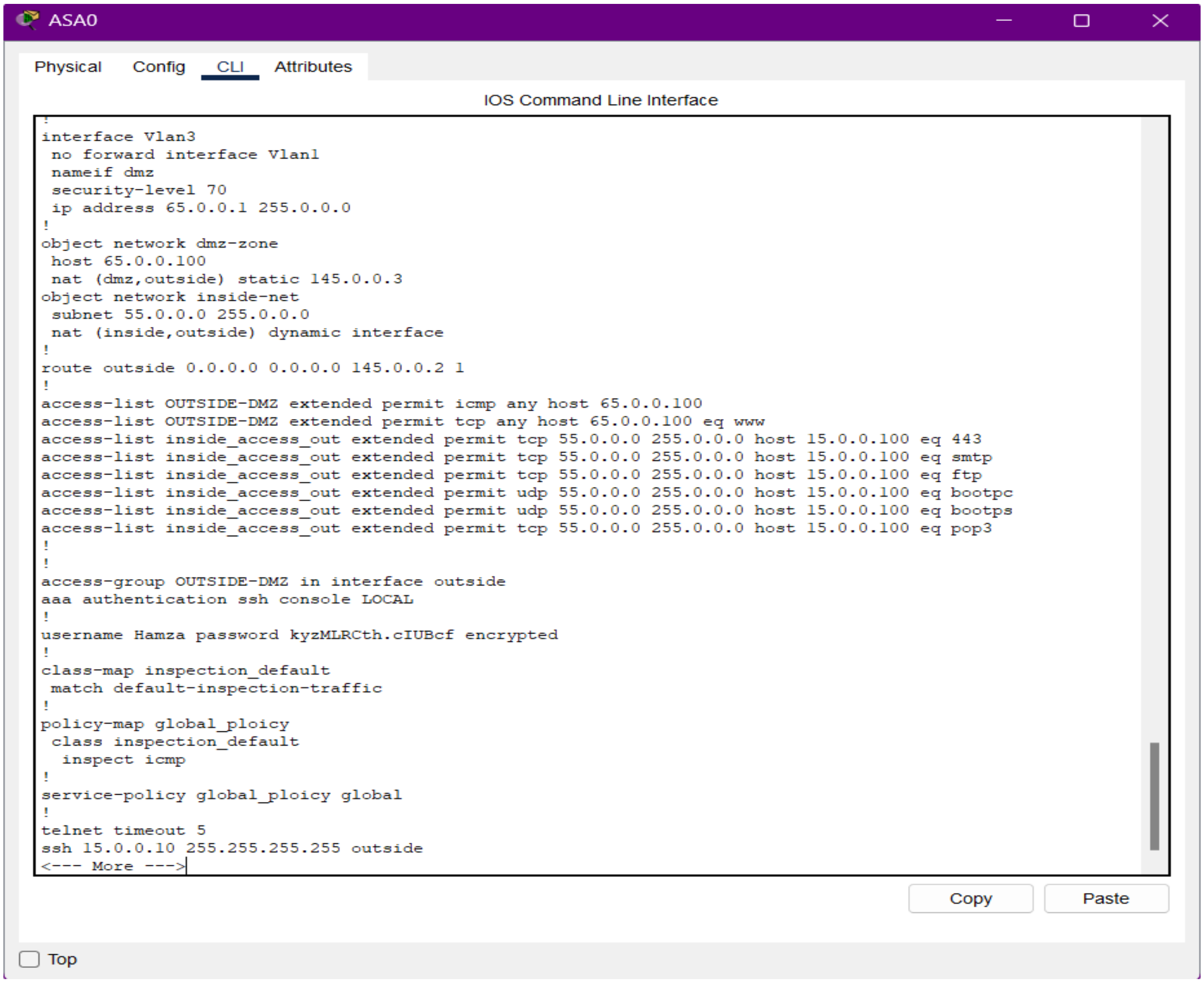
```
Aqaba(config)#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------------------
1    inside                           up        Et0/1, Et0/3, Et0/4, Et0/5
                                                Et0/6, Et0/7
2    outside                          up        Et0/0
3    dmz                              up        Et0/2
4    -                                down
Aqaba(config)#
```

This displays the VLANs configured in the ASA firewall in Tech global and ports in each VLAN.



```
interface Vlan1
 nameif inside
 security-level 100
 ip address 55.0.0.1 255.0.0.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 145.0.0.1 255.0.0.0
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 65.0.0.1 255.0.0.0
```

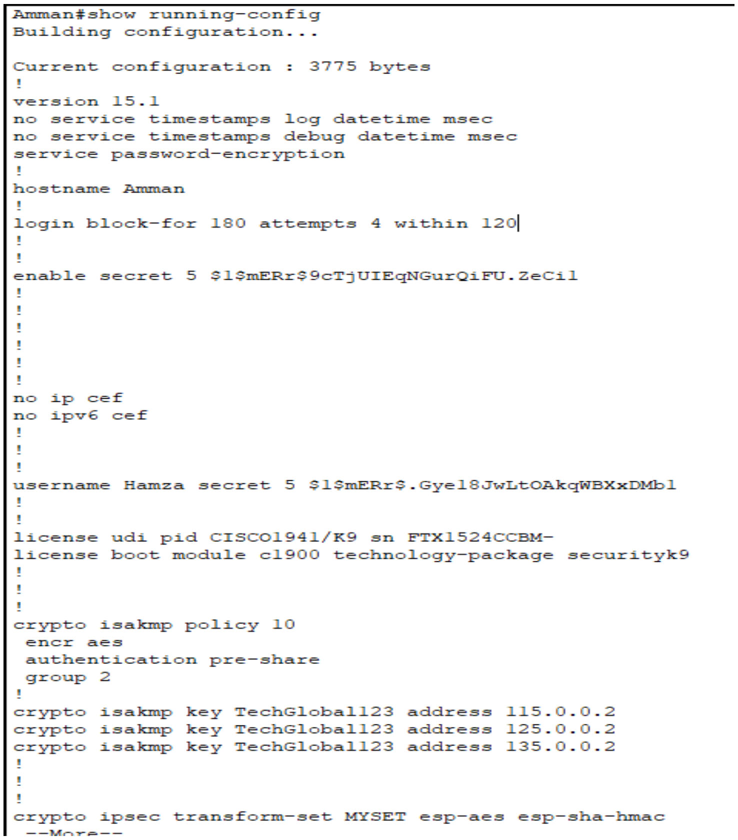
This image displays configuration of each VLAN (name, security level, IP address).



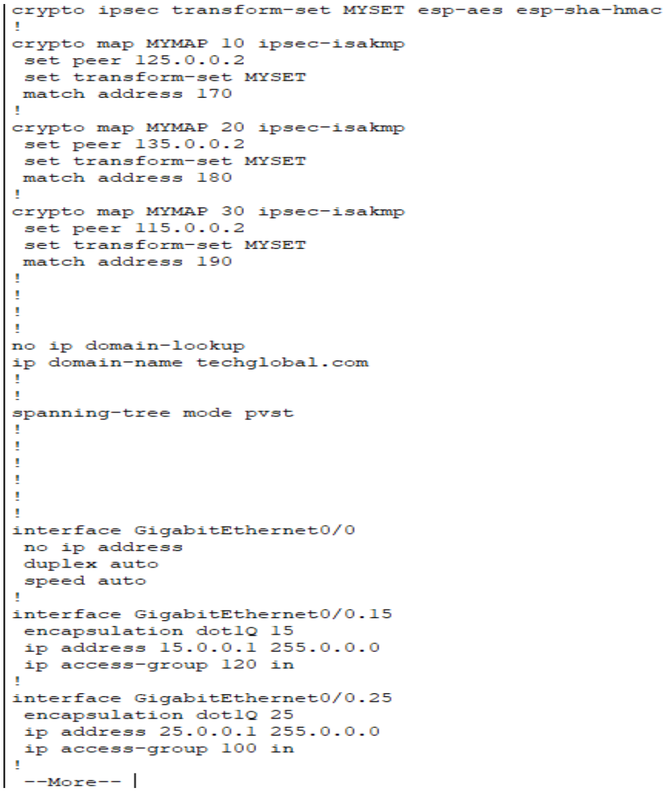
```
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 65.0.0.1 255.0.0.0
!
object network dmz-zone
 host 65.0.0.100
 nat (dmz,outside) static 145.0.0.3
object network inside-net
 subnet 55.0.0.0 255.0.0.0
 nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 145.0.0.2 1
!
access-list OUTSIDE-DMZ extended permit icmp any host 65.0.0.100
access-list OUTSIDE-DMZ extended permit tcp any host 65.0.0.100 eq www
access-list inside_access_out extended permit tcp 55.0.0.0 255.0.0.0 host 15.0.0.100 eq 443
access-list inside_access_out extended permit tcp 55.0.0.0 255.0.0.0 host 15.0.0.100 eq smtp
access-list inside_access_out extended permit tcp 55.0.0.0 255.0.0.0 host 15.0.0.100 eq ftp
access-list inside_access_out extended permit udp 55.0.0.0 255.0.0.0 host 15.0.0.100 eq bootpc
access-list inside_access_out extended permit udp 55.0.0.0 255.0.0.0 host 15.0.0.100 eq bootps
access-list inside_access_out extended permit tcp 55.0.0.0 255.0.0.0 host 15.0.0.100 eq pop3
!
!
access-group OUTSIDE-DMZ in interface outside
aaa authentication ssh console LOCAL
!
username Hamza password kyzMLRCth.cIUBcf encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_ploicy
 class inspection_default
  inspect icmp
!
service-policy global_ploicy global
!
telnet timeout 5
ssh 15.0.0.10 255.255.255.255 outside
<--- More --->
```

This image describes first the configuration of DMZ VLAN , NAT, ACLs configured on ASA ,and SSH configuration to let only PC that have 15.0.0.10 to access ASA firewall.

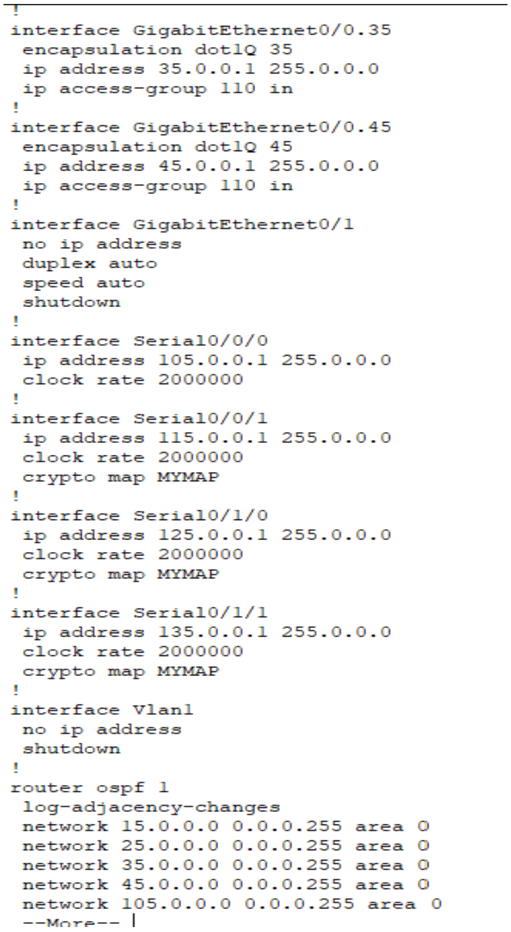
AMMAN ROUTER



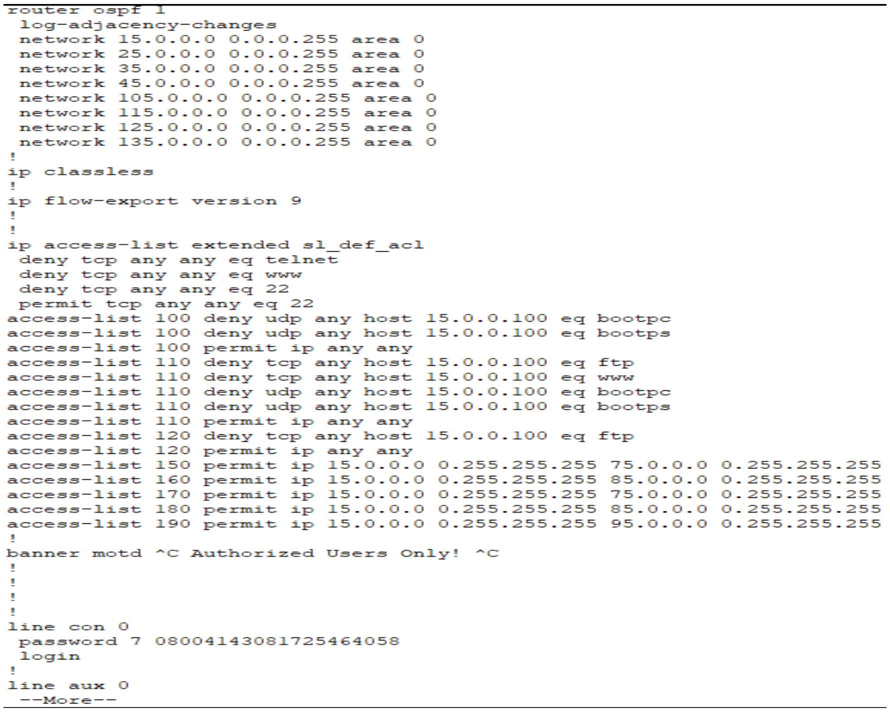
```
Amman#show running-config
Building configuration...

Current configuration : 3775 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Amman
!
login block-for 180 attempts 4 within 120
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Hamza secret 5 $1$mERr$.Gye18JwLtOAkqWBXxDMb1
!
!
license udi pid CISCO1941/K9 sn FTX1524CCBM-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp key TechGlobal123 address 115.0.0.2
crypto isakmp key TechGlobal123 address 125.0.0.2
crypto isakmp key TechGlobal123 address 135.0.0.2
!
!
!
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
 --More--
```



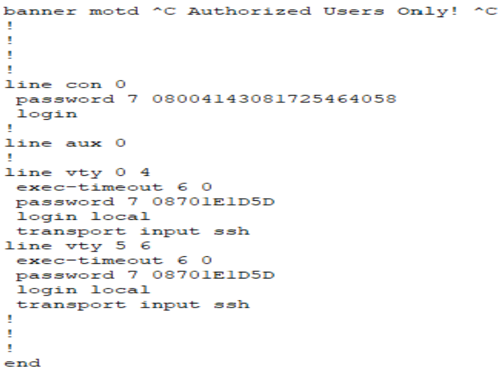
```
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
!
crypto map MYMAP 10 ipsec-isakmp
 set peer 125.0.0.2
 set transform-set MYSET
 match address 170
!
crypto map MYMAP 20 ipsec-isakmp
 set peer 135.0.0.2
 set transform-set MYSET
 match address 180
!
crypto map MYMAP 30 ipsec-isakmp
 set peer 115.0.0.2
 set transform-set MYSET
 match address 190
!
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 15.0.0.1 255.0.0.0
 ip access-group 120 in
!
interface GigabitEthernet0/0.25
 encapsulation dot1Q 25
 ip address 25.0.0.1 255.0.0.0
 ip access-group 100 in
!
 --More-- 
```



```
!
interface GigabitEthernet0/0.35
 encapsulation dot1Q 35
 ip address 35.0.0.1 255.0.0.0
 ip access-group 110 in
!
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45
 ip address 45.0.0.1 255.0.0.0
 ip access-group 110 in
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 105.0.0.1 255.0.0.0
 clock rate 2000000
!
interface Serial0/0/1
 ip address 115.0.0.1 255.0.0.0
 clock rate 2000000
 crypto map MYMAP
!
interface Serial0/1/0
 ip address 125.0.0.1 255.0.0.0
 clock rate 2000000
 crypto map MYMAP
!
interface Serial0/1/1
 ip address 135.0.0.1 255.0.0.0
 clock rate 2000000
 crypto map MYMAP
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 15.0.0.0 0.0.0.255 area 0
 network 25.0.0.0 0.0.0.255 area 0
 network 35.0.0.0 0.0.0.255 area 0
 network 45.0.0.0 0.0.0.255 area 0
 network 105.0.0.0 0.0.0.255 area 0
 --More--
```

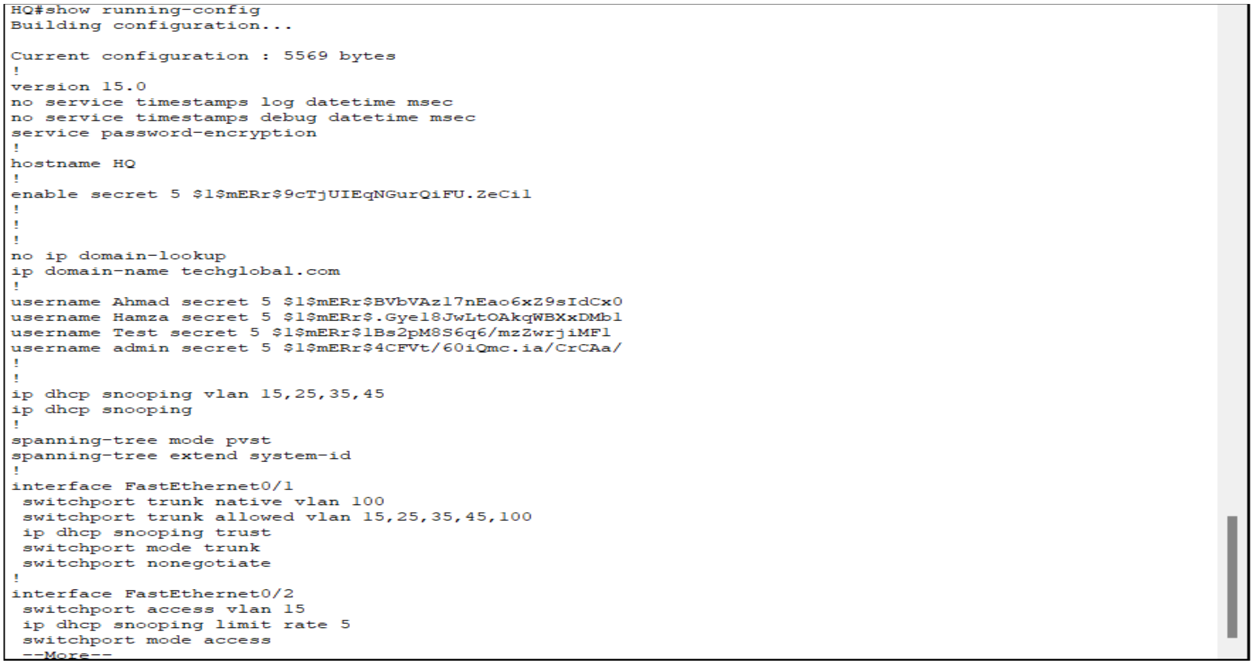


```
router ospf 1
 log-adjacency-changes
 network 15.0.0.0 0.0.0.255 area 0
 network 25.0.0.0 0.0.0.255 area 0
 network 35.0.0.0 0.0.0.255 area 0
 network 45.0.0.0 0.0.0.255 area 0
 network 105.0.0.0 0.0.0.255 area 0
 network 115.0.0.0 0.0.0.255 area 0
 network 125.0.0.0 0.0.0.255 area 0
 network 135.0.0.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
access-list 100 deny udp any host 15.0.0.100 eq bootpc
access-list 100 deny udp any host 15.0.0.100 eq bootps
access-list 100 permit ip any any
access-list 110 deny tcp any host 15.0.0.100 eq ftp
access-list 110 deny tcp any host 15.0.0.100 eq www
access-list 110 deny udp any host 15.0.0.100 eq bootpc
access-list 110 deny udp any host 15.0.0.100 eq bootps
access-list 110 permit ip any any
access-list 120 deny tcp any host 15.0.0.100 eq ftp
access-list 120 permit ip any any
access-list 150 permit ip 15.0.0.0 0.255.255.255 75.0.0.0 0.255.255.255
access-list 160 permit ip 15.0.0.0 0.255.255.255 85.0.0.0 0.255.255.255
access-list 170 permit ip 15.0.0.0 0.255.255.255 75.0.0.0 0.255.255.255
access-list 180 permit ip 15.0.0.0 0.255.255.255 85.0.0.0 0.255.255.255
access-list 190 permit ip 15.0.0.0 0.255.255.255 95.0.0.0 0.255.255.255
!
banner motd ^C Authorized Users Only! ^C
!
!
!
!
line con 0
 password 7 08004143081725464058
 login
!
line aux 0
 --More--
```

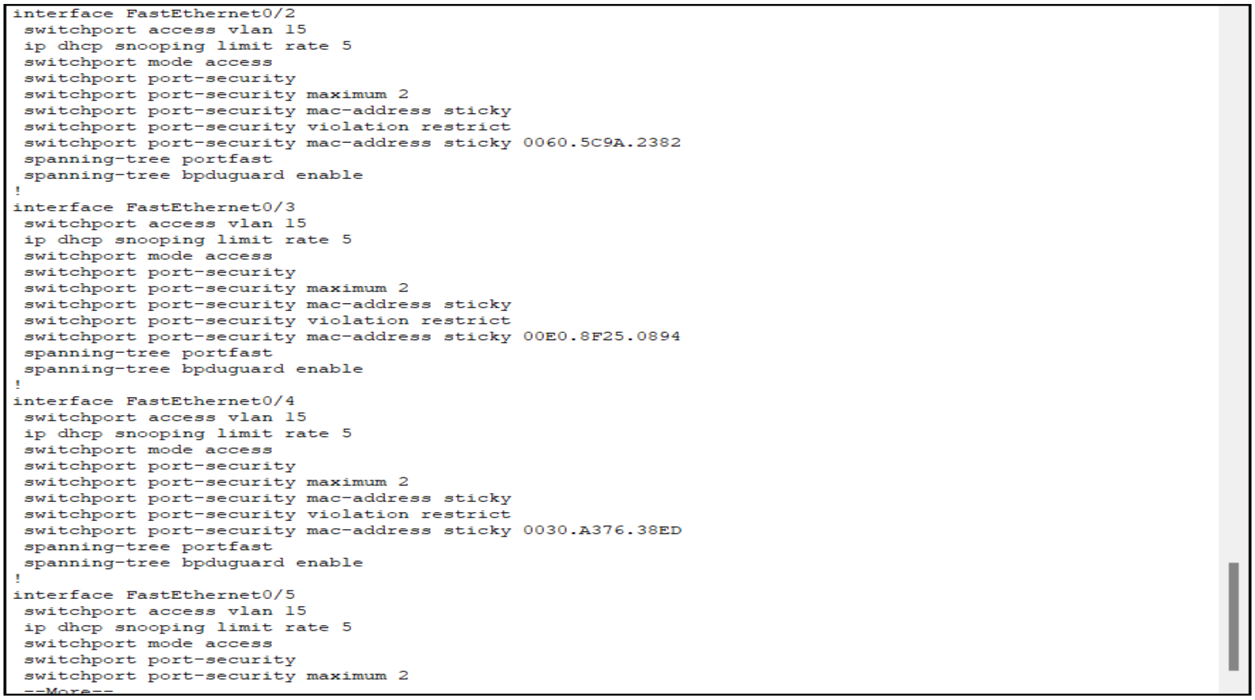


```
banner motd ^C Authorized Users Only! ^C
!
!
!
!
line con 0
 password 7 0800414308172546405 8
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 6 0
 password 7 08701E1D5D
 login local
 transport input ssh
line vty 5 6
 exec-timeout 6 0
 password 7 08701E1D5D
 login local
 transport input ssh
!
!
!
end
```

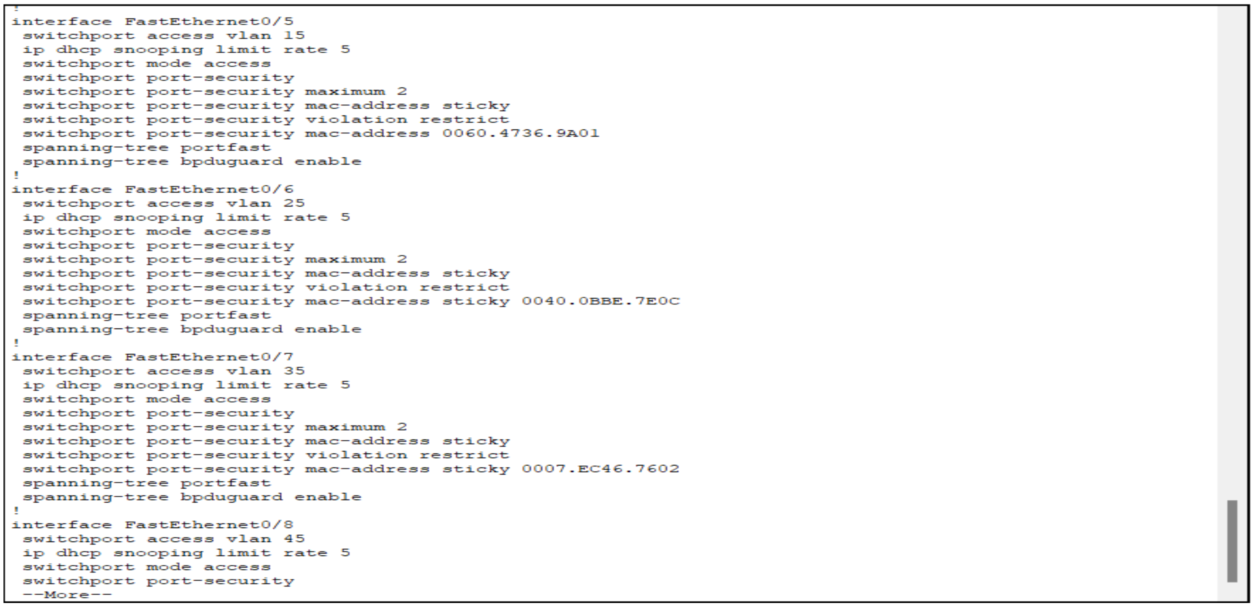
AMMAN SWITCH



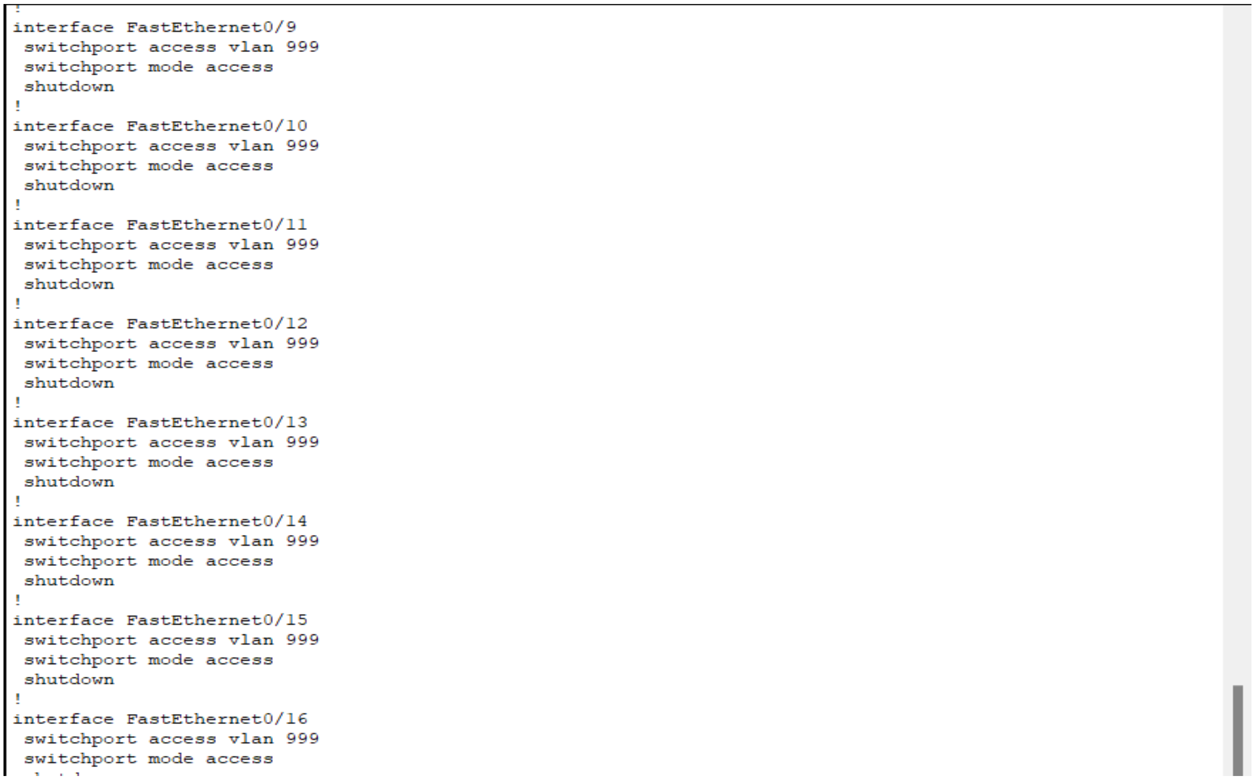
```
HQ#show running-config
Building configuration...

Current configuration : 5569 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname HQ
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
username Ahmad secret 5 $1$mERr$BVbVAzl7nEao6xZ9sIdCx0
username Hamza secret 5 $1$mERr$.Gyel8JwLtOAkqWBXxDMbl
username Test secret 5 $1$mERr$lBs2pM8S6q6/mzZwrjiMFl
username admin secret 5 $1$mERr$4CFVt/60iQmc.ia/CrCAa/
!
!
ip dhcp snooping vlan 15,25,35,45
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 15,25,35,45,100
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 --More--
```



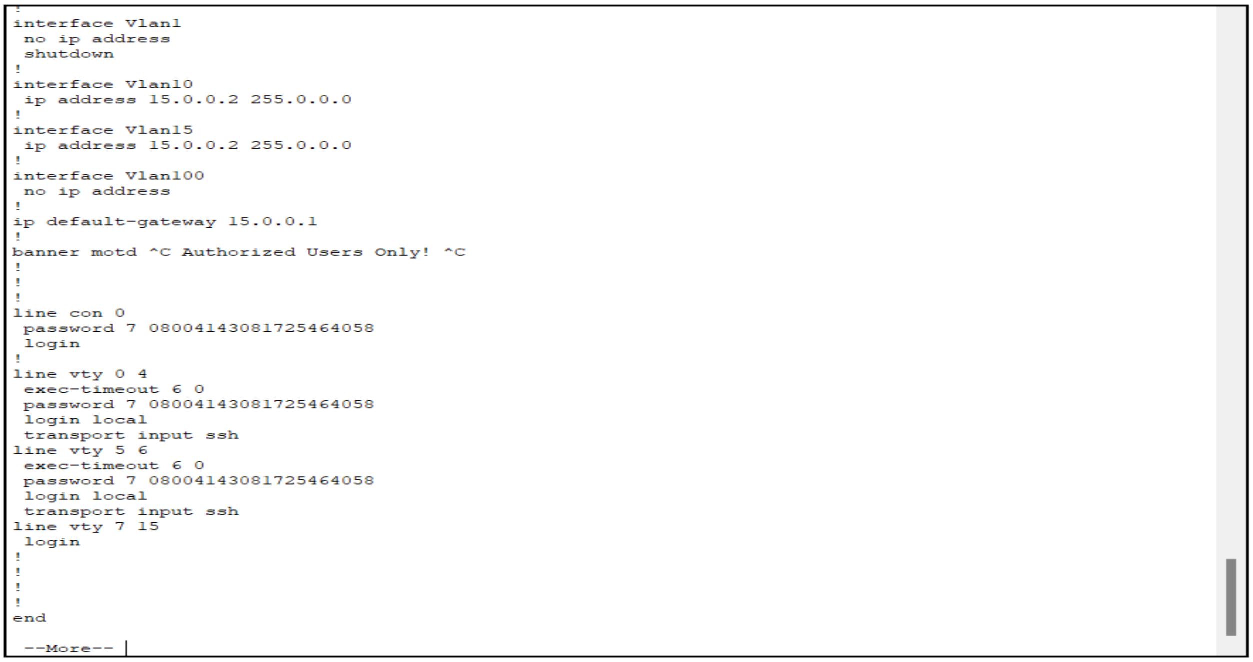
```
interface FastEthernet0/2
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.5C9A.2382
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.8F25.0894
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0030.A376.38ED
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 --More--
```



```
!
interface FastEthernet0/5
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address 0060.4736.9A01
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 switchport access vlan 25
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0040.0BBE.7E0C
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/7
 switchport access vlan 35
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0007.EC46.7602
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/8
 switchport access vlan 45
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 --More--
```

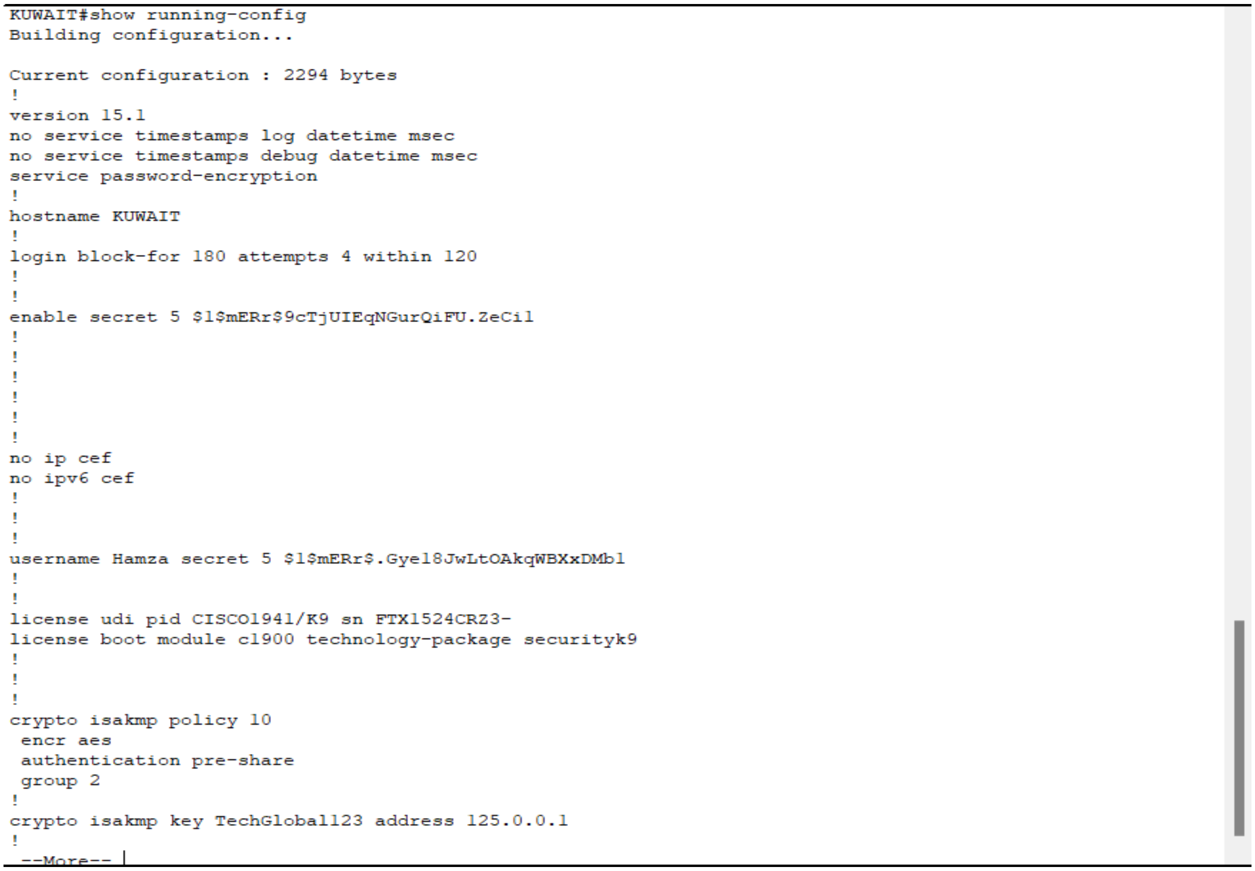


```
!
interface FastEthernet0/9
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/12
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 999
 switchport mode access
```

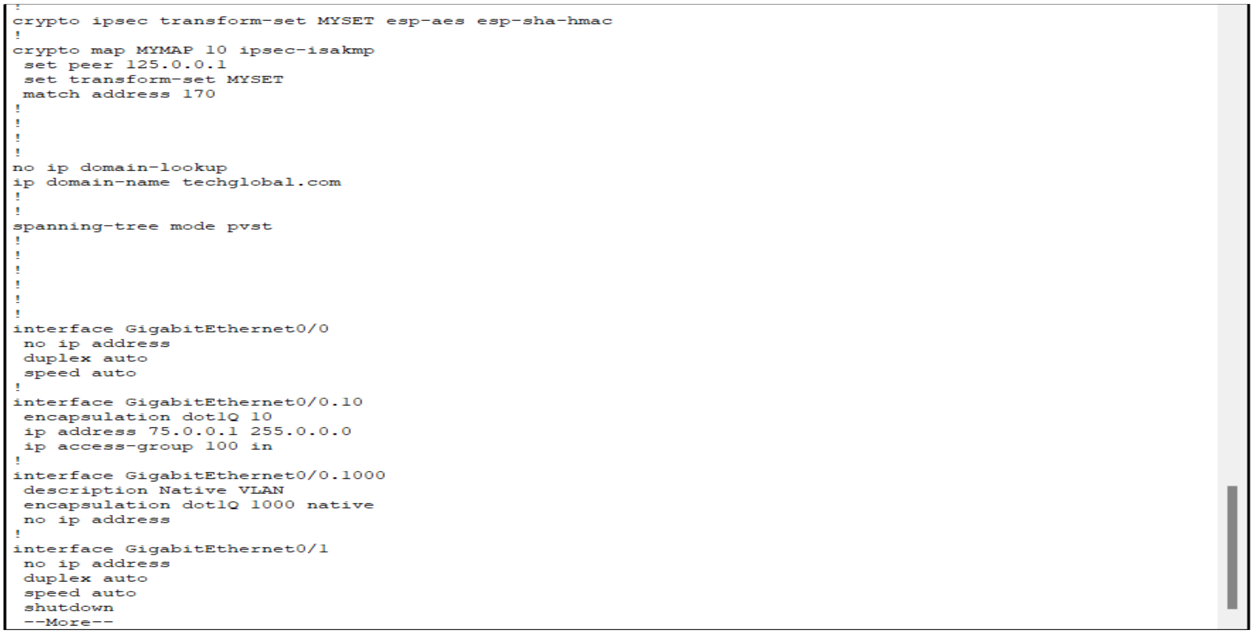


```
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 15.0.0.2 255.0.0.0
!
interface Vlan15
 ip address 15.0.0.2 255.0.0.0
!
interface Vlan100
 no ip address
!
ip default-gateway 15.0.0.1
!
banner motd ^C Authorized Users Only! ^C
!
!
!
line con 0
 password 7 08004143081725464058
 login
!
line vty 0 4
 exec-timeout 6 0
 password 7 08004143081725464058
 login local
 transport input ssh
line vty 5 6
 exec-timeout 6 0
 password 7 08004143081725464058
 login local
 transport input ssh
line vty 7 15
 login
!
!
!
!
end

 --More--
```

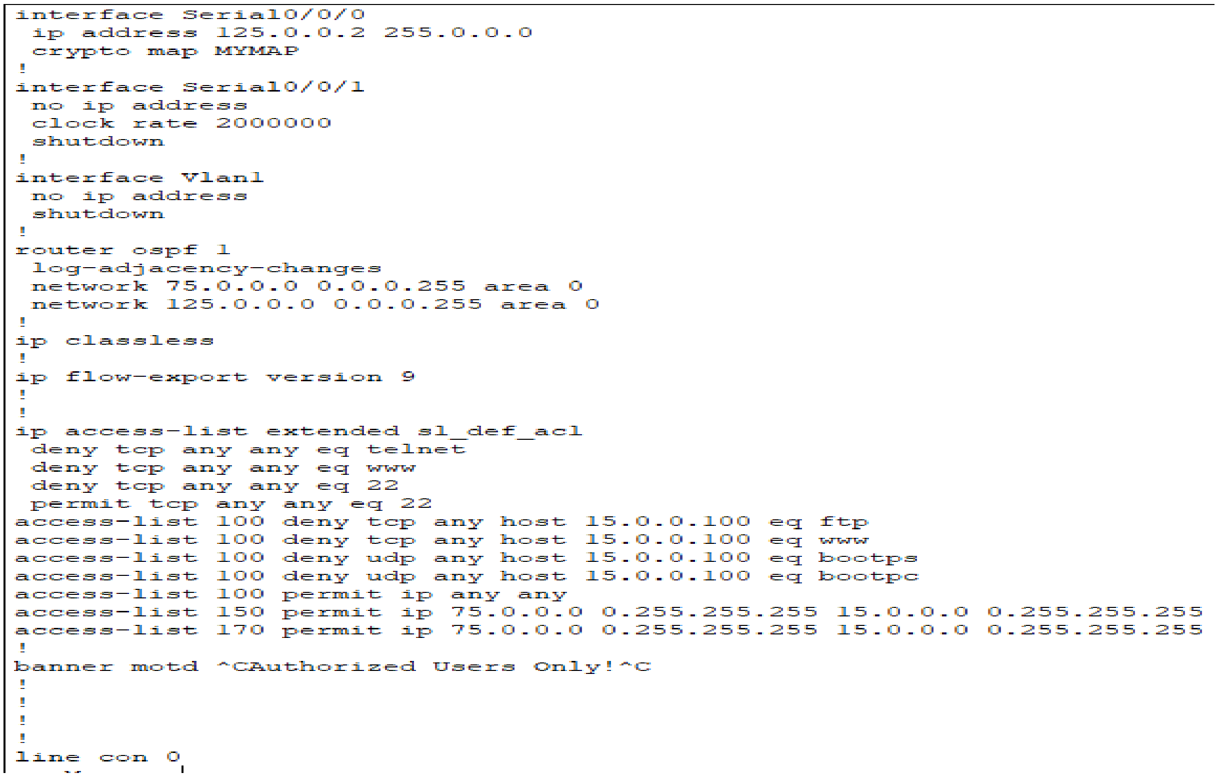
KUWAIT ROUTER



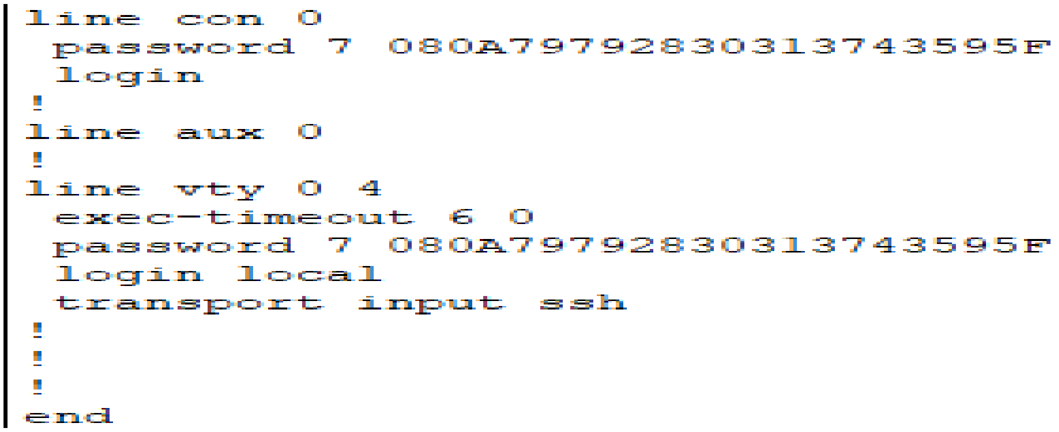
```
KUWAIT#show running-config
Building configuration...

Current configuration : 2294 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname KUWAIT
!
login block-for 180 attempts 4 within 120
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Hamza secret 5 $1$mERr$.Gye18JwLtOAkqWBXxDMbl
!
!
license udi pid CISCO1941/K9 sn FTX1524CRZ3-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp key TechGlobal123 address 125.0.0.1
!
 --More--
```



```
!
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
!
crypto map MYMAP 10 ipsec-isakmp
 set peer 125.0.0.1
 set transform-set MYSET
 match address 170
!
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 75.0.0.1 255.0.0.0
 ip access-group 100 in
!
interface GigabitEthernet0/0.1000
 description Native VLAN
 encapsulation dot1Q 1000 native
 no ip address
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
 --More--
```

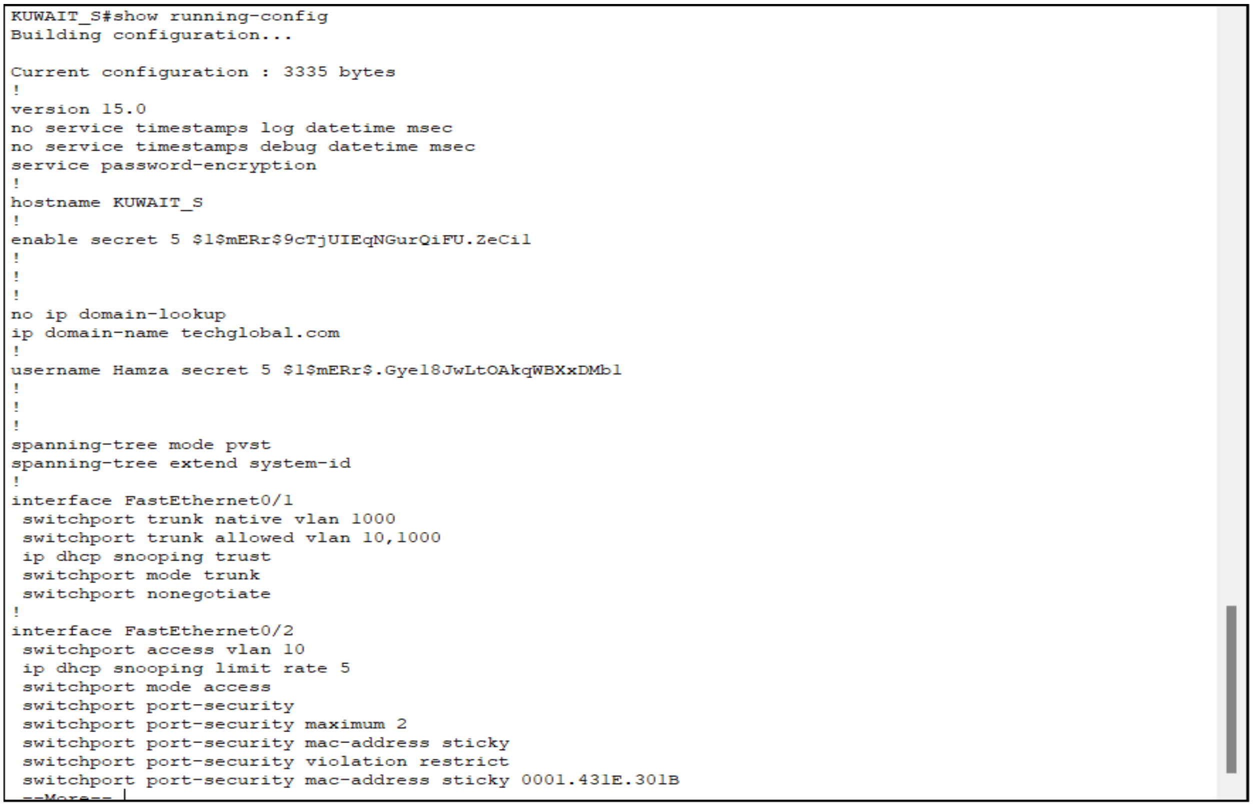


```
interface Serial0/0/0
 ip address 125.0.0.2 255.0.0.0
 crypto map MYMAP
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 75.0.0.0 0.0.0.255 area 0
 network 125.0.0.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
access-list 100 deny tcp any host 15.0.0.100 eq ftp
access-list 100 deny tcp any host 15.0.0.100 eq www
access-list 100 deny udp any host 15.0.0.100 eq bootps
access-list 100 deny udp any host 15.0.0.100 eq bootpc
access-list 100 permit ip any any
access-list 150 permit ip 75.0.0.0 0.255.255.255 15.0.0.0 0.255.255.255
access-list 170 permit ip 75.0.0.0 0.255.255.255 15.0.0.0 0.255.255.255
!
banner motd ^CAuthorized Users Only!^C
!
!
!
!
line con 0
```

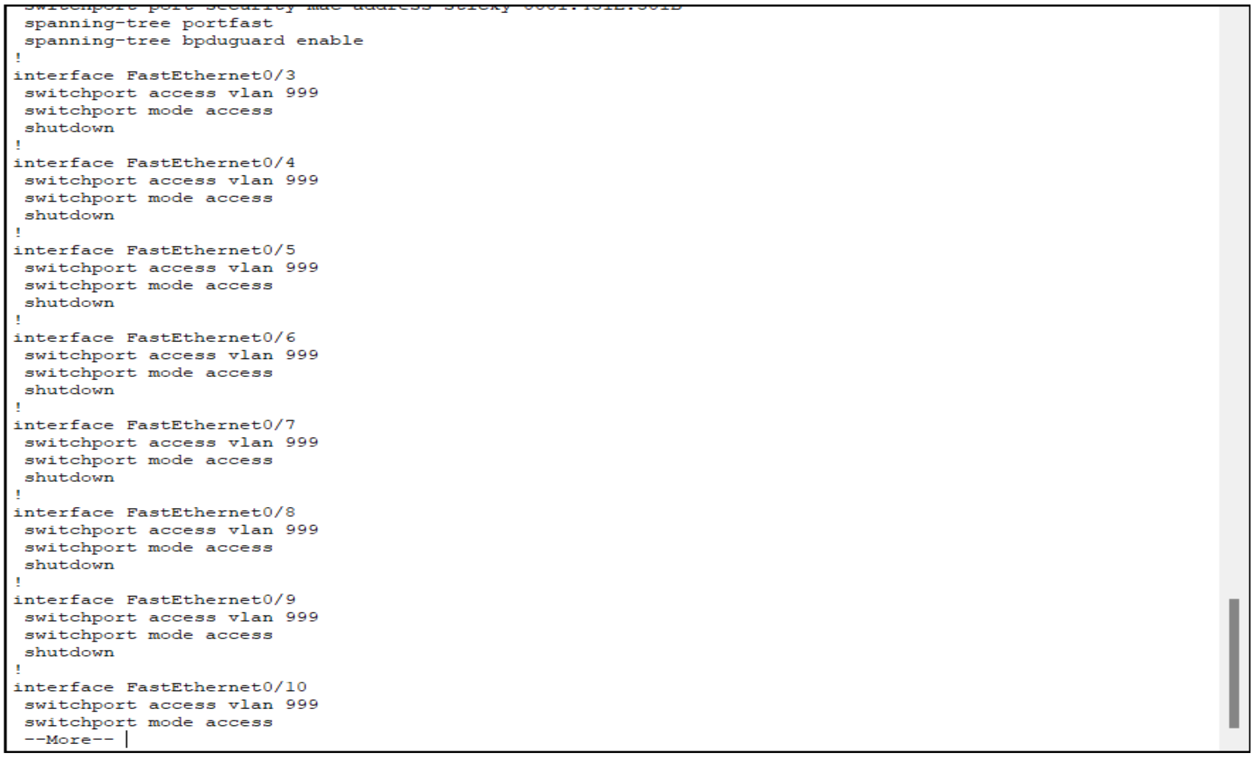


```
line con 0
 password 7 080A7979283031374359 5F
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 6 0
 password 7 080A7979283031374359 5F
 login local
 transport input ssh
!
!
!
end
```

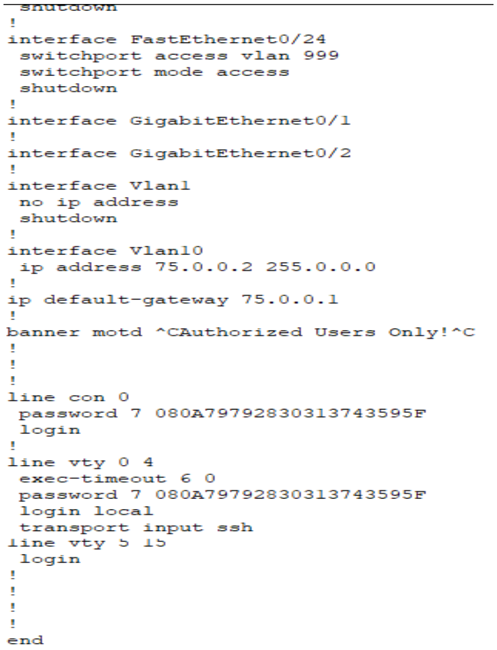
KUWAIT SWITCH



```
KUWAIT_S#show running-config
Building configuration...

Current configuration : 3335 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname KUWAIT_S
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
username Hamza secret 5 $1$mERr$.Gye18JwLtOAkqWBXxDMbl
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 10,1000
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.431E.301B
 --More--
```

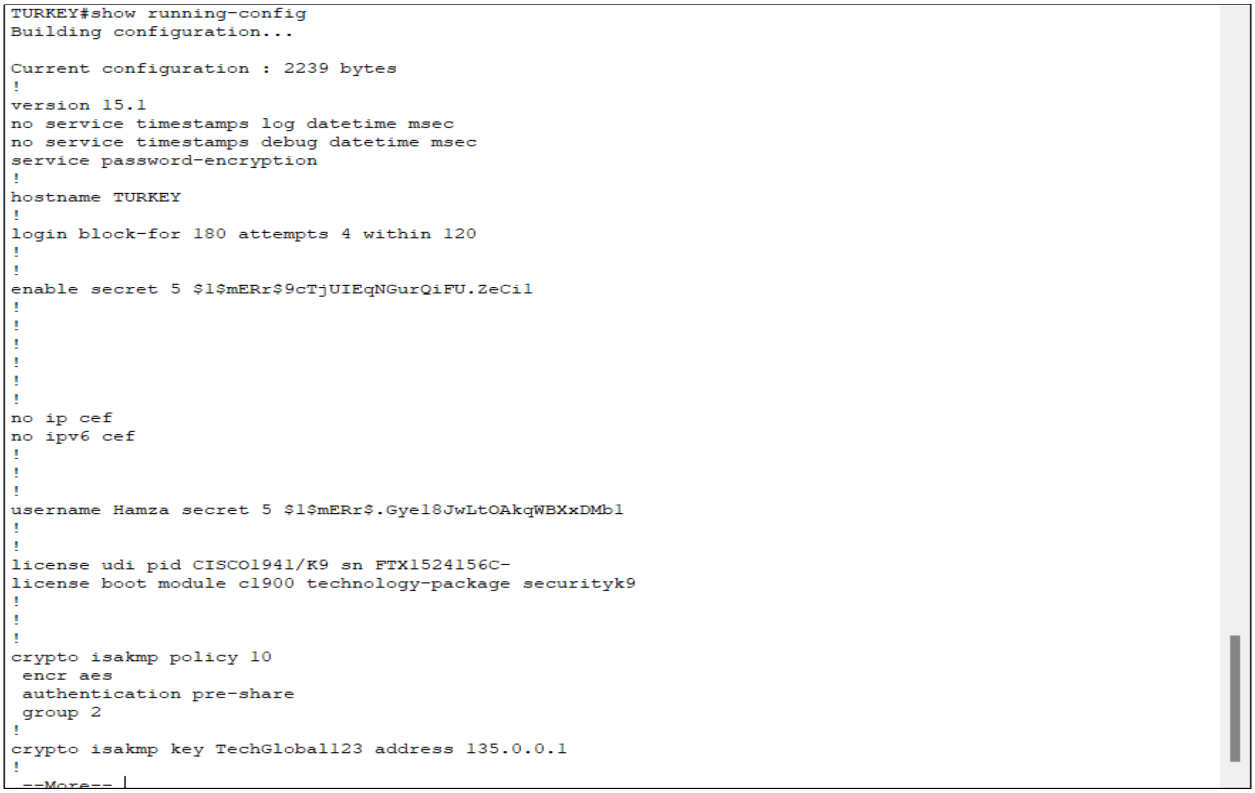


```
 switchport port-security mac-address sticky 0001.431E.301B
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/7
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 999
 switchport mode access
 --More--
```

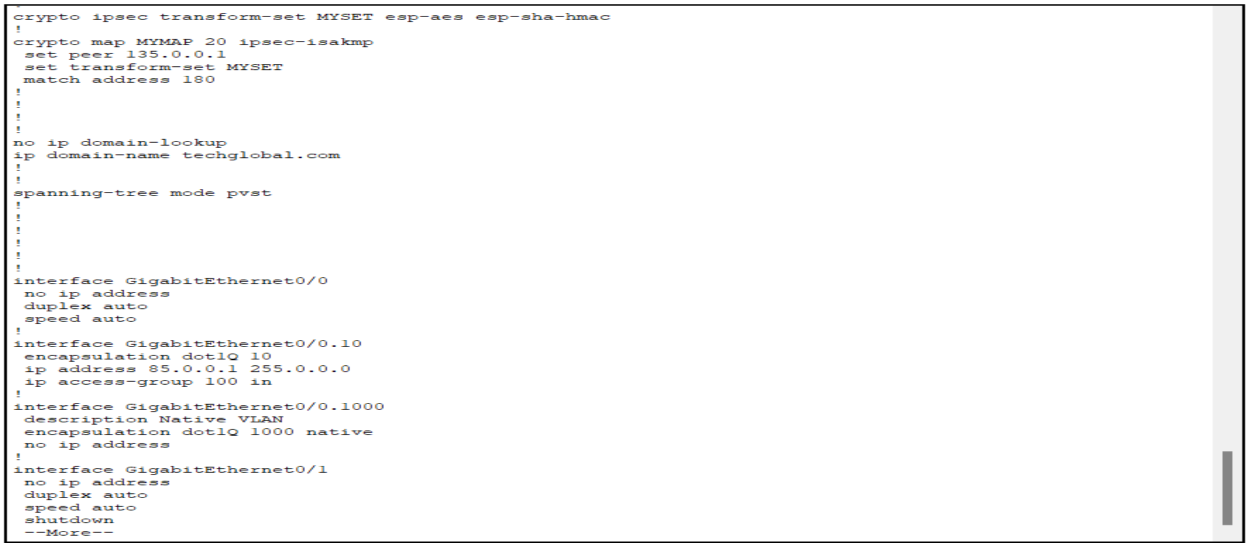


```
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 75.0.0.2 255.0.0.0
!
ip default-gateway 75.0.0.1
!
banner motd ^CAuthorized Users Only!^C
!
!
!
line con 0
 password 7 080A79792830313743595F
 login
!
line vty 0 4
 exec-timeout 6 0
 password 7 080A79792830313743595F
 login local
 transport input ssh
line vty 5 15
 login
!
!
!
!
end
```

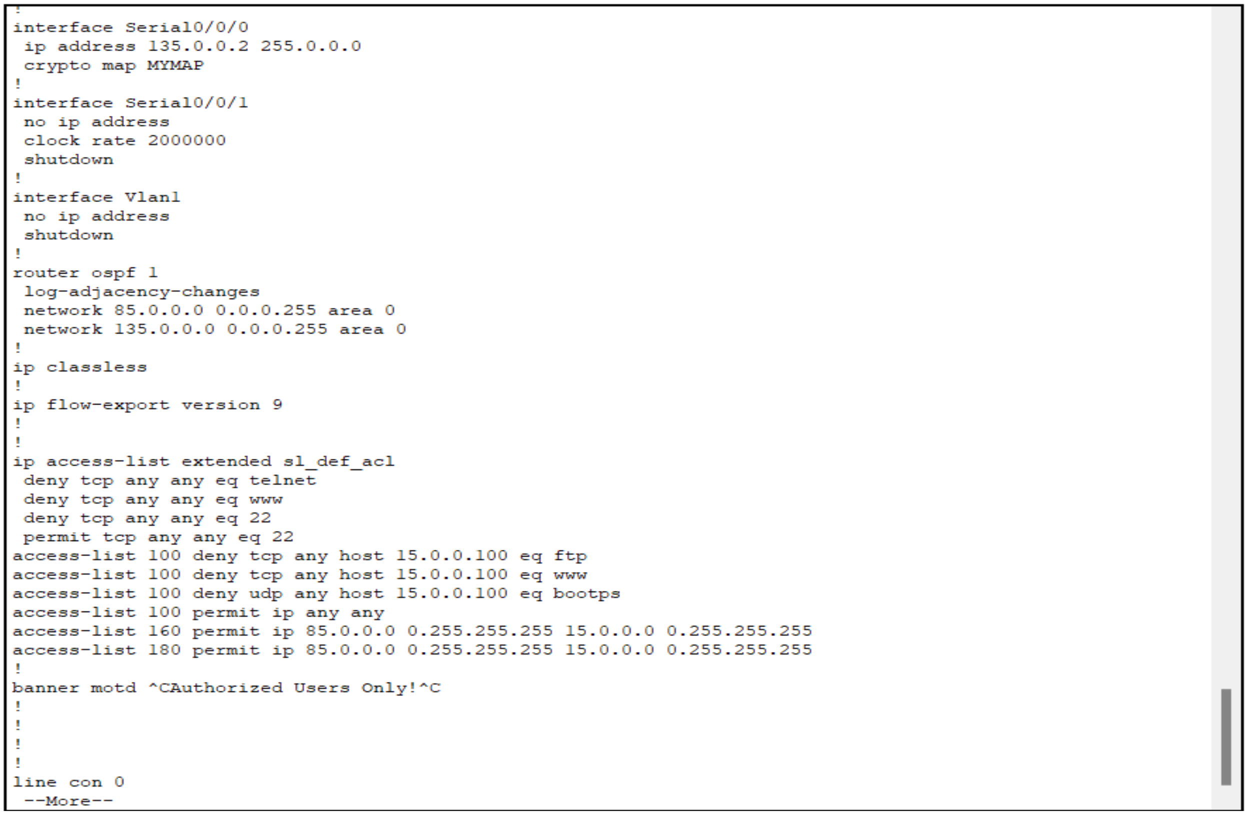
TURKEY ROUTER



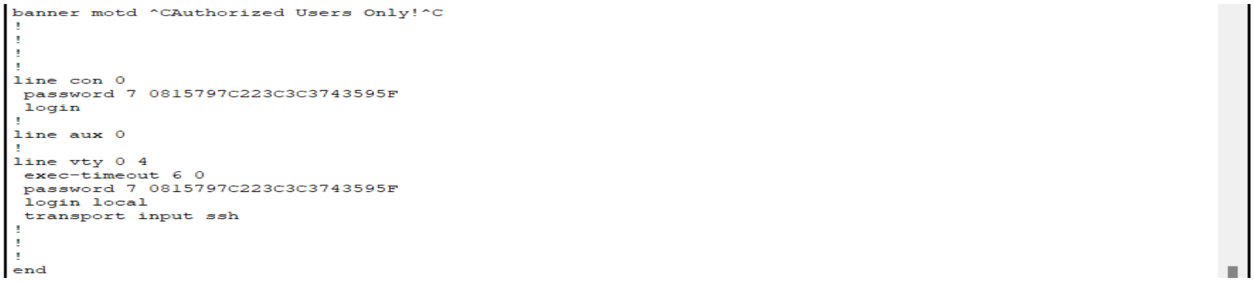
```
TURKEY#show running-config
Building configuration...

Current configuration : 2239 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname TURKEY
!
login block-for 180 attempts 4 within 120
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Hamza secret 5 $1$mERr$.Gye18JwLtOAkqWBXxDMbl
!
!
license udi pid CISCO1941/K9 sn FTX1524156C-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp key TechGlobal123 address 135.0.0.1
!
 --More--
```



```
!
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
!
crypto map MYMAP 20 ipsec-isakmp
 set peer 135.0.0.1
 set transform-set MYSET
 match address 180
!
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 85.0.0.1 255.0.0.0
 ip access-group 100 in
!
interface GigabitEthernet0/0.1000
 description Native VLAN
 encapsulation dot1Q 1000 native
 no ip address
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
 --More--
```

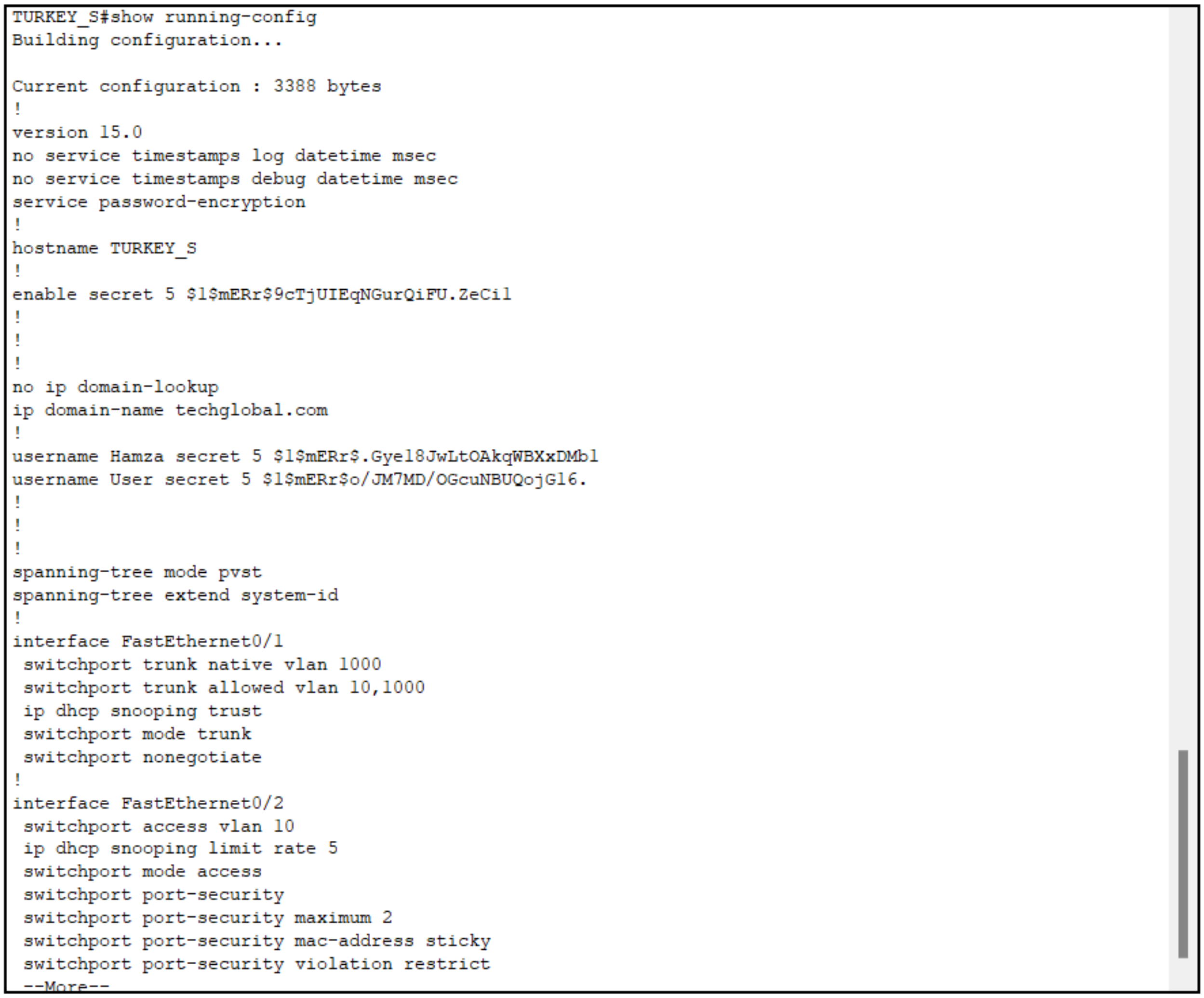


```
!
interface Serial0/0/0
 ip address 135.0.0.2 255.0.0.0
 crypto map MYMAP
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 85.0.0.0 0.0.0.255 area 0
 network 135.0.0.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
access-list 100 deny tcp any host 15.0.0.100 eq ftp
access-list 100 deny tcp any host 15.0.0.100 eq www
access-list 100 deny udp any host 15.0.0.100 eq bootps
access-list 100 permit ip any any
access-list 160 permit ip 85.0.0.0 0.255.255.255 15.0.0.0 0.255.255.255
access-list 180 permit ip 85.0.0.0 0.255.255.255 15.0.0.0 0.255.255.255
!
banner motd ^CAuthorized Users Only!^C
!
!
!
!
line con 0
 --More--
```

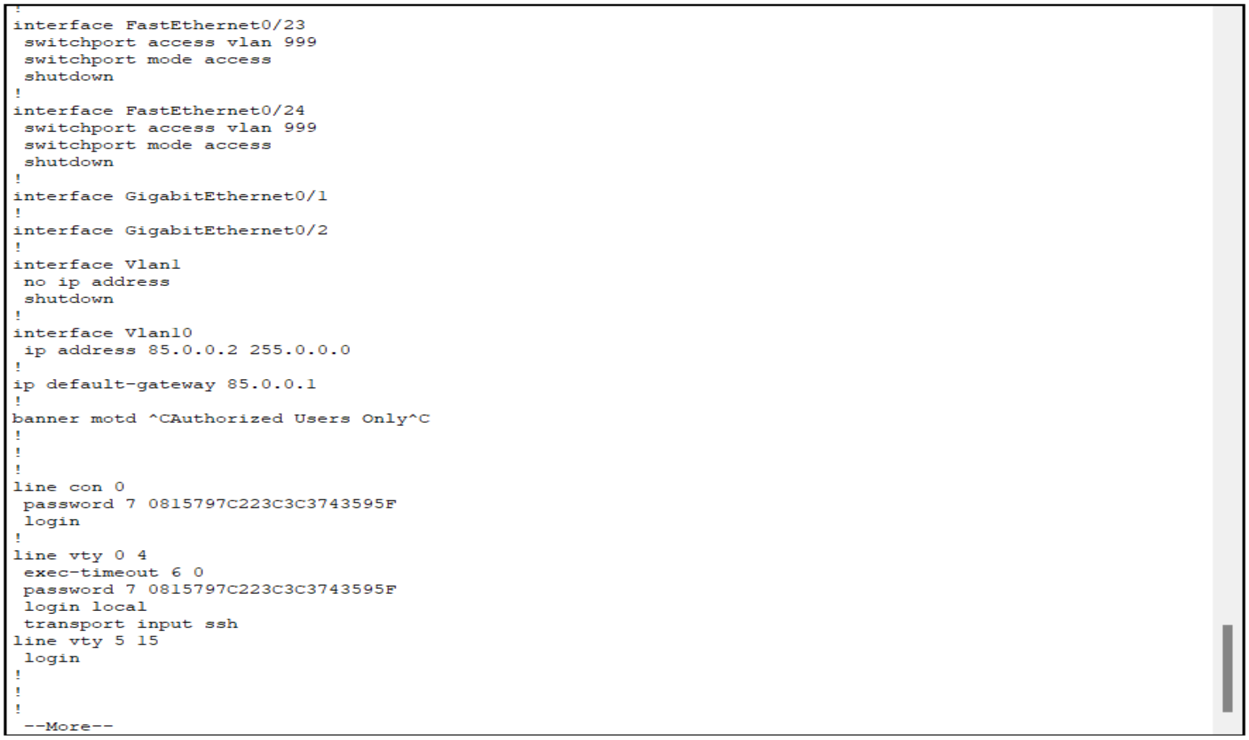


```
banner motd ^CAuthorized Users Only!^C
!
!
!
!
line con 0
 password 7 0815797C223C3C3743595F
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 6 0
 password 7 0815797C223C3C3743595F
 login local
 transport input ssh
!
!
!
end
```

TURKEY SWITCH

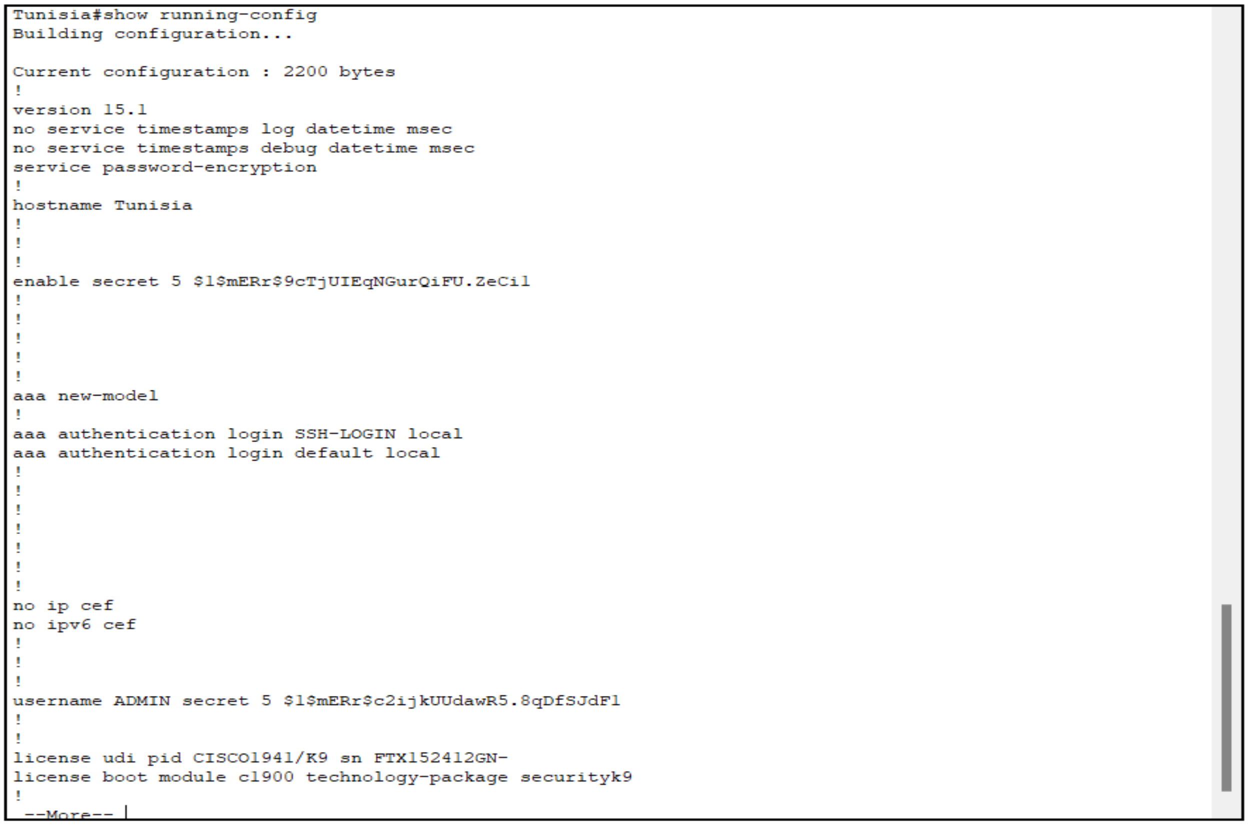


```
TURKEY_S#show running-config
Building configuration...

Current configuration : 3388 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname TURKEY_S
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
username Hamza secret 5 $1$mERr$.Gyel8JwLtOAkqWBXxDMbl
username User secret 5 $1$mERr$o/JM7MD/OGcuNBUQojGl6.
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 10,1000
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 --More--
```

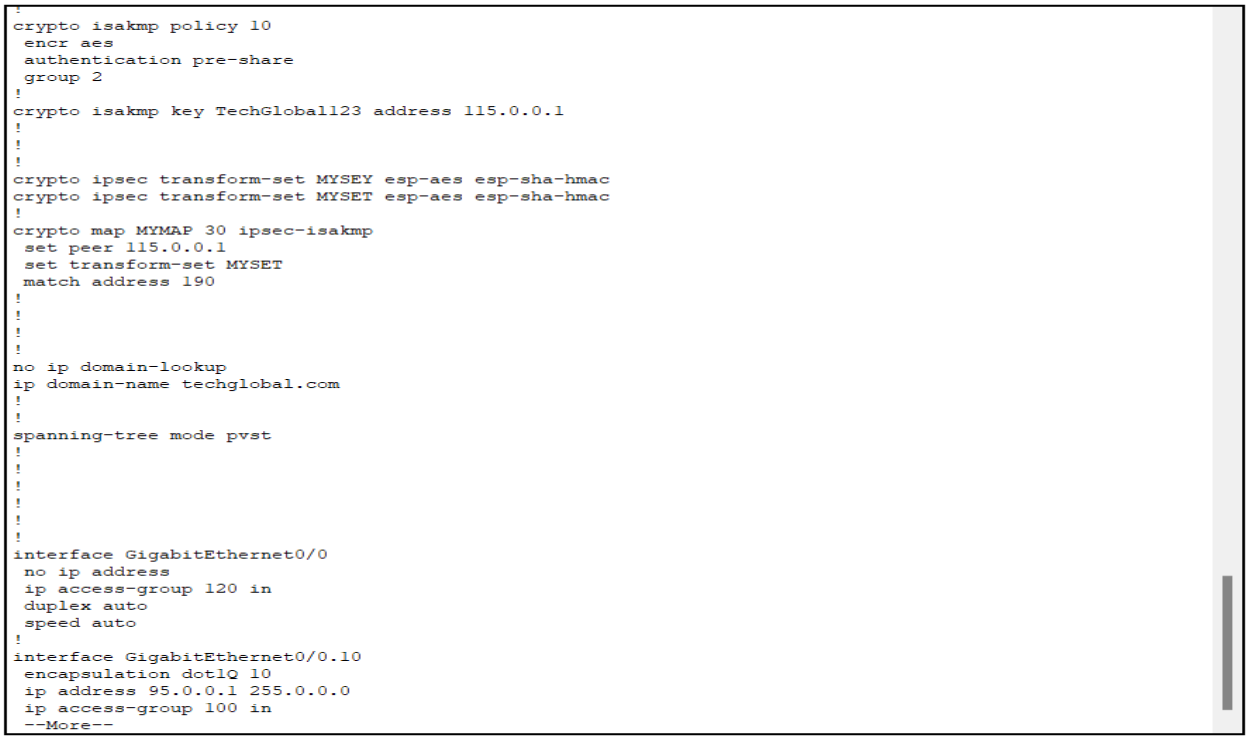


```
!
interface FastEthernet0/23
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 85.0.0.2 255.0.0.0
!
ip default-gateway 85.0.0.1
!
banner motd ^CAuthorized Users Only^C
!
!
!
line con 0
 password 7 0815797C223C3C3743595F
 login
!
line vty 0 4
 exec-timeout 6 0
 password 7 0815797C223C3C3743595F
 login local
 transport input ssh
line vty 5 15
 login
!
!
!
 --More--
```

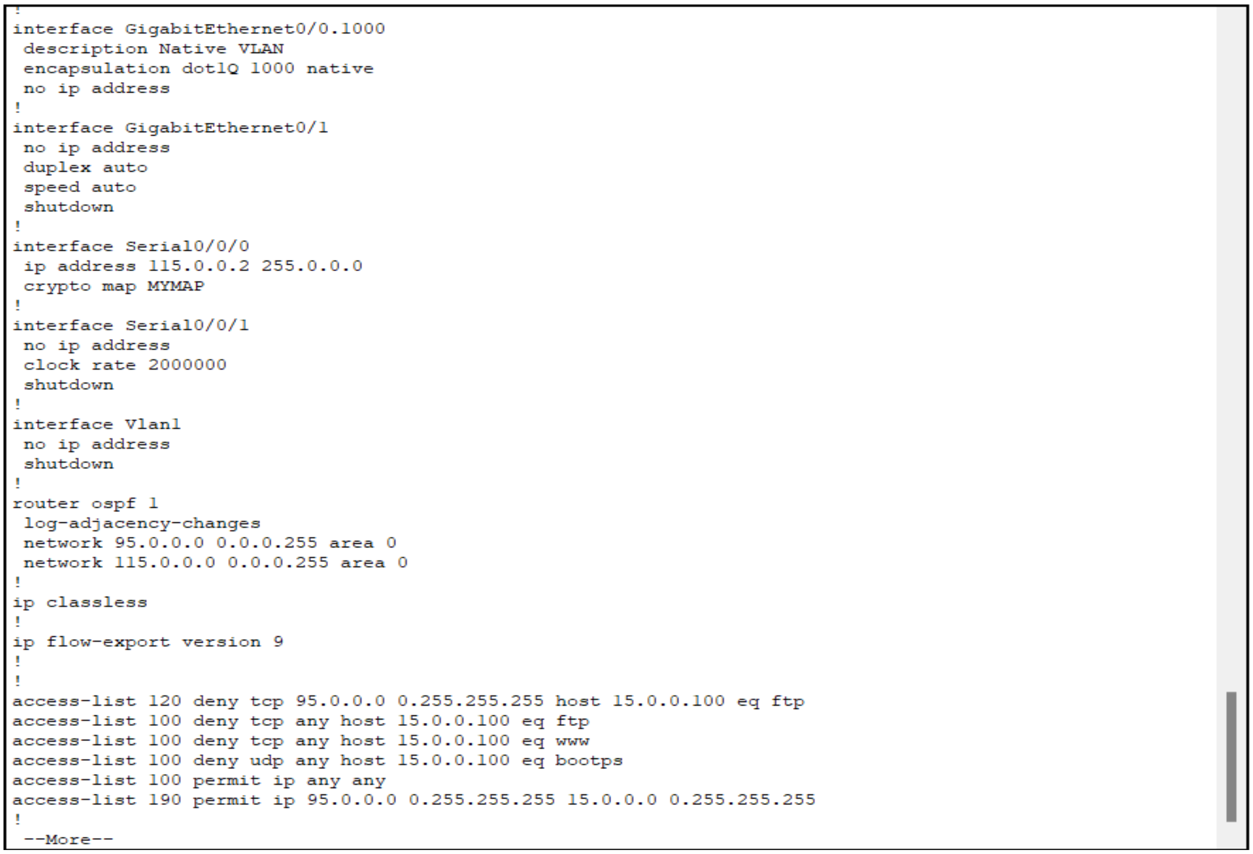
TUNISIA ROUTER



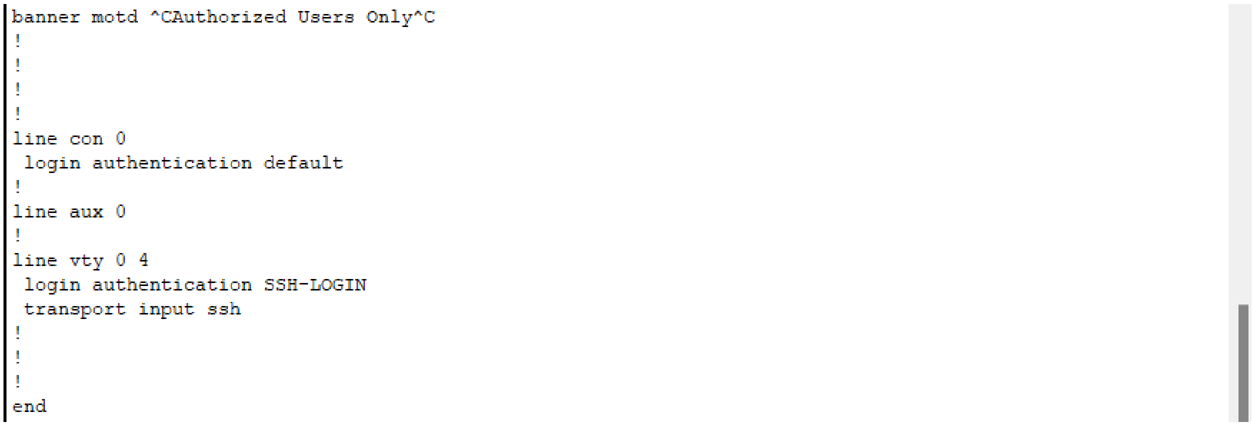
```
Tunisia#show running-config
Building configuration...

Current configuration : 2200 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Tunisia
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
aaa new-model
!
aaa authentication login SSH-LOGIN local
aaa authentication login default local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username ADMIN secret 5 $1$mERr$c2ijkUUdawR5.8qDfSJdFl
!
!
license udi pid CISCO1941/K9 sn FTX152412GN-
license boot module c1900 technology-package securityk9
!
 --More--
```



```
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp key TechGlobal123 address 115.0.0.1
!
!
!
crypto ipsec transform-set MYSEY esp-aes esp-sha-hmac
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
!
crypto map MYMAP 30 ipsec-isakmp
 set peer 115.0.0.1
 set transform-set MYSET
 match address 190
!
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 ip access-group 120 in
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 95.0.0.1 255.0.0.0
 ip access-group 100 in
 --More--
```

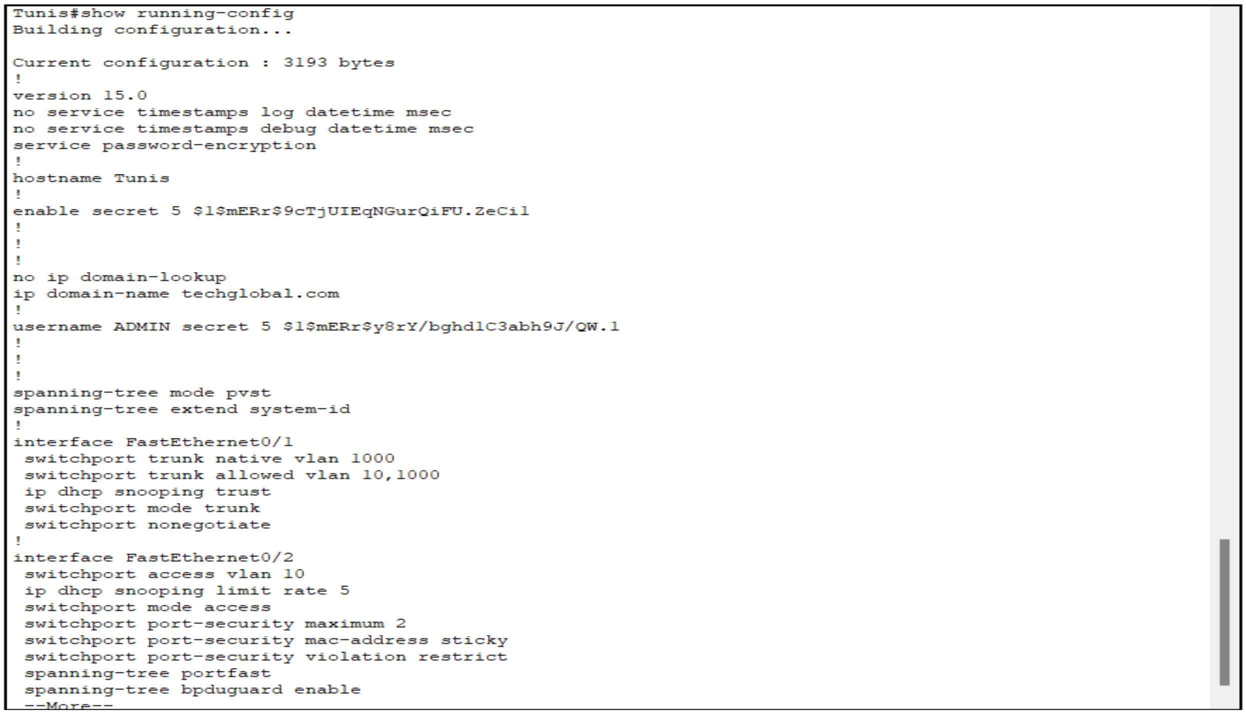


```
!
interface GigabitEthernet0/0.1000
 description Native VLAN
 encapsulation dot1Q 1000 native
 no ip address
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 115.0.0.2 255.0.0.0
 crypto map MYMAP
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 95.0.0.0 0.0.0.255 area 0
 network 115.0.0.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 120 deny tcp 95.0.0.0 0.255.255.255 host 15.0.0.100 eq ftp
access-list 100 deny tcp any host 15.0.0.100 eq ftp
access-list 100 deny tcp any host 15.0.0.100 eq www
access-list 100 deny udp any host 15.0.0.100 eq bootps
access-list 100 permit ip any any
access-list 190 permit ip 95.0.0.0 0.255.255.255 15.0.0.0 0.255.255.255
!
 --More--
```

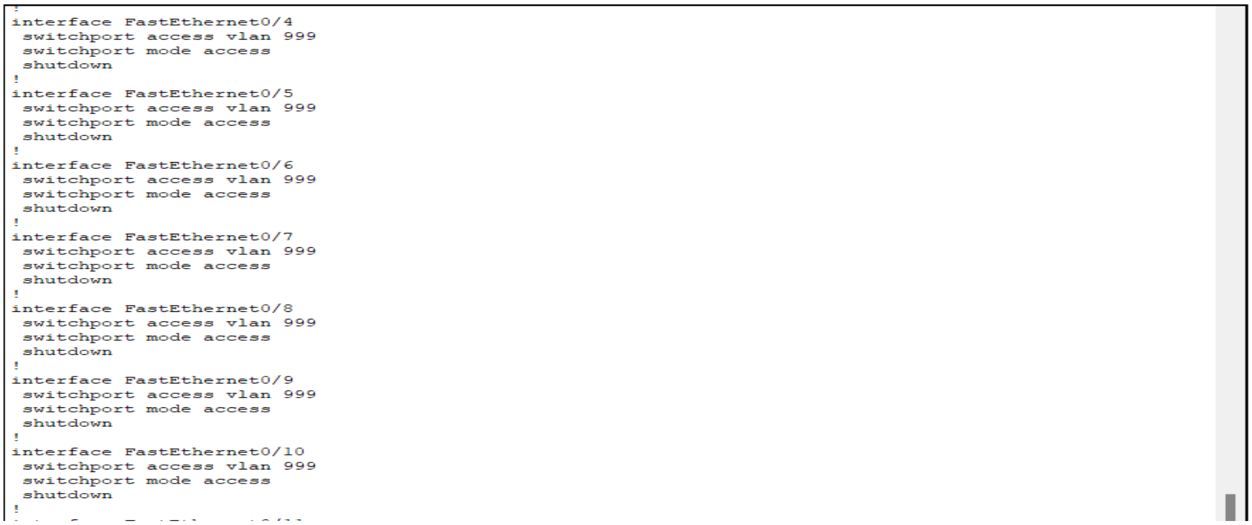


```
banner motd ^CAuthorized Users Only^C
!
!
!
!
line con 0
 login authentication default
!
line aux 0
!
line vty 0 4
 login authentication SSH-LOGIN
 transport input ssh
!
!
!
end
```

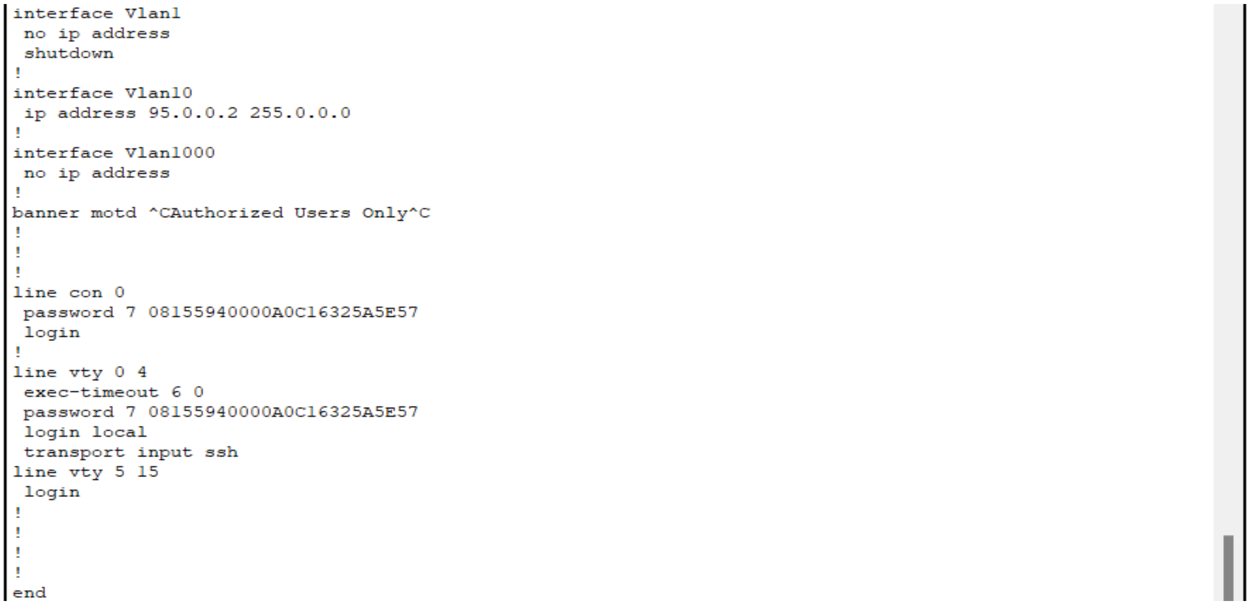
TUNISIA SWITCH



```
Tunis#show running-config
Building configuration...

Current configuration : 3193 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Tunis
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
username ADMIN secret 5 $1$mERr$y8rY/bghdlC3abh9J/QW.1
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 10,1000
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
 --More--
```

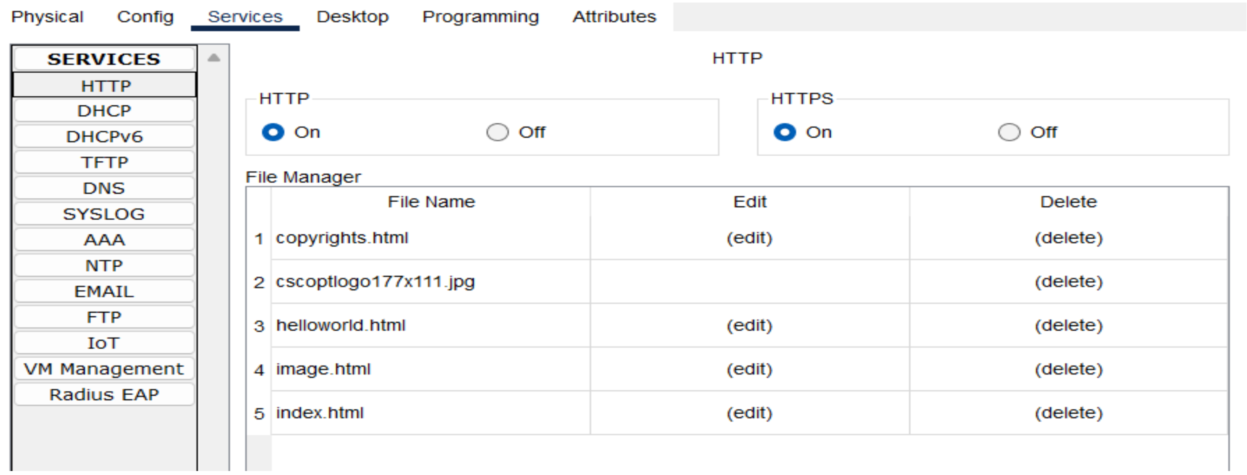


```
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/7
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/11
```



```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 95.0.0.2 255.0.0.0
!
interface Vlan1000
 no ip address
!
banner motd ^CAuthorized Users Only^C
!
!
!
line con 0
 password 7 08155940000A0C16325A5E57
 login
!
line vty 0 4
 exec-timeout 6 0
 password 7 08155940000A0C16325A5E57
 login local
 transport input ssh
line vty 5 15
 login
!
!
!
!
end
```

SERVER CONFIGURATION



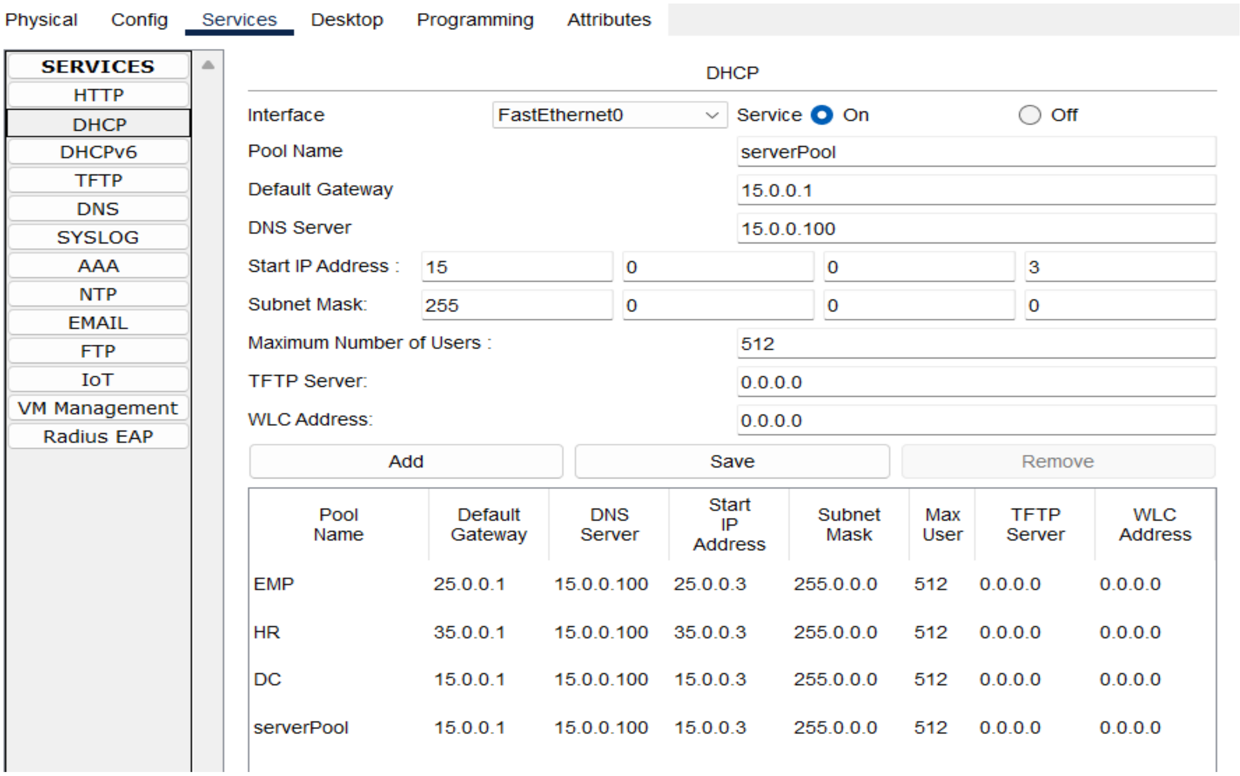
HTTP

HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

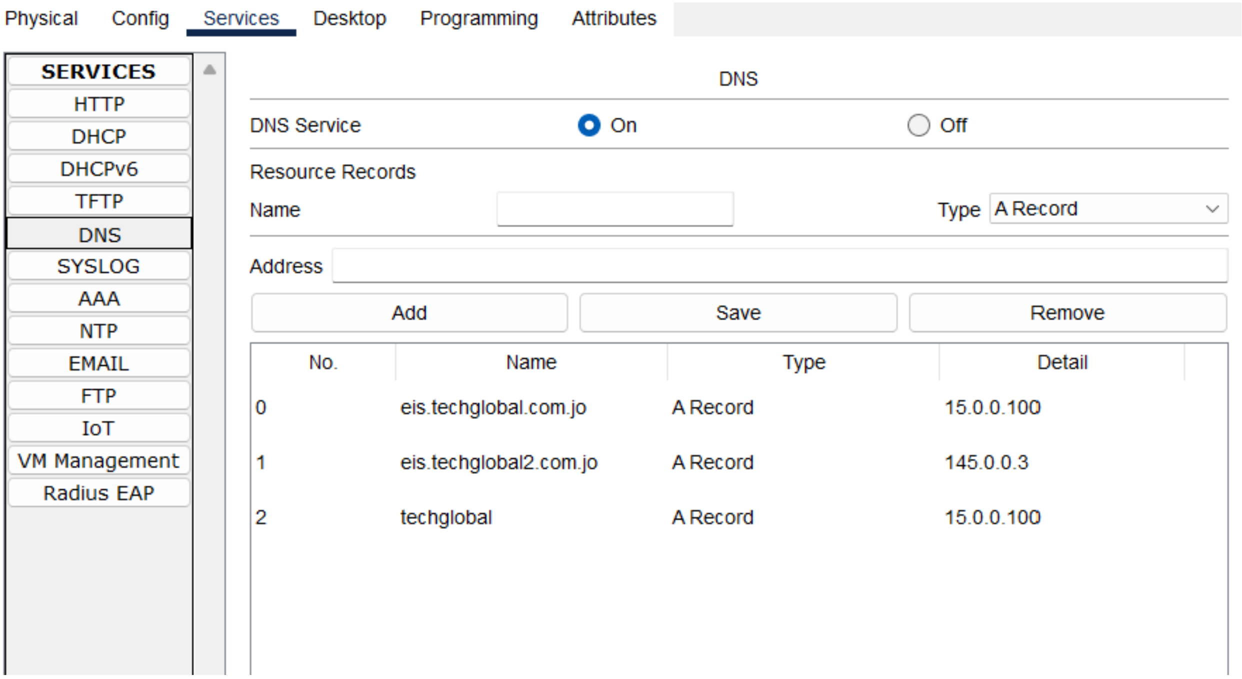


DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name	serverPool
Default Gateway	15.0.0.1
DNS Server	15.0.0.100
Start IP Address :	15 . 0 . 0 . 3
Subnet Mask:	255 . 0 . 0 . 0
Maximum Number of Users :	512
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
EMP	25.0.0.1	15.0.0.100	25.0.0.3	255.0.0.0	512	0.0.0.0	0.0.0.0
HR	35.0.0.1	15.0.0.100	35.0.0.3	255.0.0.0	512	0.0.0.0	0.0.0.0
DC	15.0.0.1	15.0.0.100	15.0.0.3	255.0.0.0	512	0.0.0.0	0.0.0.0
serverPool	15.0.0.1	15.0.0.100	15.0.0.3	255.0.0.0	512	0.0.0.0	0.0.0.0



DNS

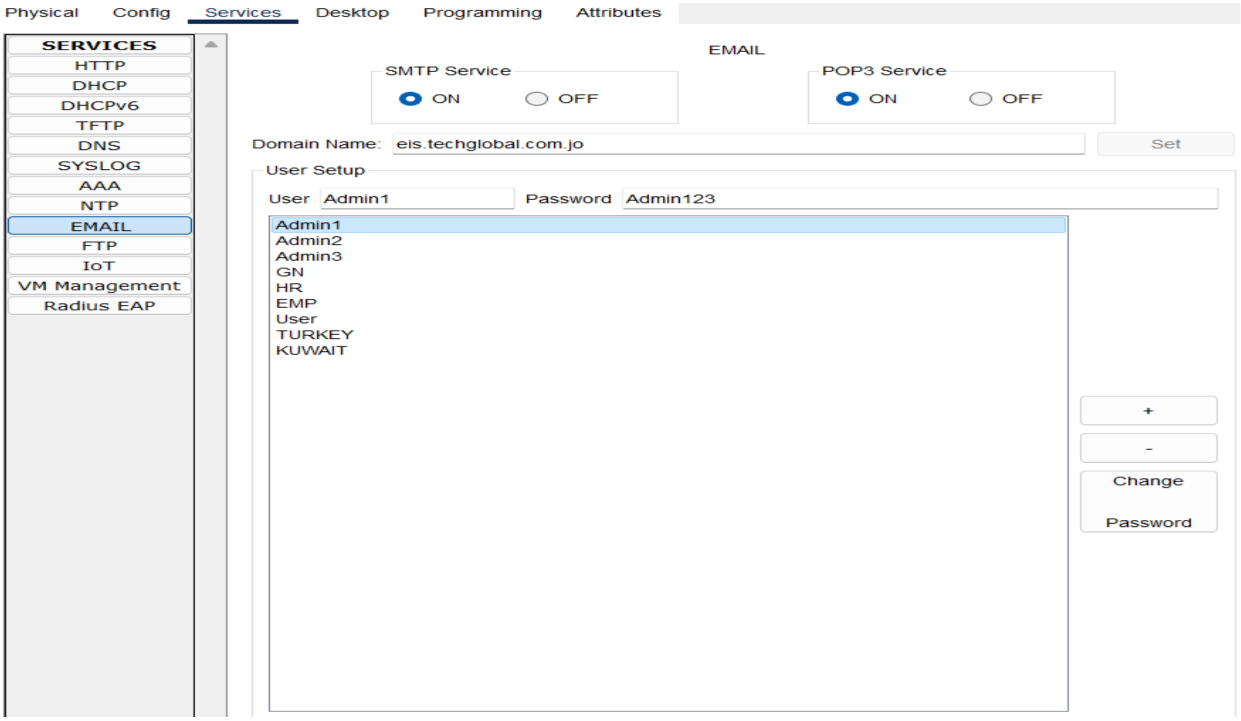
DNS Service ● On ○ Off

Resource Records

Name Type A Record

Address

No.	Name	Type	Detail
0	eis.techglobal.com.jo	A Record	15.0.0.100
1	eis.techglobal2.com.jo	A Record	145.0.0.3
2	techglobal	A Record	15.0.0.100



EMAIL

SMTP Service ● ON ○ OFF

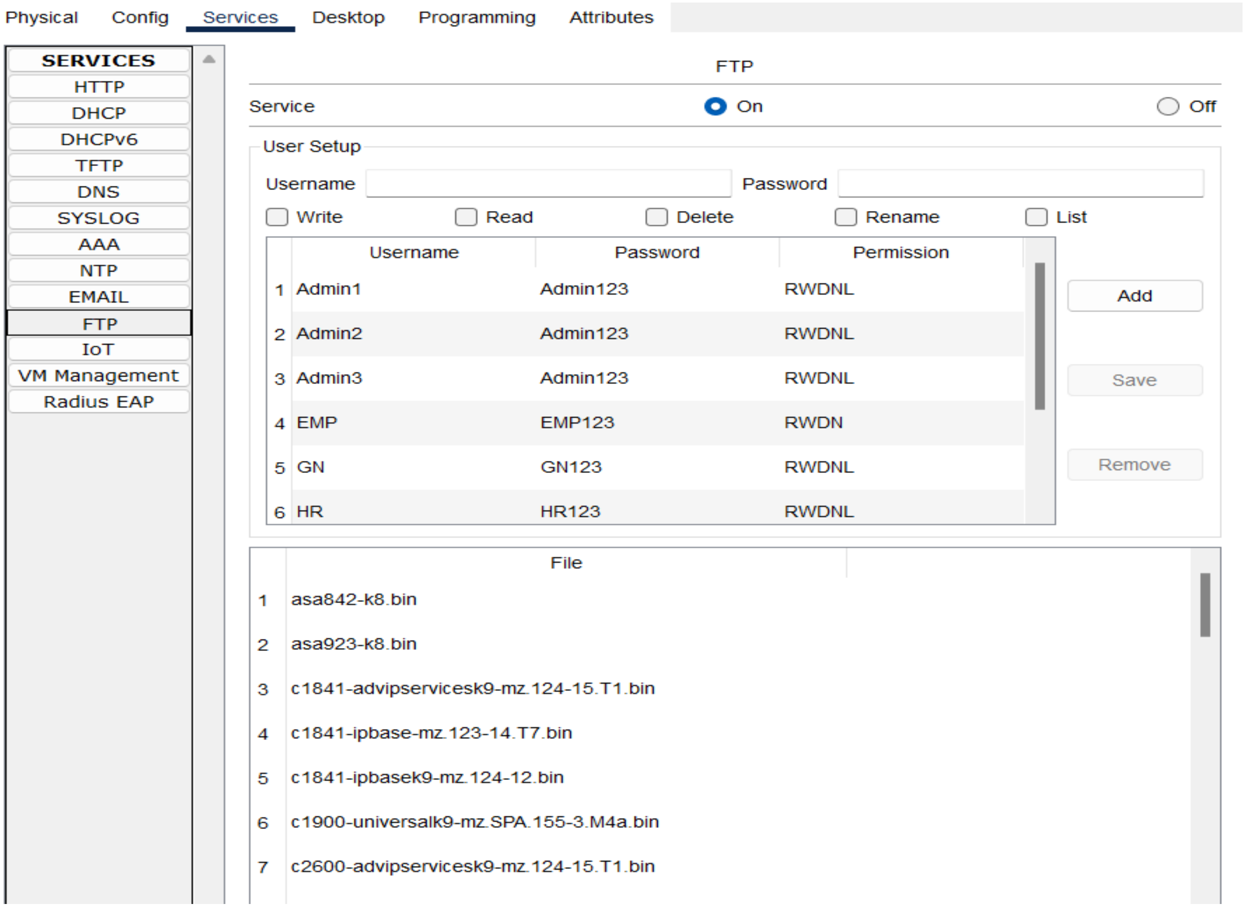
POP3 Service ● ON ○ OFF

Domain Name: eis.techglobal.com.jo

User Setup

User Admin1 Password Admin123

Admin1
Admin2
Admin3
GN
HR
EMP
User
TURKEY
KUWAIT



FTP

Service ● On ○ Off

User Setup

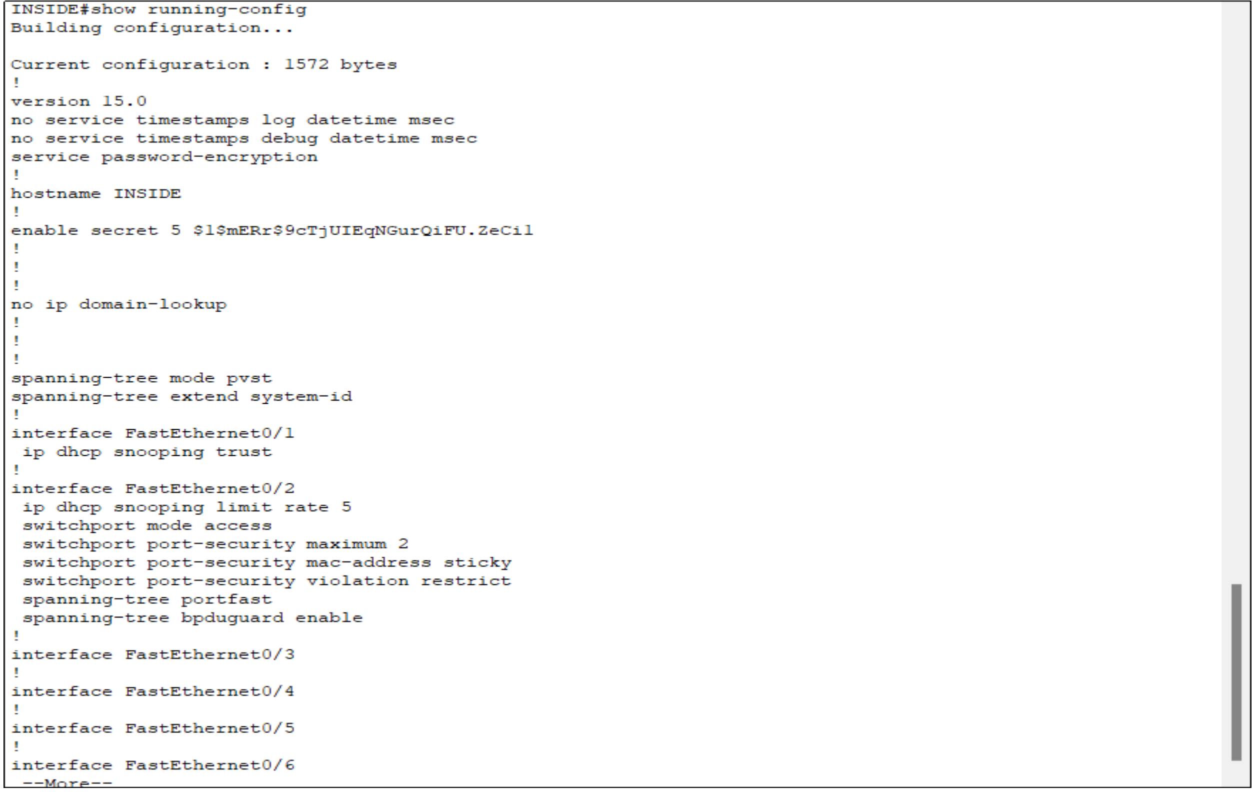
Username Password

□ Write □ Read □ Delete □ Rename □ List

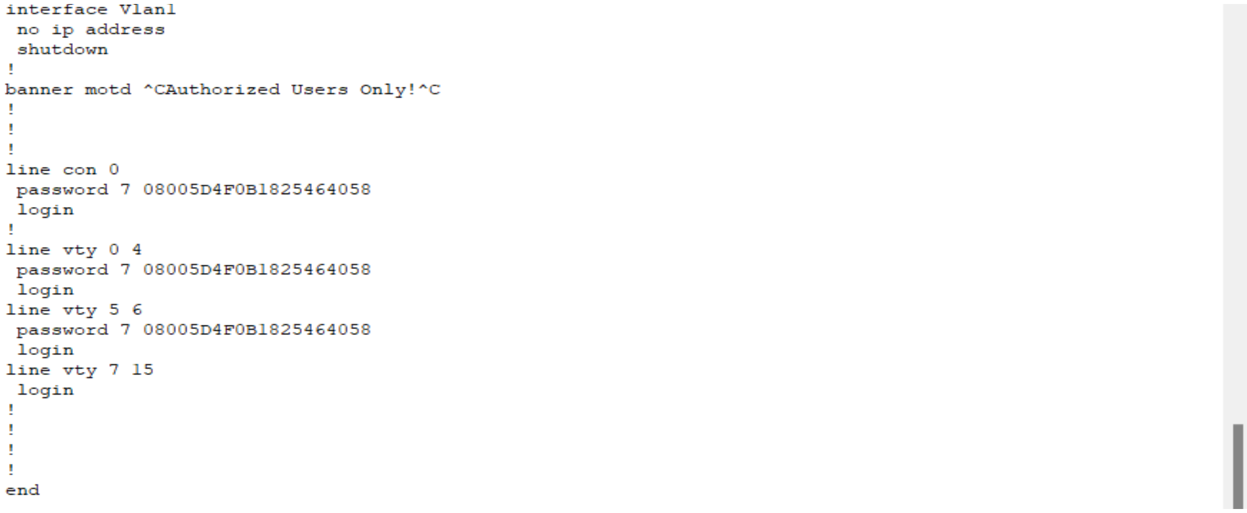
	Username	Password	Permission
1	Admin1	Admin123	RWDNL
2	Admin2	Admin123	RWDNL
3	Admin3	Admin123	RWDNL
4	EMP	EMP123	RWDN
5	GN	GN123	RWDNL
6	HR	HR123	RWDNL

	File
1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin
7	c2600-advipservicesk9-mz.124-15.T1.bin

AQABA INSIDE SWITCH

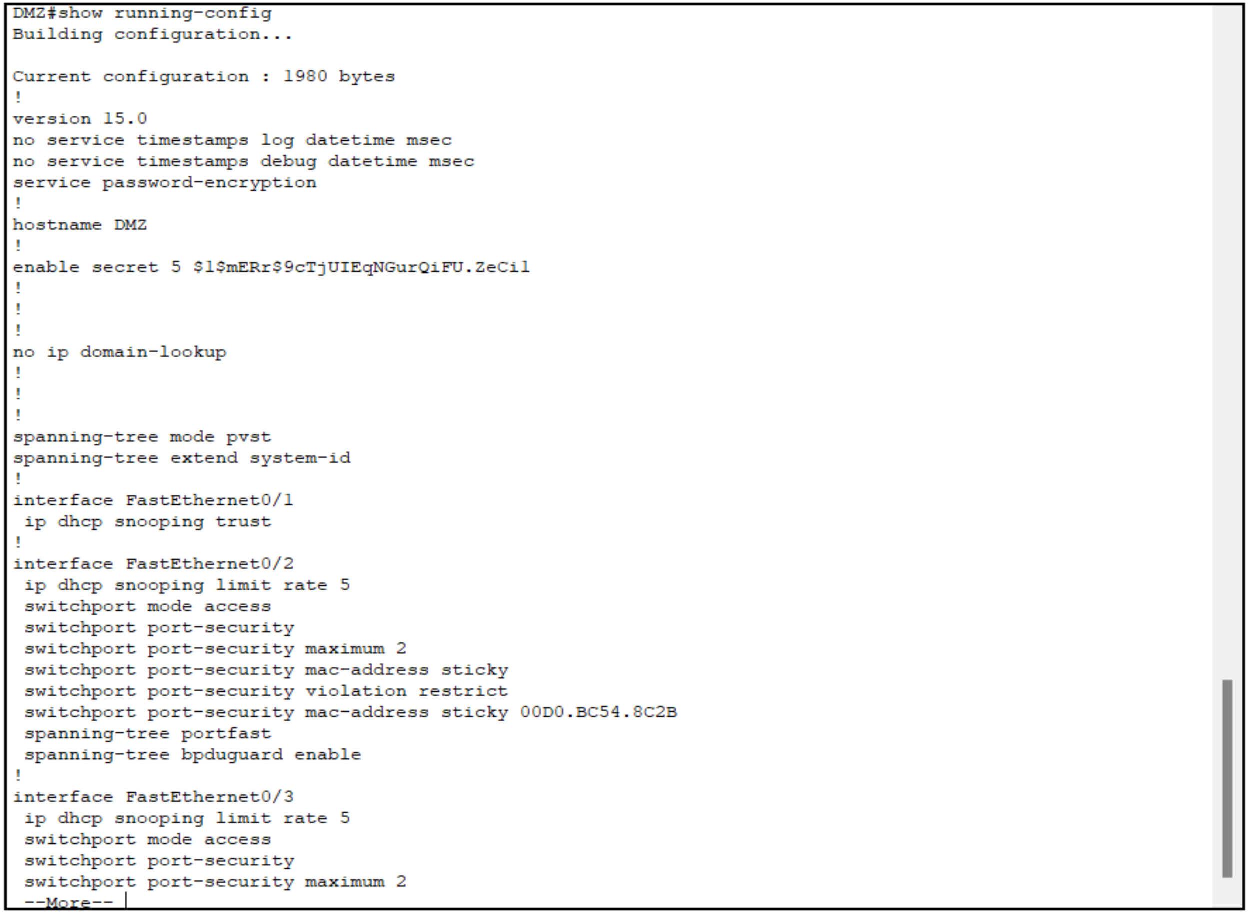


```
INSIDE#show running-config
Building configuration...

Current configuration : 1572 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname INSIDE
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 ip dhcp snooping trust
!
interface FastEthernet0/2
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 --More--
```

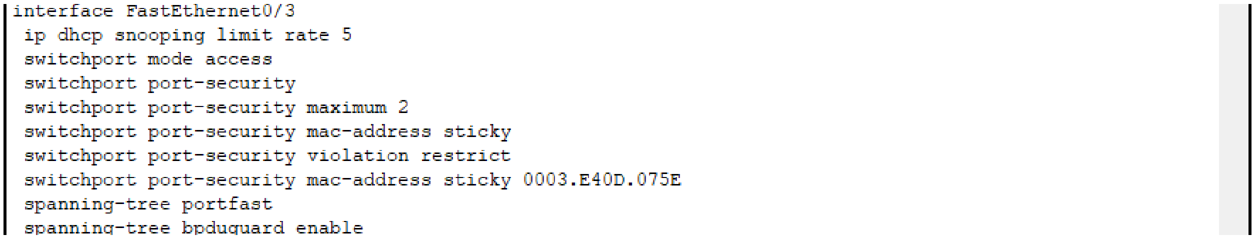


```
interface Vlan1
 no ip address
 shutdown
!
banner motd ^CAuthorized Users Only!^C
!
!
!
line con 0
 password 7 08005D4F0B1825464058
 login
!
line vty 0 4
 password 7 08005D4F0B1825464058
 login
line vty 5 6
 password 7 08005D4F0B1825464058
 login
line vty 7 15
 login
!
!
!
!
end
```

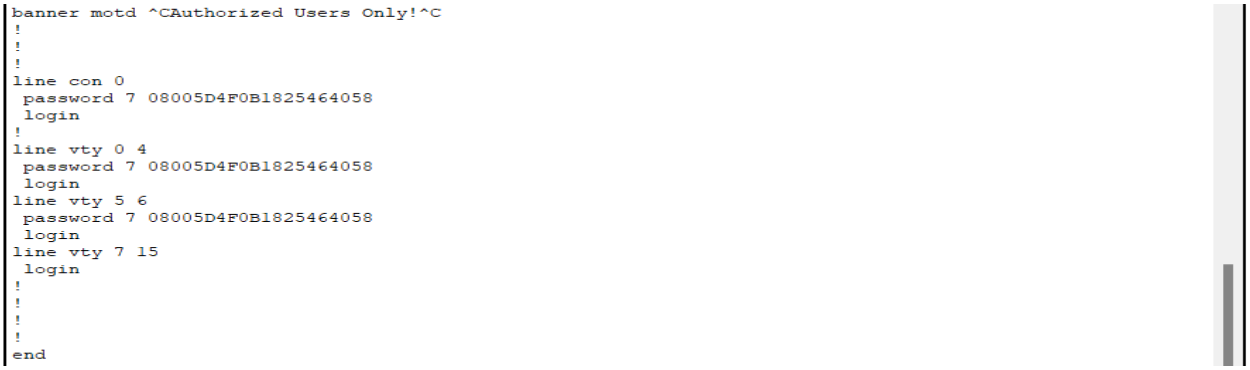
AQABA DMZ SWITCH



```
DMZ#show running-config
Building configuration...

Current configuration : 1980 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname DMZ
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 ip dhcp snooping trust
!
interface FastEthernet0/2
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00D0.BC54.8C2B
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 --More--
```

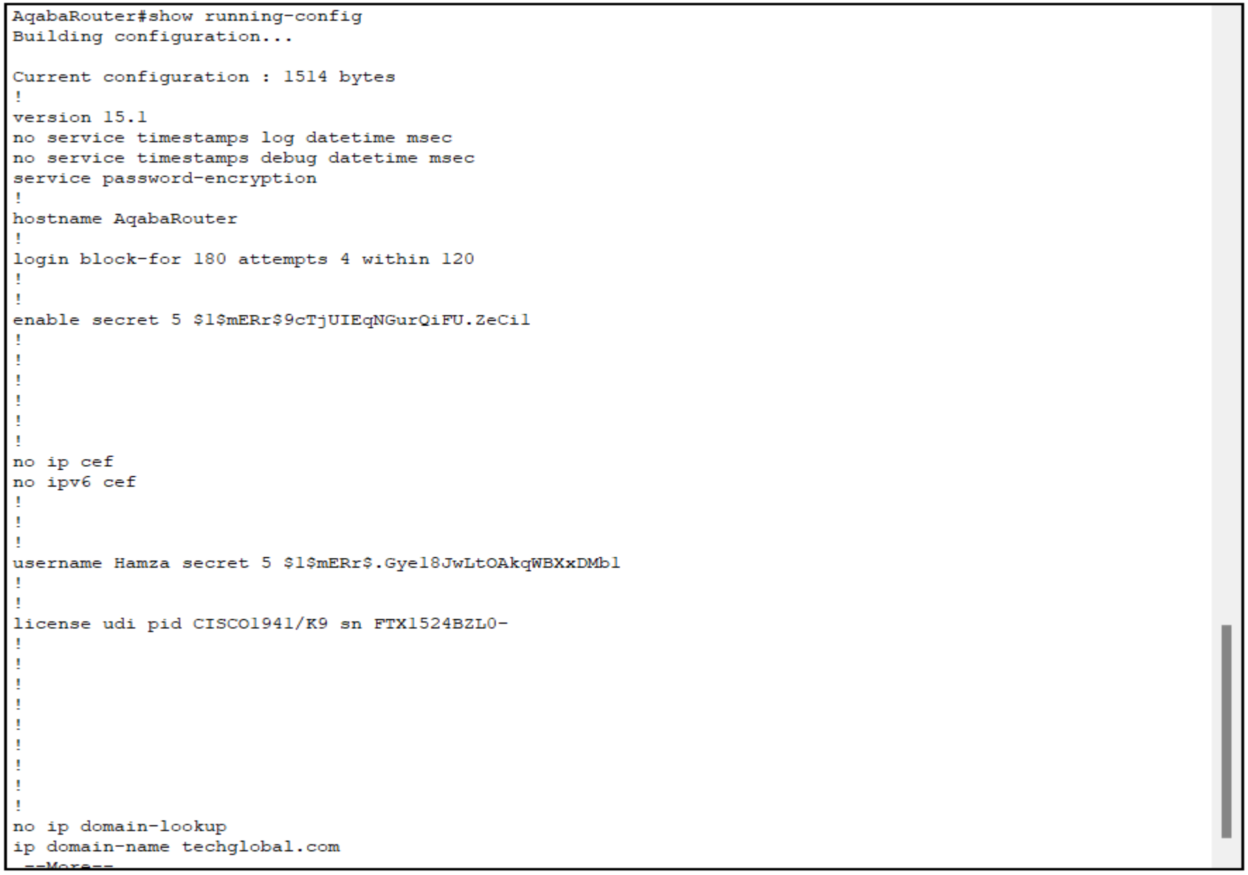


```
interface FastEthernet0/3
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0003.E40D.075E
 spanning-tree portfast
 spanning-tree bpduguard enable
```

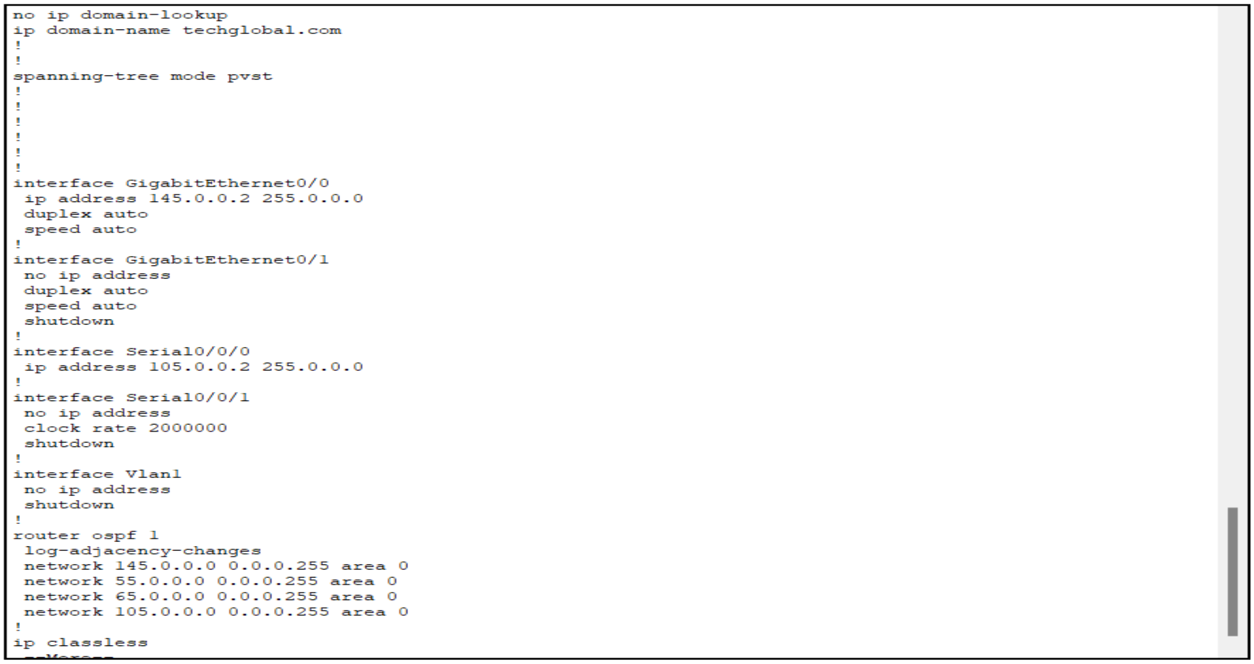


```
banner motd ^CAuthorized Users Only!^C
!
!
!
line con 0
 password 7 08005D4F0B1825464058
 login
!
line vty 0 4
 password 7 08005D4F0B1825464058
 login
line vty 5 6
 password 7 08005D4F0B1825464058
 login
line vty 7 15
 login
!
!
!
!
end
```

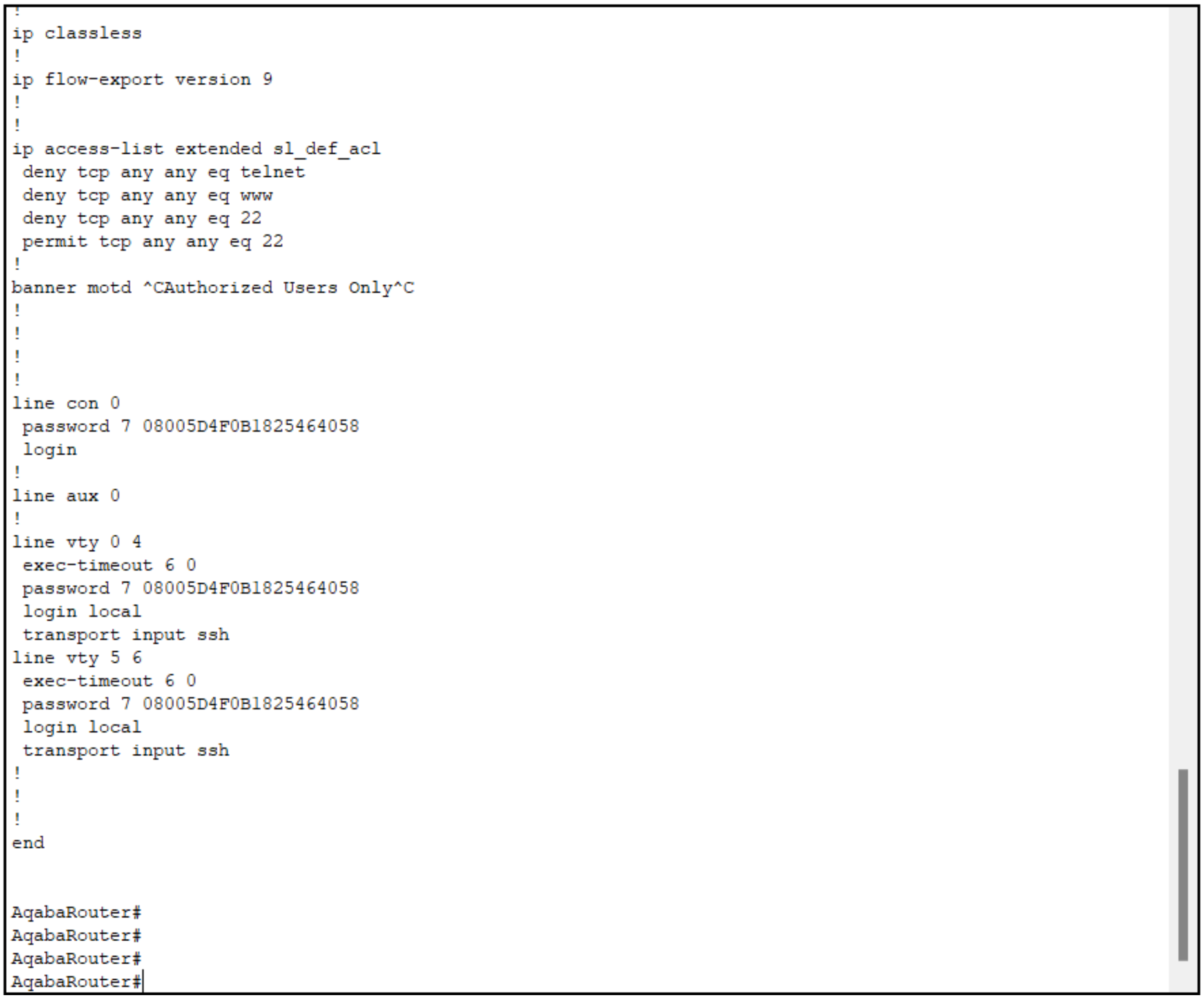
AQABA ROUTER



```
AqabaRouter#show running-config
Building configuration...

Current configuration : 1514 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname AqabaRouter
!
login block-for 180 attempts 4 within 120
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Hamza secret 5 $1$mERr$.Gye18JwLtOAkqWBXxDMbl
!
!
license udi pid CISCO1941/K9 sn FTX1524BZL0-
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
 --More--
```

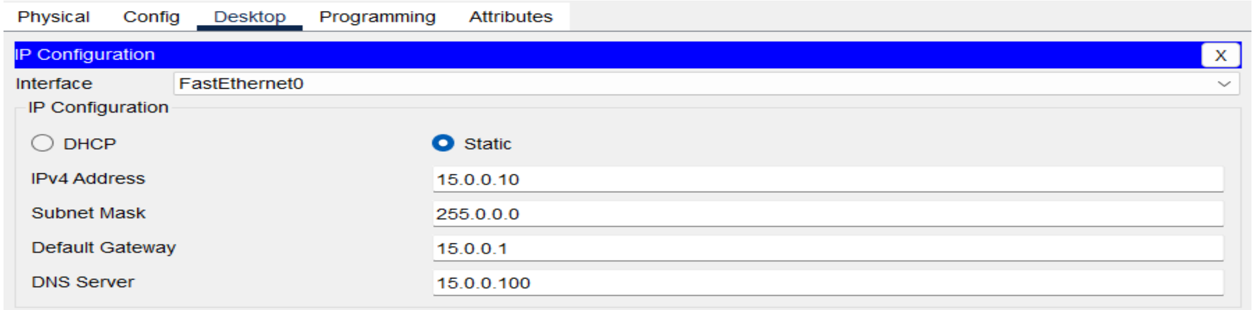


```
no ip domain-lookup
ip domain-name techglobal.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 145.0.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 105.0.0.2 255.0.0.0
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 145.0.0.0 0.0.0.255 area 0
 network 55.0.0.0 0.0.0.255 area 0
 network 65.0.0.0 0.0.0.255 area 0
 network 105.0.0.0 0.0.0.255 area 0
!
ip classless
 --More--
```



```
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
!
banner motd ^CAuthorized Users Only^C
!
!
!
!
line con 0
 password 7 08005D4F0B1825464058
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 6 0
 password 7 08005D4F0B1825464058
 login local
 transport input ssh
line vty 5 6
 exec-timeout 6 0
 password 7 08005D4F0B1825464058
 login local
 transport input ssh
!
!
!
end


AqabaRouter#
AqabaRouter#
AqabaRouter#
AqabaRouter#
```

PC SETTINGS WITH STATIC IP ADDRESS



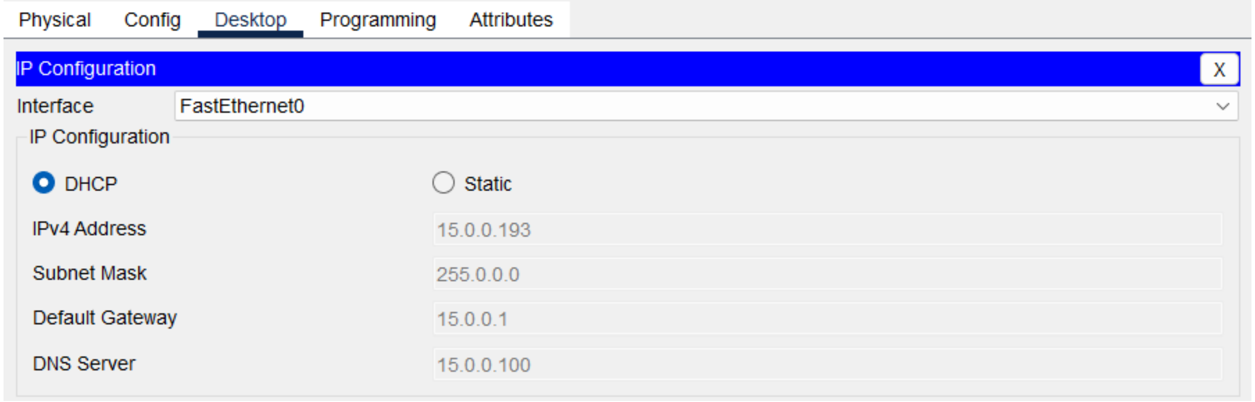
Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	15.0.0.10
Subnet Mask	255.0.0.0
Default Gateway	15.0.0.1
DNS Server	15.0.0.100

PC SETTINGS WITH DYNAMIC IP ADDRESS (GATEWAY WILL CHANGE DEPEND ON VLAN)



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 15.0.0.193

Subnet Mask: 255.0.0.0

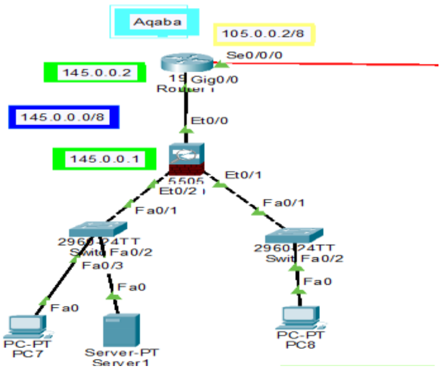
Default Gateway: 15.0.0.1

DNS Server: 15.0.0.100

CHOICES MADE IN DURING IMPLEMENTATION

USING ASA 5505

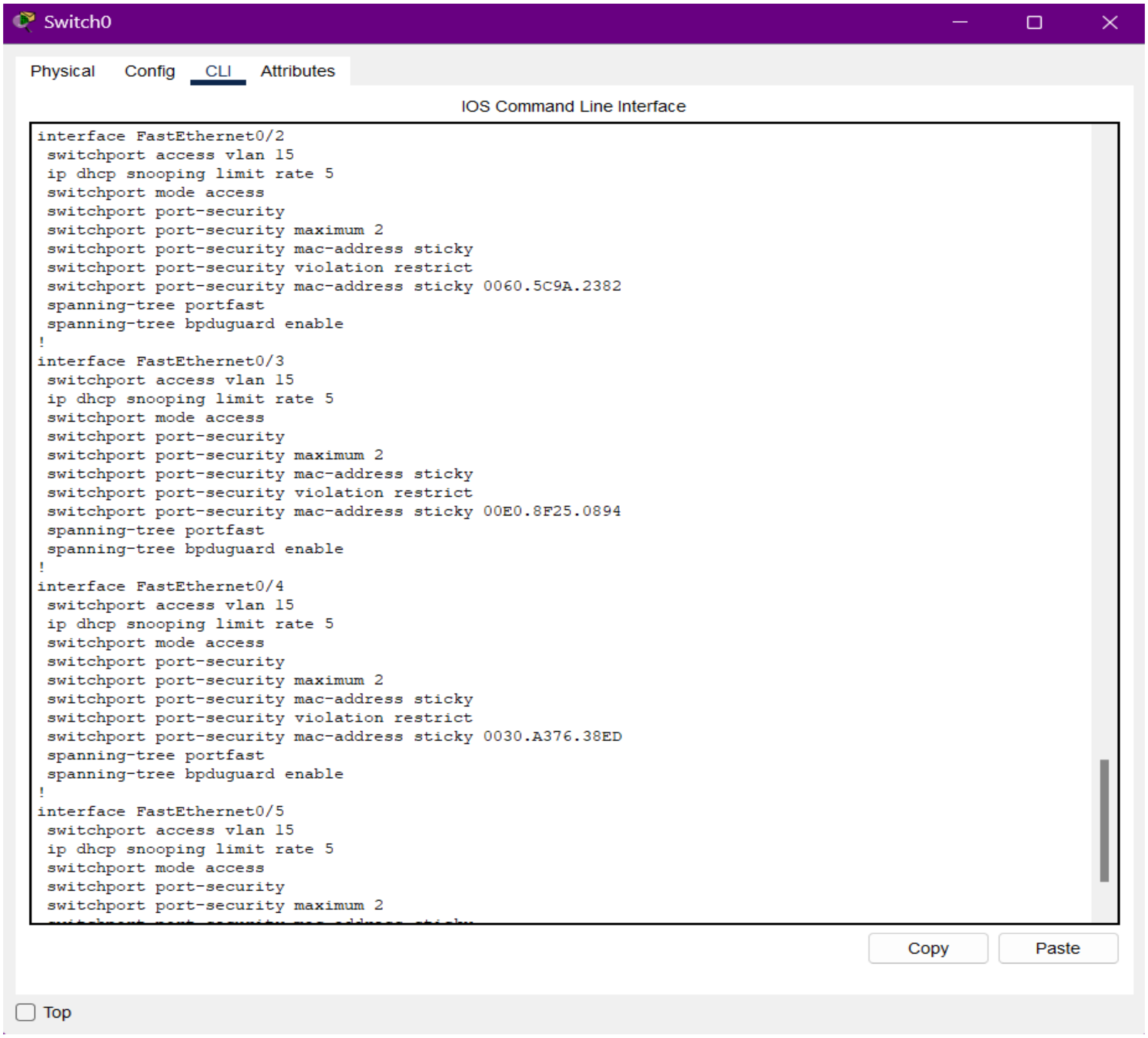
In packet tracer, I used ASA 5505 over 5506 ASA because ASA 5505 contains default VLANs for inside and outside to facilitate the firewall configuration.5506 does not contains default VLANs or ethernet cables, so I decided to use ASA 5505.



SWITCHPORT PORT-SECUIRTY MAC-ADDRESS STICKY

In Tech global scenario, I used in port security to define and learn MAC address automatically or dynamically (sticky) not manually (Put MAC address manually). I used it because I heard that if I used manually and restart the switch, the learned MAC addresses will remove. On the other hand, sticky option is dynamically learn the MAC addresses so it will not effect our network in switches restarting case.

In addition, sticky option gives us the ability to easily learn MAC addresses with less time instead of manually learned that could take long time and effort.



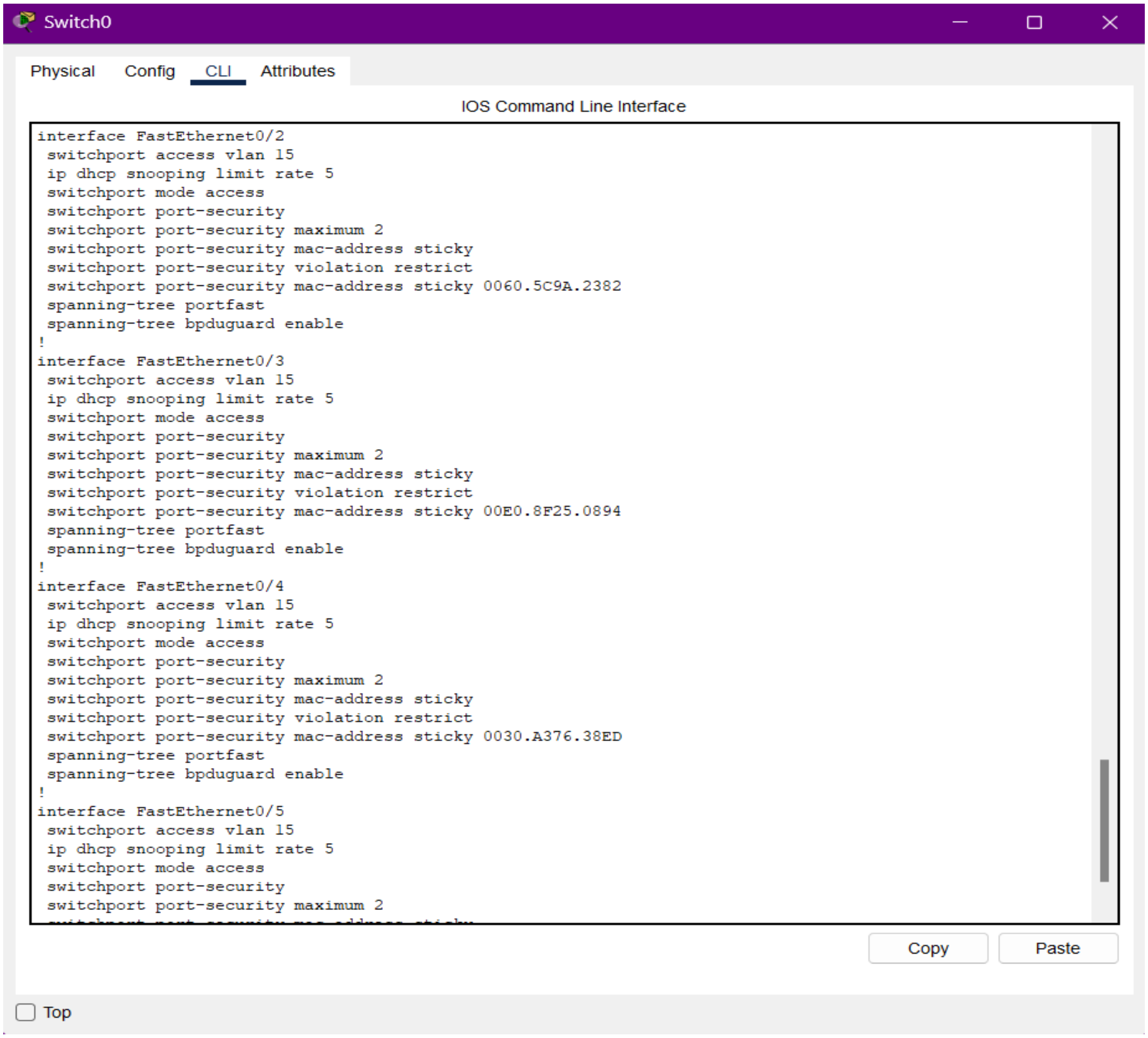
```
interface FastEthernet0/2
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.5C9A.2382
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.8F25.0894
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0030.A376.38ED
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
```

This image represents the configuration of a switch ports including MAC address sticky command to give evidence of sticky implementation.

SWITCHPORT PORT-SECURITY VIOLATION RESTRICT

Also, in port security configuration, I used restrict (put procedures if the port faced violation (violation means the port exceeds the limit of max MAC addresses). Protect means drop the packet, Shutdown means drop the packet and error disabled, restrict means drop the packet and notify the admin (there is a violation)) option over protect and shutdown.

Restrict is more secure and it offers a fair balance. It protects the network by banning illegal connections while remaining the connection to the port active. This guarantees that network resources are not completely impacted.

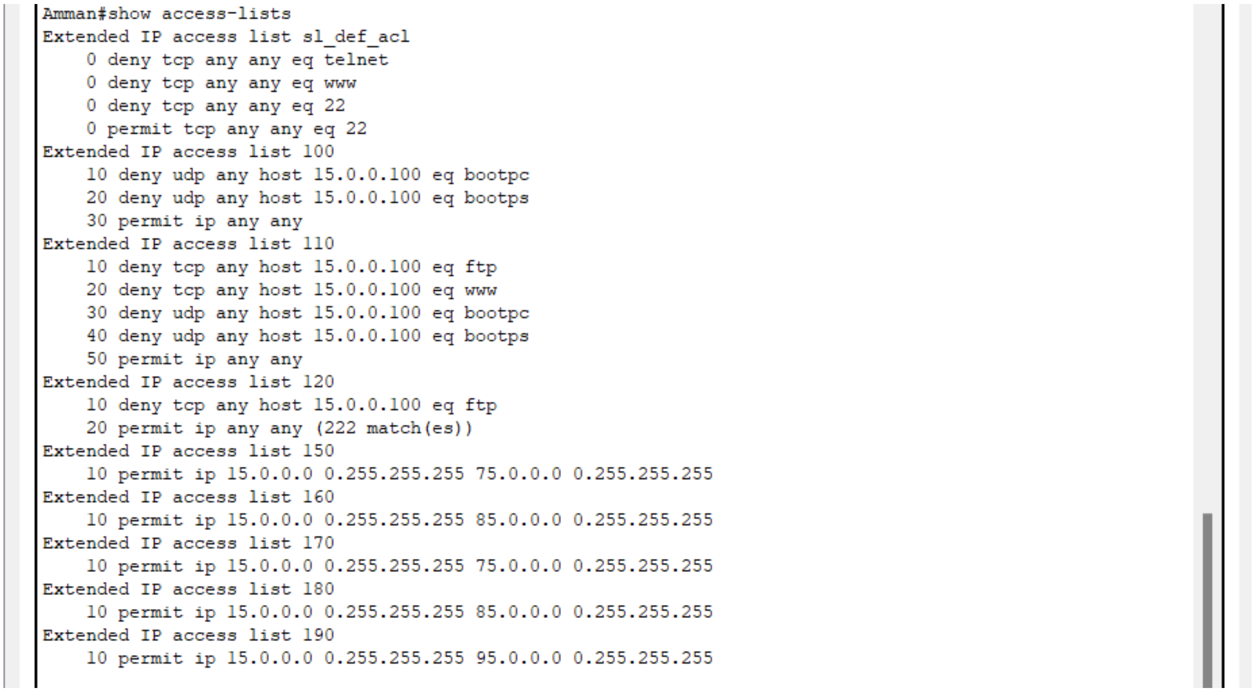


```
interface FastEthernet0/2
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.5C9A.2382
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.8F25.0894
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0030.A376.38ED
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 switchport access vlan 15
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
```

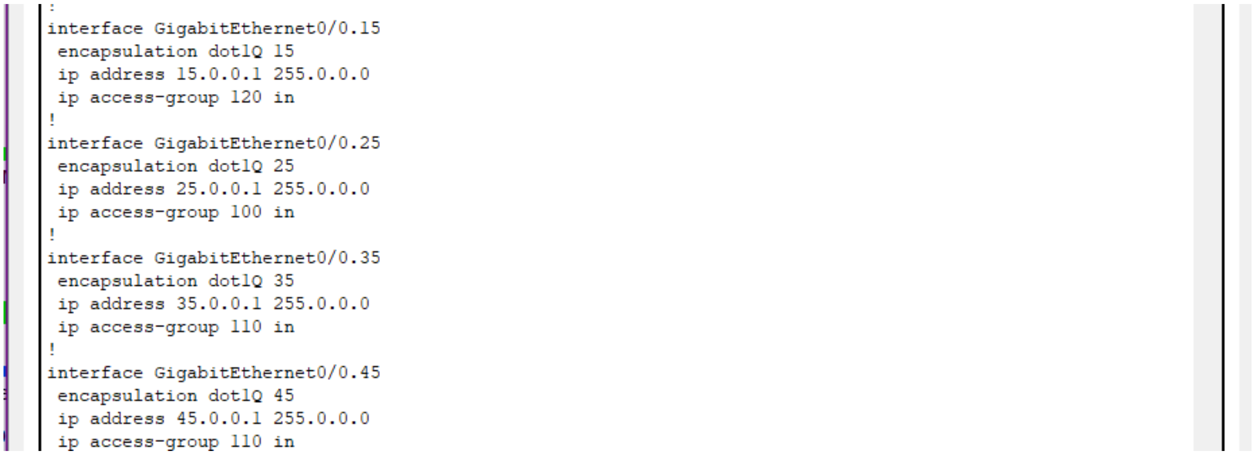
This image represents the configuration of a switch ports including violation command to give evidence of restrict option implementation.

EXTENDED ACLS

IN context of access lists, I preferred to use extended over standard ACL because I wanted to filter traffic based on source and destination addresses, network protocols such as tcp ,udp,etc, and port numbers. In addition, based on the requirements of Tech global, it is necessary to use extended to block specific devices to reach certain services on server.



```
Amman#show access-lists
Extended IP access list sl_def_acl
    0 deny tcp any any eq telnet
    0 deny tcp any any eq www
    0 deny tcp any any eq 22
    0 permit tcp any any eq 22
Extended IP access list 100
    10 deny udp any host 15.0.0.100 eq bootpc
    20 deny udp any host 15.0.0.100 eq bootps
    30 permit ip any any
Extended IP access list 110
    10 deny tcp any host 15.0.0.100 eq ftp
    20 deny tcp any host 15.0.0.100 eq www
    30 deny udp any host 15.0.0.100 eq bootpc
    40 deny udp any host 15.0.0.100 eq bootps
    50 permit ip any any
Extended IP access list 120
    10 deny tcp any host 15.0.0.100 eq ftp
    20 permit ip any any (222 match(es))
Extended IP access list 150
    10 permit ip 15.0.0.0 0.255.255.255 75.0.0.0 0.255.255.255
Extended IP access list 160
    10 permit ip 15.0.0.0 0.255.255.255 85.0.0.0 0.255.255.255
Extended IP access list 170
    10 permit ip 15.0.0.0 0.255.255.255 75.0.0.0 0.255.255.255
Extended IP access list 180
    10 permit ip 15.0.0.0 0.255.255.255 85.0.0.0 0.255.255.255
Extended IP access list 190
    10 permit ip 15.0.0.0 0.255.255.255 95.0.0.0 0.255.255.255
```



```
!
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 15.0.0.1 255.0.0.0
 ip access-group 120 in
!
interface GigabitEthernet0/0.25
 encapsulation dot1Q 25
 ip address 25.0.0.1 255.0.0.0
 ip access-group 100 in
!
interface GigabitEthernet0/0.35
 encapsulation dot1Q 35
 ip address 35.0.0.1 255.0.0.0
 ip access-group 110 in
!
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45
 ip address 45.0.0.1 255.0.0.0
 ip access-group 110 in
```

These images represent the configuration of extended ACLs on Amman router and deploy ACL on specific router interface.

COMPARE BETWEEN IPSEC AND SSH PROTOCOLS

IPsec	SSL
Internet layer	Application layer
Contains various protocols that offers security for IP	Securely send information over the internet
Encrypts all IP	Encrypts only data between user and application
Need expert to configure it (complex configuration)	Not necessary to be expert to configure it (simple configuration)
Implemented to secure VPN	Implemented to secure web transactions
Changes are necessary to the operating system for implementation. No changes have to be made to the application.	No changes have to be made to the operating system for implementation; however, changes have to be made to the application.
Has pre shared key	Hasn’t pre shared key (use credentials)

(Difference between IPSec and SSL 2023) [1]

IMPORTANCE OF NETWORK SECURITY

In these days, the security is one of the most important sectors due to the increasing number of attackers and methods to illegal access network or system. Security in any network protects the stored data, especially sensitive data, from unauthorized access.

It also creates trust between users and company due to the robust security that the company implements thus increase the reputation in the market. In addition, it also protects data even when it transferred between devices to avoid any data breach or cyber security attacks by using different methods like encryption.

Cyber-attacks have various threats on the company such as loosing sensitive data, and effect the network (downtime), which result in finical losses, but when using network security, we can reduce and prevent cyber-attacks from accessing to the network thus increasing in profit of the company. Network security enables companies to stay in line with regulations to minimize possible losses in money due to penalties or legal action.

Finally, for companies that work remotely most of the time, network security improves and increases the security level of the remote work by securing the user’s connections.

(Power, Understanding the importance of network security 2024) [2]

TEST PLAN

AIM

The main purpose of using the test plan is to test and evaluate the network performance and functionalities implemented in the network.

TESTING SCHEDULE

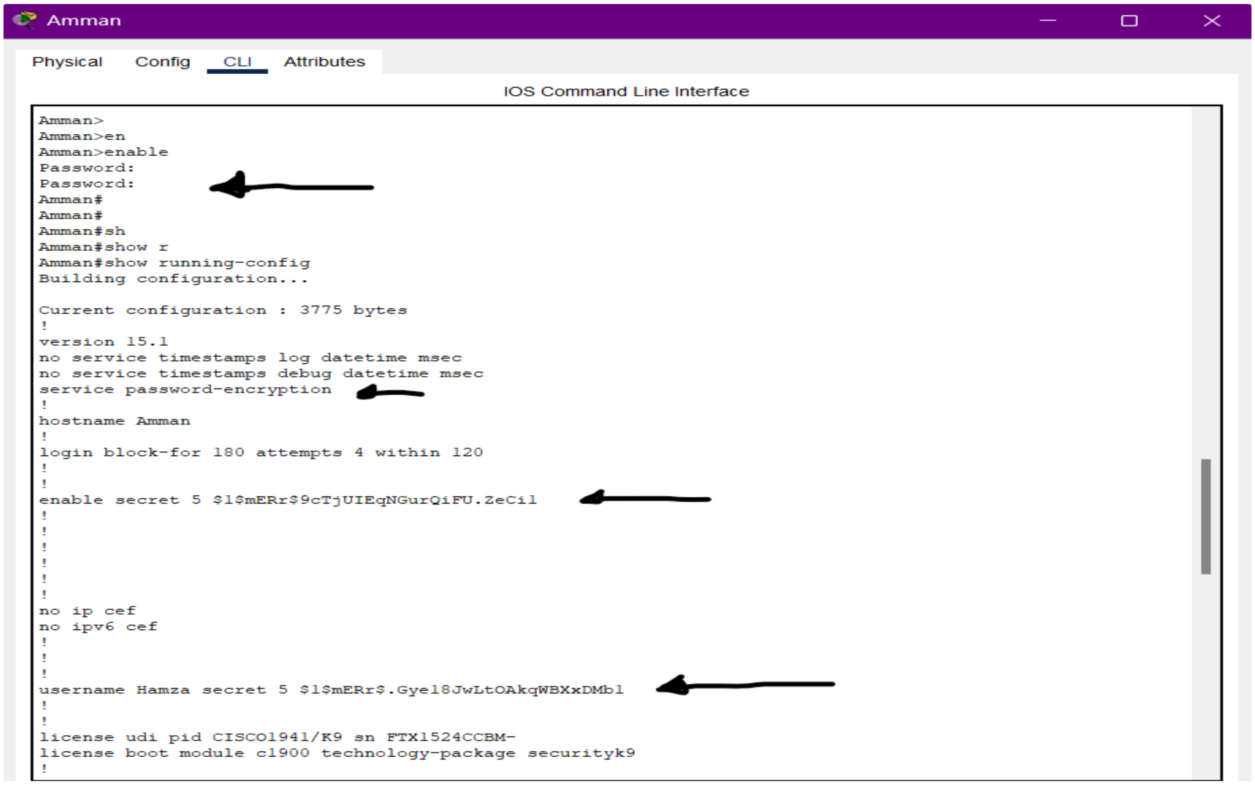
Test Category	**Test Conducted**	**Expected Result**	**How to Perform in Packet Tracer**	**Status**
Security Configuration	Password Configuration Check	Setting strong password on each router and switch.	By Using the **show running-config** command.	Pass
	Implement password encryption	All passwords must be encrypted	By Using the **show running-config** command.	Pass
	SSH measures	SSH implemented on routers and switches	By Using the **show running-config** command. Or by using authorized PC and type "**ssh -l username and target ip address**"	Pass
	SSH measures of ASA firewall	SSH implemented on the ASA and only who have 15.0.0.10 IP address to access it	Type "**ssh -l username and target IP address**"	Pass
	Port Security measures	Implement only 2 MAC address to each port with "restrict" mode violation	**show port-security interface [interface]** to view all port security measure	Pass

Test Category	**Test Conducted**	**Expected Result**	**How to Perform in Packet Tracer**	**Status**
	DHCP Security measures	DHCP snooping implemented	Command → **show ip dhcp snooping**.	Pass
VPN Connectivity	VPN connectivity between remote offices and DC	Excellent and implemented VPN connectivity	From PC, **ping** each remote office on 15.0.0.100	Pass
VLAN connectivity	Check connectivity between offices	Connectivity established between offices	**Ping Ip address**	Pass
Service Accessibility	HTTPs and DNS Access	VLANs and LANs must use HTTPs and name (DNS)	From PC →desktop →web browser → use DNS name	Pass
	FTP Access	Only EMP and AQABA use ftp	Command prompt → ftp 15.0.0.100	Pass
	DHCP access	Only Data center accessed to DHCP	Desktop → IP configuration → changed to DHCP option	Pass
	HTTP access	Only EMP can access HTTP	From PC →desktop →web browser → use DNS name	Pass
Disaster Recovery	Redundant HTTPS Server	Access HTTPs server from DMZ with IP address 145.0.0.3	From PC →desktop →web browser → use DNS name	Pass
AAA	AAA authentication	AAA is implemented on	Tunisia router → CLI → enter username	Pass

Test Category	Test Conducted	Expected Result	How to Perform in Packet Tracer	Status
	on Tunisia router	only Tunisia network	ADMIN→ password @SecureP@$$W0rd#	

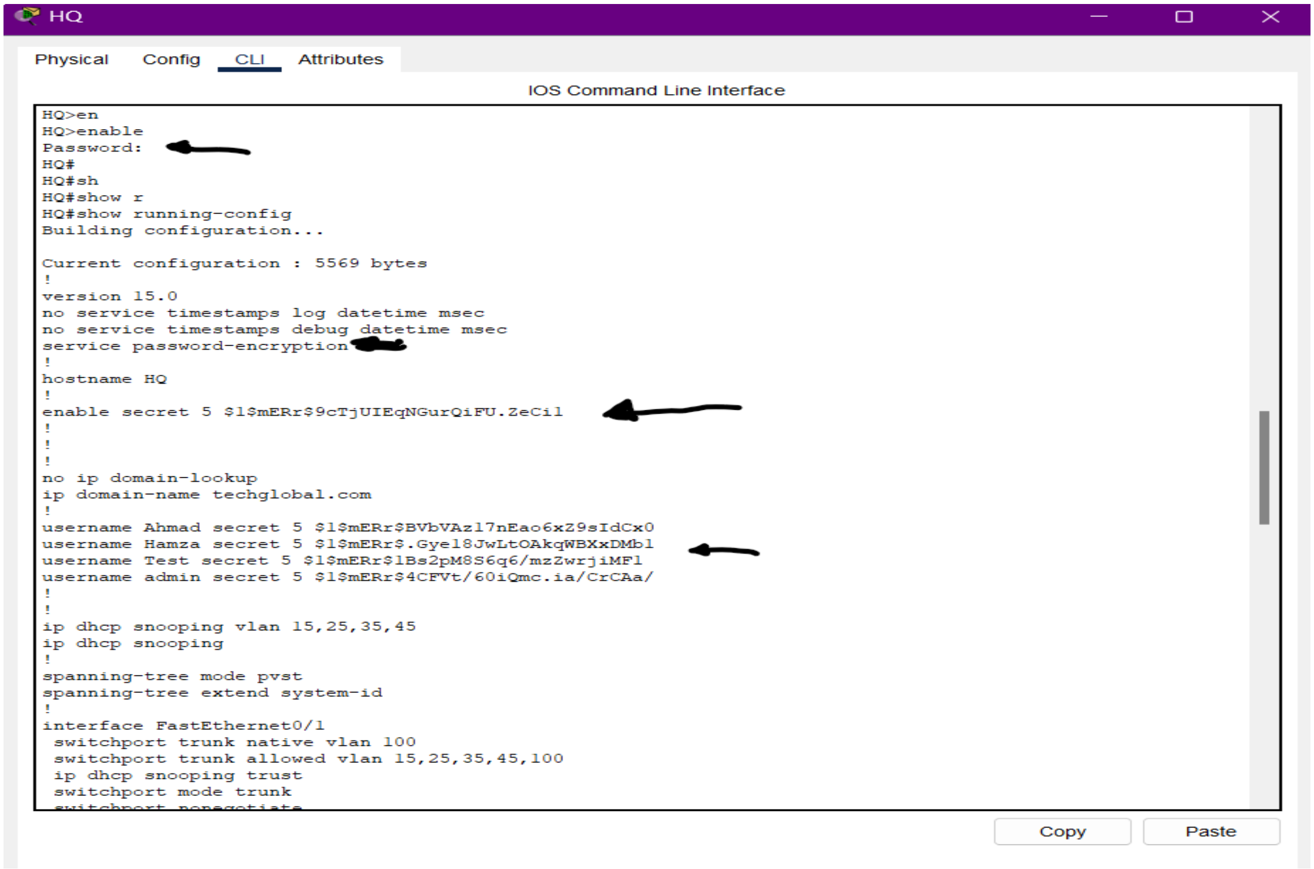
PASSWORD CONFIGURATION SCREEN SHOTS

Amman router



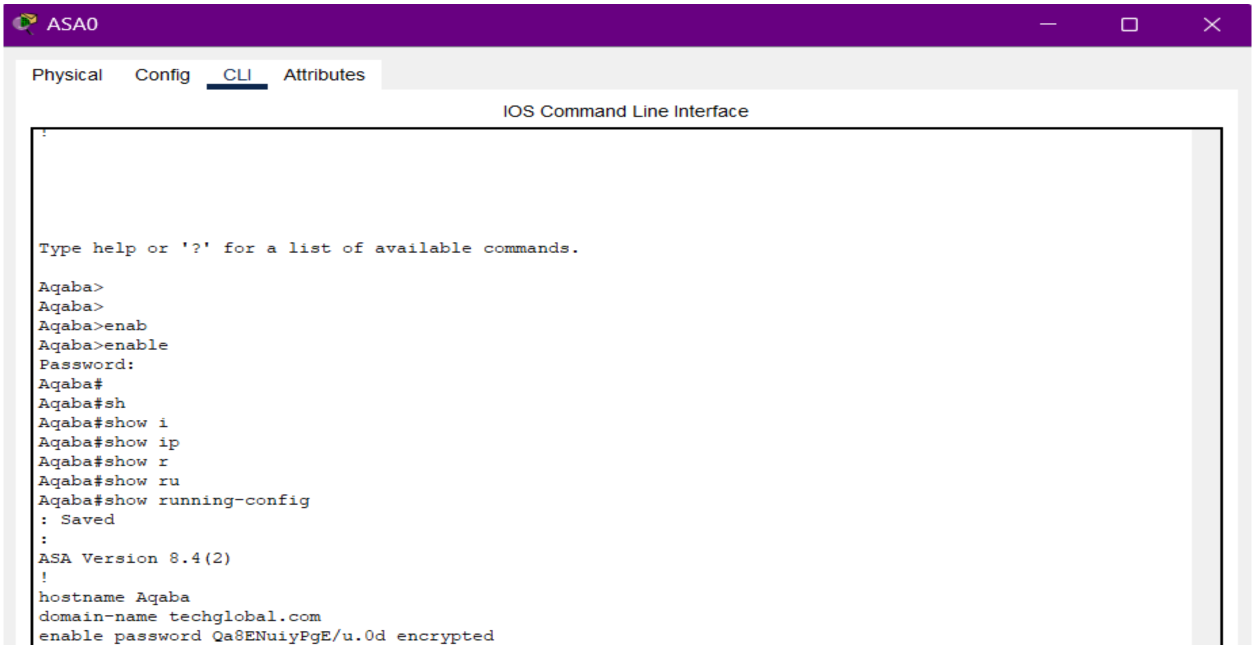
```
Amman>
Amman>en
Amman>enable
Password:
Password:
Amman#
Amman#
Amman#sh
Amman#show r
Amman#show running-config
Building configuration...

Current configuration : 3775 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Amman
!
login block-for 180 attempts 4 within 120
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Hamza secret 5 $1$mERr$.Gyel8JwLtOAkqWBXxDMbl
!
!
license udi pid CISCO1941/K9 sn FTX1524CCBM-
license boot module c1900 technology-package securityk9
!
```

Amman switch



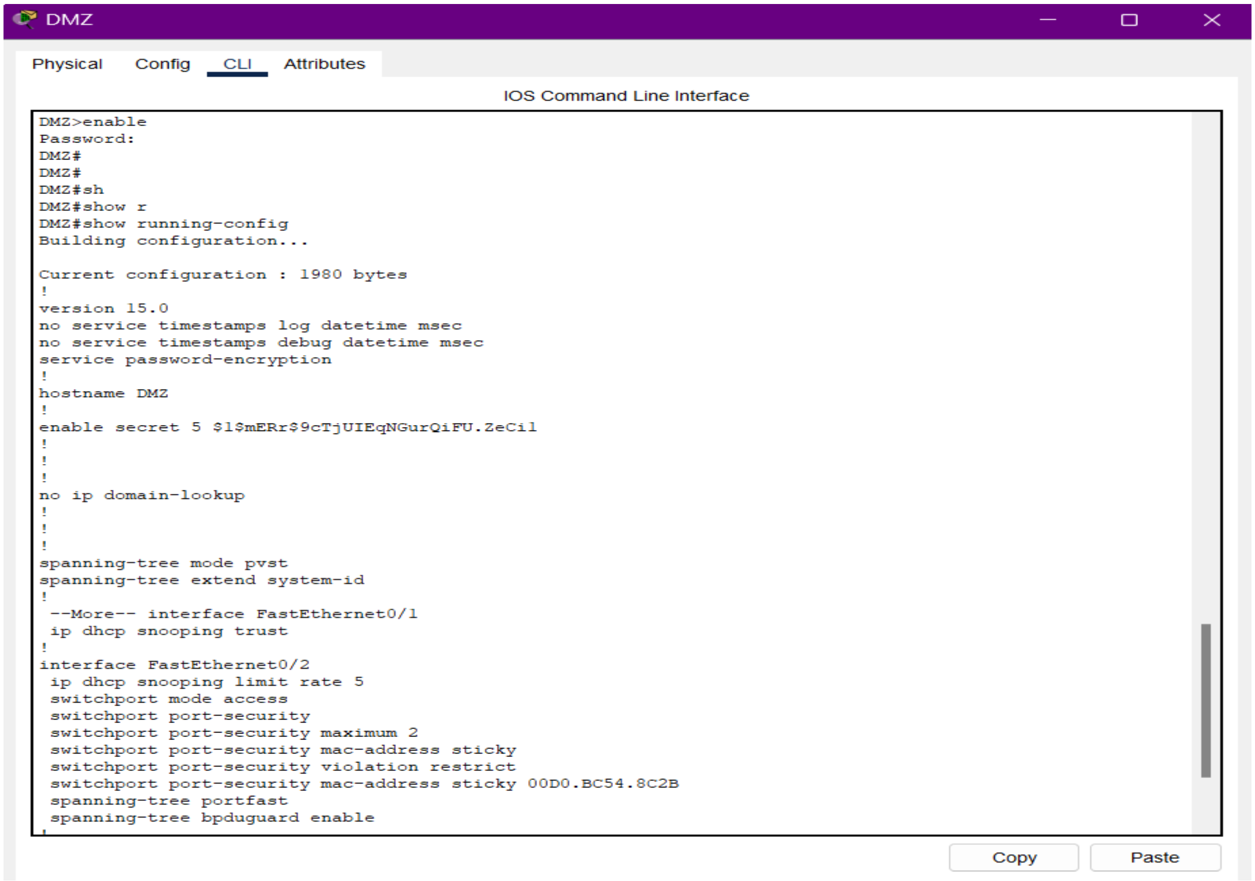
```
HQ>en
HQ>enable
Password:
HQ#
HQ#sh
HQ#show r
HQ#show running-config
Building configuration...

Current configuration : 5569 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname HQ
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
username Ahmad secret 5 $1$mERr$BVbVAzl7nEao6xZ9sIdCx0
username Hamza secret 5 $1$mERr$.Gyel8JwLtOAkqWBXxDMbl
username Test secret 5 $1$mERr$1Bs2pM8S6q6/mzZwrjiMFl
username admin secret 5 $1$mERr$4CFVt/60iQmc.ia/CrCAa/
!
!
ip dhcp snooping vlan 15,25,35,45
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 15,25,35,45,100
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
```

Aqaba

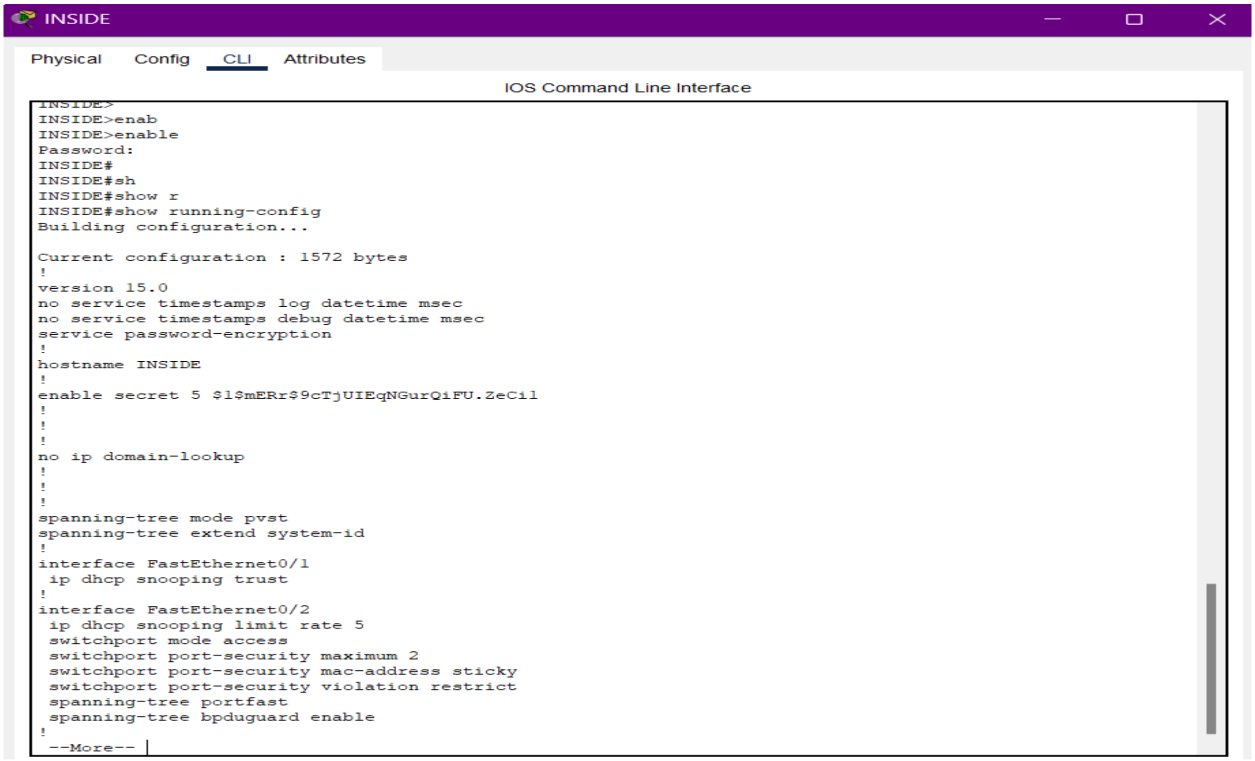


```
!



Type help or '?' for a list of available commands.

Aqaba>
Aqaba>
Aqaba>enab
Aqaba>enable
Password:
Aqaba#
Aqaba#sh
Aqaba#show i
Aqaba#show ip
Aqaba#show r
Aqaba#show ru
Aqaba#show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname Aqaba
domain-name techglobal.com
enable password Qa8ENuiyPgE/u.0d encrypted
```

Switches in Aqaba:

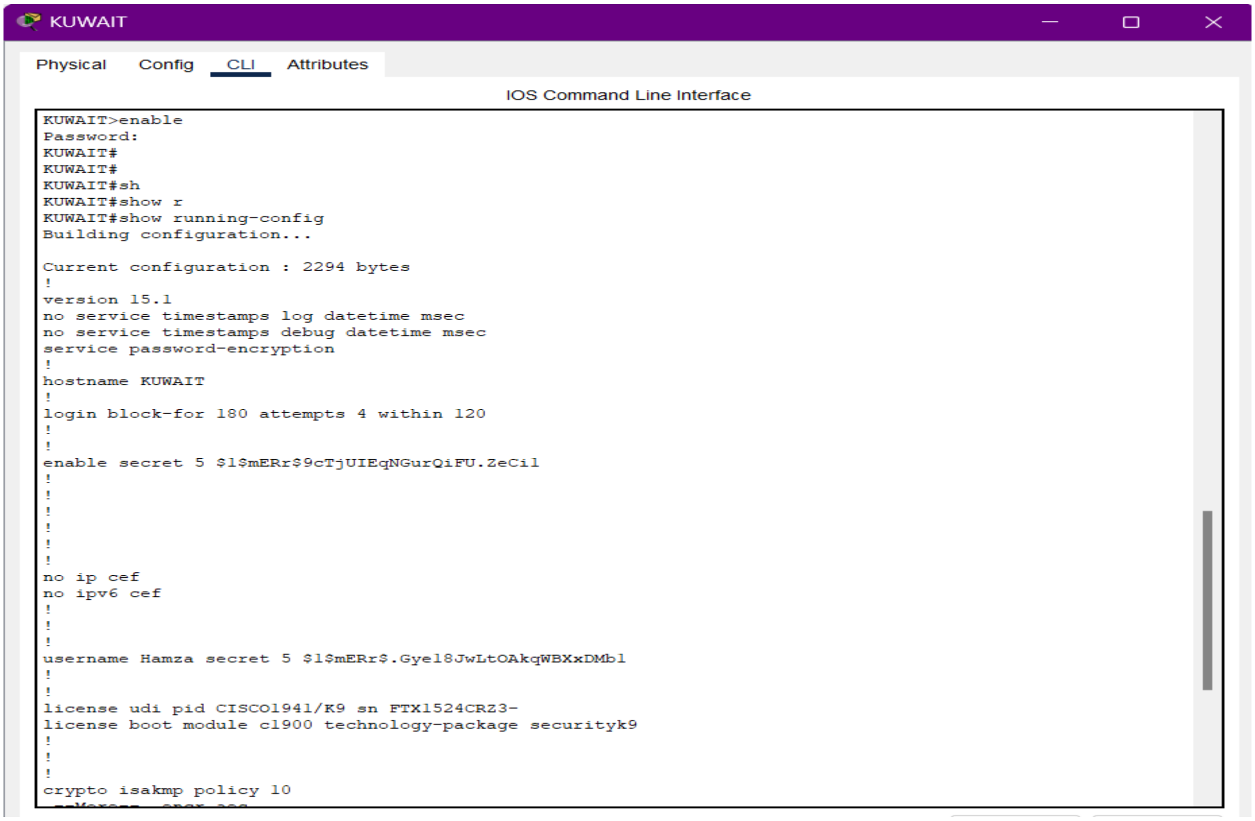


```
DMZ>enable
Password:
DMZ#
DMZ#
DMZ#sh
DMZ#show r
DMZ#show running-config
Building configuration...

Current configuration : 1980 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname DMZ
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
 --More-- interface FastEthernet0/1
 ip dhcp snooping trust
!
interface FastEthernet0/2
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00D0.BC54.8C2B
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```



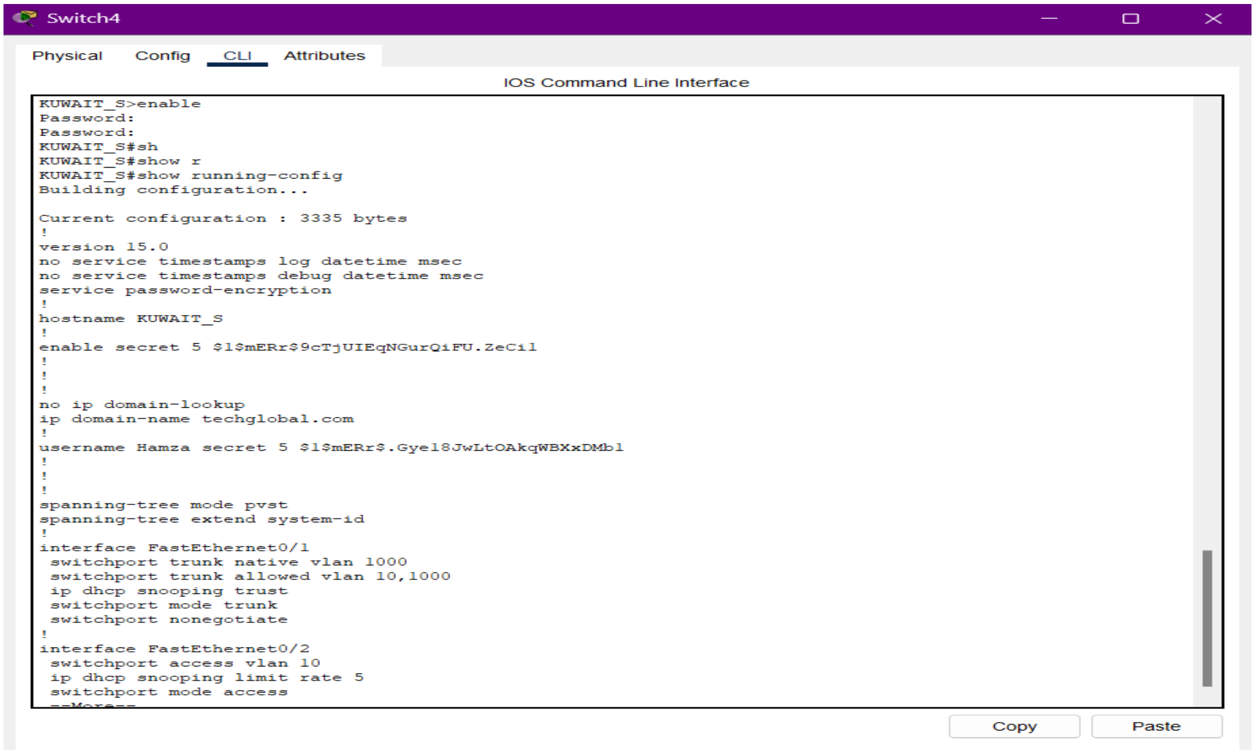
```
INSIDE>
INSIDE>enab
INSIDE>enable
Password:
INSIDE#
INSIDE#sh
INSIDE#show r
INSIDE#show running-config
Building configuration...

Current configuration : 1572 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname INSIDE
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 ip dhcp snooping trust
!
interface FastEthernet0/2
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
!
 --More--
```

KUWAIT router



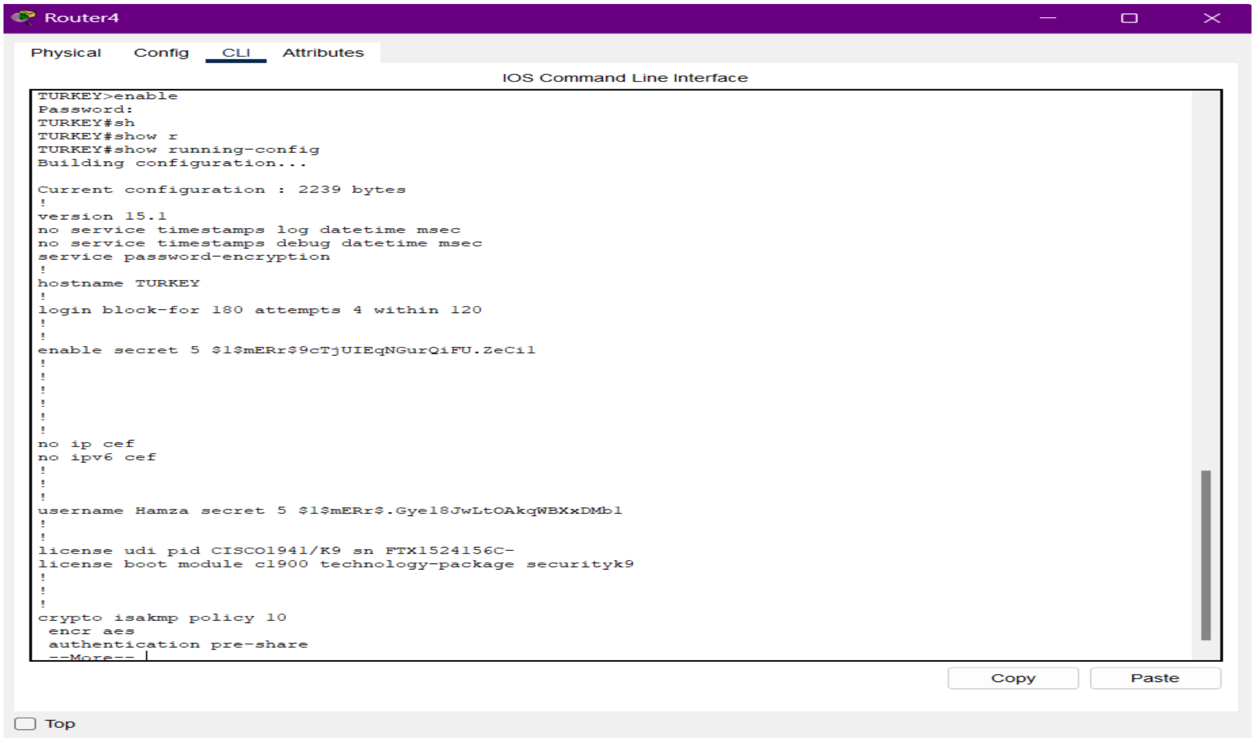
```
KUWAIT>enable
Password:
KUWAIT#
KUWAIT#
KUWAIT#sh
KUWAIT#show r
KUWAIT#show running-config
Building configuration...

Current configuration : 2294 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname KUWAIT
!
login block-for 180 attempts 4 within 120
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Hamza secret 5 $1$mERr$.Gyel8JwLtOAkqWBXxDMbl
!
!
license udi pid CISCO1941/K9 sn FTX1524CRZ3-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 --More--
```

Switch



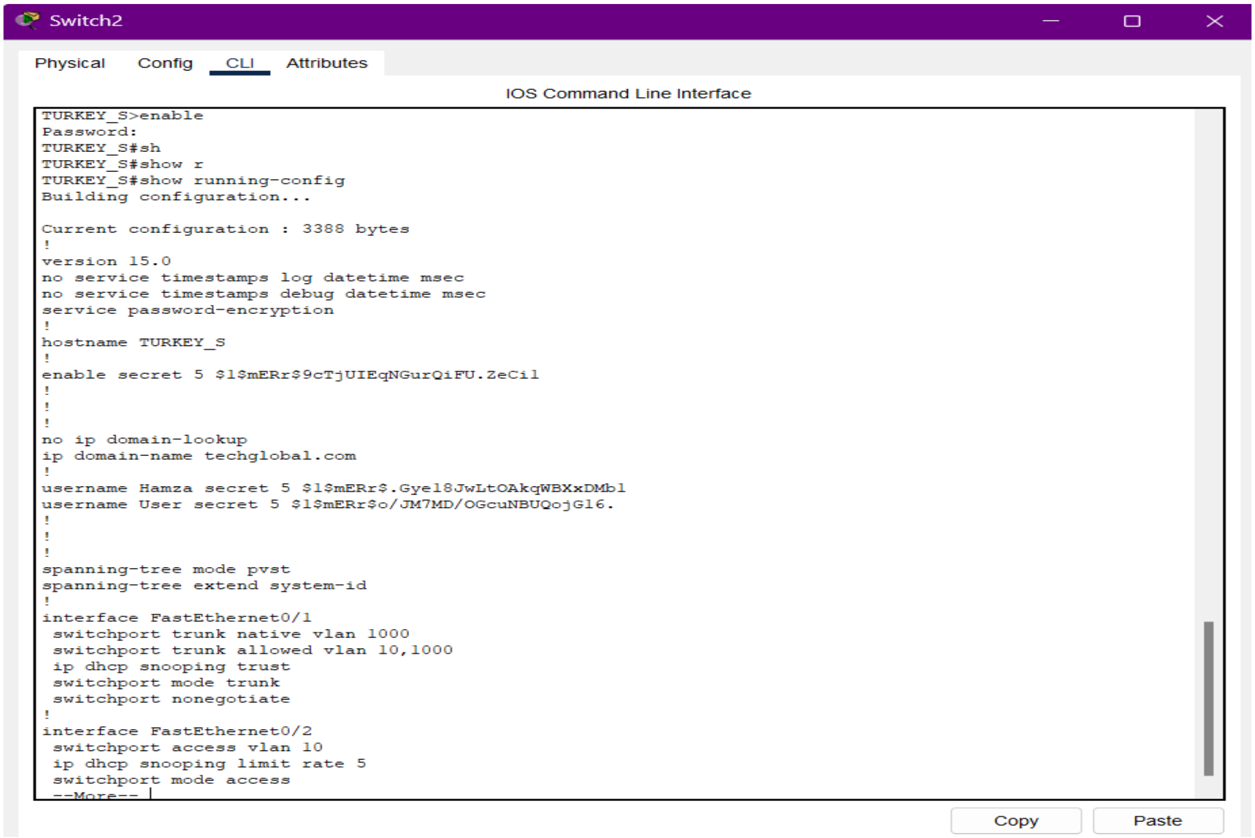
```
KUWAIT_S>enable
Password:
Password:
KUWAIT_S#sh
KUWAIT_S#show r
KUWAIT_S#show running-config
Building configuration...

Current configuration : 3335 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname KUWAIT_S
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
username Hamza secret 5 $1$mERr$.Gyel8JwLtOAkqWBXxDMbl
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 10,1000
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
 --More--
```

Turkey router



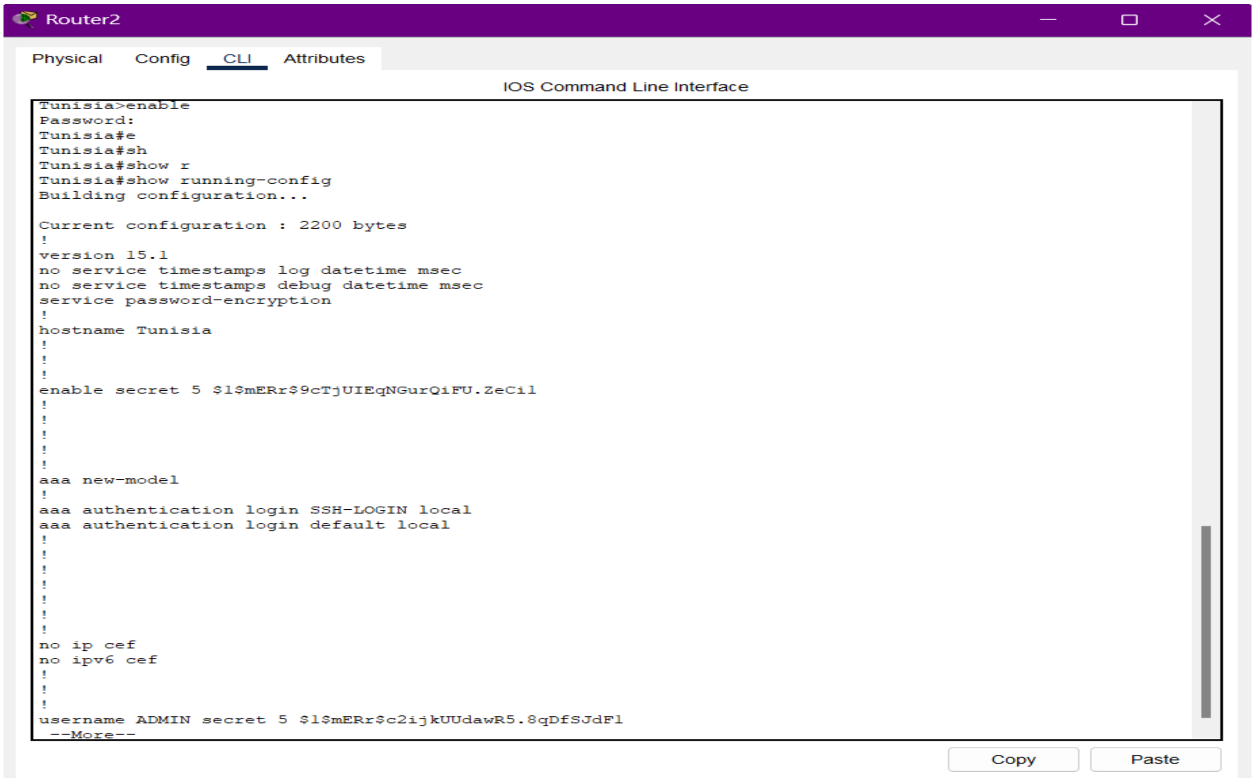
```
TURKEY>enable
Password:
TURKEY#sh
TURKEY#show r
TURKEY#show running-config
Building configuration...

Current configuration : 2239 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname TURKEY
!
login block-for 180 attempts 4 within 120
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Hamza secret 5 $1$mERr$.Gyel8JwLtOAkqWBXxDMbl
!
!
license udi pid CISCO1941/K9 sn FTX1524156C-
license boot module c1900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 --More--
```

Switch



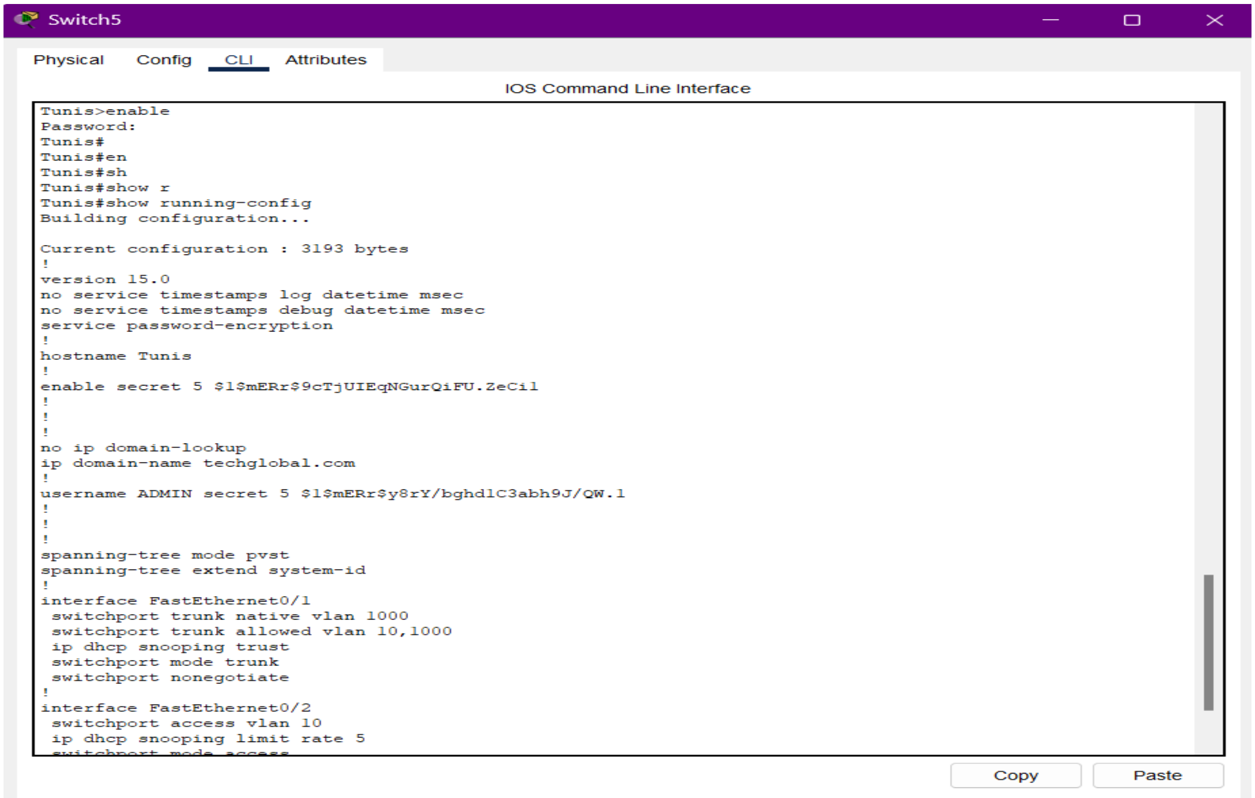
```
TURKEY_S>enable
Password:
TURKEY_S#sh
TURKEY_S#show r
TURKEY_S#show running-config
Building configuration...

Current configuration : 3388 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname TURKEY_S
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
username Hamza secret 5 $1$mERr$.Gyel8JwLtOAkqWBXxDMbl
username User secret 5 $1$mERr$o/JM7MD/OGcuNBUQojG16.
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 10,1000
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
 --More--
```

Tunisia router



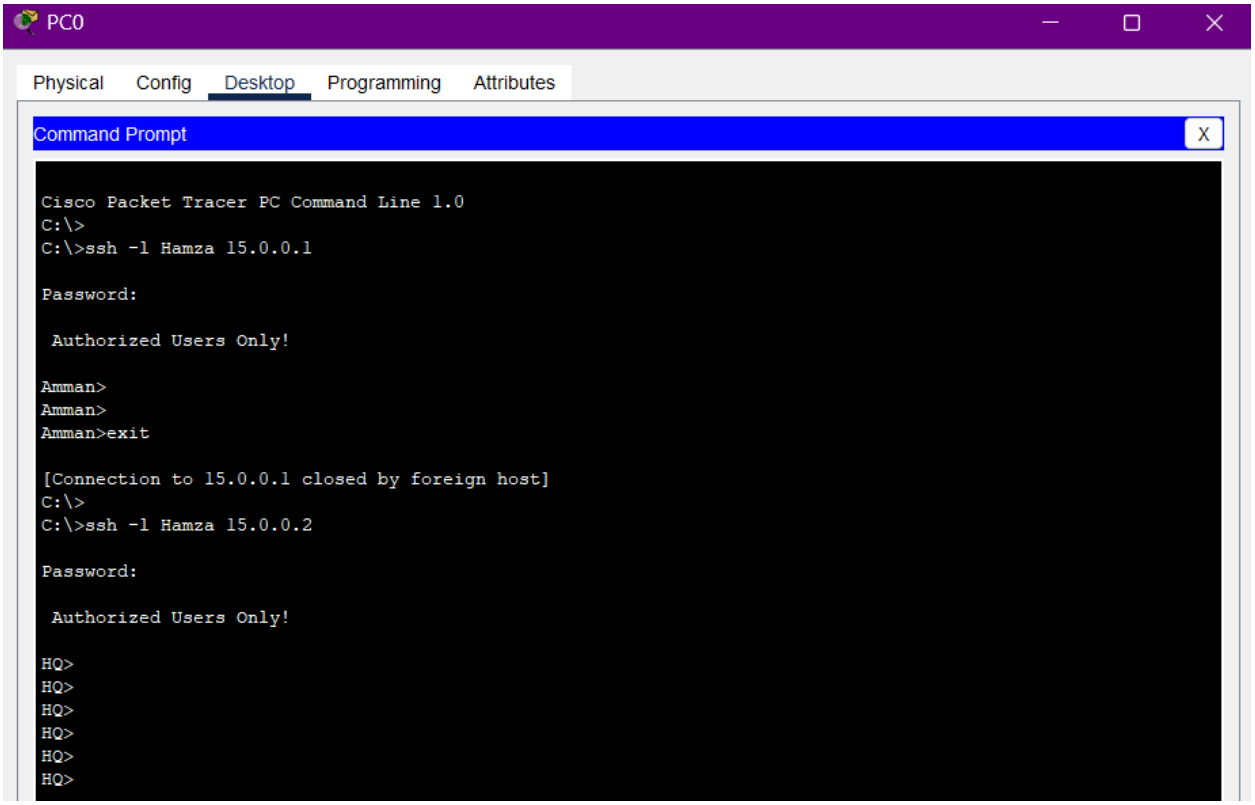
```
Tunisia>enable
Password:
Tunisia#e
Tunisia#sh
Tunisia#show r
Tunisia#show running-config
Building configuration...

Current configuration : 2200 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Tunisia
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
!
!
aaa new-model
!
aaa authentication login SSH-LOGIN local
aaa authentication login default local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username ADMIN secret 5 $1$mERr$c2ijkUUdawR5.8qDfSJdFl
 --More--
```

Switches



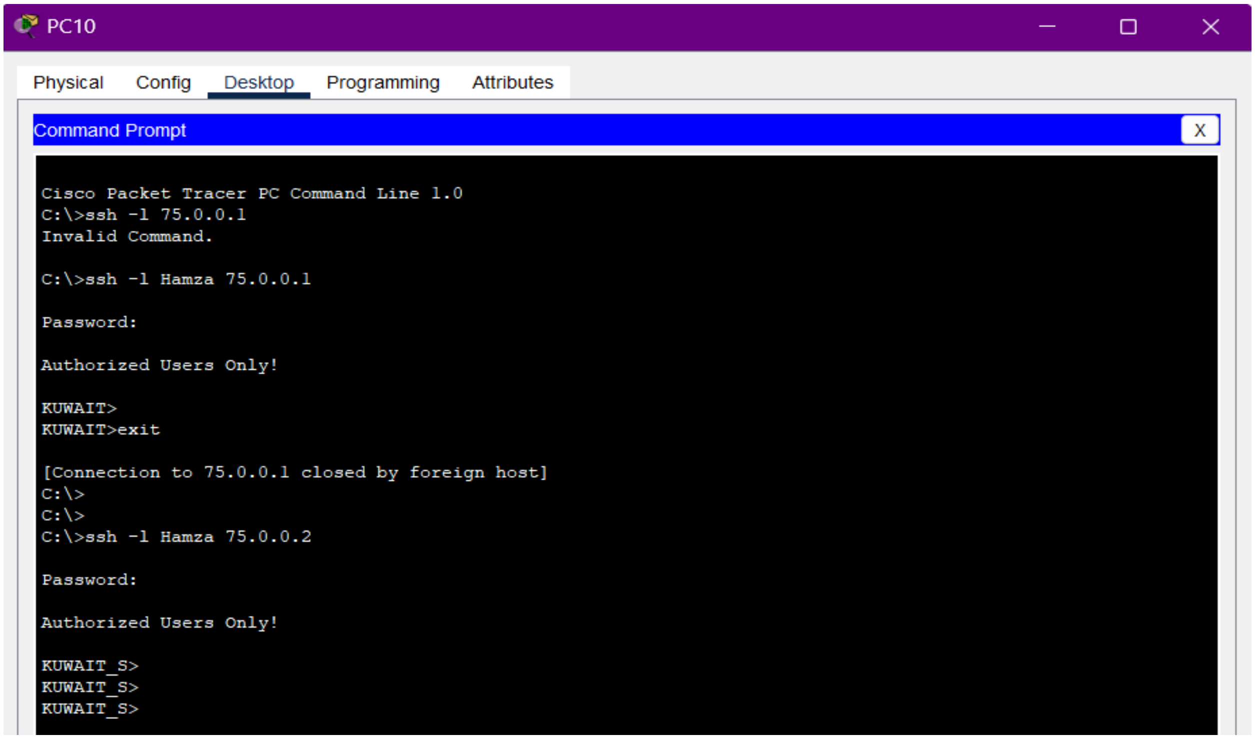
```
Tunis>enable
Password:
Tunis#
Tunis#en
Tunis#sh
Tunis#show r
Tunis#show running-config
Building configuration...

Current configuration : 3193 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Tunis
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
!
no ip domain-lookup
ip domain-name techglobal.com
!
username ADMIN secret 5 $1$mERr$y8rY/bghdlC3abh9J/QW.1
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 1000
 switchport trunk allowed vlan 10,1000
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
```

SSH Amman router and switch



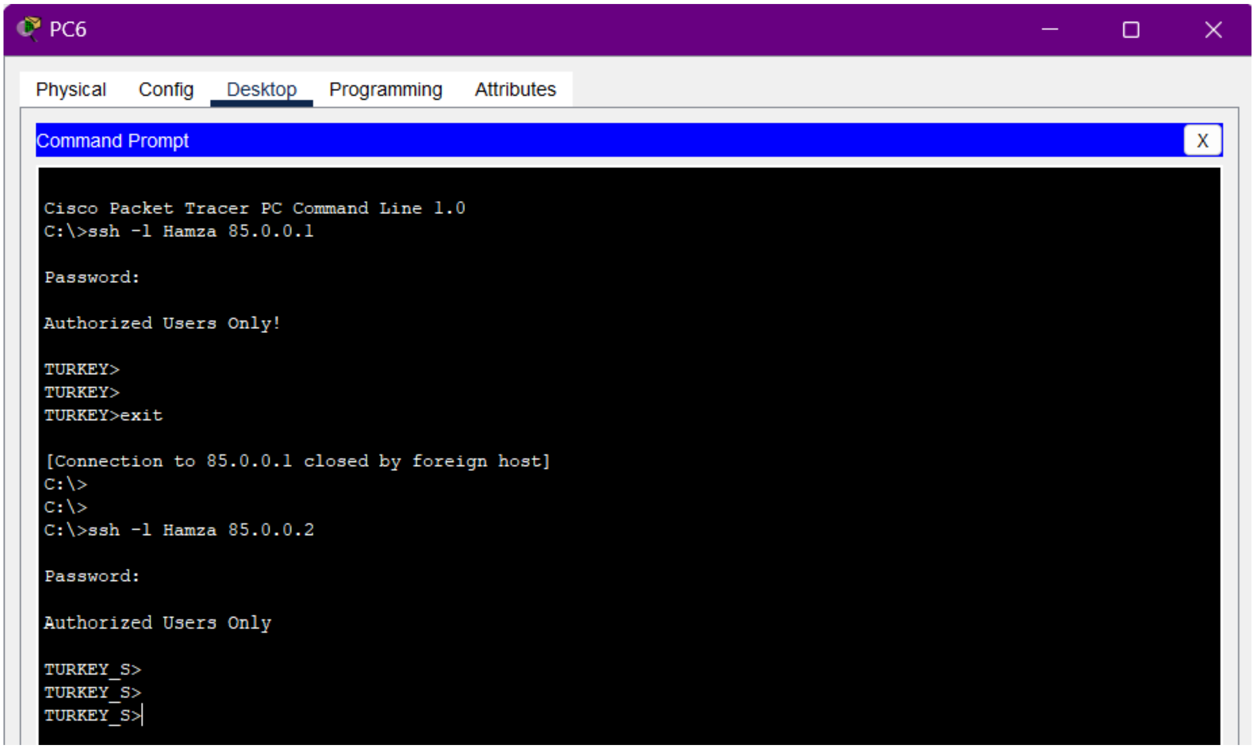
```
Cisco Packet Tracer PC Command Line 1.0
C:\>
C:\>ssh -l Hamza 15.0.0.1

Password:

 Authorized Users Only!

Amman>
Amman>
Amman>exit

[Connection to 15.0.0.1 closed by foreign host]
C:\>
C:\>ssh -l Hamza 15.0.0.2

Password:

 Authorized Users Only!

HQ>
HQ>
HQ>
HQ>
HQ>
HQ>
```

SSH Kuwait router and switch



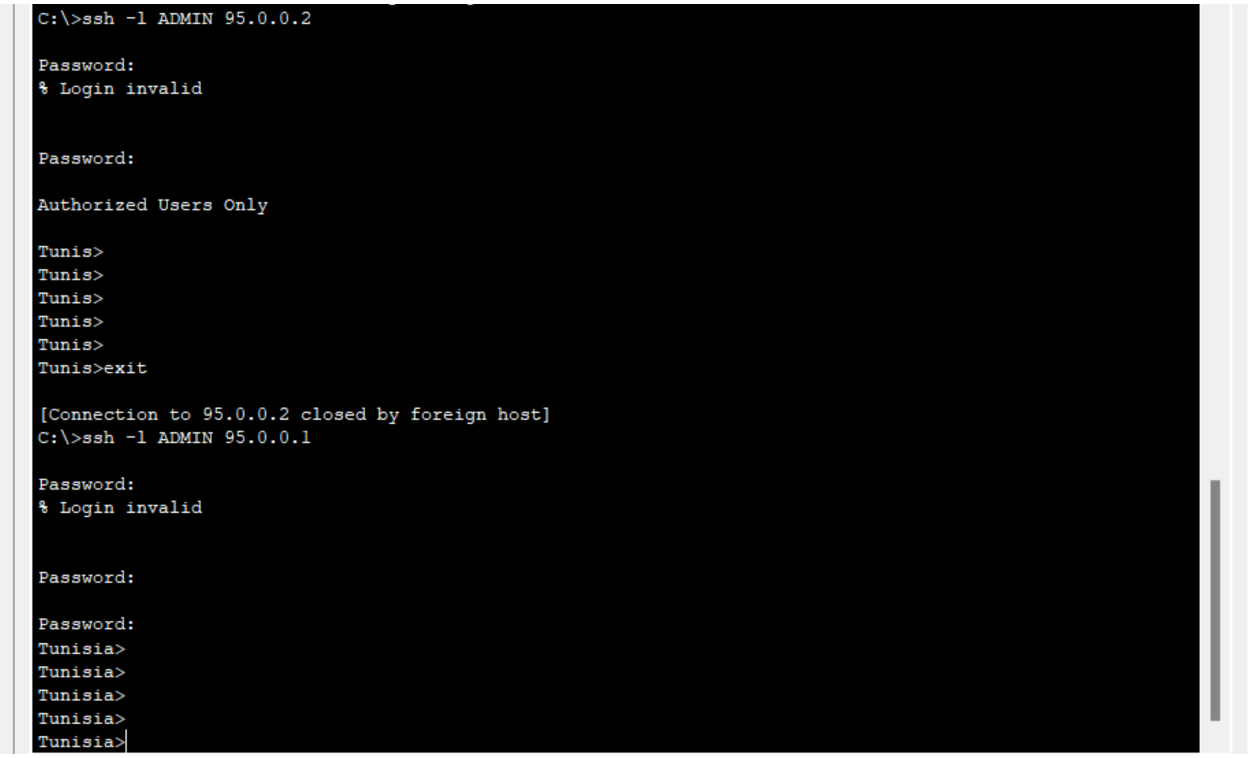
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l 75.0.0.1
Invalid Command.

C:\>ssh -l Hamza 75.0.0.1

Password:

Authorized Users Only!

KUWAIT>
KUWAIT>exit

[Connection to 75.0.0.1 closed by foreign host]
C:\>
C:\>
C:\>ssh -l Hamza 75.0.0.2

Password:

Authorized Users Only!

KUWAIT_S>
KUWAIT_S>
KUWAIT_S>
```

SSH Turkey router and switch



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Hamza 85.0.0.1

Password:

Authorized Users Only!

TURKEY>
TURKEY>
TURKEY>exit

[Connection to 85.0.0.1 closed by foreign host]
C:\>
C:\>
C:\>ssh -l Hamza 85.0.0.2

Password:

Authorized Users Only

TURKEY_S>
TURKEY_S>
TURKEY_S>
```

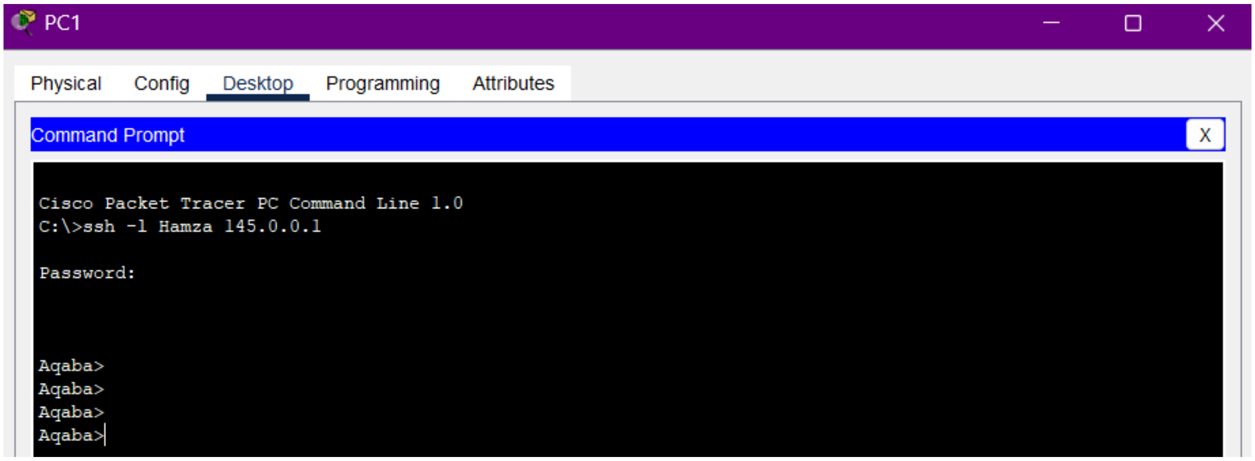
SSH Tunisia router and switch



```
C:\>ssh -l ADMIN 95.0.0.2

Password:
% Login invalid


Password:

Authorized Users Only

Tunis>
Tunis>
Tunis>
Tunis>
Tunis>
Tunis>exit

[Connection to 95.0.0.2 closed by foreign host]
C:\>ssh -l ADMIN 95.0.0.1

Password:
% Login invalid


Password:

Password:
Tunisia>
Tunisia>
Tunisia>
Tunisia>
Tunisia>
```

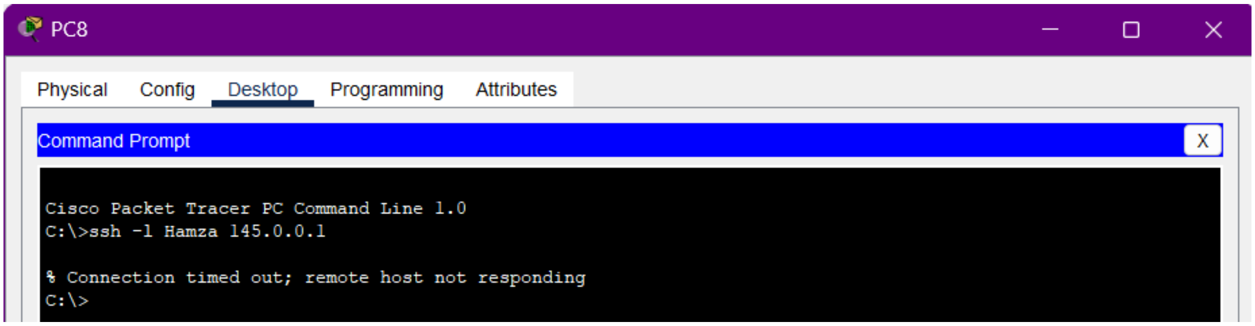
SSH Aqaba (15.0.0.10 is only accessed to ASA)

PC with 15.0.0.10 IP address:



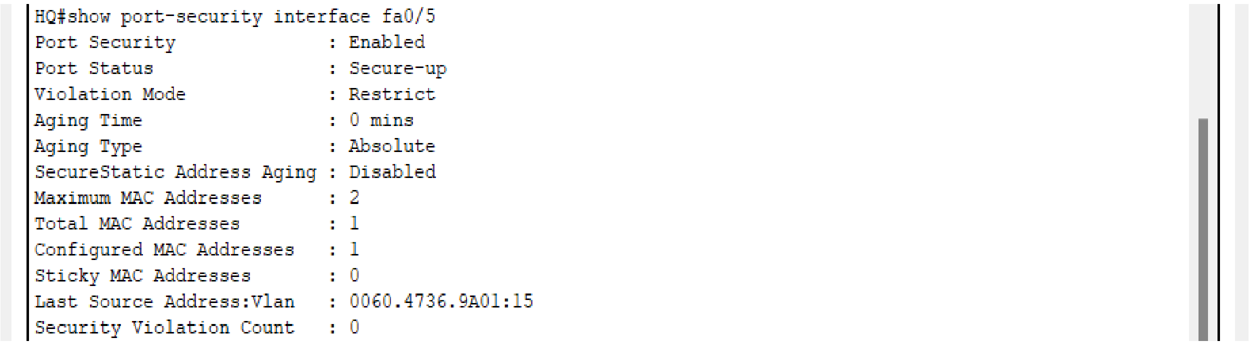
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Hamza 145.0.0.1

Password:



Aqaba>
Aqaba>
Aqaba>
Aqaba>
```

Trying to access firewall remotely from a PC with 55.0.0.10 IP address:



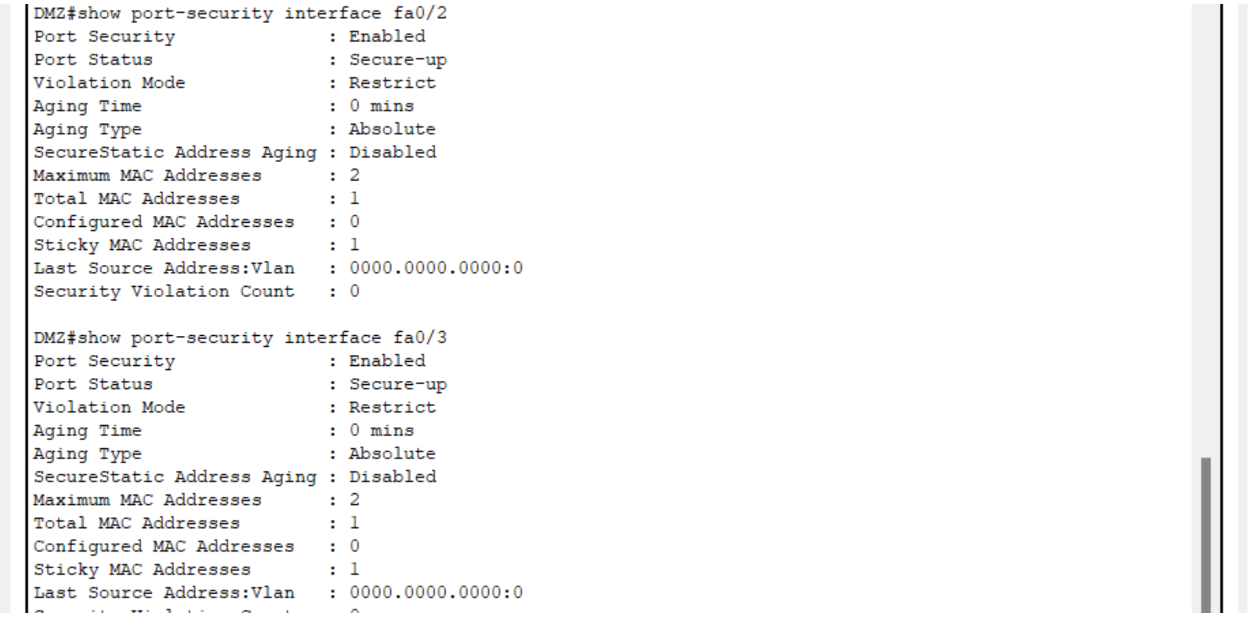
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Hamza 145.0.0.1

% Connection timed out; remote host not responding
C:\>
```

Amman security ports



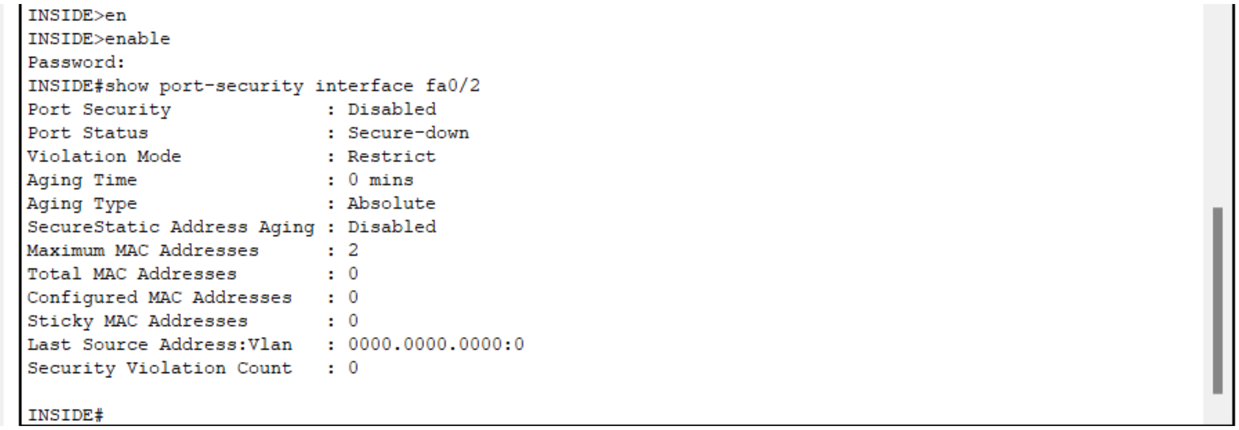
```
HQ#show port-security interface fa0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0060.4736.9A01:15
Security Violation Count   : 0
```

Aqaba DMZ security ports



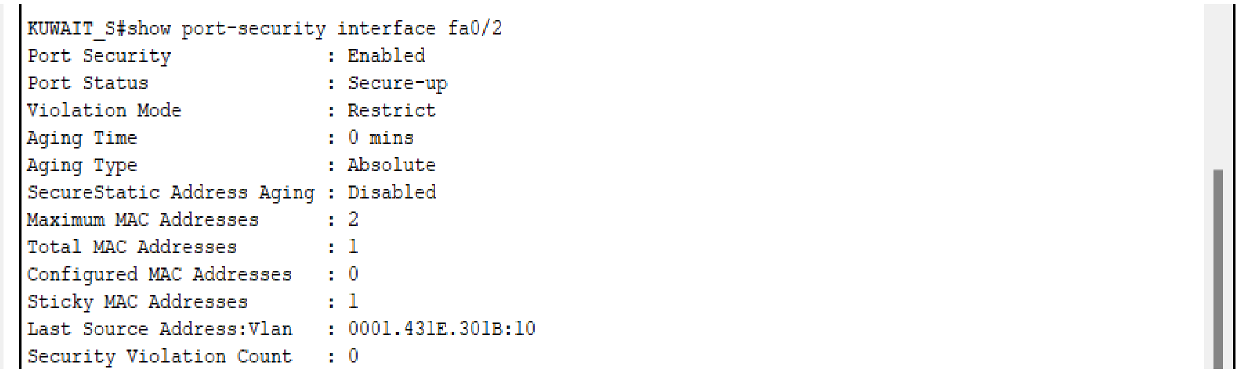
```
DMZ#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

DMZ#show port-security interface fa0/3
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0000.0000.0000:0
```

Aqaba INSIDE security ports



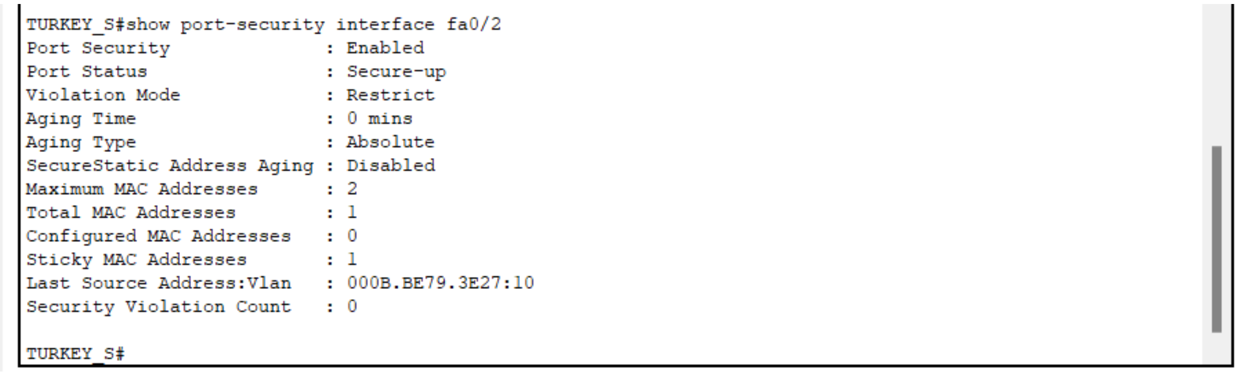
```
INSIDE>en
INSIDE>enable
Password:
INSIDE#show port-security interface fa0/2
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

INSIDE#
```

Kuwait security ports



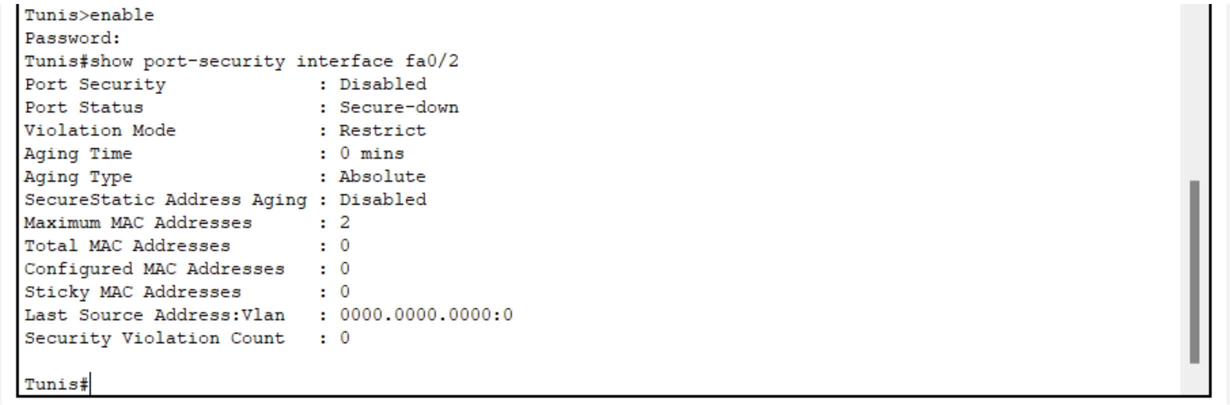
```
KUWAIT_S#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.431E.301B:10
Security Violation Count   : 0
```

Turkey security ports



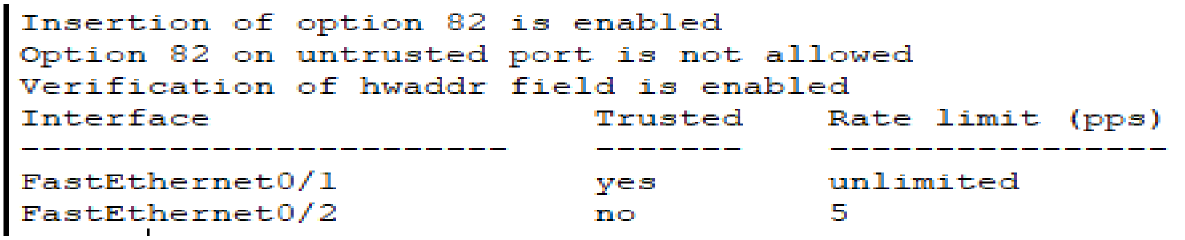
```
TURKEY_S#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 000B.BE79.3E27:10
Security Violation Count   : 0

TURKEY_S#
```

Tunisia security ports



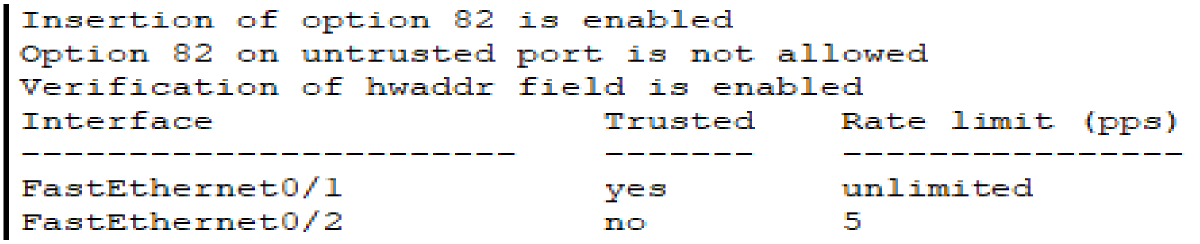
```
Tunis>enable
Password:
Tunis#show port-security interface fa0/2
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

Tunis#
```

Tunisia DHCP



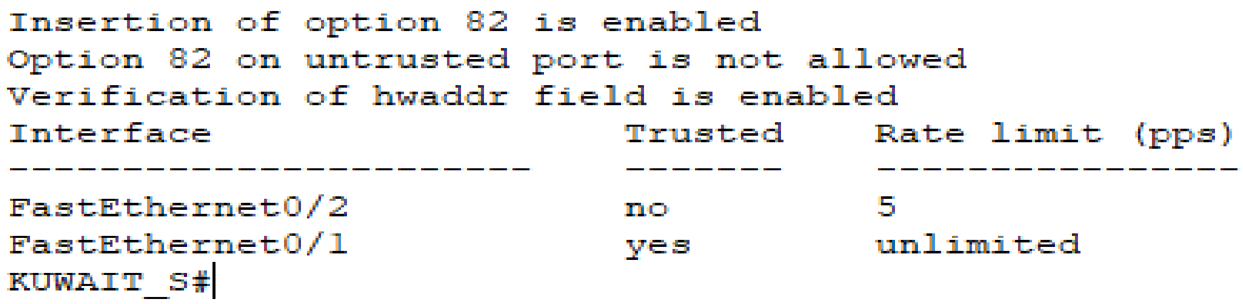
```
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/2            no         5
```

Turkey DHCP



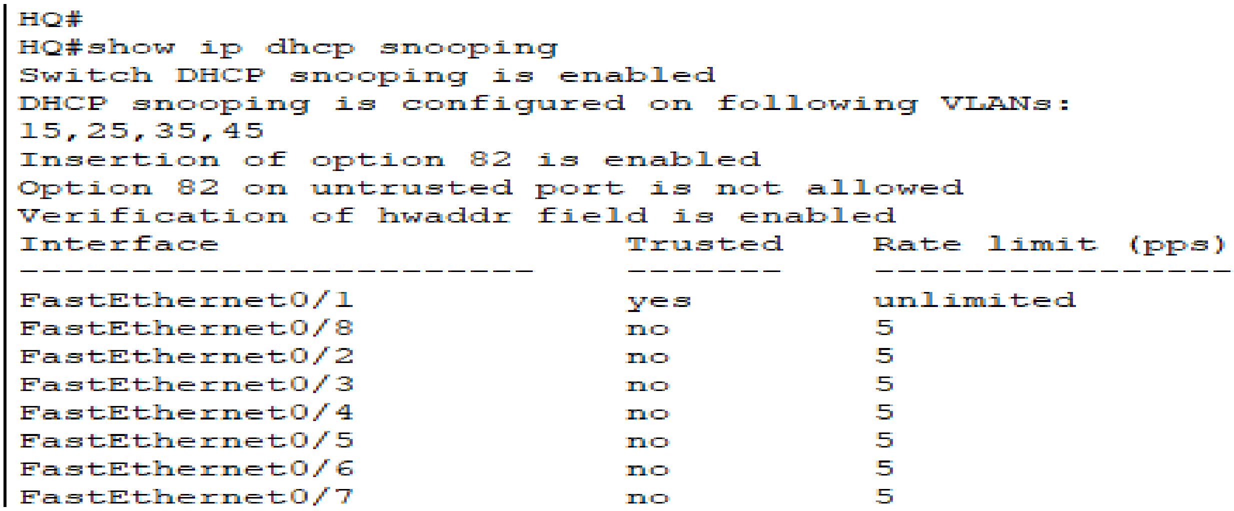
```
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/2            no         5
```

Kuwait DHCP



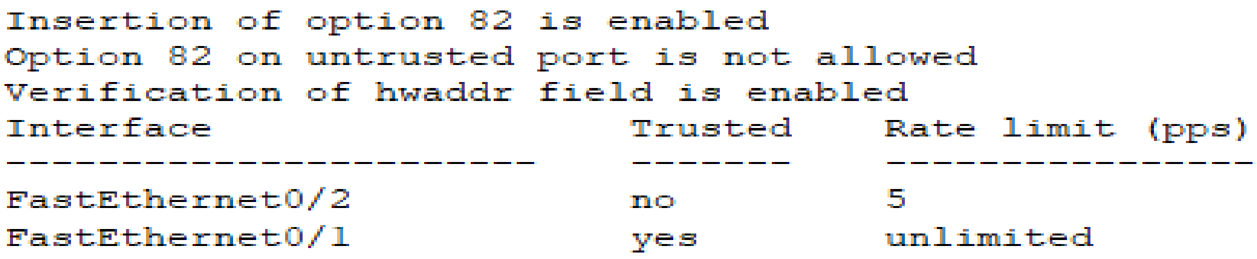
```
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                   Trusted    Rate limit (pps)
-----------------------     -------    ----------------
FastEthernet0/2             no         5
FastEthernet0/1             yes        unlimited
KUWAIT_S#
```

Amman DHCP



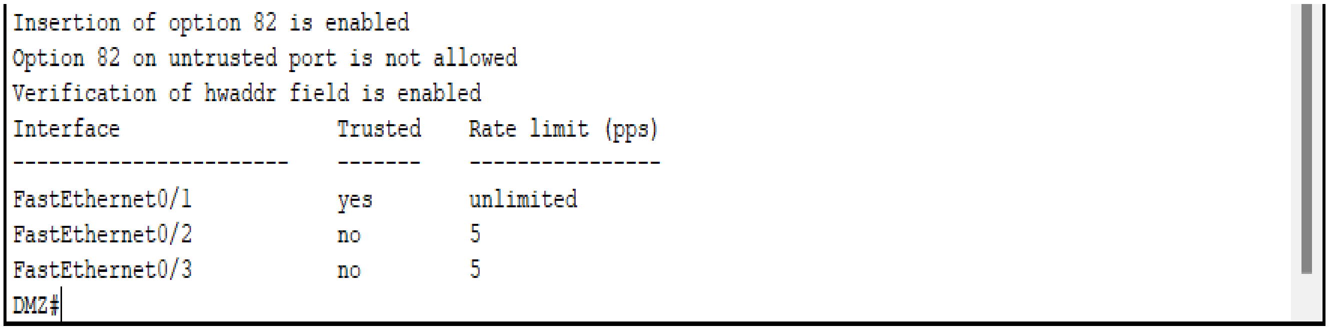
```
HQ#
HQ#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
15,25,35,45
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                   Trusted    Rate limit (pps)
-----------------------     -------    ----------------
FastEthernet0/1             yes        unlimited
FastEthernet0/8             no         5
FastEthernet0/2             no         5
FastEthernet0/3             no         5
FastEthernet0/4             no         5
FastEthernet0/5             no         5
FastEthernet0/6             no         5
FastEthernet0/7             no         5
```

Aqaba Inside DHCP



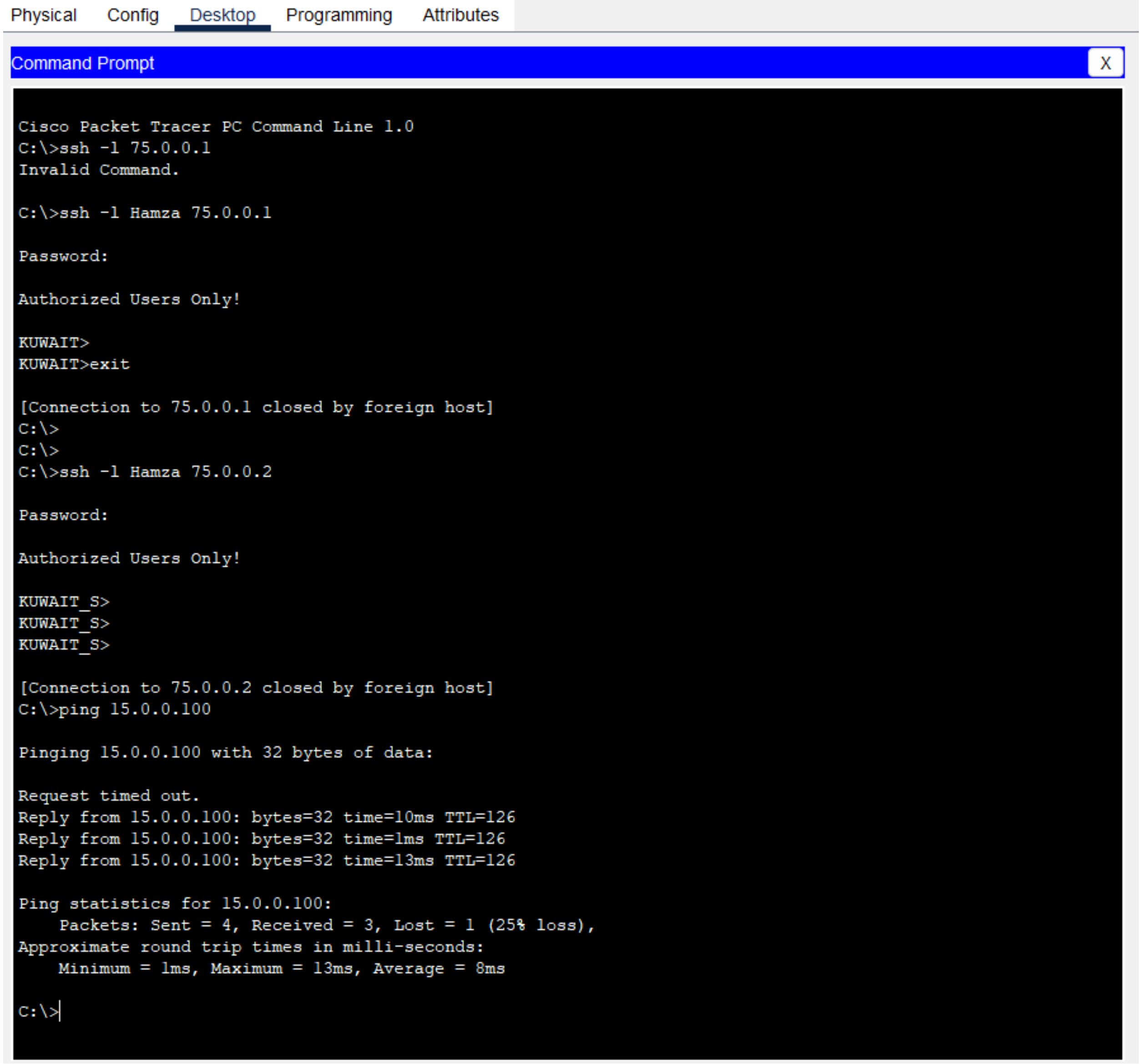
```
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                   Trusted    Rate limit (pps)
-----------------------     -------    ----------------
FastEthernet0/2             no         5
FastEthernet0/1             yes        unlimited
```

Aqaba DMZ DHCP



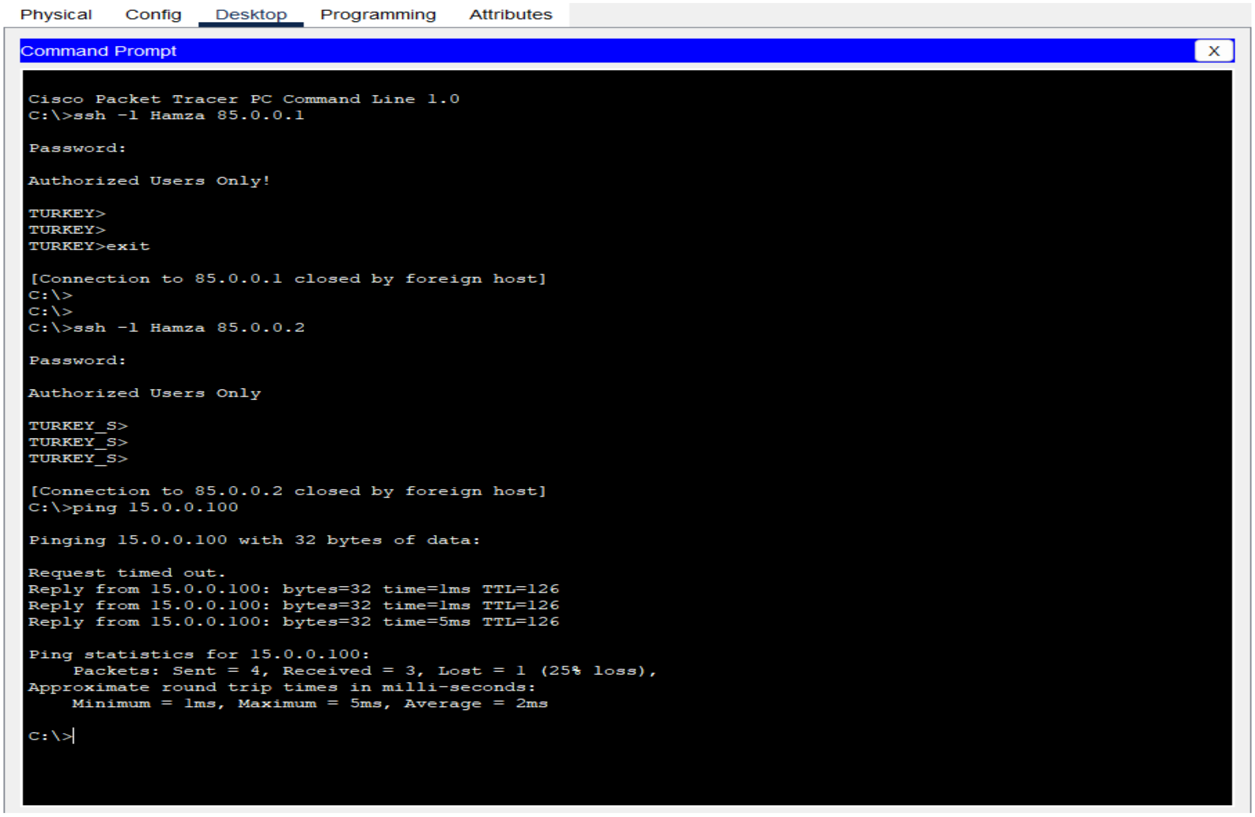
```
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                   Trusted    Rate limit (pps)
-----------------------     -------    ----------------
FastEthernet0/1             yes        unlimited
FastEthernet0/2             no         5
FastEthernet0/3             no         5
DMZ#
```

VPN between KUWAIT and DC



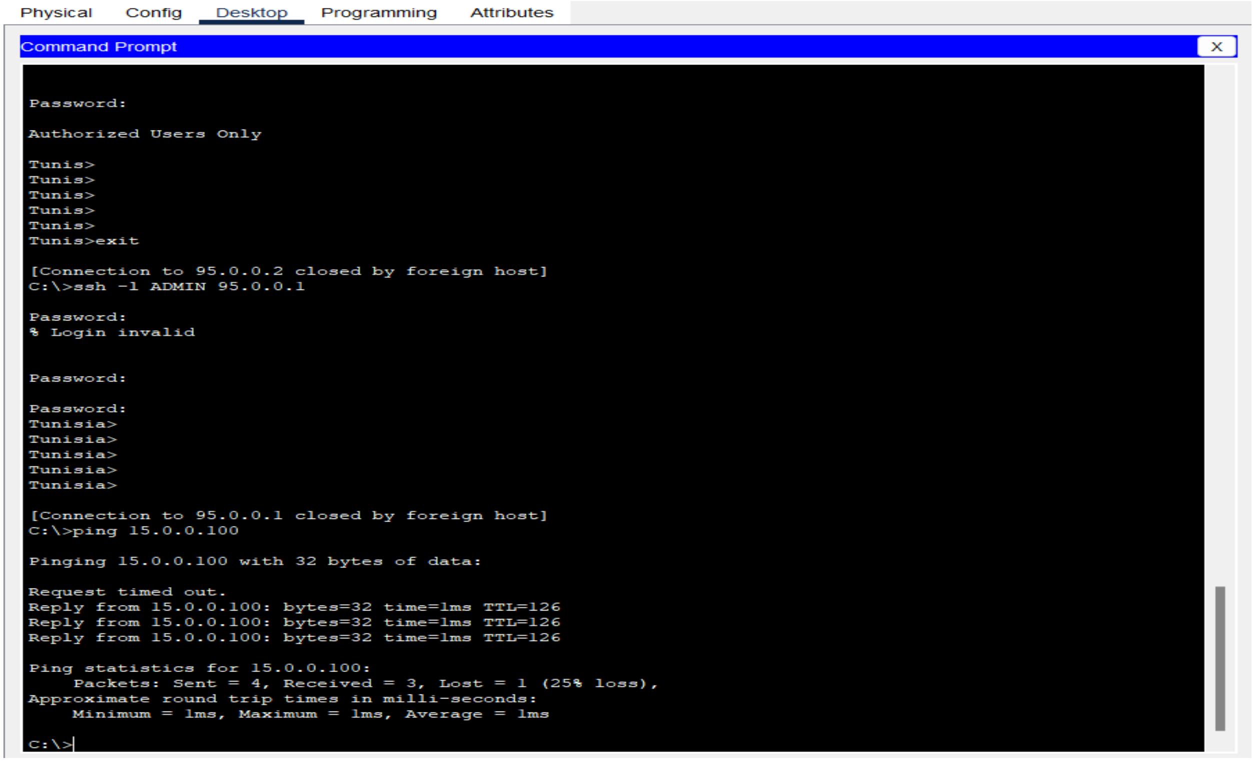
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l 75.0.0.1
Invalid Command.

C:\>ssh -l Hamza 75.0.0.1

Password:

Authorized Users Only!

KUWAIT>
KUWAIT>exit

[Connection to 75.0.0.1 closed by foreign host]
C:\>
C:\>
C:\>ssh -l Hamza 75.0.0.2

Password:

Authorized Users Only!

KUWAIT_S>
KUWAIT_S>
KUWAIT_S>

[Connection to 75.0.0.2 closed by foreign host]
C:\>ping 15.0.0.100

Pinging 15.0.0.100 with 32 bytes of data:

Request timed out.
Reply from 15.0.0.100: bytes=32 time=10ms TTL=126
Reply from 15.0.0.100: bytes=32 time=1ms TTL=126
Reply from 15.0.0.100: bytes=32 time=13ms TTL=126

Ping statistics for 15.0.0.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 8ms

C:\>
```

VPN connectivity between Turkey and DC



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Hamza 85.0.0.1

Password:

Authorized Users Only!

TURKEY>
TURKEY>
TURKEY>exit

[Connection to 85.0.0.1 closed by foreign host]
C:\>
C:\>
C:\>ssh -l Hamza 85.0.0.2

Password:

Authorized Users Only

TURKEY_S>
TURKEY_S>
TURKEY_S>

[Connection to 85.0.0.2 closed by foreign host]
C:\>ping 15.0.0.100

Pinging 15.0.0.100 with 32 bytes of data:

Request timed out.
Reply from 15.0.0.100: bytes=32 time=1ms TTL=126
Reply from 15.0.0.100: bytes=32 time=1ms TTL=126
Reply from 15.0.0.100: bytes=32 time=5ms TTL=126

Ping statistics for 15.0.0.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>
```

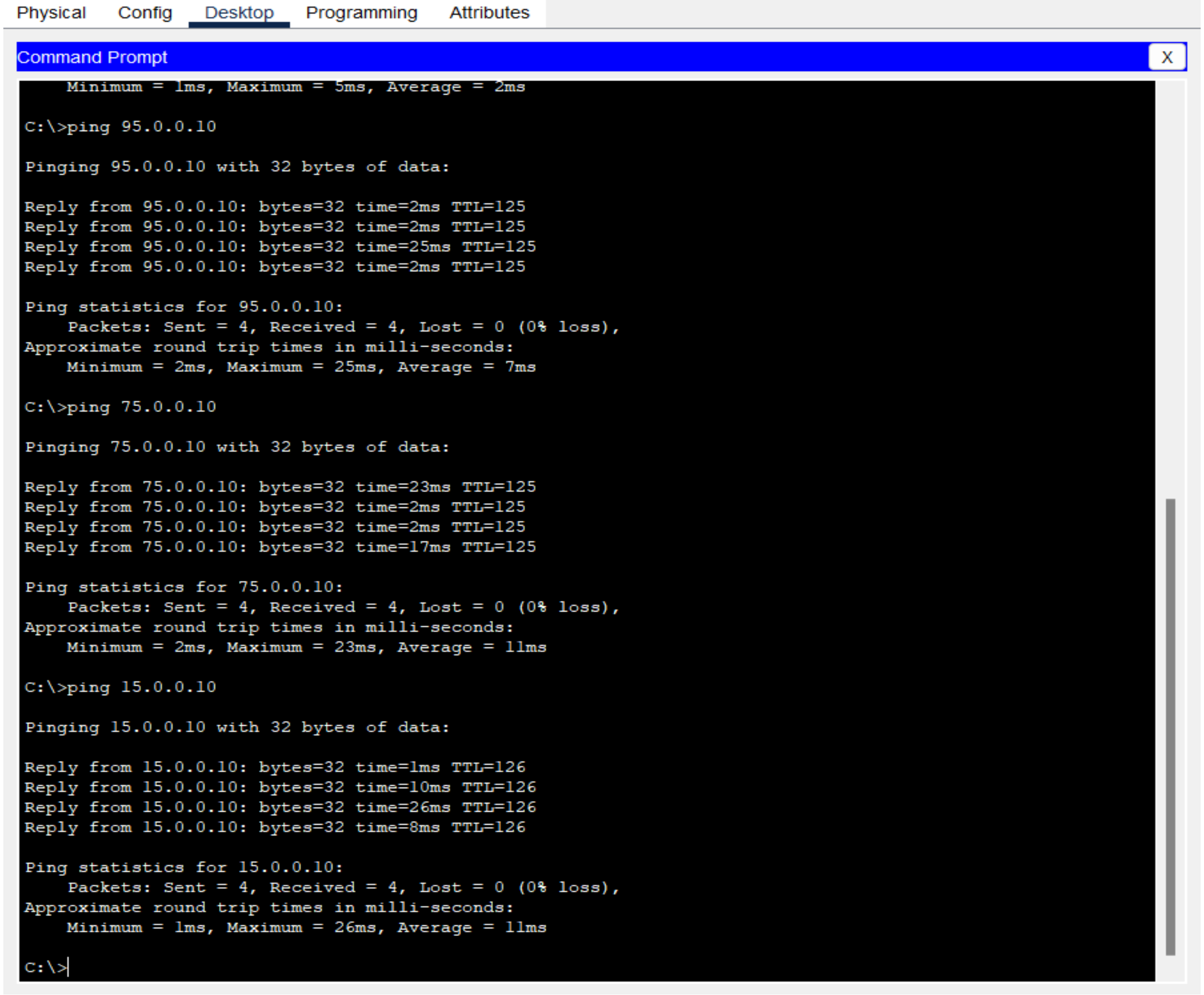
VPN connectivity between Tunisia and DC



```
Password:

Authorized Users Only

Tunis>
Tunis>
Tunis>
Tunis>
Tunis>
Tunis>exit

[Connection to 95.0.0.2 closed by foreign host]
C:\>ssh -l ADMIN 95.0.0.1

Password:
% Login invalid


Password:

Password:
Tunisia>
Tunisia>
Tunisia>
Tunisia>
Tunisia>

[Connection to 95.0.0.1 closed by foreign host]
C:\>ping 15.0.0.100

Pinging 15.0.0.100 with 32 bytes of data:

Request timed out.
Reply from 15.0.0.100: bytes=32 time=1ms TTL=126
Reply from 15.0.0.100: bytes=32 time=1ms TTL=126
Reply from 15.0.0.100: bytes=32 time=1ms TTL=126

Ping statistics for 15.0.0.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Connectivity between Turkey and Tunisia and Kuwait

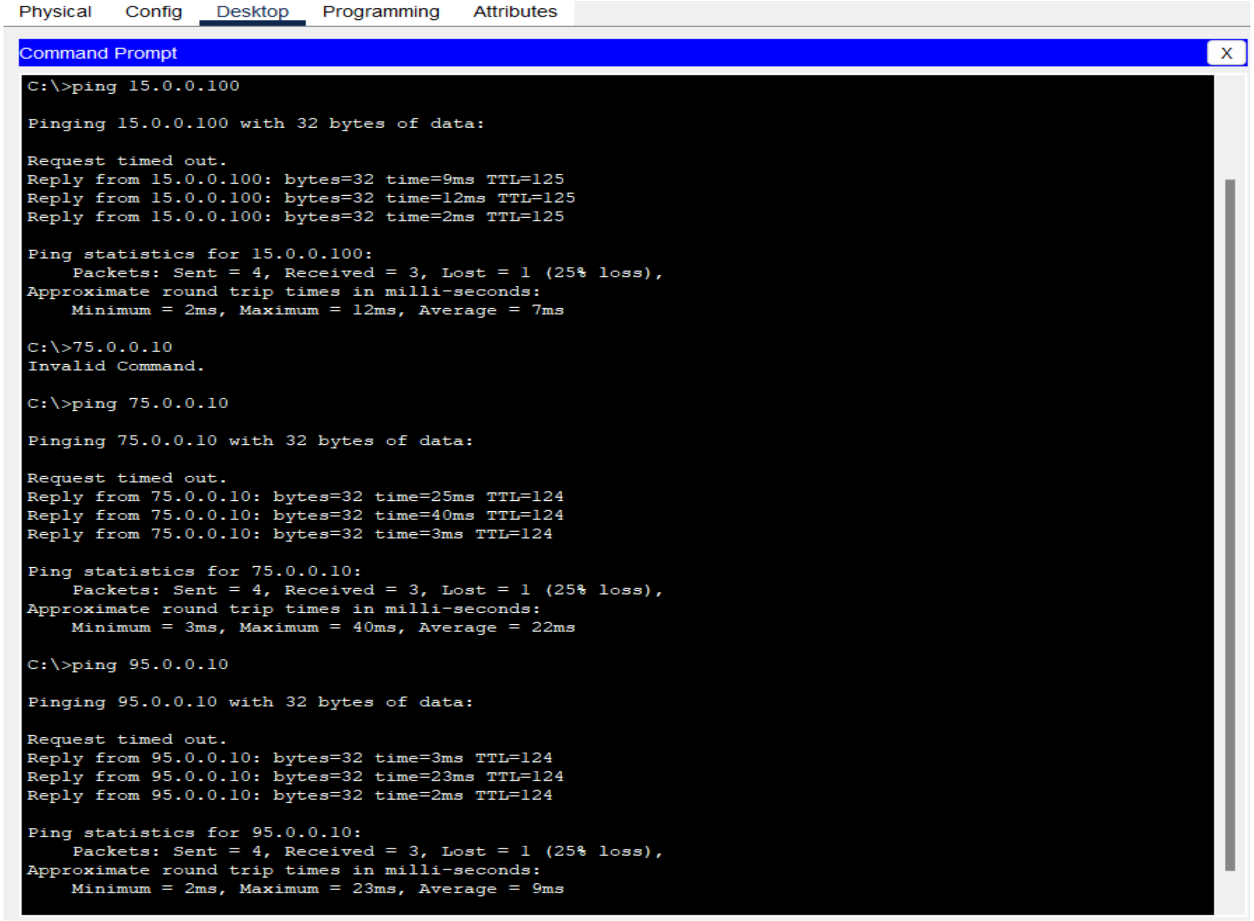
From PC in Turkey:



```
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>ping 95.0.0.10

Pinging 95.0.0.10 with 32 bytes of data:

Reply from 95.0.0.10: bytes=32 time=2ms TTL=125
Reply from 95.0.0.10: bytes=32 time=2ms TTL=125
Reply from 95.0.0.10: bytes=32 time=25ms TTL=125
Reply from 95.0.0.10: bytes=32 time=2ms TTL=125

Ping statistics for 95.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 25ms, Average = 7ms

C:\>ping 75.0.0.10

Pinging 75.0.0.10 with 32 bytes of data:

Reply from 75.0.0.10: bytes=32 time=23ms TTL=125
Reply from 75.0.0.10: bytes=32 time=2ms TTL=125
Reply from 75.0.0.10: bytes=32 time=2ms TTL=125
Reply from 75.0.0.10: bytes=32 time=17ms TTL=125

Ping statistics for 75.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 23ms, Average = 11ms

C:\>ping 15.0.0.10

Pinging 15.0.0.10 with 32 bytes of data:

Reply from 15.0.0.10: bytes=32 time=1ms TTL=126
Reply from 15.0.0.10: bytes=32 time=10ms TTL=126
Reply from 15.0.0.10: bytes=32 time=26ms TTL=126
Reply from 15.0.0.10: bytes=32 time=8ms TTL=126

Ping statistics for 15.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 26ms, Average = 11ms

C:\>
```

Connectivity between Aqaba, Amman (DC), Kuwait and Tunisia

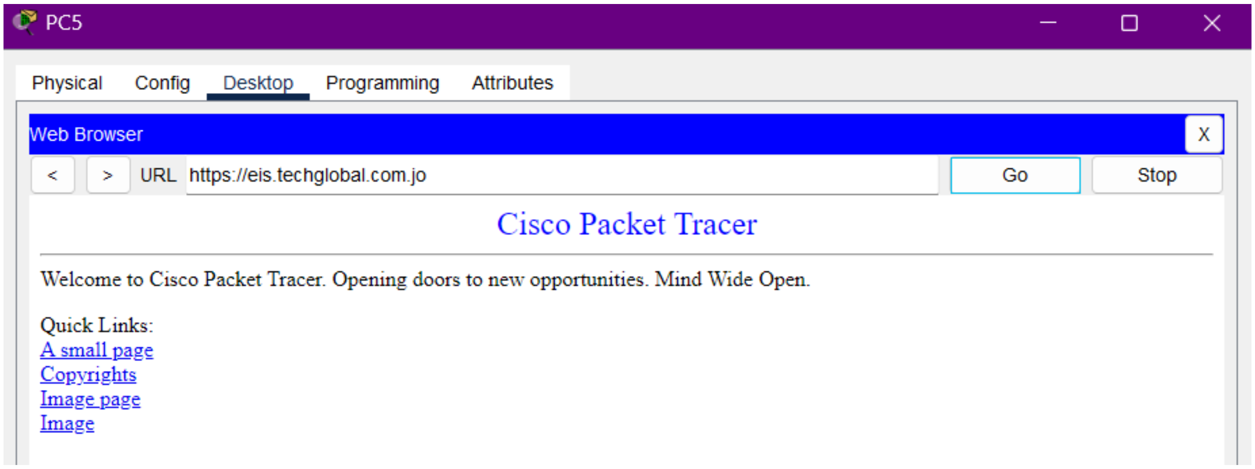
PC from INSIDE network in Aqaba:



```
C:\>ping 15.0.0.100

Pinging 15.0.0.100 with 32 bytes of data:

Request timed out.
Reply from 15.0.0.100: bytes=32 time=9ms TTL=125
Reply from 15.0.0.100: bytes=32 time=12ms TTL=125
Reply from 15.0.0.100: bytes=32 time=2ms TTL=125

Ping statistics for 15.0.0.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 12ms, Average = 7ms

C:\>75.0.0.10
Invalid Command.

C:\>ping 75.0.0.10

Pinging 75.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 75.0.0.10: bytes=32 time=25ms TTL=124
Reply from 75.0.0.10: bytes=32 time=40ms TTL=124
Reply from 75.0.0.10: bytes=32 time=3ms TTL=124

Ping statistics for 75.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 40ms, Average = 22ms

C:\>ping 95.0.0.10

Pinging 95.0.0.10 with 32 bytes of data:

Request timed out.
Reply from 95.0.0.10: bytes=32 time=3ms TTL=124
Reply from 95.0.0.10: bytes=32 time=23ms TTL=124
Reply from 95.0.0.10: bytes=32 time=2ms TTL=124

Ping statistics for 95.0.0.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 23ms, Average = 9ms
```

HTTPs and DNS accessibility

VLAN 45



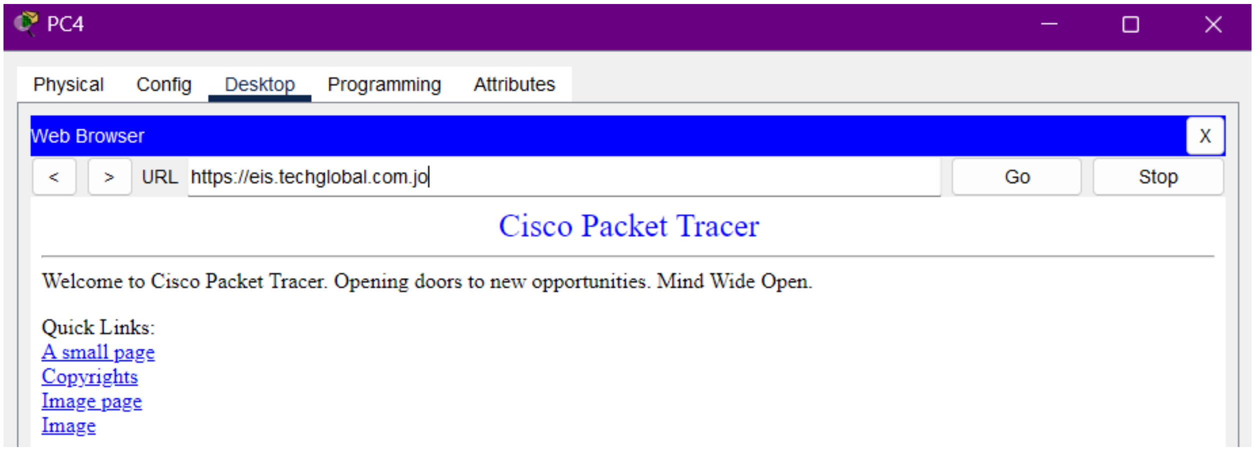
URL https://eis.techglobal.com.jo

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

VLAN 35



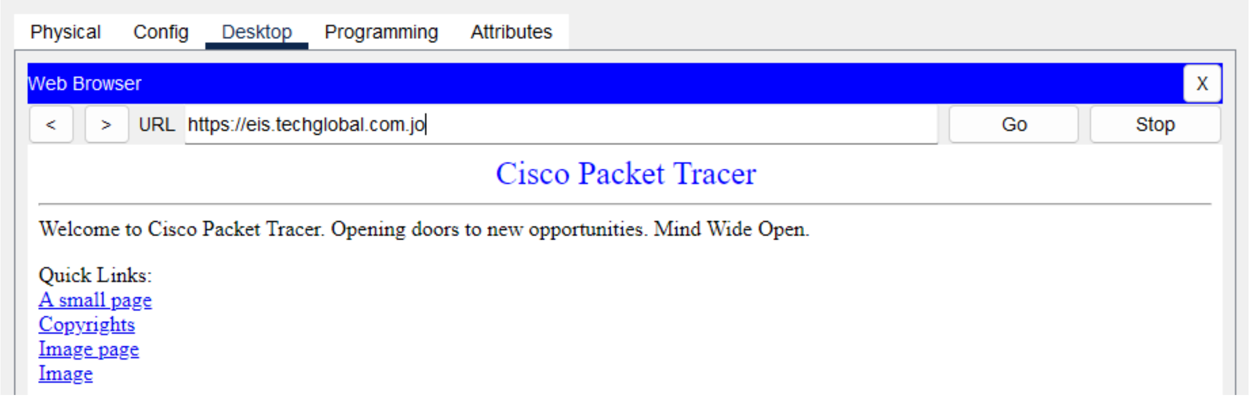
https://eis.techglobal.com.jo

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

VLAN 25



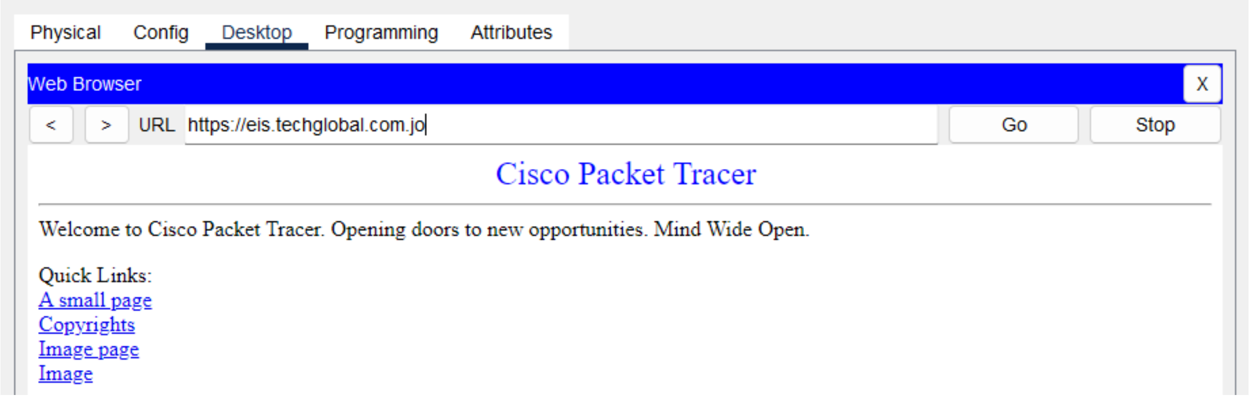
https://eis.techglobal.com.jo

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Tunisia



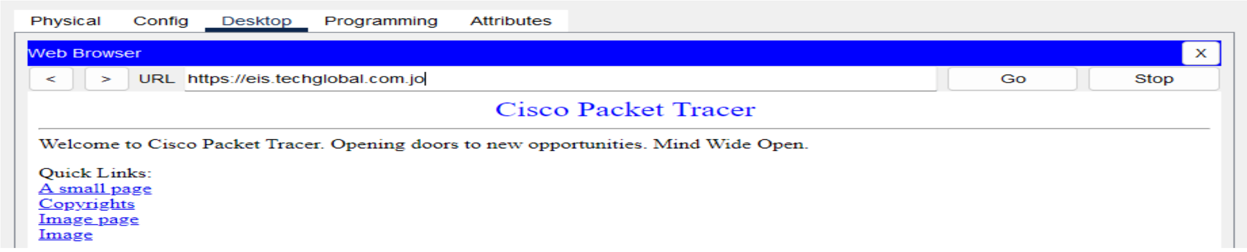
https://eis.techglobal.com.jo

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Turkey



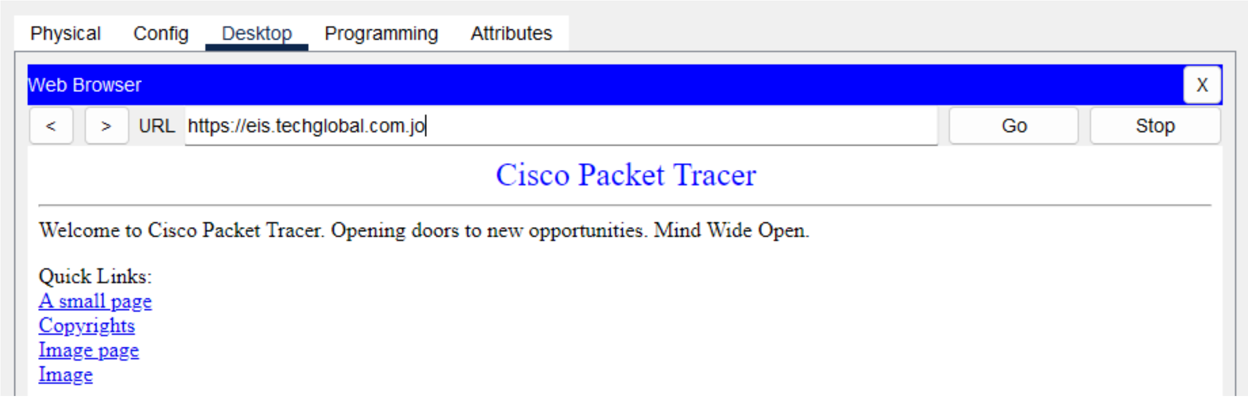
https://eis.techglobal.com.jo

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Kuwait



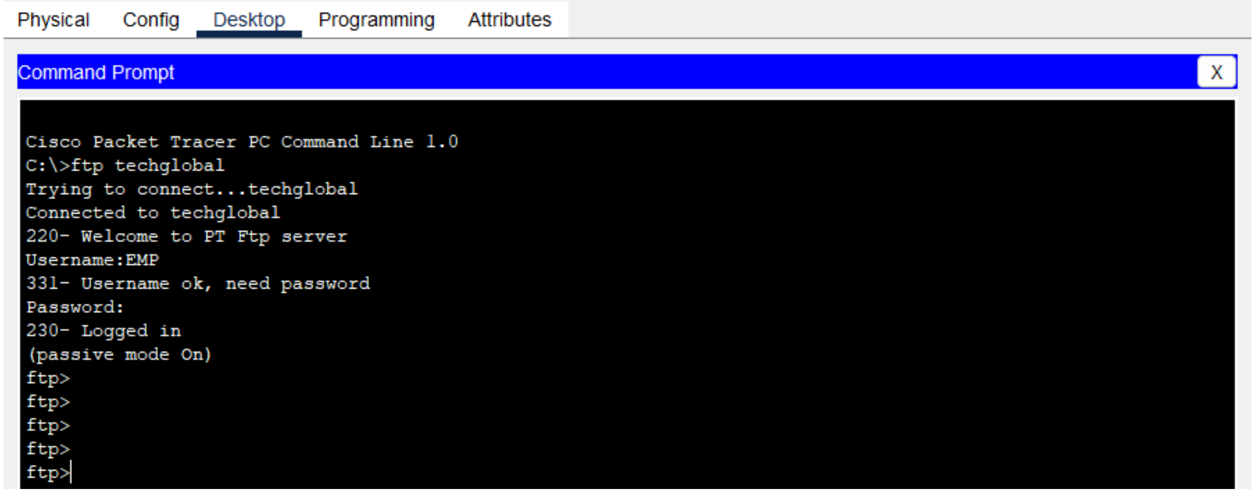
https://eis.techglobal.com.jo

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

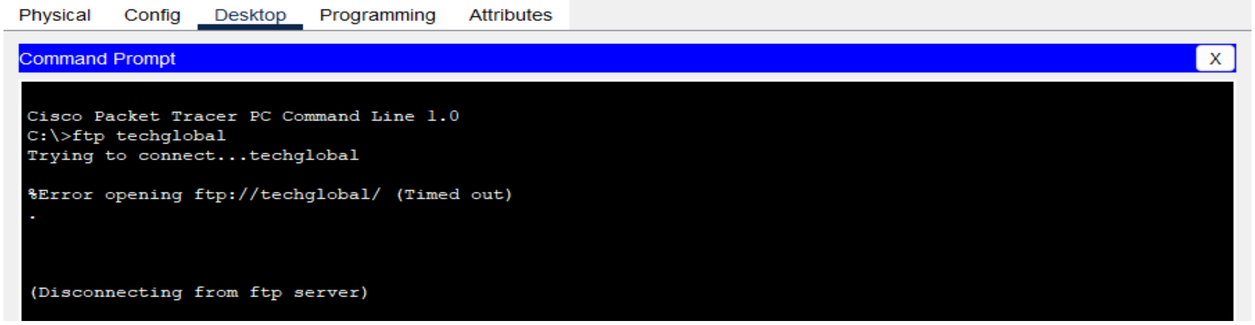
Quick Links:
A small page
Copyrights
Image page
Image

FTP EMP



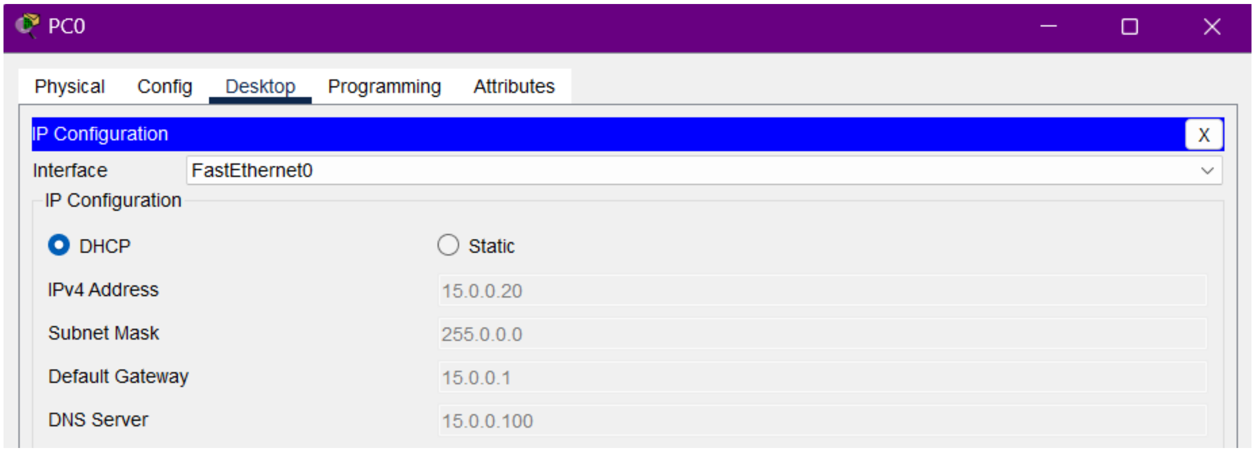
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp techglobal
Trying to connect...techglobal
Connected to techglobal
220- Welcome to PT Ftp server
Username:EMP
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
ftp>
ftp>
ftp>
ftp>
```

Trying ftp in HR VLAN :



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp techglobal
Trying to connect...techglobal

%Error opening ftp://techglobal/ (Timed out)
.


(Disconnecting from ftp server)
```

DHCP from a PC (PC 0) in data center



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

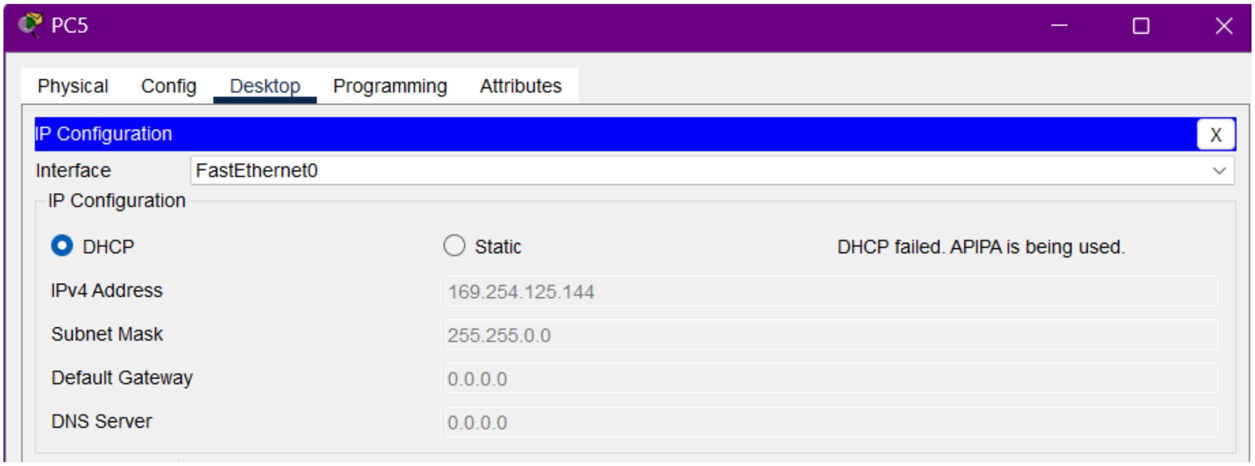
IPv4 Address: 15.0.0.20

Subnet Mask: 255.0.0.0

Default Gateway: 15.0.0.1

DNS Server: 15.0.0.100

DHCP from a PC in any other VLAN except data center VLAN



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP failed. APIPA is being used.

IPv4 Address: 169.254.125.144

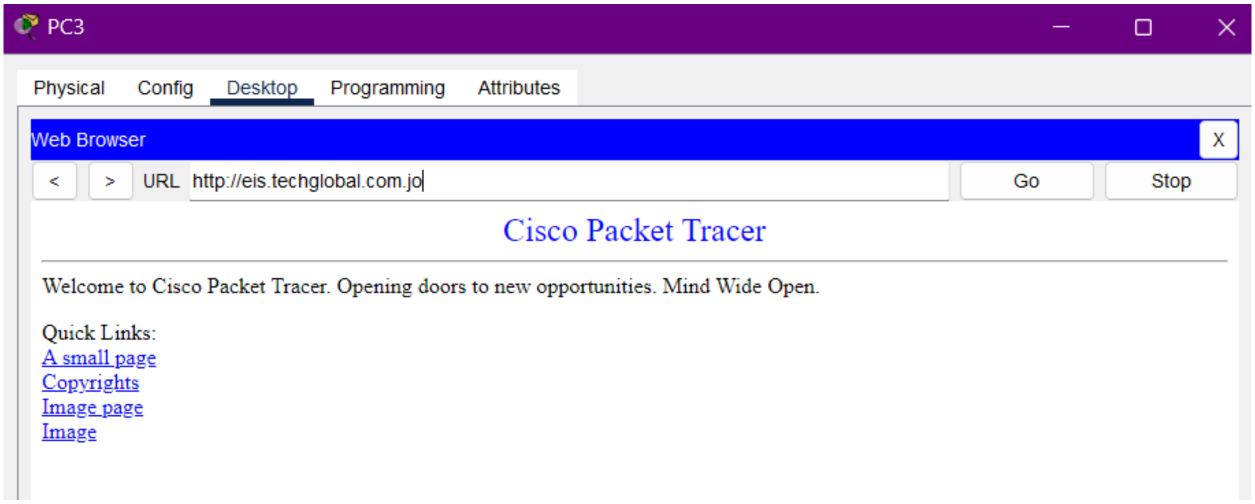
Subnet Mask: 255.255.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

HTTP access

From EMP VLAN



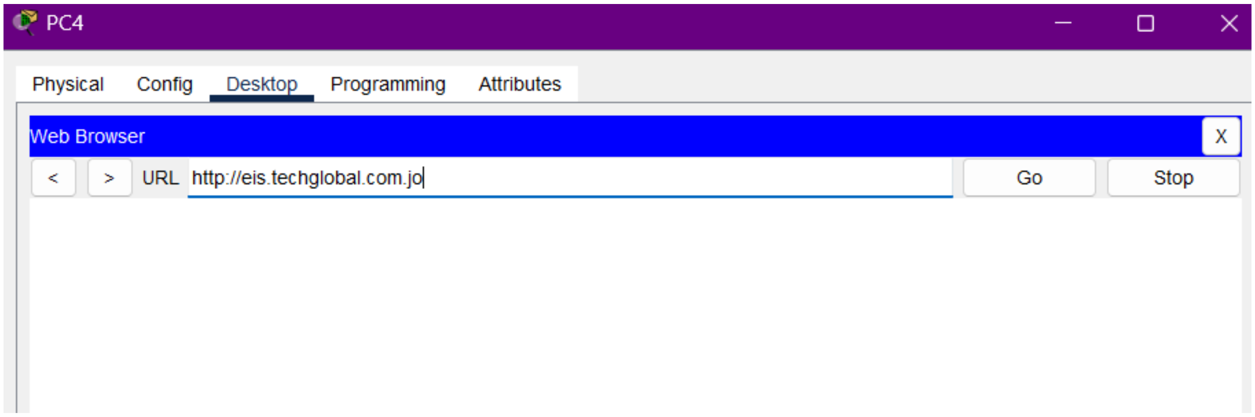
URL http://eis.techglobal.com.jo

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

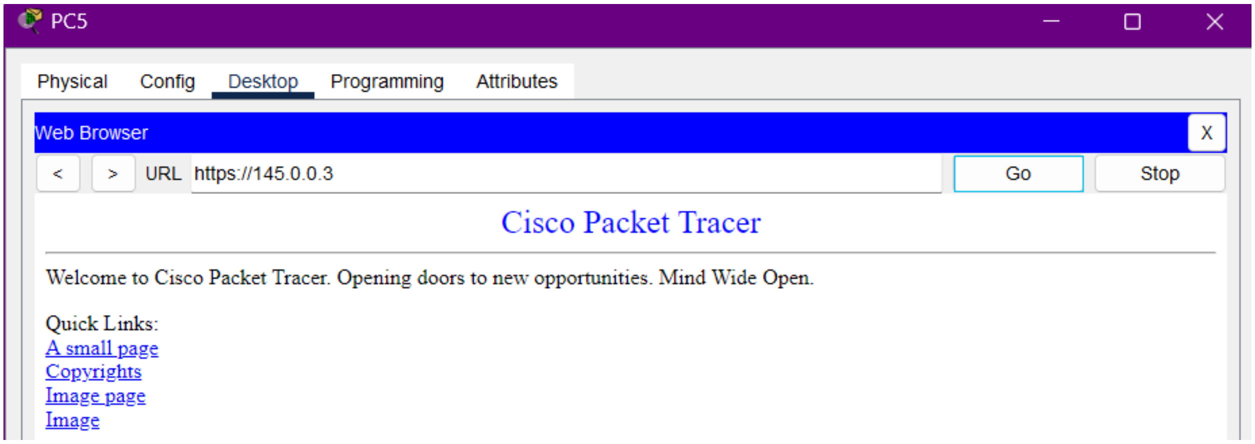
From HR VLAN



URL http://eis.techglobal.com.jo

HTTPS from DMZ

From Guest VLAN (45):



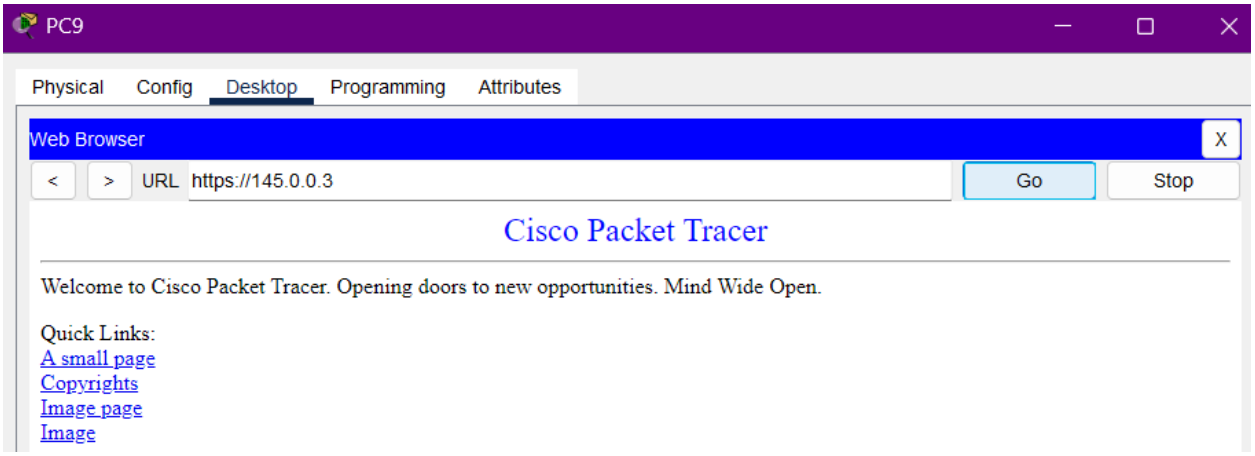
URL https://145.0.0.3

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

From Tunisia network :



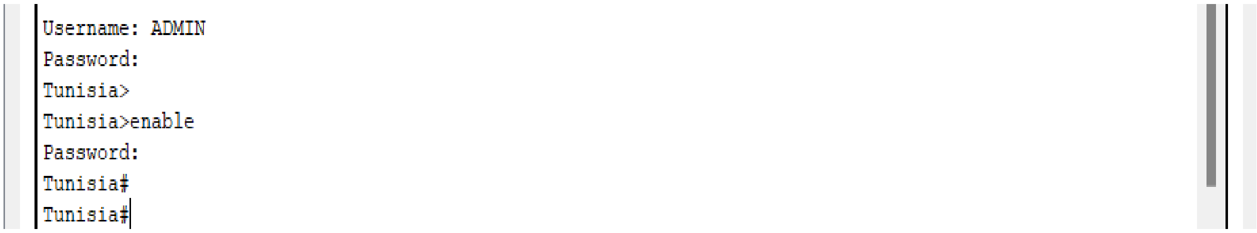
https://145.0.0.3

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

AAA on Tunisia router



```
Username: ADMIN
Password:
Tunisia>
Tunisia>enable
Password:
Tunisia#
Tunisia#
```

EVALUATE DESIGN, PLANNING, IMPLEMENTATION AND TESTING

In Tech global case, separating the project into phases was very helpful due to the requirements complexity of the Tech global network. But when using the project management phases such as planning, designing, implementation, and testing, it reduced the complexity of the network and made it easier to implement a high-performance network security by focusing on specific requirements in each phase.

The planning and designing phases were the most important phases because they included the basics and essential sectors and aspects such as understanding the requirements, location of offices like router, switch, and PC in each network, etc. So if the planning and designing phases were not correct and not achieve the target , it will negatively affect the project by implementing a misunderstanding network that not aligns with the correct requirements.

The planning and design phases were very good in Tech global network which guaranteed us to implement the best network that aligns with the network requirements and best security levels.

The implementation and testing design started after the planning and designing finished to apply those phases in the packet traces simulator, and it was very easy, less time and effort because of planning and designing phases. The testing phase was a very important phase to check and validate the Tech global network after the implementation phase and check if the requirements and design of Tech global network align with the network implemented in the packet tracer.

Overall, these phases were very important in easily implementing an effective and secure Tech global network with effortless and less time that without using management phases (planning, designing, implementation and testing). These phases have contributed to this project and gave me the ability to achieve this project successfully.

IMPROVEMENT RECOMMENDATIONS

For improvements, I prefer to use automated network options for handling configurations, reducing mistakes made by humans and time savings. Implement more security measures like IPS or IDS to enhance the security of the Tech global network.

Implement load balancing to separate network traffic to enhance the performance of the network. Use monitoring tools to keep monitoring and watch the network performance and identify if a failure happened to the network. Finally, implement backup strategy for network data and configuration to recover any important data if needed.

QUALITY OF SERVICE

Quality of service (QOS) contains various techniques or methodologies that are used and implemented to handle network resources and make sure that operations are efficient in the network devices and services. In addition, it is used to arrange network traffic by prioritizing some traffic over others, which enhances the performance of the network by making sure that the most important applications can get suitable bandwidth, and reliability.

IMPACT (SECUIRTY CONFIGURATION) ON QOS

Measures implemented in Tech Global or other networks like VPNs or encryptions will need higher bandwidth to perform well, but in the event that VPNs or encryptions aren't allocated in the right way, it will negatively reduce the performance of the network, not just the VPN or encryption.

In addition, security procedures, such as extensive packet inspection and analyzing traffic, involve enough QoS configurations in order to focus on applications that are sensitive to latency, therefore guaranteeing and upholding high levels of safety. Also, security configurations offer an important effect on QoS rules, making sure high-priority traffic remains safe and delivered via adequate bandwidth as well as low latency.

QoS is a key component that enhances security through effectively controlling sources including memory, keeping network efficiency with no overpowering operations related to security.

(What is quality of service (QoS) in networking?)[3]

REFERENCES

[1] Difference between IPSec and SSL (2023) GeeksforGeeks. Available at: https://www.geeksforgeeks.org/difference-between-ipsec-and-ssl/ (Accessed: 25 January 2024).

[2] Power, C. (2024) Understanding the importance of network security, Power Consulting. Available at: https://powerconsulting.com/blog/why-is-network-security-important/ (Accessed: 25 January 2024).

[3] What is quality of service (QoS) in networking? (no date) Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service (Accessed: 25 January 2024).