Assessment II - Skills Integration Challenge II

Name: Syed Asghar Abbas Zaidi	Student ID: 07201

1. Objective

The Objectives of this assessment are:

- Construct a technical policy for the given network
- Configure basic ASA device hardening and secure network management
- Configure DHCP and NAT on the ASA device
- Configure the ASA firewall to implement security policies
- Configure a site-to-site IPsec VPN

2. Topology

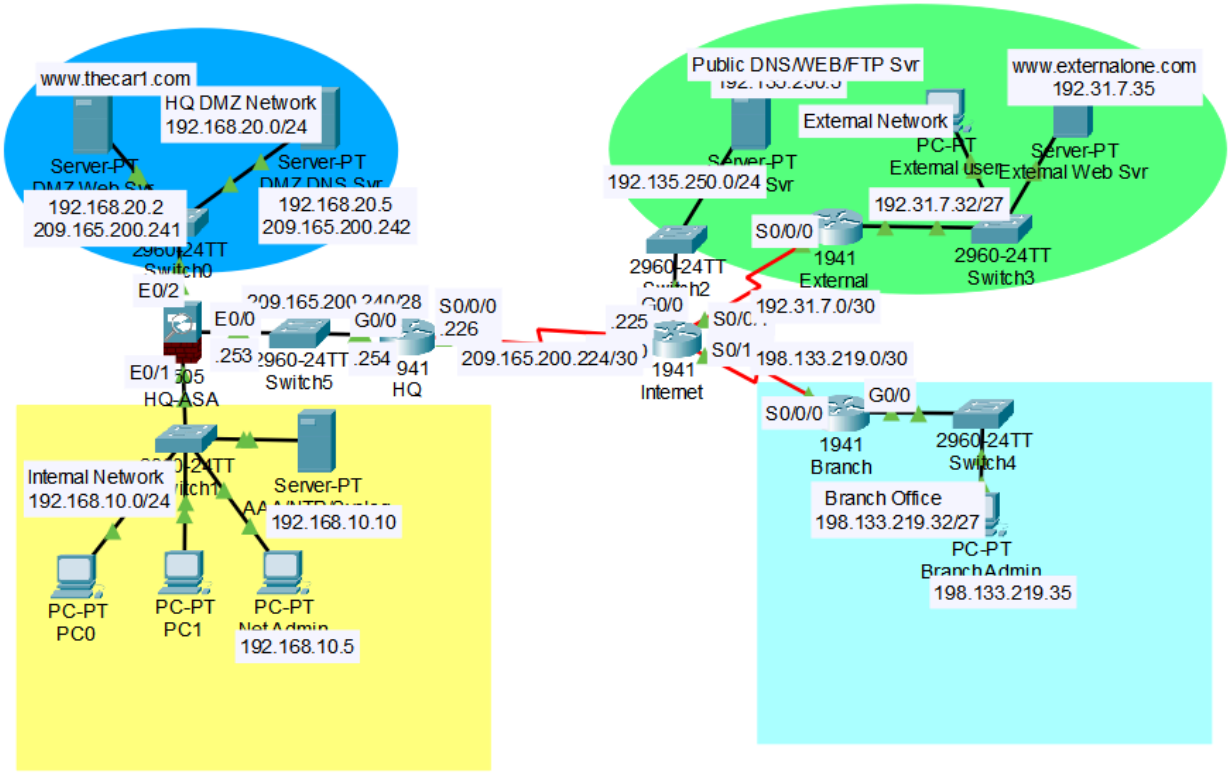


Figure 1: Topology

3. Addressing Table

Device	Interface	IP Address	Subnet Mask	Gateway	DNS server
Internet	S0/0/0	209.165.200.225	255.255.255.252	n/a	
	S0/0/1	192.31.7.1	255.255.255.252	n/a	
	G0/0	198.133.219.1	255.255.255.252	n/a	
	G0/0	192.135.250.1	255.255.255.0	n/a	
HQ	S0/0/0	209.165.200.226	255.255.255.252	n/a	
	G0/0	209.165.200.254	255.255.255.240	n/a	
HQ-ASA	E0/0	209.165.200.253	255.255.255.240	n/a	
	E0/1	192.168.10.1	255.255.255.0	n/a	
	E0/2	192.168.20.1	255.255.255.0	n/a	
Branch	S0/0/0	198.133.219.2	255.255.255.252	n/a	
	G0/0	198.133.219.62	255.255.255.224	n/a	
External Web Svr	NIC	192.31.7.35	255.255.255.224	192.31.7.62	
External PC	NIC	192.31.7.33	255.255.255.224	192.31.7.62	192.135.250.5
AAA/NTP/ Syslog Svr	NIC	192.168.10.10	255.255.255.0	192.168.10.1	
DMZ DNS Svr	NIC	192.168.20.5	255.255.255.0	192.168.20.1	
DMZ Web Svr	NIC	192.168.20.2	255.255.255.0	192.168.20.1	192.168.20.5
PC0 and PC1	NIC	DHCP client	255.255.255.0	192.168.10.1	192.168.10.10
Branch Admin	NIC	198.133.219.35	255.255.255.224	198.133.219.62	192.135.250.5
Net Admin PC	NIC	192.168.10.5	255.255.255.0	192.168.10.1	192.168.10.10

Figure 2: Addressing Table

Task 1 – Construct a Technical Policy

Construct a technical policy document that outlines the security measures, configurations, and guidelines required for the provided network scenario.

Your policy should include the following:

- Purpose and Scope of the policy.
- Security configurations (e.g., ASA hardening, DHCP, NAT, ACLs, VPN).
- Access control and monitoring guidelines.

For details on network security policies, please refer to the file 'Chapter 11 – Managing a Secure Network' on LMS.

Technical Policy Document: Network Security for Corporate Network

1. Purpose and Scope

Purpose

This policy aims to establish the technical guidelines and security measures necessary to protect the confidentiality, integrity, and availability of the corporate network infrastructure. The outlined configurations will ensure a robust and secure environment for communication between the Internet, HQ, Branch, and internal users.

Scope

The policy applies to all network devices, servers, and endpoints, including routers, switches, firewalls (ASA), PCs, and servers mentioned in the addressing table. It encompasses configurations for security hardening, access control, monitoring, and network communication protocols.

2. Security Configurations

2.1 ASA Firewall Hardening

- Enable password encryption using service password-encryption
- Restrict management access to the ASA via secure protocols like SSH, limited to internal network management IPs (192.168.10.5)
- Configure access control lists (ACLs) to permit only necessary traffic:
  - Block all traffic from untrusted sources by default
  - Allow HTTP/HTTPS traffic to the DMZ servers (192.168.20.2 and 192.168.20.5) from the Internet
  - Allow internal traffic to access the Internet via NAT
- Apply AAA (Authentication, Authorization, and Accounting) for user authentication:
  - Use the AAA/NTP/Syslog server (192.168.10.10) for centralized authentication

2.2 DHCP Configuration

- Configure DHCP for internal devices in HQ:
  - IP Pool: 192.168.10.2 - 192.168.10.254
  - Default Gateway: 192.168.10.1
  - DNS Server: 192.168.10.10
- Exclude static IPs assigned to critical devices (e.g., ASA, servers)

2.3 NAT Configuration

- Implement NAT for secure Internet access:
  - Dynamic NAT for internal users accessing external websites
  - Static NAT to map public IPs to DMZ servers for external accessibility:
    - Map 209.165.200.253 to 192.168.20.2 for the DMZ Web Server
    - Map 209.165.200.254 to 192.168.20.5 for the DMZ DNS Server

2.4 VPN Configuration
- Establish an IPsec VPN tunnel between HQ and Branch to secure inter-office communication:
  - Use pre-shared keys for Phase 1 authentication
  - Configure Phase 2 to encrypt traffic using AES-256
  - Define interesting traffic between HQ (209.165.200.254/28) and Branch (198.133.219.32/27)

3. Access Control and Monitoring Guidelines

3.1 Access Control
- Restrict administrative access to critical network devices using ACLs:
  - Permit SSH from 192.168.10.0/24 and block other sources
  - Restrict physical console access to authorized personnel
- Configure VLANs for segmentation:
  - VLAN 10: Internal Users (192.168.10.0/24)
  - VLAN 20: DMZ Servers (192.168.20.0/24)

3.2 Monitoring and Logging
- Enable Syslog on all devices to forward logs to the centralized Syslog server (192.168.10.10)
- Configure SNMP for device monitoring and send traps to the management server (192.168.10.10)
- Schedule periodic configuration backups for all critical devices

3.3 Verification and Testing
- Test ASA ACLs using tools like ping and traceroute to ensure correct traffic filtering
- Validate DHCP and NAT configurations by testing connectivity from client devices
- Perform VPN tunnel testing by pinging remote subnets

4. Enforcement

This policy must be reviewed and enforced by network administrators. Non-compliance or deviations without prior approval from the IT Security Manager will result in disciplinary action.

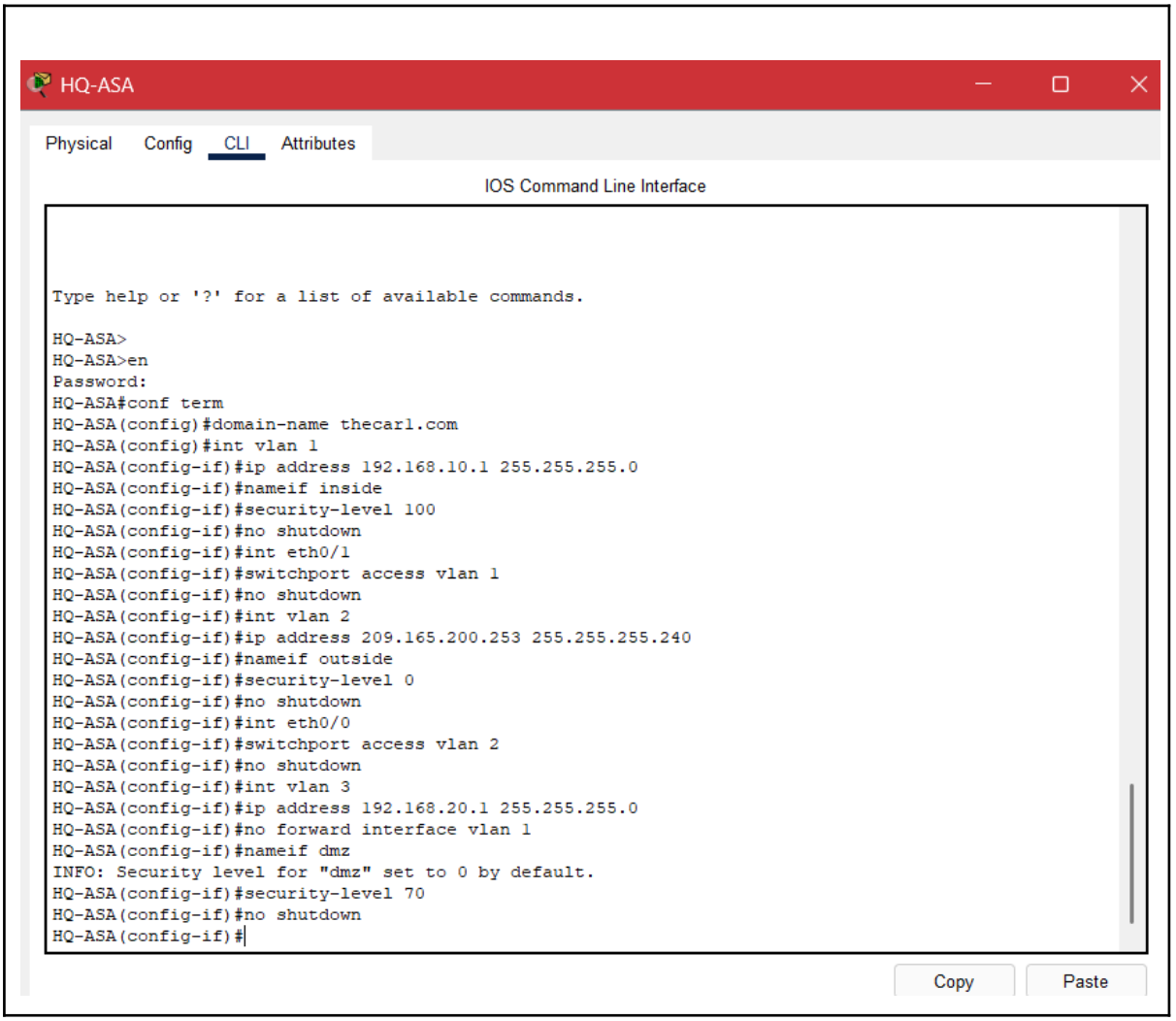
5. References

Refer to "Chapter 11 – Managing a Secure Network" for additional guidelines and configurations.

Task 2 - Configure Basic Device Hardening for the ASA device.

Note: HQ-ASA is already configured with a password **Thecar1Admin**.

1. Access HQ-ASA and enter the privileged mode with the enable password of **Thecar1Admin**.
2. Configure the domain name as **thecar1.com**.
3. Configure the inside, outside, and dmz interfaces with the following information:
    a. VLAN 1 – IP address 192.168.10.1/24, nameif **inside**, security-level **100**, assign to E0/1
    b. VLAN 2 – IP address 209.165.200.253/28, nameif **outside**, security-level **0**, assign to E0/0
    c. VLAN 3 – IP address 192.168.20.1/24, nameif **dmz**, security-level **70**, assign to E0/2
    d. Enable interfaces.

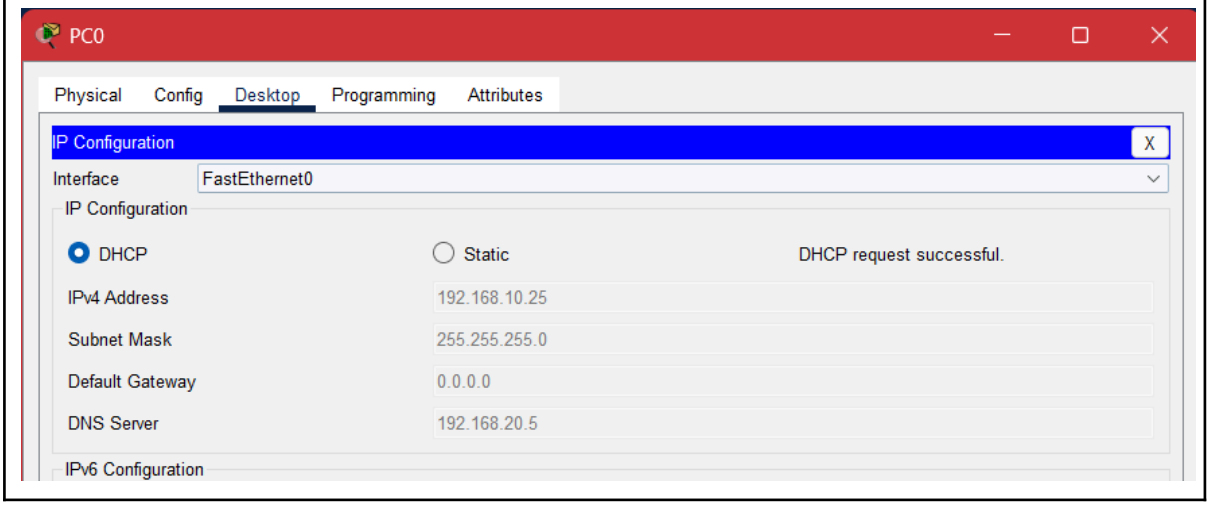


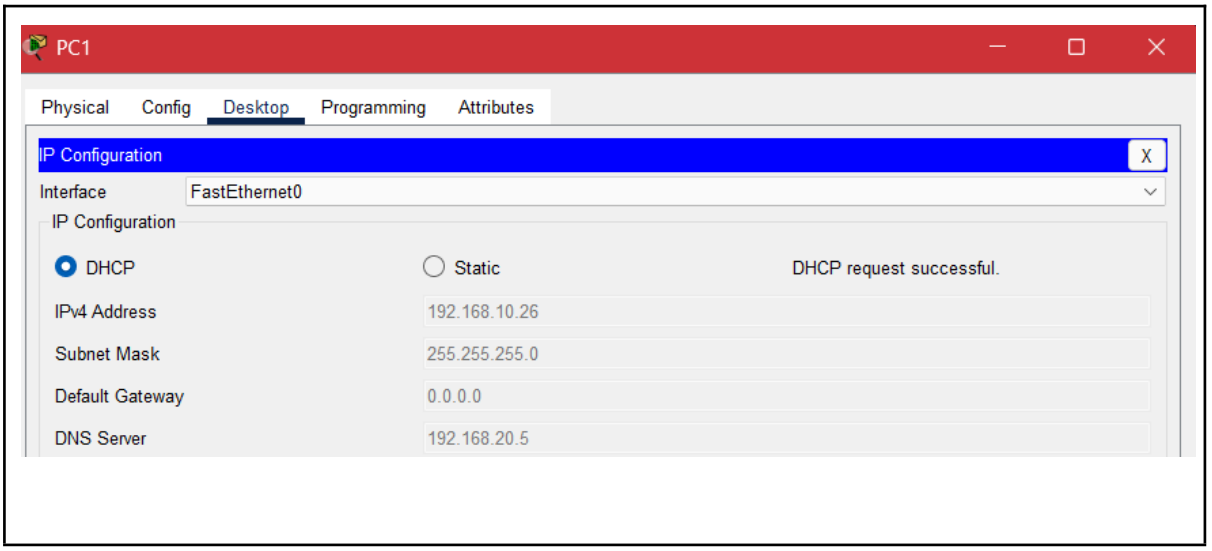
```
INFO: Security level for "dmz" set to 0 by default.
HQ-ASA(config-if)#security-level 70
HQ-ASA(config-if)#no shutdown
HQ-ASA(config-if)#int eth0/2
HQ-ASA(config-if)#switchport access vlan 3
HQ-ASA(config-if)#no shutdown
HQ-ASA(config-if)#exit
```

Task 3 - Configure DHCP service on the ASA device for the internal network.

1. The DHCP pool is 192.168.10.25 – 192.168.10.35.
2. DHCP service should provide DNS server (AAA/NTP/syslog server) information.
3. Verify that the internal users (PC0 and PC1) obtain the dynamic addressing information correctly. Attach screenshot.

```
HQ-ASA(config-if)#exit
HQ-ASA(config)#dhcpd address 192.168.10.25-192.168.10.35 inside
HQ-ASA(config)#dhcpd dns 192.168.10.10
HQ-ASA(config)#dhcpd option 3 ip 192.168.10.1
HQ-ASA(config)#dhcpd enable inside
```





Task 4 - Configure Secure Network Management for the ASA Device

1. Enable the ASA device:
   - as an NTP client to the AAA/NTP/Syslog server
   - Enable the authentication to the NTP server.
   - The authentication key is **key 1** with the password **corpkey.**

2. Configure the ASA device with AAA authentication and verify its functionality:

   Note: the HQ-ASA is preconfigured with a username **Car1Admin** with password **adminpass01**

   - Configure AAA to use the local database for SSH connections to the console port
   - Generate a RSA key pair to support with modulus size of **1024** bits.
   - Configure HQ-ASA to accept SSH connections only from the Net Admin workstation.
   - Configure SSH session timeout to be 20 minutes.

```
HQ-ASA(config)#ntp authenticate
HQ-ASA(config)#ntp authentication-key 1 md5 corpkey
HQ-ASA(config)#ntp server 192.168.10.10 key 1
HQ-ASA(config)#aaa authentication ssh console LOCAL
HQ-ASA(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
HQ-ASA(config)#ssh 192.168.10.5 255.255.255.255 inside
HQ-ASA(config)#ssh timeout 20
```

Task 5 - Configure NAT Service for the ASA device for both inside and DMZ networks.

1. Create an object **inside-nat** with subnet 192.168.10.0/24 and enable the IP addresses of the hosts in the internal network to be dynamically translated to access the external network via the outside interface.
2. Create an object **dmz-dns-server** to statically translate the DNS server in the DMZ to the public IP address.
3. Create an object **dmz-web-server** to statically translate the web server in the DMZ to the public IP address.

```
HQ-ASA(config)#object network inside-nat
HQ-ASA(config-network-object)#subnet 192.168.10.0 255.255.255.0
HQ-ASA(config-network-object)#nat (inside,outside) dynamic interface
HQ-ASA(config-network-object)#object network dmz-dns-server
HQ-ASA(config-network-object)#host 192.168.20.5
HQ-ASA(config-network-object)#nat (dmz,outside) static 209.165.200.242
HQ-ASA(config-network-object)#object network dmz-web-server
HQ-ASA(config-network-object)#host 192.168.20.2
HQ-ASA(config-network-object)#nat (dmz,outside) static 209.165.200.241
```

Task 6 - Configure ACL and firewall on the ASA device to implement the Security Policy.

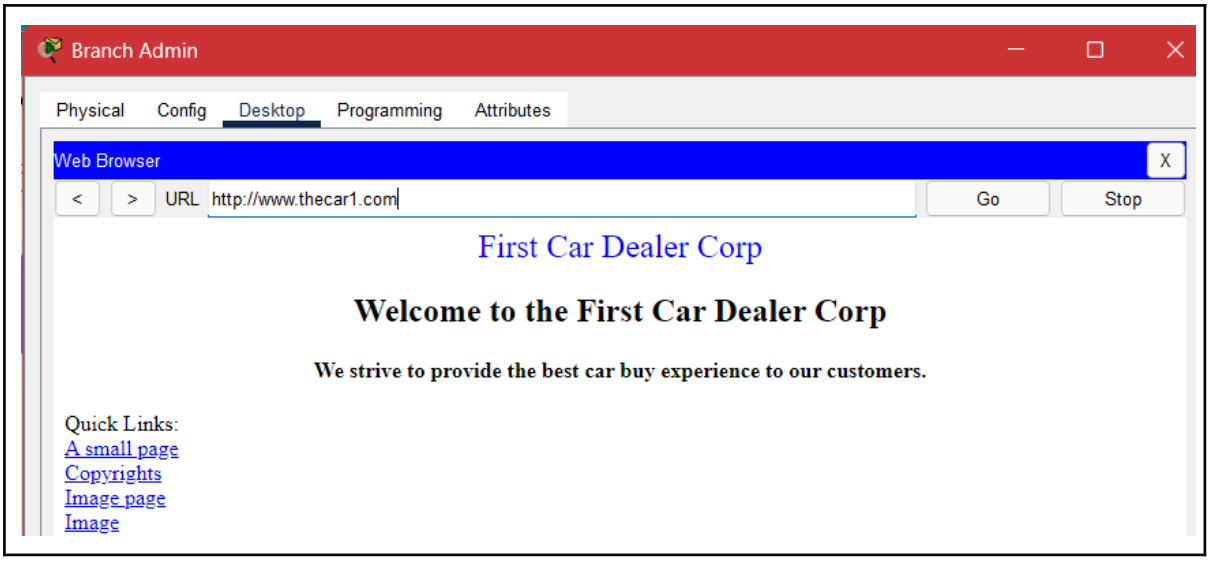
1. Modify the default MPF application inspection global service policy to enable hosts in the Internal network to access the web servers on the Internet
   - Create a class **inspection_default** that matches **default-inspection-traffic**.
   - Create a policy-map **global_policy** and specify the inspect with **dns, ftp, http, and icmp**.
   - Attach the policy map globally to all interfaces.
2. Configure an ACL to allow access to the DMZ servers from the Internet.
   - Create, apply, and verify an extended named ACL (named OUTSIDE-TO-DMZ) to filter incoming traffic to the HQ-ASA. The ACL should be created in the order specified in the following guidelines (**Please note, the order of ACL statements is significant only because of the scoring need in Packet Tracer**):
     - HTTP traffic is allowed to DMZ Web Svr.

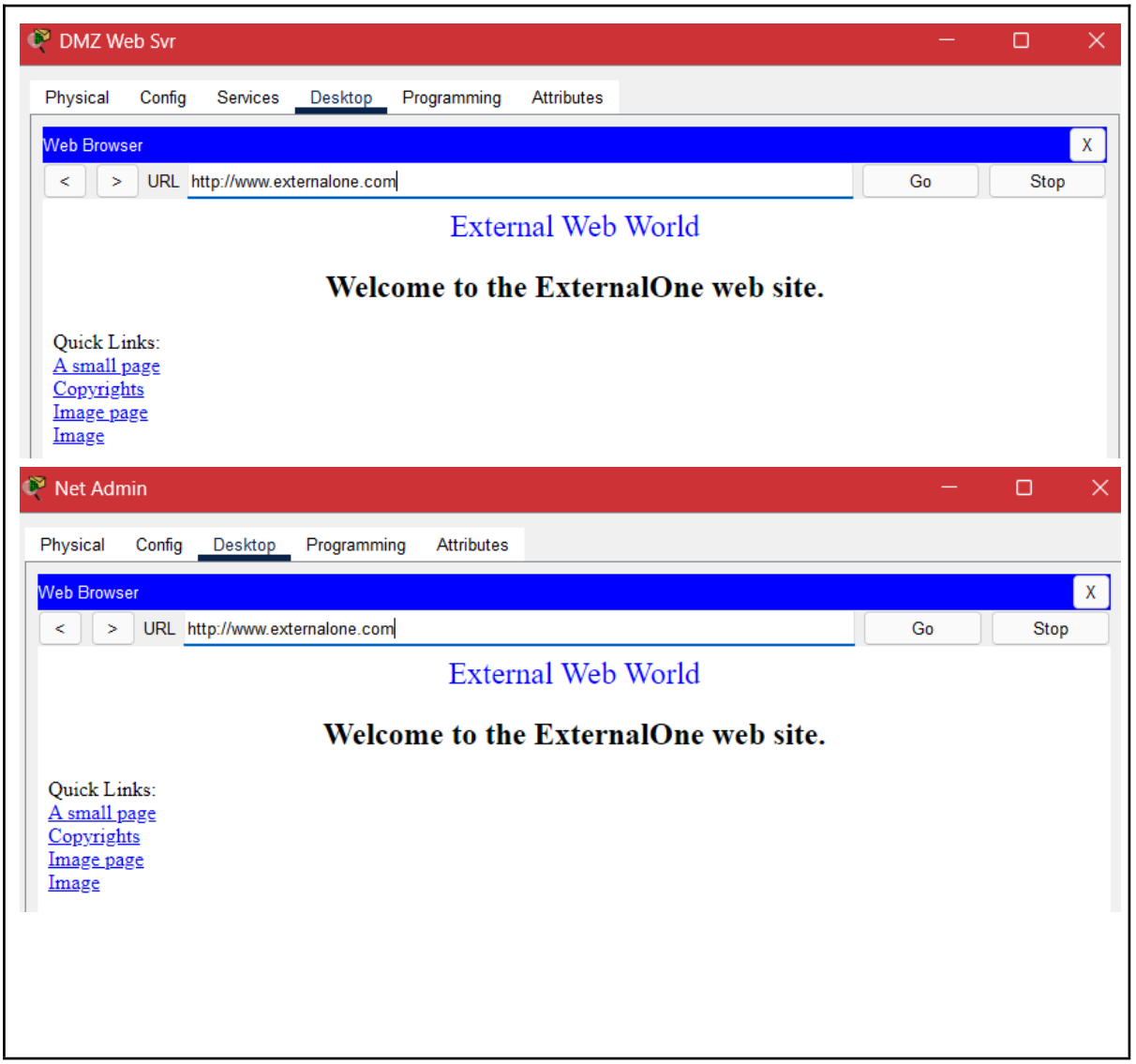
- DNS traffic (both TCP and UDP) is allowed to the DMZ DNS server (two separate ACEs).
- FTP traffic from the branch administrator workstation is allowed to the DMZ web server.
- The ACL should contain four ACEs.

```
HQ-ASA#
HQ-ASA#config t
HQ-ASA(config)#policy-map global_policy
HQ-ASA(config-pmap)#class inspection_default
HQ-ASA(config-pmap-c)#inspect dns
HQ-ASA(config-pmap-c)#inspect ftp
HQ-ASA(config-pmap-c)#inspect http
HQ-ASA(config-pmap-c)#inspect icmp
HQ-ASA(config-pmap-c)#exit
HQ-ASA(config)#service-policy global_policy global
HQ-ASA(config)#access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.241 eq 80
HQ-ASA(config)#access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.242 eq 853
HQ-ASA(config)#no access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.242 eq 853
HQ-ASA(config)#access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.242 eq 85
HQ-ASA(config)#noaccess-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.242 eq 85
                ^
% Invalid input detected at '^' marker.

HQ-ASA(config)#no access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.242 eq 85
HQ-ASA(config)#access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.242 eq 53
HQ-ASA(config)#access-list OUTSIDE-TO-DMZ extended permit udp any host 209.165.200.242 eq 53
HQ-ASA(config)#access-list OUTSIDE-TO-DMZ extended permit tcp host 198.133.219.35 host 209.165.200.241 eq 21
HQ-ASA(config)#access-group OUTSIDE-TO-DMZ in interface outside
HQ-ASA(config)#
```

- Verify HQ-ASA configurations. Both Net Admin and DMZ Web Svr can access the website www.externalone.com. Branch Admin can access the website www.thecar1.com. Branch Admin can also establish an FTP connection to the web server www.thecar1.com, using the username cisco and the password cisco. **Attach screenshot below.**





Task 7 - Configure a Site-to-Site IPsec VPN between the HQ Router and the Branch Router.

Note: The Branch and HQ routers have already been configured with a username of **CORPADMIN** and a password of **Ciscoccnas**. The enable secret password is ciscoclass.

The following tables list the parameters for the ISAKMP Phase 1 Policy and IPsec Phase 2 Policy:

ISAKMP Phase 1 Policy Parameters	
Key Distribution Method	ISAKMP
Encryption Algorithm	AES
Number of Bits	256
Hash Algorithm	SHA-1
Authentication Method	Pre-share
Key Exchange	DH 2
IKE SA Lifetime	86400
ISAKMP Key	Vpnpass101

ISAKMP Phase 2 Policy Parameters		
Parameters	HQ Router	Branch Router
Transform Set Name	VPN-SET	VPN-SET
Transform Set	esp-3des esp-sha-hmac	esp-3des esp-sha-hmac
Peer Host Name	Branch	HQ
Peer IP Address	198.133.219.2	209.165.200.226
Encrypted Network	209.165.200.240/28	198.133.219.32/27
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Figure 3: ISAKMP Policy Parameters

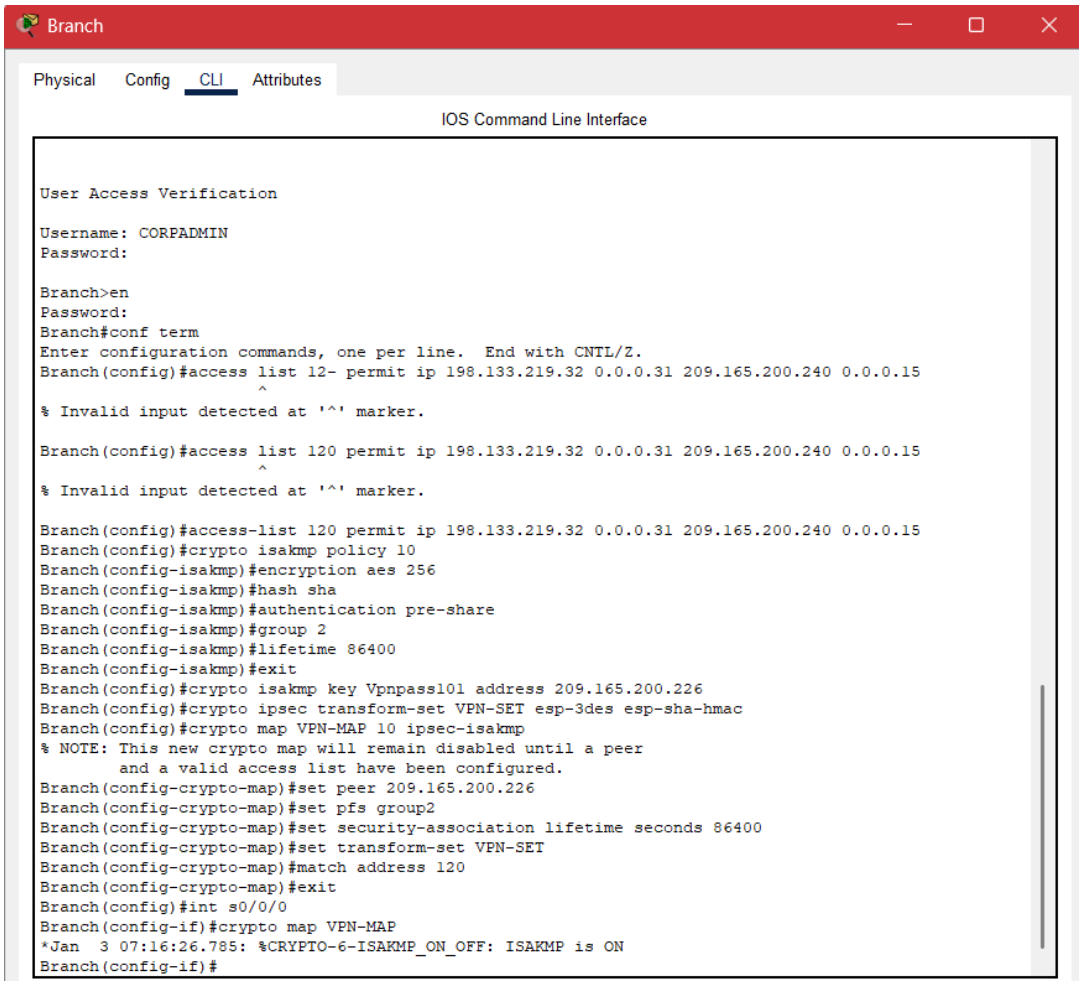
Configure an ACL (ACL 120) on the HQ router to identify the interesting traffic. The interesting traffic is all IP traffic between the two LANs (209.165.200.240/28 and 198.133.219.32/27).

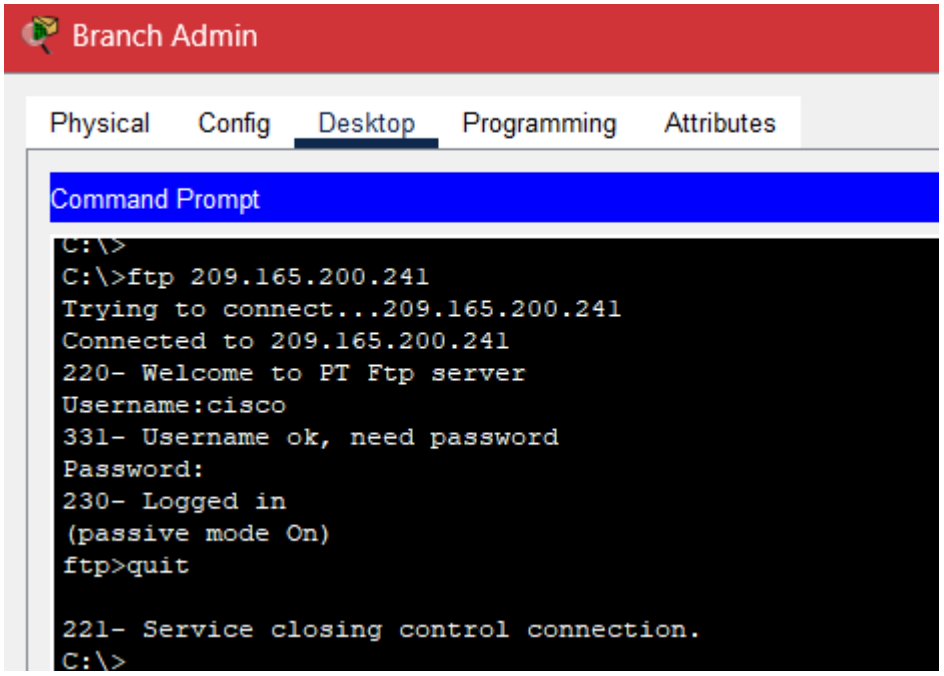
1. Configure the ISAKMP Phase 1 properties on the HQ router. The crypto ISAKMP policy is 10. Refer to the ISAKMP Phase 1 Policy Parameters Table for the specific details needed.
2. Configure the ISAKMP Phase 2 properties on the HQ router. Refer to the ISAKMP Phase 2 Policy Parameters Table for the specific details needed.
3. Bind the VPN-MAP crypto map to the outgoing interface.
4. Configure IPsec parameters on the Branch router using the same parameters as on the HQ router. Note that interesting traffic is defined as the IP traffic from the two LANs.
5. Save the running-config, then reload both the HQ and Branch routers.
6. Verify the VPN configuration by conducting an FTP session with the username cisco and the password cisco from the Branch Admin PC to the DMZ Web Svr. On the Branch router, check that the packets are encrypted. To exit the FTP session, type **quit. Attach screenshot.**

SCRIPT FOR HQ ROUTER

```
HQ>en
Password:
HQ#config t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#access-list 120 permit ip 209.165.200.240 0.0.0.15 198.133.219.32 0.0.0.31
HQ(config)#crypto isakmp policy 10
HQ(config-isakmp)#encryption aes 256
HQ(config-isakmp)#hash sha
HQ(config-isakmp)#authentication pre-share
HQ(config-isakmp)#group 2
HQ(config-isakmp)#lifetime 86400
HQ(config-isakmp)#exit
HQ(config)#crypto isakmp key Vpnpass101 address 198.133.219.2
HQ(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
HQ(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
HQ(config-crypto-map)#set peer 198.133.219.2
HQ(config-crypto-map)#set pfs group2
HQ(config-crypto-map)#set security-association lifetime seconds 86400
HQ(config-crypto-map)#set transform-set VPN-SET
HQ(config-crypto-map)#match address 120
HQ(config-crypto-map)# exit
HQ(config)#crypto map VPN-MAP
% Incomplete command.
HQ(config)#int s0/0/0
HQ(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP ON OFF: ISAKMP is ON
```

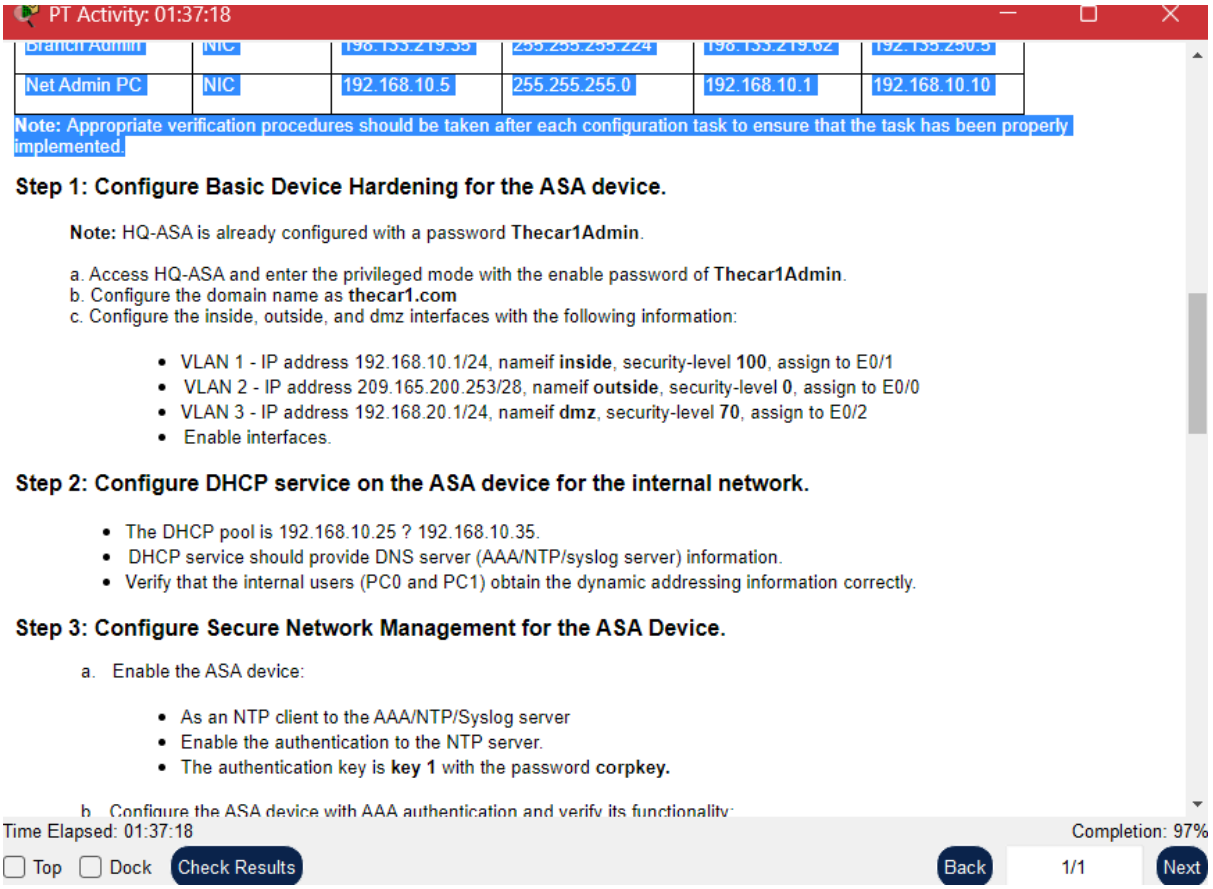
SCRIPT FOR BRANCH

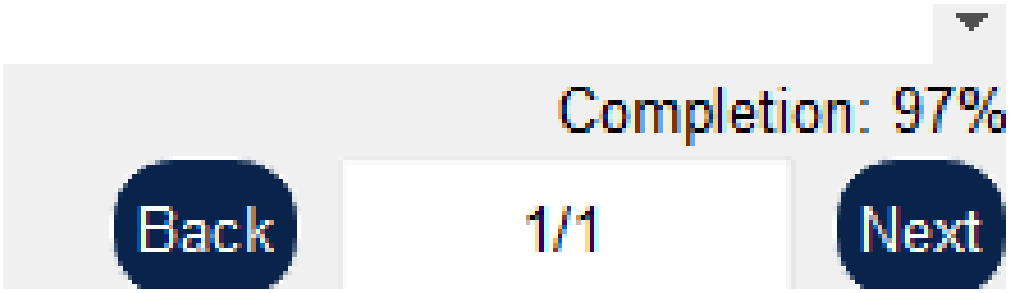

Branch
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Username: CORPADMIN
Password:
Branch>en
Password:
Branch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)#access list 12- permit ip 198.133.219.32 0.0.0.31 209.165.200.240 0.0.0.15
^
% Invalid input detected at '^' marker.
Branch(config)#access list 120 permit ip 198.133.219.32 0.0.0.31 209.165.200.240 0.0.0.15
^
% Invalid input detected at '^' marker.
Branch(config)#access-list 120 permit ip 198.133.219.32 0.0.0.31 209.165.200.240 0.0.0.15
Branch(config)#crypto isakmp policy 10
Branch(config-isakmp)#encryption aes 256
Branch(config-isakmp)#hash sha
Branch(config-isakmp)#authentication pre-share
Branch(config-isakmp)#group 2
Branch(config-isakmp)#lifetime 86400
Branch(config-isakmp)#exit
Branch(config)#crypto isakmp key Vpnpass101 address 209.165.200.226
Branch(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
Branch(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Branch(config-crypto-map)#set peer 209.165.200.226
Branch(config-crypto-map)#set pfs group2
Branch(config-crypto-map)#set security-association lifetime seconds 86400
Branch(config-crypto-map)#set transform-set VPN-SET
Branch(config-crypto-map)#match address 120
Branch(config-crypto-map)#exit
Branch(config)#int s0/0/0
Branch(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Branch(config-if)#


Branch Admin
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>
C:\>ftp 209.165.200.241
Trying to connect...209.165.200.241
Connected to 209.165.200.241
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit
221- Service closing control connection.
C:\>

Attach scripts for HQ-ASA, HQ Router and Branch Router.

ACTIVITY WAS 97% COMPLETED!





Assessment Rubric

Assessment II - Skills Integration Challenge II

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

Points Distribution

Task No.	**LR 2 Simulation**	**LR5 Results/Plots**	**LR9 Report**
Task 1			/20
Task 2	/10		
Task 3	/5		
Task 4	/10		
Task 5	/15		
Task 6	/15	/5	
Task 7	/15	/5	
Total	/70	/10	/20
CLO Mapped	CLO 1-4	CLO 1-4	CLO 1-4

For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.

Lab Evaluation Assessment Rubric

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3:Good Points 3	Level 4:Exemplary Points 4
LR2	**Program/Code / Simulation Model/ Network Model**	Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software.	Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software.	Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine.	Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software.
LR5	**Results & Plots**	Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner.	Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear.	All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing.	Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic.
LR9	**Report**	All the in-lab tasks are not included in report and / or the report is submitted too late.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date.	Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.