**Cyber Security Problem Statement**

Choose a university/college campus and analyze its network topology. Map the network using Cisco Packet Tracer and identify the security controls that are in place, such as network segmentation, intrusion detection systems, firewalls, and authentication and authorization systems. Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping, aiming to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

**Tasks:**

1. Campus Network Analysis: Choose a university or college campus and conduct an analysis of its existing network topology, including the layout, devices, and

connections.

2. Network Mapping: Utilize Cisco Packet Tracer to map the network infrastructure, representing the placement and interconnectivity of routers, switches, firewalls, and

other relevant network components.

1. Attack Surface Mapping: Conduct an attack surface mapping exercise to identify potential vulnerabilities and weaknesses within the network architecture and design, considering factors such as unauthorized access, data breaches, and network availability.

4. Secure Access Controls: Incorporate appropriate security controls (e.g., VLANs, IDP/IPS, VPN, Firewalls, password management, vulnerability management etc.) in

your design to enhance security posture.

**Deliverables:**

1. Network topology diagram depicting the existing infrastructure and attack surface findings.

2. Security assessment report highlighting identified security risks, proposed solutions, and countermeasures to mitigate attack surface risks.

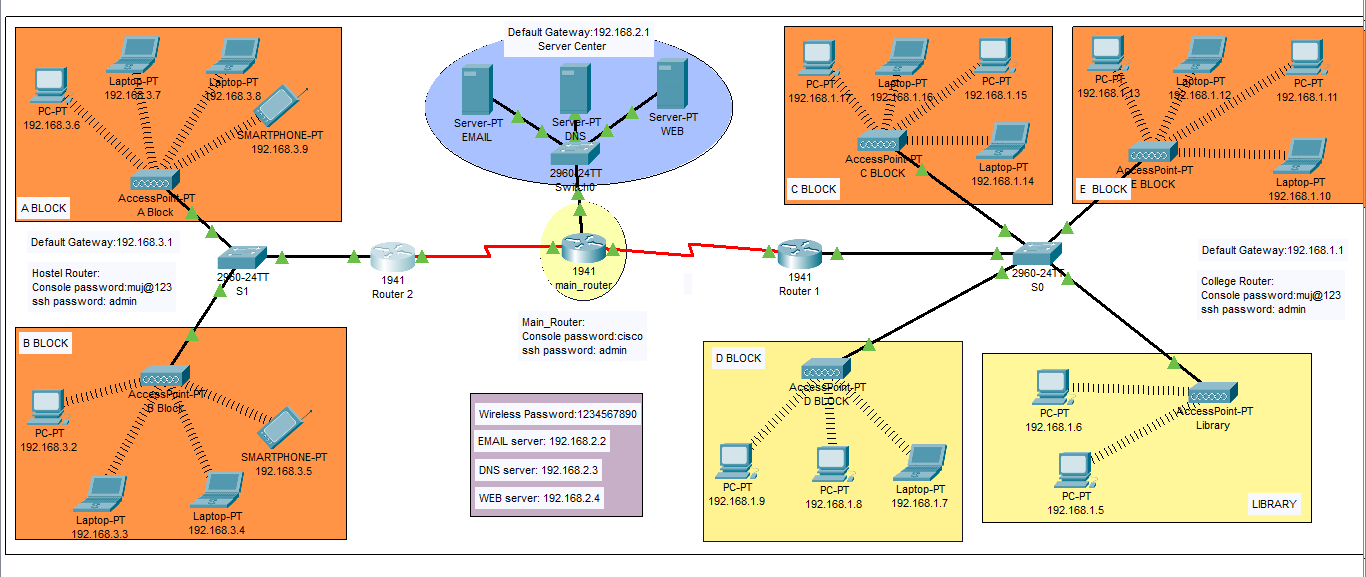
TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| 1. | Problem Statement | 1 |
| 2. | Table of Contents | 2 |
| 3. | Part-I: Network Topology Diagram and Configurations | 3 |
| 4. | Part-II: Security Assessment Report and Countermeasures | 15 |

## Part-I: Network Topology Diagram and Configurations

Network topology of the College:

We have the complete network providing various facilities to the teaching staff, non-teaching staff, and students.



The complete diagram of the College Area Network Scenario created in Packet Tracer environment.

This College network consists of the following devices:

1) Router (1941)

2) Switches (2960-24TT)

3) Email server

4) DNS server

5) WEB server (HTTP)

6) Wireless Device (Access Point)

7) PCs

8) Laptops

9) Smartphones

The design includes the following parts of the University:

A Block (Administrative Department)

Academic Blocks:

B Block

C Block

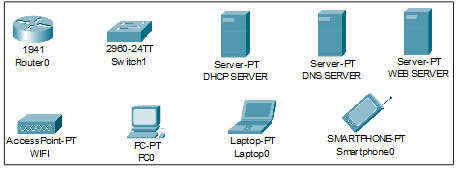
D Block

E Block

Library

Devices Used In The Network

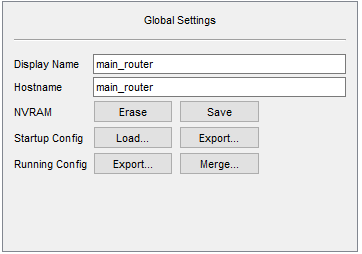
|  |  |
| --- | --- |
| Devices | Quantity |
| 1) Router (1941) | 3 |
| 2) Switches (2960-24TT) | 3 |
| 3) EMAIL server | 1 |
| 4) DNS server | 1 |
| 5) WEB server (HTTP) | 1 |
| 6) Wireless Device (Access Point) | 6 |
| 7) PCs | 10 |
| 8) Laptops | 8 |
| 9) Smartphones | 2 |

Devices used in the network

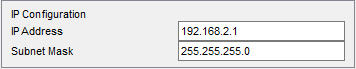
1. **Configuring IP Addresses**

screenshots of all the IP configuration below:

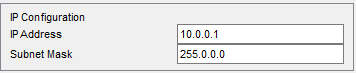
* Main Router configuration



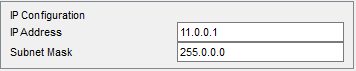
GigabitEthernet0/1



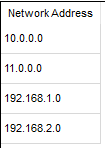
Serial0/1/0



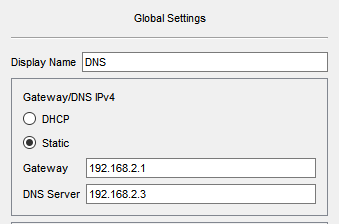
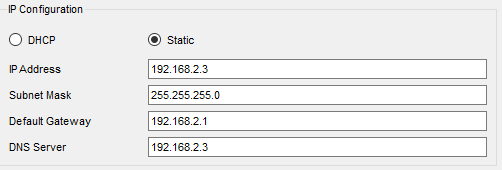
Serial0/1/1



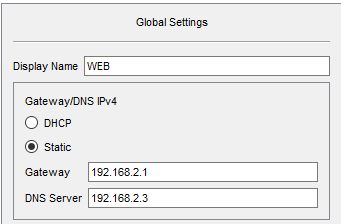
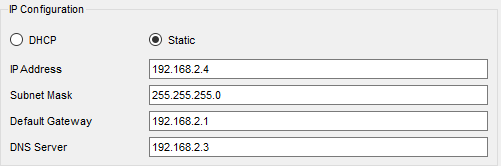
RIP



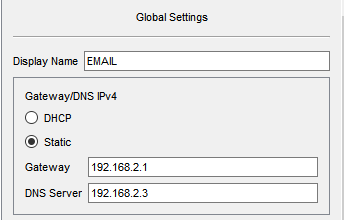
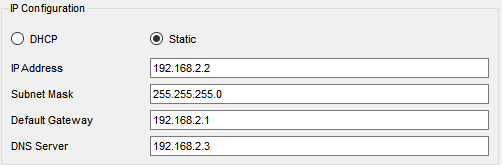
* DNS SERVER



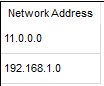
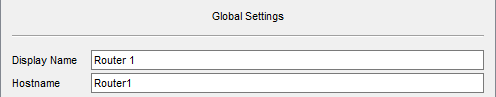
* WEB SERVER



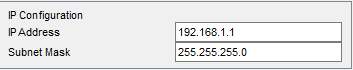
* EMAIL SERVER



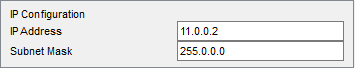
* ROUTER 1



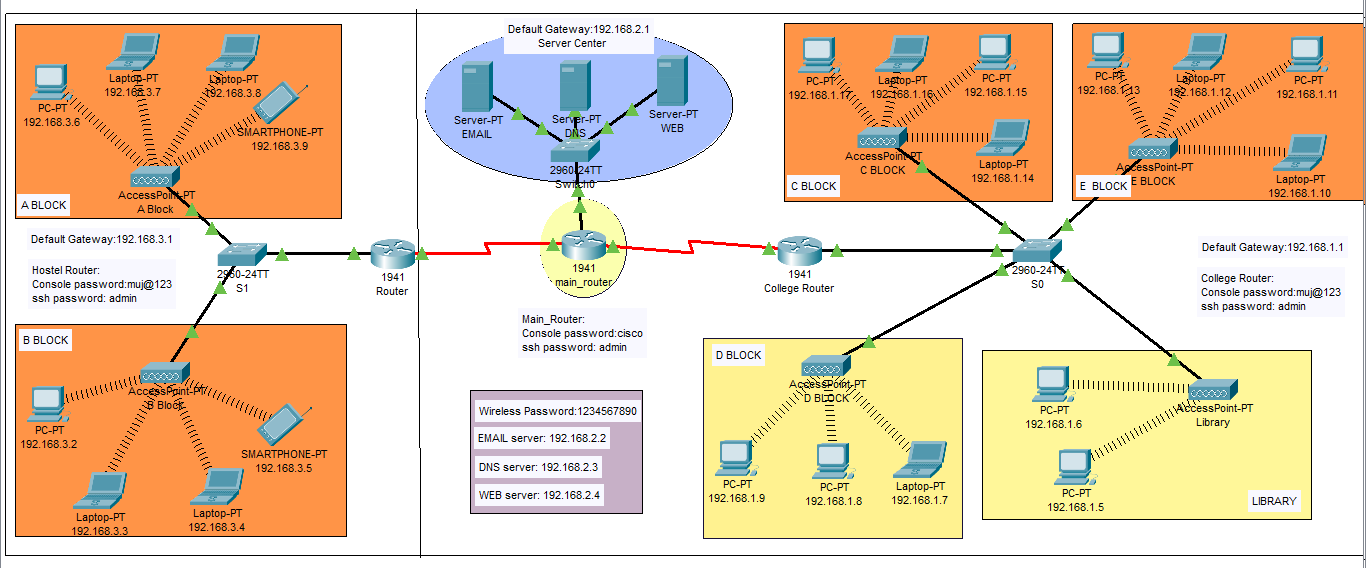
GigabitEthernet0/0



Serial0/1/0



* C BLOCK



IP Address are as follows

192.168.1.14- Laptop

192.168.1.15- PC

192.168.1.16- Laptop

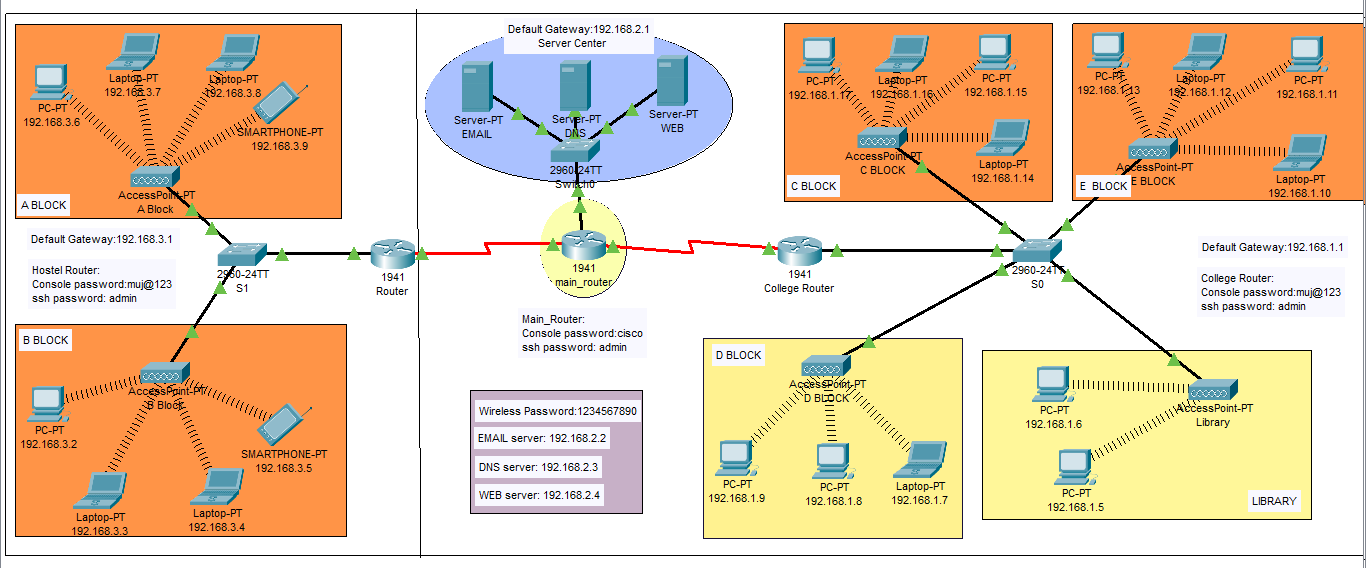
192.168.1.17- PC

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

* E BLOCK



IP Address are as follows

192.168.1.10- Laptop

192.168.1.11- PC

192.168.1.12- Laptop

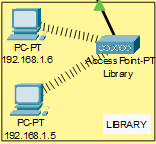
192.168.1.13- PC

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

* LIBRARY



IP Addresses are as follows

192.168.1.5- PC

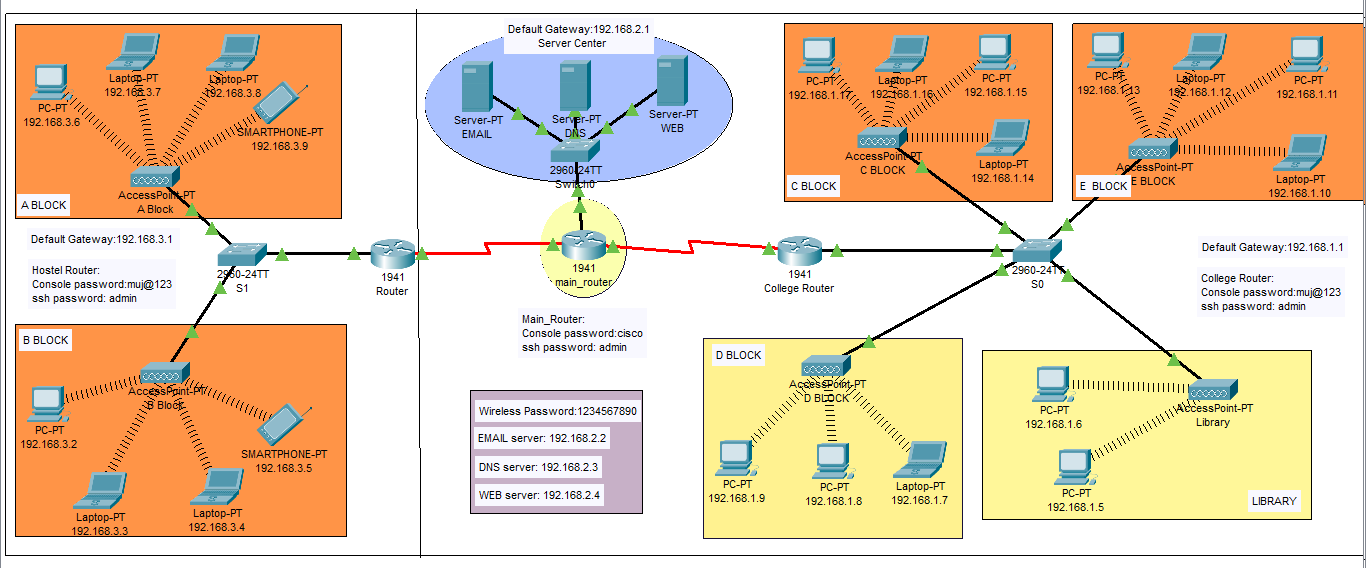
192.168.1.6- PC

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

* D BLOCK



IP Addresses are as follows

192.168.1.7- Laptop

192.168.1.8- PC

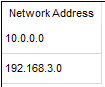
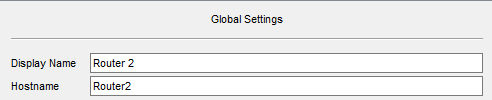
192.168.1.9- PC

Subnet Mask- 255.255.255.0

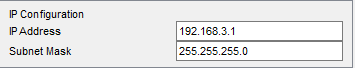
Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

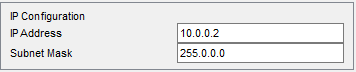
* ROUTER 2



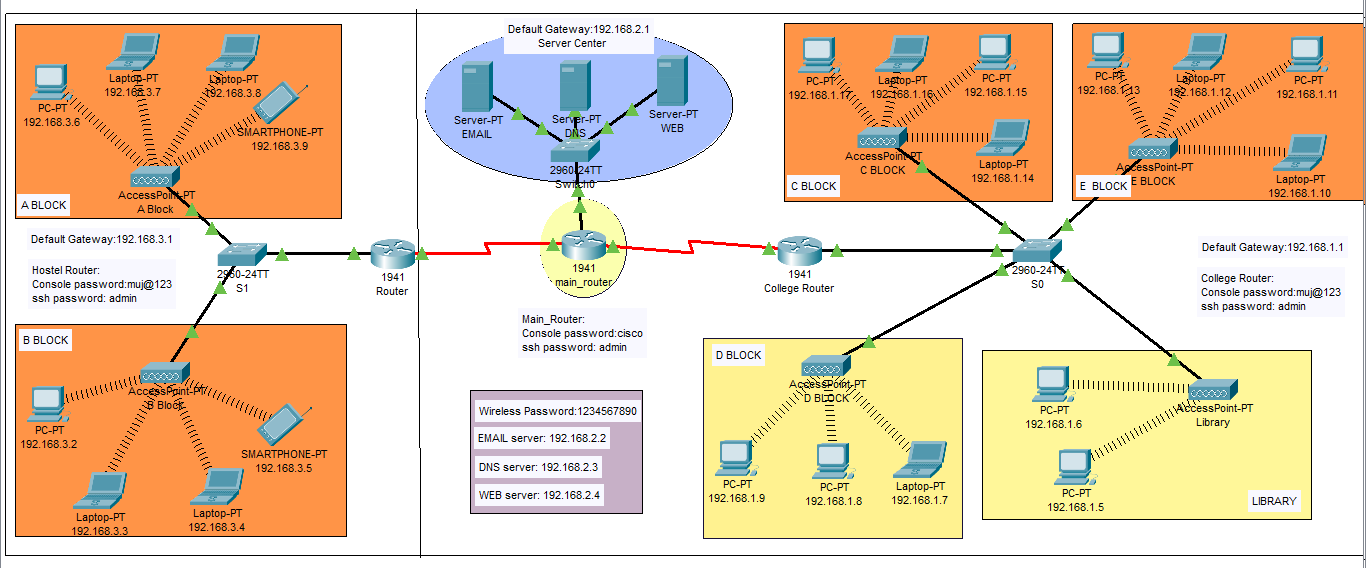
GigabitEthernet0/0



Serial0/1/0



* A BLOCK



IP Addresses are as follows

192.168.3.6- PC

192.168.3.7-Laptop

192.168.3.8- PC

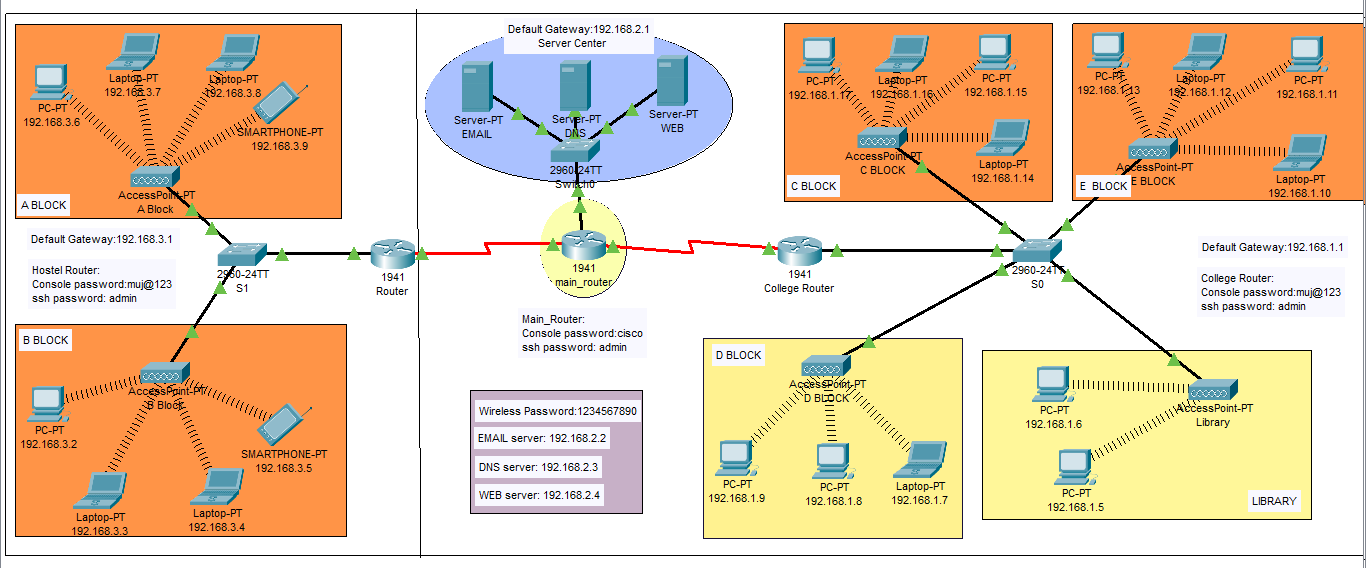
192.168.3.9- Smartphone

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.3.1

DNS Server- 192.168.2.3

* B BLOCK



IP Addresses are as follows

192.168.3.2- PC

192.168.3.3-Laptop

192.168.3.4- PC

192.168.3.5- Smartphone

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.3.1

DNS Server- 192.168.2.3

* WIRELESS ACCESS POINT

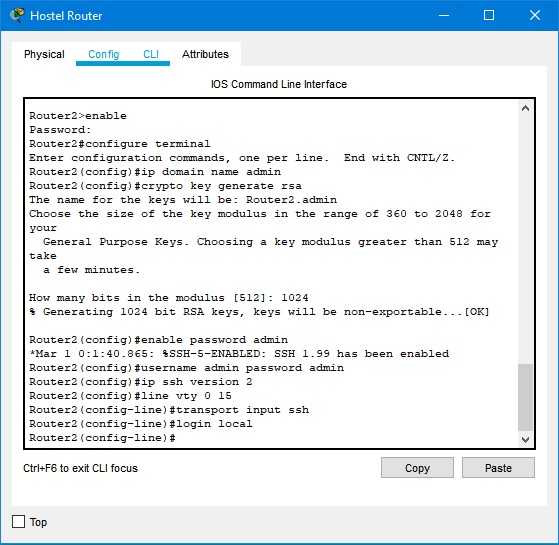
|  |  |
| --- | --- |
| SSID | Password |
| muj\_library | 1234567890 |
| muj\_D | 1234567890 |
| muj\_C | 1234567890 |
| muj\_E | 1234567890 |
| muj\_A | 1234567890 |
| muj\_B | 1234567890 |

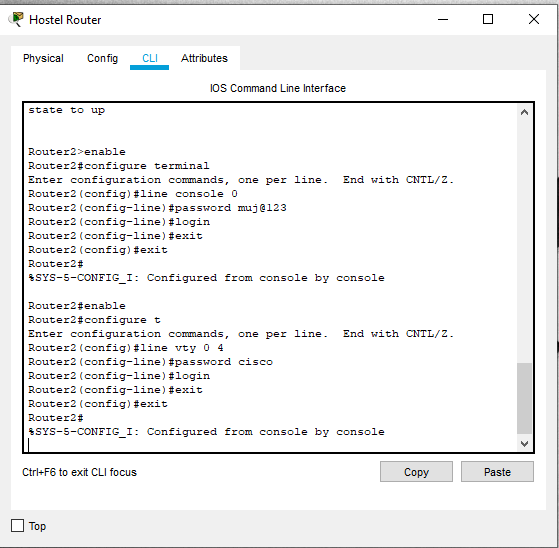
1. **Securing the network**

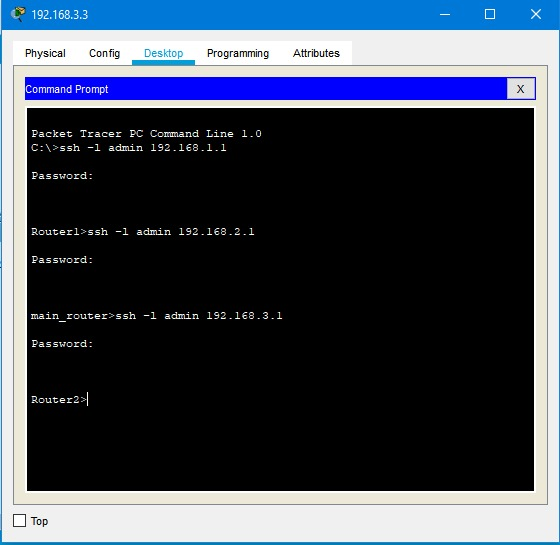
Passwords are used in accessing the router and all the wireless networks to make the access limited to College authorized users only.

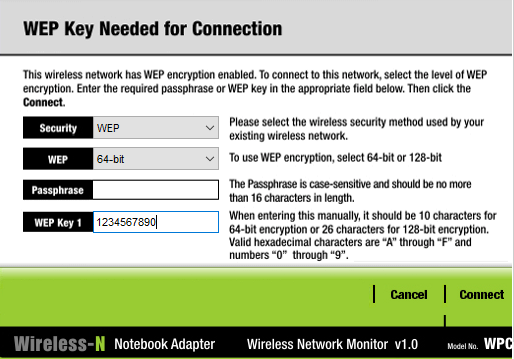
Routers are also secured with ssh (Secure Shell). Routers and their assigned passwords are mentioned below:

|  |  |
| --- | --- |
| Router Name | Passwords |
| 1. main\_router | Console password: cisco  ssh password: admin |
| 2. Router 1 | Console password:muj@123  ssh password: admin |
| 3. Router 2 | Console password:muj@123  ssh password: admin |









**Connectivity of wireless network on computing devices**

## Part-II: Security Assessment Report and Countermeasures

**1. Introduction**

This security assessment report aims to identify potential security risks and propose appropriate solutions and countermeasures to mitigate attack surface risks within the network configuration. The report covers the assessment of the C BLOCK, E BLOCK, LIBRARY, D BLOCK, ROUTER 2, A BLOCK, B BLOCK, and WIRELESS ACCESS POINT segments.

1. **Identified Security Risks**

**2.1** **Network Segmentation**

The IP address configuration reveals that multiple segments, such as C BLOCK, E BLOCK, LIBRARY, and D BLOCK, are all on the same subnet (192.168.1.0/24). This lack of proper network segmentation poses a significant risk, as an attack on one device within any of these segments could potentially compromise the entire subnet.

**2.2 Default Gateway and DNS Server Configuration**

The default gateway and DNS server for all segments (C BLOCK, E BLOCK, LIBRARY, and D BLOCK) are set to 192.168.1.1 and 192.168.2.3, respectively. This centralized configuration could lead to a single point of failure, and an attacker could potentially manipulate the DNS settings to redirect network traffic to malicious servers.

**2.3 Password Security**

While passwords are used to secure the wireless networks and routers, some of the passwords used are weak and susceptible to brute-force attacks. Additionally, the router console passwords for "Router 1" and "Router 2" are the same, which increases the risk if one of the routers is compromised.

**2.4 Lack of Network Monitoring and Intrusion Detection**

There is no mention of any network monitoring or intrusion detection systems in place. Without these security measures, the network remains vulnerable to both internal and external threats, and potential attacks may go unnoticed for an extended period.

**3. Proposed Solutions and Countermeasures**

**3.1 Network Segmentation**

To enhance security, it is recommended to implement proper network segmentation by dividing the network into smaller subnets based on user roles, departmental needs, or security requirements. Each segment should have its own subnet, which would limit the impact of an attack on a single device or segment.

**3.2 Default Gateway and DNS Server Configuration**

To reduce the risk of a single point of failure, it is advised to distribute the default gateway and DNS server configuration across multiple servers or devices. Redundancy and load balancing can be introduced to ensure uninterrupted network connectivity and name resolution.

**3.3 Password Security**

To improve password security, the following measures are suggested:

- Enforce the use of strong and complex passwords for all devices, wireless networks, and routers.

- Implement multi-factor authentication (MFA) for accessing critical devices and systems.

- Regularly update and change passwords to prevent unauthorized access.

**3.4 Network Monitoring and Intrusion Detection**

Deploy a robust network monitoring and intrusion detection system to actively monitor network traffic for suspicious activities. This will help identify potential threats, attacks, and unauthorized access attempts promptly, enabling timely responses to mitigate risks.

**4. Connectivity of Wireless Network on Computing Devices**

Ensure that all computing devices connected to the wireless networks (muj\_library, muj\_D, muj\_C, muj\_E, muj\_A, muj\_B) are adequately secured with strong passwords. Additionally, consider implementing WPA3 encryption for enhanced wireless security.

**5. Conclusion**

In conclusion, the current network configuration exposes several security risks that should be addressed promptly to protect the network and its assets from potential cyber threats. Implementing the proposed solutions and countermeasures will significantly improve the security posture and reduce the attack surface risks.