Cisco VIP 2024

Name of Main applicant	**:**	**Harshal Jagannath Jagdale**
PRN	**:**	**202301070191**
AICTE CISCO internship registration no.	**:**	**STU664634077e57d1715876871**
Networking Academy ID	**:**	**1059424142**
Mob No	**:**	**+91 90758 25191**
College Email ID	**:**	**202301070191@mitaoe.ac.in**
Professional Email ID	**:**	**harshaljagdale1747@gmail.com**

Cyber Shield: Defending the network

Problem Statement :-

Your College is hosting the Student and Faculty Details in Private Server within the Premise. Few more Branch of Colleges are now opening, and you are required to leverage the Cloud Services to host and manage the Student and Faculty details, securely in a central location for all Branches. Please Note, College wants to offload the management and maintenance of the Servers. Using your Netacad Cloud Security Course, design the DB hosting service, which is resilient, fast, On-Demand Scalable and Secure.

PART 1 :-

Analyse your existing university/college campus network topology. Map it out the using Cisco Packet Tracer and identify the security controls that are in place today. Consider and note how network segmentation is done. Observe what kind of intrusion detection systems, firewalls, authentication and authorization systems are in place. Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping. Aim to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

MADE BY: HARSHAL J JAGDALE 1059424142

Tasks :-

1. Campus Network Analysis: Conduct an analysis of your college campus 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.
3. Attack Surface Mapping: Conduct an attack surface mapping exercise to identify potential vulnerabilities and weaknesses within the network architecture and design. Consider factors such as unauthorized access, data breaches, and network availability.

Deliverables :-

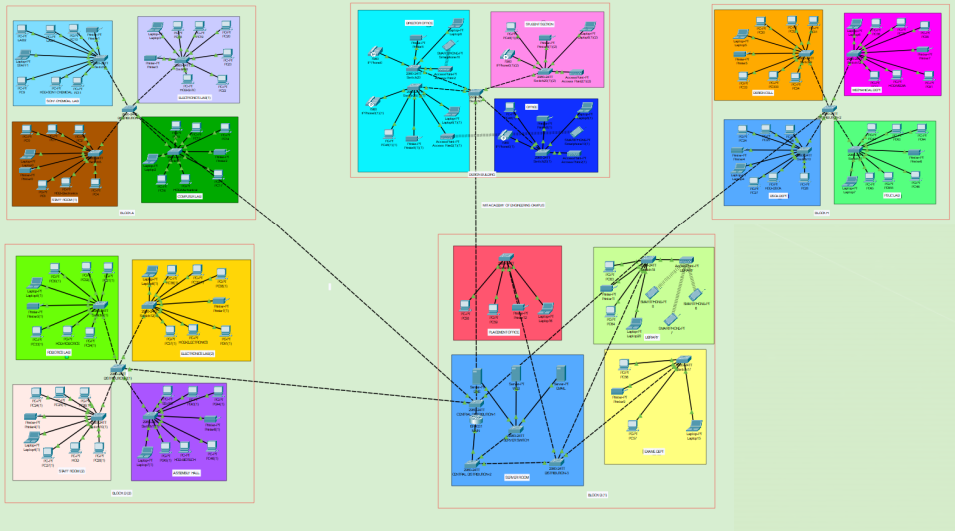
1. Network topology diagram depicting the existing infrastructure and attack surface findings.
2. Security assessment report highlighting identified security risks, proposed solutions and countermeasures to mitigate attack surface risks.

MADE BY: HARSHAL J JAGDALE 1059424142

1. Campus Network Analysis :-

Network Layout :-

There is a network layout in place which has a well-organized way of connecting various network devices such as switches, routers, access points, firewalls, computers and servers across different buildings in the campus.



MADE BY: HARSHAL J JAGDALE 1059424142

Configured Devices :-

Routers : Are placed strategically to ensure that data flow between networks can be managed.
Switches : Act as mediators within the network segments so that data exchange can happen.
Access points : Provide wireless services all over the campus
Firewalls : Protect the edges of networks.
Computers : Are split into students' and faculty's member.
Servers : Used for Web, Email, DNS, Database and Backup services.
Connections : All devices are connected using high-speed ethernet cables and wireless protocols

2. Network Mapping Using Cisco Packet Tracer :-

Attached Harshal_CyberSecurity.pkt file Where I have made the Network Mapping of my University MIT AOE Using Cisco Packet Tracer

3. Attack Surface Mapping :-

Identification of Vulnerabilities :

- Open Ports: Identify and assess the necessity of open ports on routers and switches, recommending closures or security enhancements where needed.
- Weak Passwords: Audit all devices for weak or default passwords and enforce a strict password policy.
- Encryption Gaps: Evaluate the encryption methods used for data in transit and at rest, proposing upgrades to more secure protocols where necessary.
- Outdated Firmware: Check for outdated firmware versions that may expose the network to security risks and plan for regular updates.

Potential Entry Points for Cyber-Attacks:

- Wireless Access Points: Ensure all wireless connections are secured with WPA2 or WPA3 encryption to prevent unauthorized access.
- Web Servers: Update and secure all public-facing web servers to mitigate the risk of cyberattacks.
- Shared Passwords: Implement policies to prohibit password sharing and encourage the use of personal credentials.
- Physical Security: Enhance physical security measures to prevent unauthorized physical access to critical network infrastructure.

MADE BY: HARSHAL J JAGDALE 1059424142

Proposed Solutions and Countermeasures :

To robustly secure our university's network and address the identified vulnerabilities, we recommend the following specific technological and procedural countermeasures :

- Technological Upgrades :

  Update and Patch Management Implement a centralized patch management system to ensure all network devices, including routers, switches, and servers, are always updated with the latest security patches.

- Strengthen Password Security :

  Enforce a strict password policy that requires complex passwords combining letters, numbers, and special characters. Implement MFA(Multi-Factor Authentication) across all systems, especially for administrative access and remote connections.

- Enhance Network Encryption:

  Deploy end-to-end encryption for data in transit using protocols such as TLS(Transport Layer Security) and SSL(Secure Sockets Layer). Ensure that sensitive data stored on servers is encrypted at rest using robust encryption standards.

MADE BY: HARSHAL J JAGDALE 1059424142

- Secure Wireless Networks:
  Upgrade all wireless networks to use WPA3 encryption. Regularly audit and restrict the use of legacy wireless equipment or protocols that do not support the latest security standards.

- Advanced Intrusion Detection and Prevention Systems (IDPS):
  Deploy sophisticated IDS/IPS solutions that can detect and respond to both known and emerging threats. Regularly update IDS/IPS signatures and monitor network traffic for anomalies.

- Firewall Optimization:
  Review and reconfigure firewall rules to minimize unnecessary open ports and to segment the network effectively, restricting traffic between critical network segments.

- Regular Security Audits and Penetration Testing:
  Schedule annual third-party security audits and regular penetration testing to identify and remediate vulnerabilities before they can be exploited.

MADE BY: HARSHAL J JAGDALE 1059424142

- Security Training and Awareness Programs:

  Conduct ongoing security training sessions for all university staff and students, focusing on the importance of security best practices, recognizing phishing attempts, and secure handling of sensitive information.

- Incident Response Planning:

  Develop and regularly update an incident response plan that includes clear procedures and roles for responding to cybersecurity incidents. Conduct simulated cyberattack exercises to ensure all team members understand their responsibilities during an incident.

- Physical Security Measures:

  Improve physical security controls to protect network infrastructure from unauthorized physical access, including surveillance systems, access controls, and secure locking mechanisms for server rooms and data centers.

MADE BY: HARSHAL J JAGDALE 1059424142

Conclusion :-

The implementation of these proposed solutions and countermeasures is crucial for safeguarding our university's network against potential cyber threats. As digital threats continue to evolve in complexity and severity, the proactive enhancement of our network's security infrastructure and policies is not merely beneficial but essential. These measures will not only protect sensitive academic data but also safeguard the personal information of our students and staff, thereby maintaining the trust and integrity of our institution. Adopting these recommendations will fortify our defenses and ensure that our network remains resilient against cyber threats, supporting our ongoing commitment to providing a secure and reliable digital environment for all educational activities.

MADE BY: HARSHAL J JAGDALE 1059424142

PART 2 :-

Your college has hired you to design and architect a hybrid working environment for its faculty and students. Faculty members will be provided with laptops by the college to connect to the college network and access faculty specific services & resources. These should be accessible from home as well as on campus. Students are allowed to connect using their personal devices to access student specific services & resources from home as well as on campus. Campus network services should not be exposed to public internet and accessible only via restricted networks.

Tasks & Deliverables :-

1. Explore options for how to achieve this and what kind of network security product can provide this capability
2. Update the campus network topology with the new components
3. Explain the reasoning behind your choices detailing the risks & advantages of your proposed solution
4. Write the policies you would apply (can use simple English language commands)

MADE BY: HARSHAL J JAGDALE 1059424142

Solution :-

1. Explore Options for Network Security Products:

Products and Technologies:

1. Virtual Private Network (VPN) :-
    - Product Example: Cisco AnyConnect Secure Mobility Client.
    - Use: Securely connects faculty and students to the college network from remote locations by encrypting traffic and using strong authentication methods.

2. Network Access Control (NAC) :-
    - Product Example: Cisco Identity Services Engine (ISE)
    - Use: Manages and enforces security compliance on all devices that access the network, ensuring that only authorized devices can access specific resources.

MADE BY: HARSHAL J JAGDALE 1059424142

3. Multi-Factor Authentication (MFA) :-

    - Product Example: Duo Security.
    - Use: Adds an additional layer of security by requiring two or more verification methods to gain access to the network, reducing the risk of unauthorized access.

4. Cloud Access Security Broker (CASB) :-

    - Product Example: Cisco Cloud lock.
    - Use: Protects data in cloud services and ensures that only authorized users can access sensitive information remotely.

MADE BY: HARSHAL J JAGDALE 1059424142

Updating the Campus Network Topology :-

New Components :-

1. VPN Gateways:
   Placement: Deployed at the network perimeter to handle incoming VPN connections securely.

2. NAC Solutions:
   Placement: Integrated with the network infrastructure to monitor and control access at various network access points.

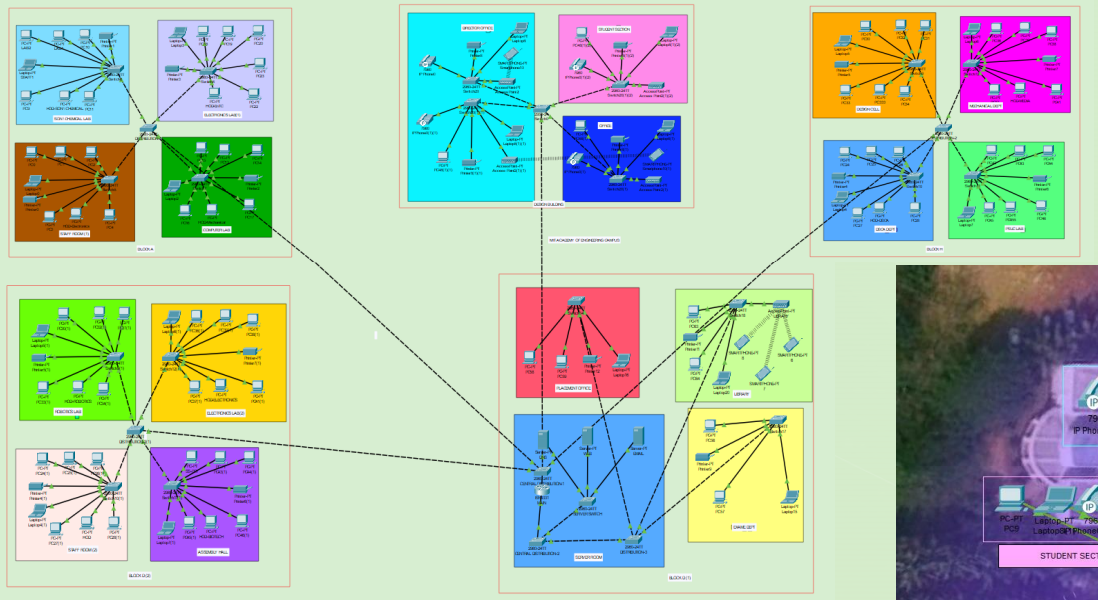
3. MFA Systems:
   Integration: Across all user access points to the network, including initial login portals and cloud-based services access.

4. CASB Systems:
   Placement: Deployed between the organization’s on-premises infrastructure and the cloud provider’s infrastructure to enforce security policies when accessing cloud-based resources.

MADE BY: HARSHAL J JAGDALE 1059424142

Updated Network Topology Diagram :-

The diagram will include the newly added VPN gateways, NAC appliances, and points of MFA integration, demonstrating the comprehensive approach to securing remote access.



MADE BY: HARSHAL J JAGDALE 1059424142

Risks & Advantages :-

1. VPN :
   - Risks: Potential for decreased network performance due to encryption overhead.
   - Advantages: Provides secure remote access, encrypts data in transit, and effectively extends the network perimeter in a controlled manner.
2. NAC :
   - Risks: Complex configuration and maintenance.
   - Advantages: Ensures that only compliant and authorized devices can connect to the network, significantly reducing the risk of infected devices compromising the network.
3. MFA :
   - Risks: User resistance due to added complexity in the login process.
   - Advantages: Greatly enhances security by mitigating the risk of compromised passwords leading to unauthorized access.
4. CASB :
   - Risks: Can be resource-intensive in terms of monitoring and managing cloud access.
   - Advantages: Provides visibility and control over data in the cloud, ensuring compliance and data security across remote access scenarios.

MADE BY: HARSHAL J JAGDALE 1059424142

Conclusion :-

Implementing these technologies will create a robust hybrid working environment that supports the dynamic needs of faculty and students. It ensures secure and controlled access to network resources from both on-campus and remote locations, while maintaining compliance with security policies and protecting against potential cyber threats. This design not only meets the current needs but is scalable for future expansion and integration with emerging technologies. This comprehensive plan provides the necessary details to implement a secure and efficient hybrid working environment tailored to the unique requirements of the academic setting, ensuring security, flexibility, and compliance.

MADE BY: HARSHAL J JAGDALE 1059424142

PART 3 :-

The college has discovered that students are misusing campus resources and accessing irrelevant sites. They want a solution which will restrict access to only allowed categories of web content.

Tasks & Deliverables :-

1. Explore how this can be achieved and what kind of network security product can provide this capability.
2. Update the campus network topology with new component(s)
3. Explain the reasoning behind your choice, detailing the risks & advantages of your proposed solution
4. Write the policies you would apply (can use simple English language commands)

MADE BY: HARSHAL J JAGDALE 1059424142

Solution :-

Explore Options for Network Security Products

Products and Technologies :

1. Web Content Filtering Solutions :
    - Product Example: Cisco Umbrella
    - Use: Provides DNS-based security by blocking access to websites based on categories, security risks, or specific URLs, ensuring that only approved content is accessible.

2. Firewall with Integrated Security Services :
    - Product Example: Cisco Firepower
    - Use: Offers capabilities such as URL filtering, malware detection, and intrusion prevention, which can be configured to enforce web access policies.

MADE BY: HARSHAL J JAGDALE 1059424142

Updating campus network topology

New Components

1. Cisco Umbrella:
    - Placement: Integrated at the DNS layer to filter internet traffic and prevent access to non-approved websites before a connection is even established.

2. Cisco Firepower:
    - Placement: Deployed alongside existing firewalls to enhance security with deep packet inspection and real-time threat intelligence.

Updated Network Topology Diagram:

They will include Cisco Umbrella for DNS filtering and Cisco Firepower for enhanced firewall protection, showing their integration points within the existing network infrastructure.

MADE BY: HARSHAL J JAGDALE 1059424142

Risks & Advantages:

1. **Cisco Umbrella:**

    - Risks: Over blocking can occur, where legitimate educational sites might be inadvertently blocked if not properly categorized.

    - Advantages: Provides a first line of defense at the DNS layer, which is effective in preventing access to unwanted sites quickly and efficiently.

2. **Cisco Firepower:**

    - Risks: May require significant resources to manage and maintain, especially with frequent updates and policy changes.

    - Advantages: Offers comprehensive network protection that extends beyond URL filtering to include threat detection and response capabilities.

MADE BY: HARSHAL J JAGDALE 1059424142

Sample Policies for Web Content Filtering :-

1. Block Access to Non-Educational Entertainment Sites:

   Deny access to categories "Entertainment, Gaming, Social Media" during school hours

2. Allow Educational and Research-Related Websites:

   Allow access to categories "Education, Research" at all times. And allow student to access some use full web side for study

3. Restrict Certain High-Bandwidth Activities:

   Deny access to categories "Streaming Media, File Sharing" except during non-school hours using this we can avoid to leaks of important files

4. Custom Rules for Specific Needs:

   Allow access to "youtube.com/edu" for educational videos; deny "youtube.com/watch" .block websites categorized under "Adult Content, Gambling" at all times

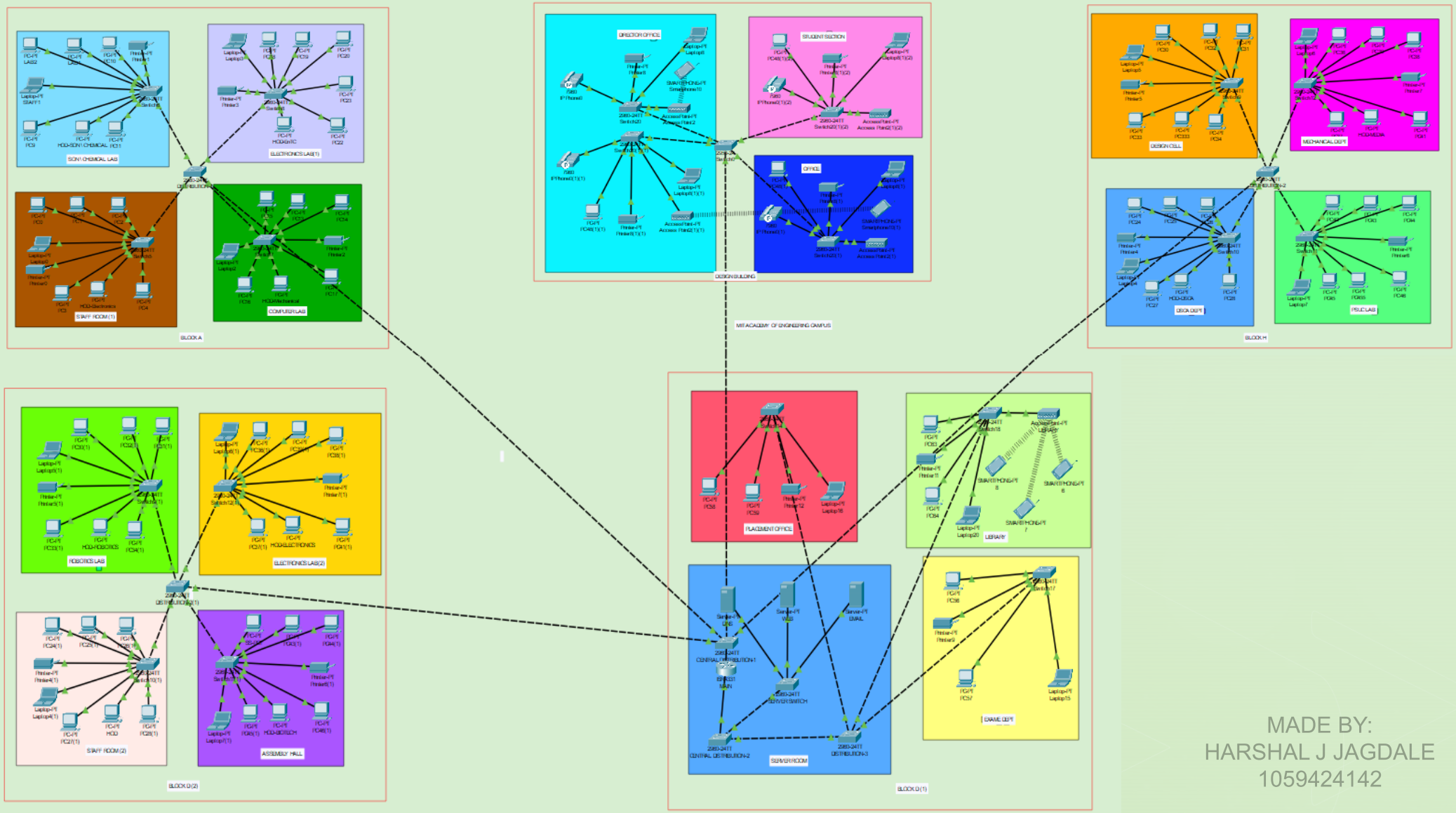
MADE BY: HARSHAL J JAGDALE 1059424142

Conclusions :

The deployment of Cisco Umbrella alongside Cisco Firepower will enable the college to effectively manage and monitor web traffic, ensuring that only content relevant to educational and research activities is accessible. This solution not only maximizes network resource utilization but also fosters a safer and more productive educational environment. By implementing these comprehensive content filtering measures, the college can maintain control over its network usage and prevent misuse, aligning technology use with educational goals and policies.

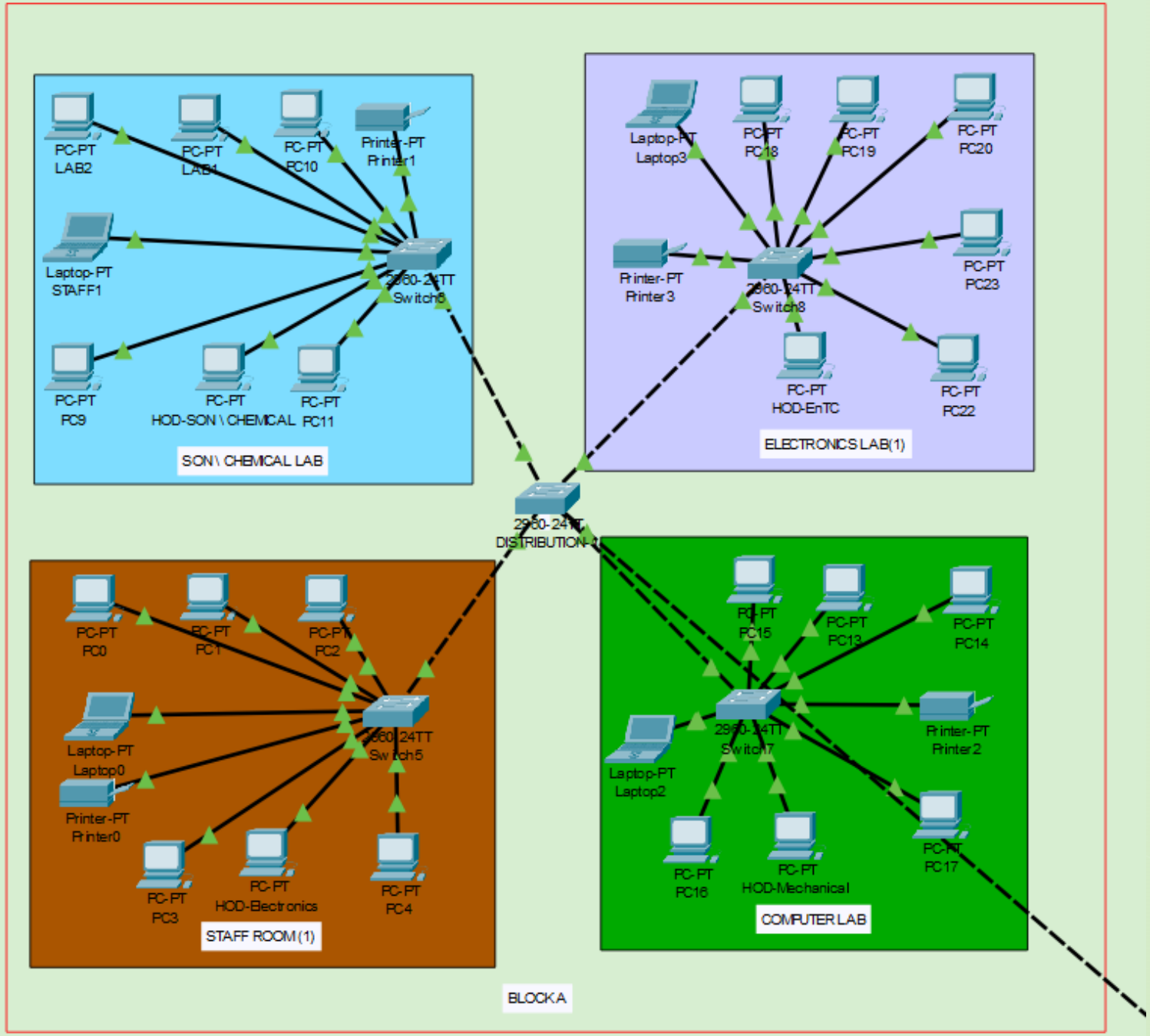
MADE BY: HARSHAL J JAGDALE 1059424142

Logical Diagram Of Cisco Packet Tracer :-

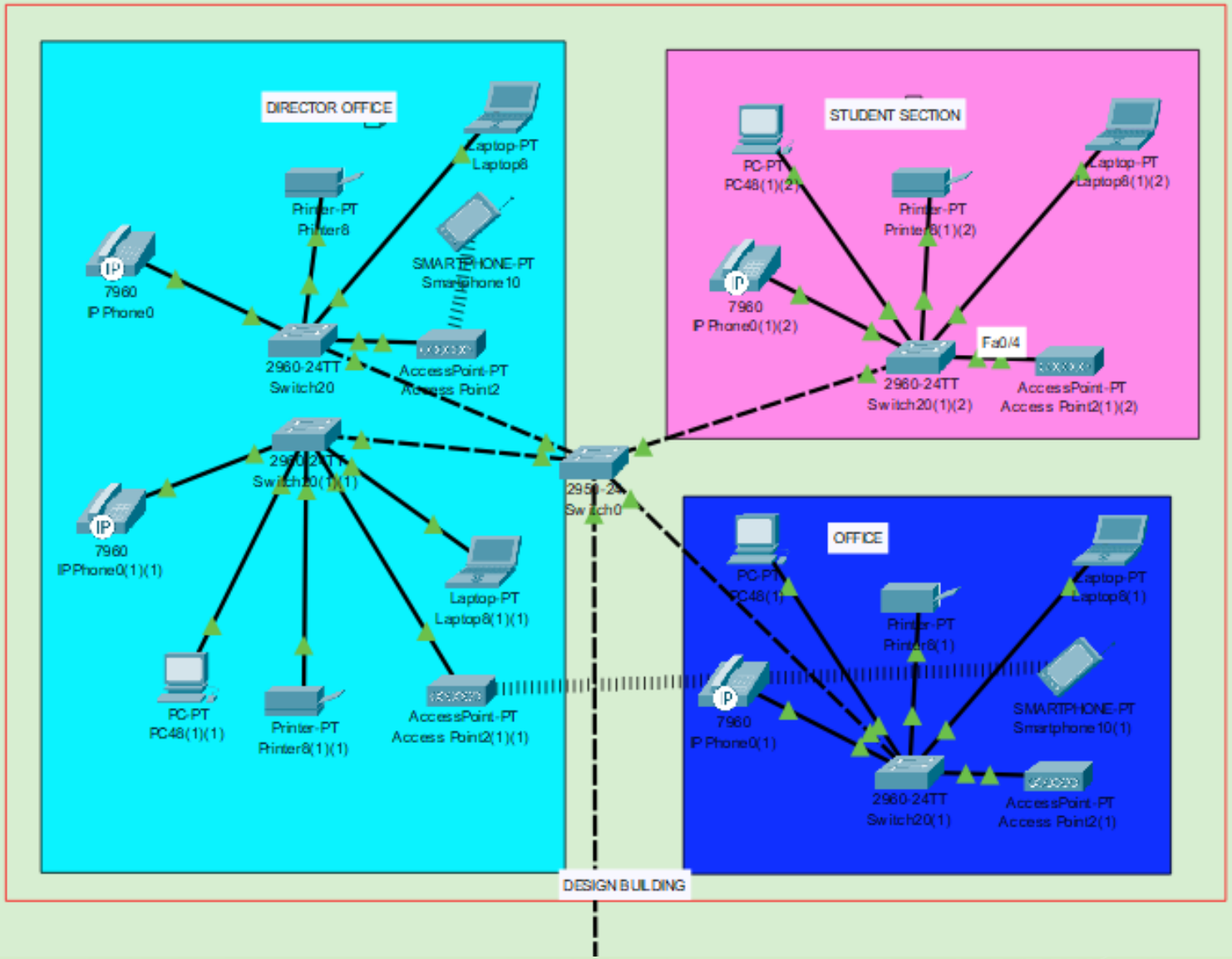


MADE BY:
HARSHAL J JAGDALE
1059424142

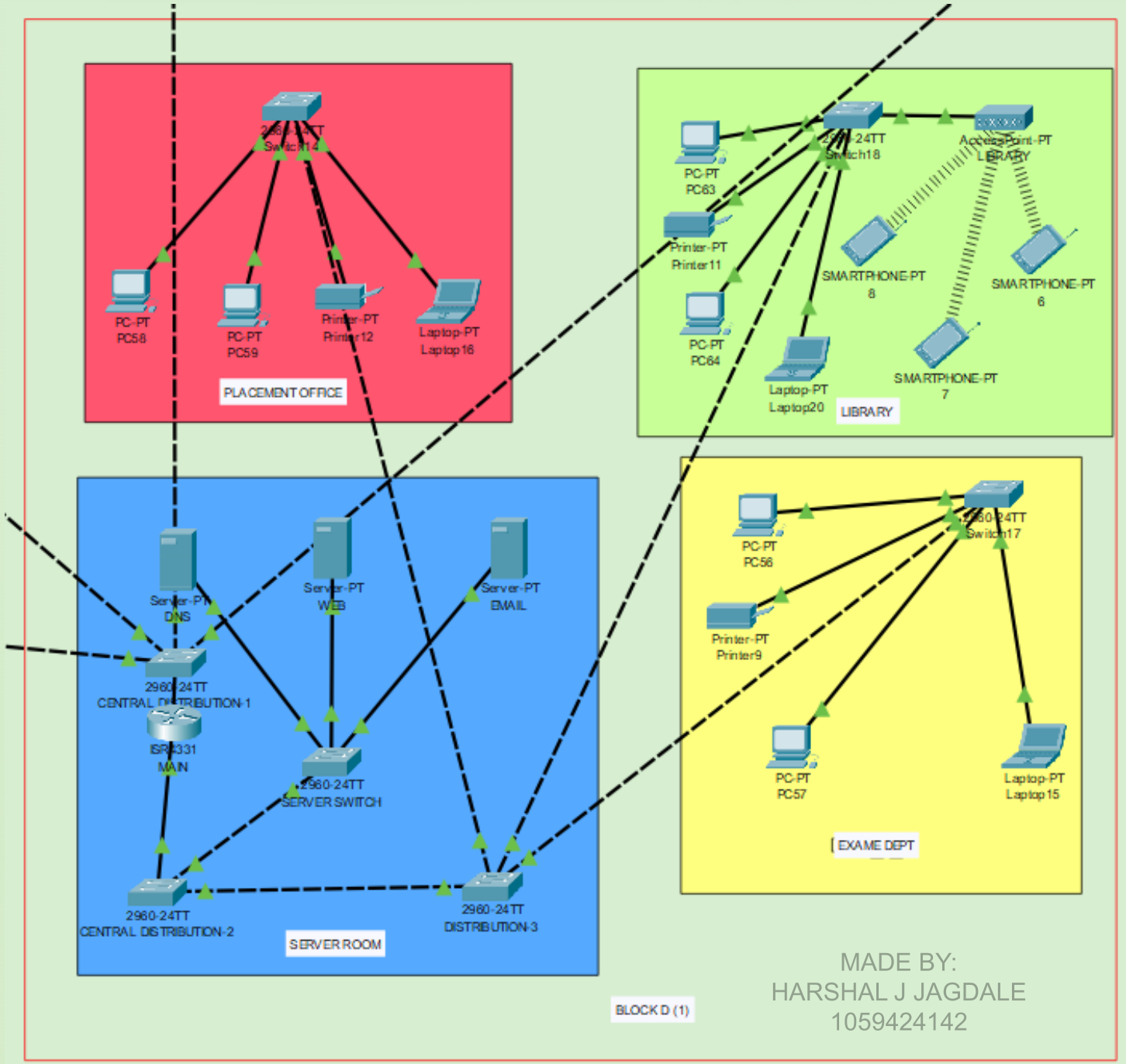
MADE BY: HARSHAL J JAGDALE 1059424142



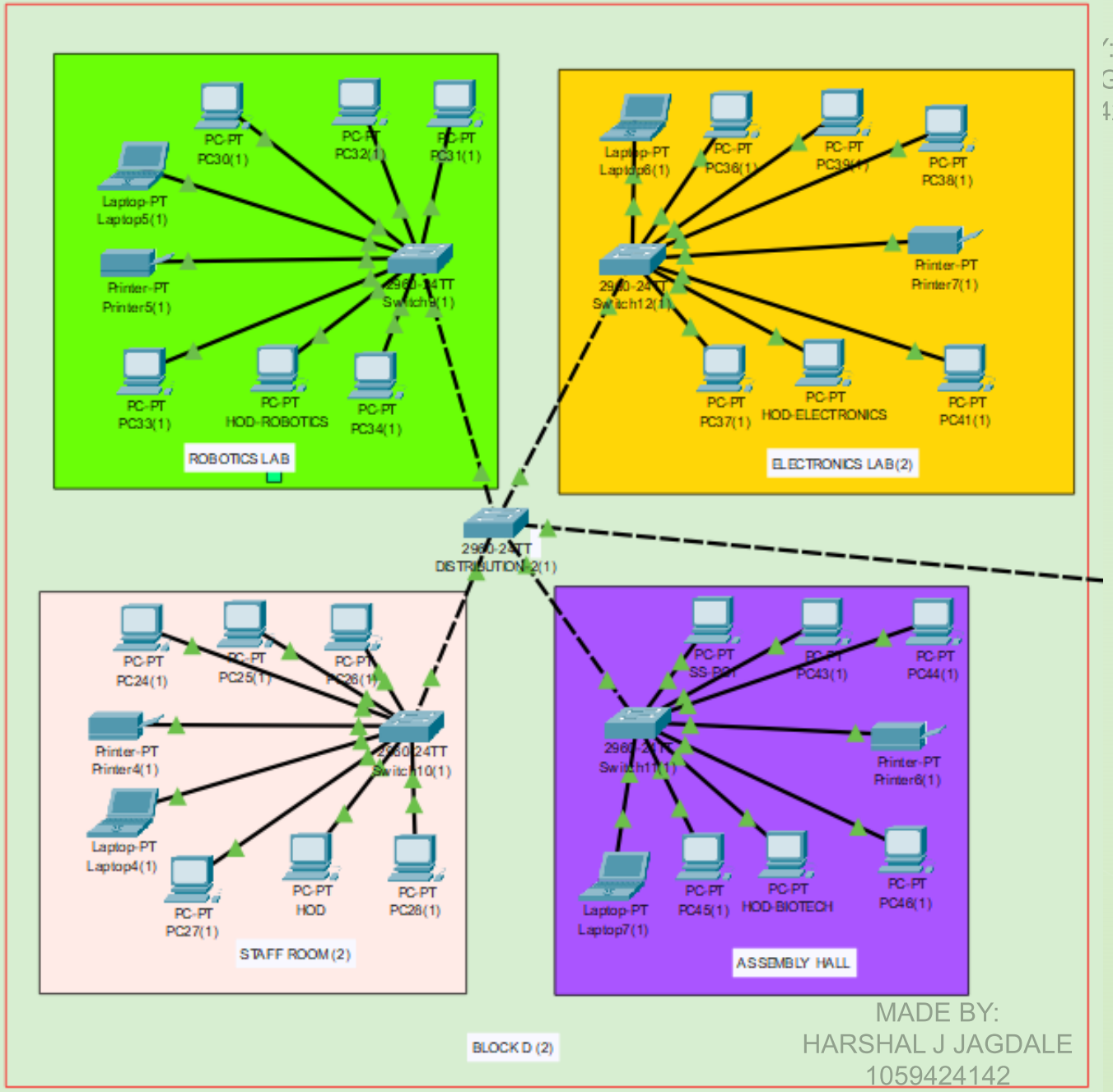
MADE BY: HARSHAL J JAGDALE 1059424142



MADE BY: HARSHAL J JAGDALE 1059424142

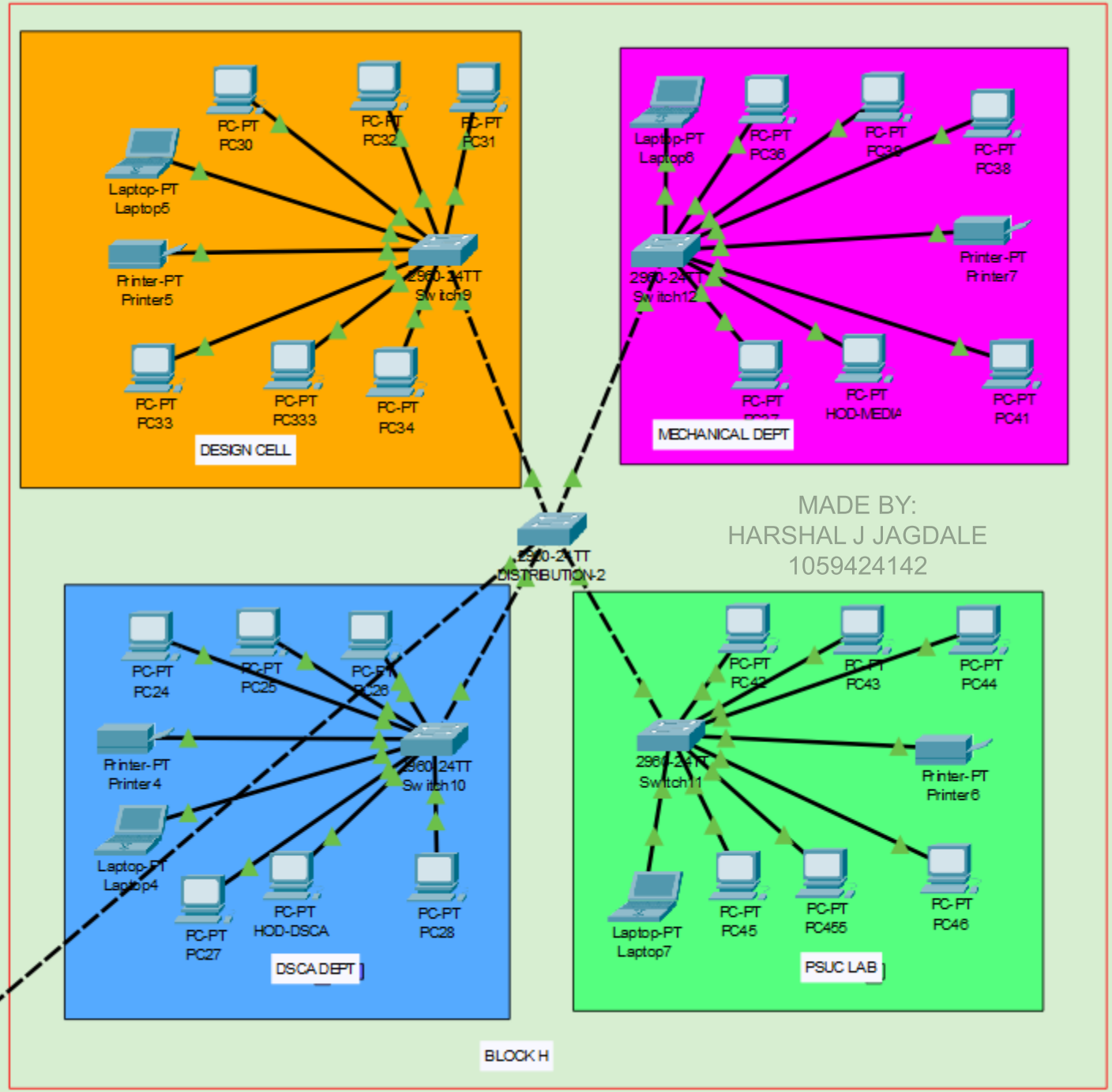


MADE BY: HARSHAL J JAGDALE 1059424142



MADE BY:
HARSHAL J JAGDALE
1059424142

MADE BY: HARSHAL J JAGDALE 1059424142



HA

MADE BY:
HARSHAL J JAGDALE
1059424142

MADE BY: HARSHAL J JAGDALE 1059424142

Physical Diagram Of Cisco Packet Tracer :-

MADE BY: HARSHAL J JAGDALE 1059424142

MADE BY: HARSHAL J JAGDALE 1059424142

Reference Site :-

- https://www.google.com
- https://www.netacad.com/portal/learning
- https://www.youtube.com
- https://www.netacad.com/courses/packet-tracer

MADE BY: HARSHAL J JAGDALE 1059424142

Google Drive Link :-

1. **Cisco Packet Tracer Design:-**

   https://docs.google.com/presentation/d/1Rkl7IkFZEm3rBUHgqqvf5WsX4va-8zsW/edit?usp=drive_link&ouid=100894033329763834488&rtpof=true&sd=true

2. **Cisco Internship Folder :-**

   https://drive.google.com/drive/folders/1IQSKQyuYHDDEtbZsyjTojHtSZdkAOiRQ?usp=drive_link

3. **Cisco Internship ppt :-**

   https://drive.google.com/file/d/1riboUsB7s_pUWWJQjd7dNlyExH1JuFlJ/view?usp=drive_link

MADE BY: HARSHAL J JAGDALE 1059424142