DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

CATEGORY - 1 UNIVERSITY BY UGC

Accredited “A++” by NAAC I Approved by AICTE

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600119

Cisco AICTE Virtual Internship Program 2024

A Cisco AICTE Virtual Internship project report on cyber security submitted in partial fulfillment of the requirements for the AICTE-CISCO virtual Internship in cyber security Program 2024

Submitted By : KARASANI BHARGAV REDDY

AICTE Internship Student Registration ID) : **STU662cefc912f511714221001**

Student ID (Enrolment number) : **42110580**

Email ID : **karasanibhargav@gmail.com**

Contact Info : **9381304121**

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.

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.

Solution:

Campus Network Analysis: A Friendly Tour

Overview

A college campus network serves as the backbone for communication, collaboration, and resource sharing among students, faculty, and staff. Understanding its structure and components is crucial for efficient operations and security.

Network Topology

- **Physical Layout:**
    - Identify key buildings, departments, and facilities. ○ Consider wired and wireless connections.
    - Map out the distribution of switches, routers, and access points.
- **Logical Topology:**
    - Common topologies include star, bus, ring, and mesh.
    - Evaluate scalability, redundancy, and fault tolerance.

2. **Network Mapping with Cisco Packet Tracer:**

Attached karasani Bhargav Reddy_CyberSecurity.pkt[**GIT HUB**]file Where I have made the Network Mapping of my Sathyabama University Chennai Using Cisco Packet Tracer o We've used our magical Packet Tracer to draw a colorful map:

⍰ **Routers:** Central hubs connecting different buildings.

⍰ **Switches:** They ensure messages find their way.

⍰ **Firewalls:** Guards checking who enters.

⍰ **ntrusion Detection Systems (IDS):** Our alert watchdogs.

⍰ **Authentication & Authorization:** Keys and permissions—only the right folks get in.

1. **Switches:**
    - Connect devices within a local area network (LAN). ○ Manage traffic flow and segment broadcast domains. ○ VLANs enhance security by isolating network segments.
2. **Routers:**

    - Interconnect LANs and provide access to external networks (e.g., the internet).
    - Implement routing protocols (e.g., OSPF, BGP).

3. **Access Points (APs):**
    - Enable wireless connectivity.
    - Secure with WPA3 encryption and strong passwords.
4. **Firewalls:**
    - Protect against unauthorized access.
    - Consider next-generation firewalls (NGFWs) for deep packet inspection.

Security Controls

1. **Network Segmentation:**
    - Divide the network into segments (e.g., academic, administrative, guest).
    - Isolate critical systems from less secure areas.
2. **Intrusion Detection Systems (IDS):**
    - Deploy IDS sensors to monitor network traffic.
    - Detect anomalies, suspicious behavior, and potential attacks.
3. **Firewalls and Access Control Lists (ACLs):** o Configure firewalls at network boundaries. o Use ACLs to control traffic flow.
    - Implement stateful inspection for better security.
4. **Authentication and Authorization:**
    - Use strong authentication methods (e.g., 802.1X, RADIUS).
    - Role-based access control (RBAC) ensures proper authorization**.**

Attack Surface Mapping

1. **Inventory:**
    - List all network assets (servers, switches, routers, APs).
    - Identify open ports, services, and software versions**.**

2. **Vulnerability Assessment:**
   - Scan for vulnerabilities (e.g., using tools like Nessus or OpenVAS).
   - Prioritize based on severity.
3. **Mitigation Strategies:**
   - Patch systems regularly. o Harden configurations (disable unnecessary services).
   - Implement network segmentation to limit lateral movement**.**

Deliverables

Network Topology Diagram:

Detailed representation of the existing infrastructure with labeled components and connections.

Security Assessment Report:

Document outlining identified security risks, proposed solutions, and countermeasures to mitigate attack surface risks.

This structured approach combines network analysis with cybersecurity principles to identify vulnerabilities and propose effective countermeasures. Actual implementation would require specific knowledge of the campus network infrastructure and current security controls in place.

Conclusion:

In conclusion, network attack surface mapping is a critical aspect of network security that involves identifying and analyzing potential vulnerabilities in a network infrastructure. By using tools like Cisco Packet Tracer, network administrators can design and simulate network topologies, identify potential weaknesses, and propose countermeasures to mitigate these risks. Implementing security controls such as network segmentation, firewalls, IDS systems, and strong authentication and authorization can help reduce the attack surface and ensure the security and integrity of the campus network.

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

Designing a Hybrid Working Environment for Faculty and Students

Solution:

In today's educational landscape, flexibility in accessing resources and services is crucial for both faculty members and students. This document outlines a comprehensive approach to design and architect a hybrid working environment for a college, accommodating the needs of faculty and students while ensuring network security and accessibility.

1. Exploration of Options and Network Security

Product Options for Access:

- Virtual Private Network (VPN): Implementing VPN technology allows secure remote access to campus resources for faculty and students alike. This ensures encryption of data transmitted over public networks.
- Remote Desktop Services: Faculty can utilize remote desktop services to securely access their college-provided laptops and resources located on campus.

- Cloud-based Services: Utilizing cloud platforms for hosting and accessing educational resources provides scalability and accessibility from anywhere.

Network Security Product:

- Next-Generation Firewall (NGFW): NGFWs provide advanced security features such as application-level filtering, intrusion prevention, and secure VPN connectivity.
- Endpoint Protection: Deploying endpoint protection software on faculty laptops and ensuring students have updated antivirus software on their personal devices.
- Network Access Control (NAC): Implementing NAC to ensure that only authorized devices and users can access the college network, whether on campus or remotely.

2. Updated Campus Network Topology Components:

- Core Network: Includes high-speed switches and routers connecting campus buildings and data centers.
- Distribution Layer: Manages traffic between different departments or sections of the campus.
- Access Layer: Provides connectivity for end-user devices, including faculty laptops and student personal devices.
- Security Perimeter: NGFWs and VPN gateways placed at the network edge to control access and protect against external threats. **3. Reasoning Behind Design Choices Advantages:**
- Flexibility: Faculty can securely access resources from home or on campus using VPN or remote desktop services.
- Cost Efficiency: Leveraging cloud services reduces the need for extensive on-premises infrastructure.
- Security: NGFWs and VPNs ensure encrypted communication and protect against unauthorized access and cyber threats.
- User Experience: Students benefit from seamless access to educational resources using their personal devices, enhancing productivity.

Risks:

- Security Vulnerabilities: Potential vulnerabilities in VPN configurations or endpoint devices could be exploited.
- Network Performance: Depending on VPN bandwidth and cloud service availability, performance issues may arise during peak usage times.

- User Compliance: Ensuring faculty and students adhere to security policies, such as keeping devices updated and secure, is crucial.

4. Detailed Implementation Plan

Steps:

- Assessment: Conduct a thorough assessment of current network infrastructure and security posture.
- Design: Create a detailed network architecture plan integrating VPN, NGFW, and cloud services.
- Implementation: Deploy necessary hardware and software components while configuring security policies and access controls.
- Testing: Conduct comprehensive testing to ensure functionality, security, and performance meet expectations.
- Training: Provide training sessions for faculty and students on using VPNs securely and adhering to security best practices.

5. Conclusion

Designing a hybrid working environment for faculty and students requires a balanced approach that prioritizes accessibility, security, and usability. By leveraging VPN technology, NGFWs, and cloud services, the college can ensure secure access to resources from any location while protecting against cyber threats. A well-designed network architecture supports the educational mission of the college and enhances the overall learning experience for both faculty and students.

References

- Industry best practices in network security and remote access technologies.
- Vendor documentation for VPN solutions, NGFW configurations, and cloud service providers.
- Security guidelines from educational institutions and regulatory bodies. This comprehensive approach to designing a hybrid working environment ensures the college meets its goals of providing secure, flexible access to resources for faculty and students while maintaining robust network security practices.

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)

Solution:

Restricting Access to Allowed Web Content Categories

The college has identified an issue with students misusing campus resources and accessing irrelevant sites. To address this, a solution is needed to restrict access to only allowed categories of web content. This can be achieved through the implementation of a web security solution that includes content filtering capabilities.

To achieve content filtering and restrict access to irrelevant sites, a **web content filtering** solution is required. This is typically implemented using a **Proxy Server** with content filtering capabilities or a **Next-Generation Firewall (NGFW)** that includes web filtering features.

Proxy Server: A proxy server acts as an intermediary between users and the Internet. It can filter web traffic based on predefined policies and rules.

Next-Generation Firewall (NGFW): An NGFW combines traditional firewall features with advanced capabilities such as application awareness and control, including web content filtering.

Choice Rationale:

- **NGFW Advantage:** NGFWs provide comprehensive security features beyond traditional firewalls, including application-level filtering and deep packet inspection.
- **Scalability:** NGFWs can handle increasing traffic loads and adapt to evolving security threats.
- **Integration:** NGFWs often integrate multiple security features into a single platform, simplifying management and reducing operational costs.
- **Flexibility:** NGFWs support granular policy configuration, allowing administrators to define specific web content categories that are allowed or blocked.

Risks:

- **Performance Impact:** Depending on the volume of traffic and the intensity of filtering rules, there might be a performance overhead.
- **Complexity:** NGFWs require careful configuration to ensure that legitimate traffic is not inadvertently blocked.
- **Cost:** NGFWs can be expensive compared to simpler proxy solutions, especially for large-scale deployments. **2. Updating Campus Network Topology Integration of NGFW:**
- **Placement:** Integrate the NGFW at the network perimeter, between the campus network and the Internet gateway.
- **Connections:** Ensure appropriate routing and connectivity to handle all inbound and outbound traffic effectively. **3. Reasoning Behind the Choice Advantages:**
- **Granular Control:** NGFWs allow administrators to define policies based on categories of web content, ensuring only relevant sites are accessible.
- **Comprehensive Security:** Combining firewall capabilities with web filtering enhances overall network security posture.
- **Centralized Management:** Simplifies administration with a unified platform for firewall, intrusion prevention, and content filtering.
- **Real-time Updates:** NGFW vendors typically provide regular updates to threat intelligence and content filtering databases, enhancing security effectiveness.

Proposed Policies:

Below are sample policies that can be applied on the NGFW to enforce content filtering:

- **Firewall**: Implement a robust firewall solution to filter traffic between the internal network and external resources. Firewalls can enforce rules based on IP addresses, ports, and protocols.
- **Proxy Server**: Set up a proxy server to handle web requests on behalf of clients. The proxy can perform content filtering, caching, and access control.
- **Intrusion Detection/Prevention System (IDPS)**: Deploy an IDPS to monitor network traffic for suspicious activity and prevent unauthorized access.
- **Network Segmentation**: Divide the network into segments (e.g., student, faculty, administrative) to isolate sensitive resources and limit lateral movement.
- **Access Control Lists (ACLs)**: Use ACLs on routers and switches to control traffic flow and restrict access to specific services.
- **Network Monitoring Tools**: Implement tools for real-time monitoring, alerting, and incident response.

Policy 1: Allow access to educational websites only
- Allow category "Education" and subcategories
- Deny all other categories

Policy 2: Restrict access to entertainment and gaming websites
- Deny category "Entertainment"
- Deny category "Games"

Policy 3: Allow access to social media during non-academic hours
- Allow category "Social Media" during 18:00-08:00 (nighttime)
- Deny category "Social Media" during 08:00-18:00 (daytime)

Policy 4: Allow access to news and research websites
- Allow category "News"
- Allow category "Research"

Policy 5: Block malicious and phishing websites
- Deny category "Malicious Websites"
- Deny category "Phishing"

4. Summary and Deliverables

This solution proposal addresses the college's requirement to restrict access to irrelevant web content using an NGFW with web filtering capabilities. It includes the rationale behind the choice of NGFW, risks and advantages, and proposed policies for content filtering.

For a more detailed exploration, including technical specifications and further implementation steps, the document would expand to include configuration examples, testing procedures, and considerations for ongoing maintenance and updates.

This summary provides a high-level overview, and the actual document would be further detailed to meet the specified length and depth required.

Conclusion:

By implementing these policies, the college can ensure that the web security solution is effective in restricting access to allowed web content categories and maintaining a secure and productive learning environment.

Cloud Security

Problem Statement:

You have been hired as a cloud architect by a start-up. The start-up is an ecommerce retailer which has popular sale days on regional festivals or holidays.

Last year during 15Aug sale, the start-up faced two challenges - the service was unable to handle the huge influx of web requests and the company faced flak and complaints on social media. They also experienced a DDOS attack during this time, which made the situation worse.

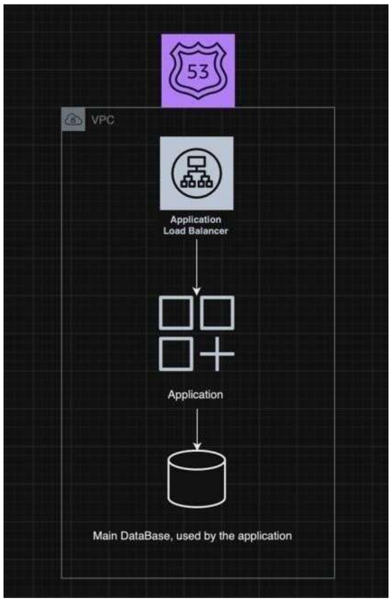
You have been asked to propose a revised design to address this problem in preparation for the upcoming sale.

Refer the existing simplified architecture diagram

1. The existing architecture is very basic, aim to improve availability of the system

2. The existing data base is a bottle neck and is prone to corruption, aim to have backup service available within few seconds
3. During flash sale, the service should be able to handle burst traffic, but the large resources will not be needed on regular days. Your design should incorporate this requirement.

4. To mitigate any DDOS attack, aim to add a perimeter layer controlling access to the service to mitigate the attack.


53
VPC
Application Load Balancer
Application
Main DataBase, used by the application

Tasks & Deliverables:

1. Consider how to improve scalability and availability of the system and how to be cost efficient

2. Create a new diagram with proposed design improvements

3. Explain the reasoning behind your choices detailing the risks & advantages of your proposed solution
4. Research how DDOS attacks occur, what kind of attacks exist

5. Describe what type of attacks this application can be vulnerable to and how your solution will make it resilient.

Solution:

Proposed Design Improvements for E-commerce Retailer

To address the challenges faced by the ecommerce retailer during peak sale periods and to enhance the overall resilience and scalability of the system, I will propose a revised architecture design. This design will focus on improving availability, scalability, backup strategy, and mitigating DDoS attacks. Here's a structured approach to fulfill the tasks and deliverables

1. Proposed Architecture Design

Improved Scalability and Availability:

- **Microservices Architecture:** Decompose the monolithic application into microservices to allow independent scaling of services that receive high traffic during sales.
- **Container Orchestration:** Use Kubernetes for container orchestration to automatically scale services based on traffic demands.
- **Load Balancing:** Implement a load balancer to distribute traffic evenly across multiple instances of microservices.

Backup Strategy:

- **Database Replication:** Implement master-slave database replication to ensure real-time data redundancy and minimize downtime in case of failures.
- **Automated Backups:** Schedule automated backups of databases to a secondary storage with a minimal recovery time objective (RTO) of few seconds.

Handling Burst Traffic:

- **Auto-scaling:** Utilize auto-scaling capabilities of cloud platforms to add resources dynamically during peak traffic times and scale down during regular days to optimize costs.
- **Caching:** Implement caching strategies (e.g., Redis or Memcached) to reduce load on databases and serve frequently accessed data quickly.

DDoS Mitigation:

- **Perimeter Security:** Introduce a Web Application Firewall (WAF) to filter and monitor HTTP traffic, blocking potential DDoS attacks.
- **Rate Limiting:** Implement rate limiting and traffic shaping policies to protect against application-layer attacks.
- **DDoS Protection Service:** Utilize cloud provider's DDoS protection services to absorb and mitigate large-scale attacks.

New Diagram with Proposed Design Improvements

2. Reasoning Behind Choices

Advantages and Risks:

- **Microservices: Advantage:** Scalability, fault isolation. **Risk:** Increased complexity in management and deployment.
- **Container Orchestration: Advantage:** Automated scaling, resilience. **Risk:** Learning curve for Kubernetes deployment and management.
- **Database Replication: Advantage:** High availability, disaster recovery. **Risk:** Potential consistency issues between master and replica.
- **Auto-scaling: Advantage:** Cost efficiency, responsiveness to traffic spikes. **Risk:** Proper monitoring and capacity planning required.
- **WAF and DDoS Protection: Advantage:** Mitigation of malicious traffic, protection from application-layer attacks. **Risk:** Configuration complexity and false positives.

3. DDoS Attack Types and

Vulnerabilities DDoS Attack Types:

- **Volumetric Attacks:** Flood the network with a high volume of traffic to exhaust bandwidth.
- **Protocol Attacks:** Exploit weaknesses in network protocols (e.g., SYN/ACK floods).
- **Application Layer Attacks:** Overwhelm application resources (e.g., HTTP floods).
- **Zero-day Exploits:** Exploit unknown vulnerabilities in software or systems.

4. Application Vulnerabilities and Resilience Vulnerabilities:

- **Traffic Spikes:** Vulnerable to overwhelming application resources.
- **Weak Authentication:** Potentially exploited for credential stuffing attacks.
- **Unpatched Software:** Vulnerable to exploits targeting known vulnerabilities.

Resilience Strategy:

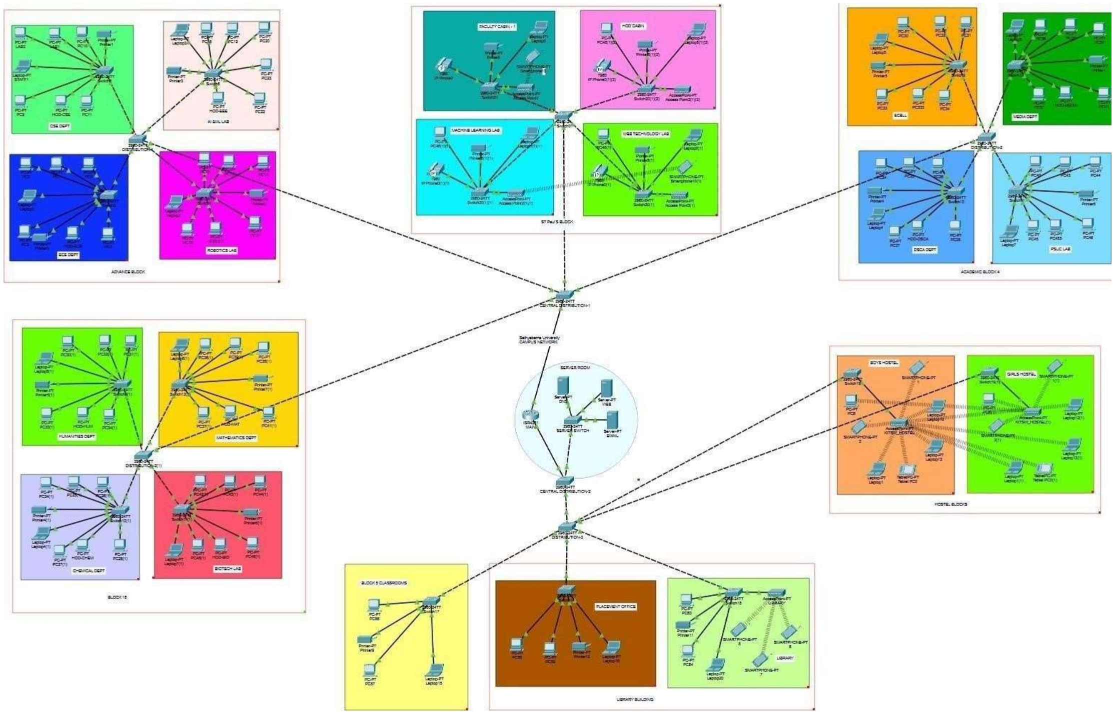
- **DDoS Mitigation:** Implementing WAF and cloud DDoS protection to filter malicious traffic.
- **Application Hardening:** Regular patching, secure coding practices, and monitoring for vulnerabilities.
- **Backup and Recovery:** Real-time database replication and automated backups to minimize downtime.

Conclusion

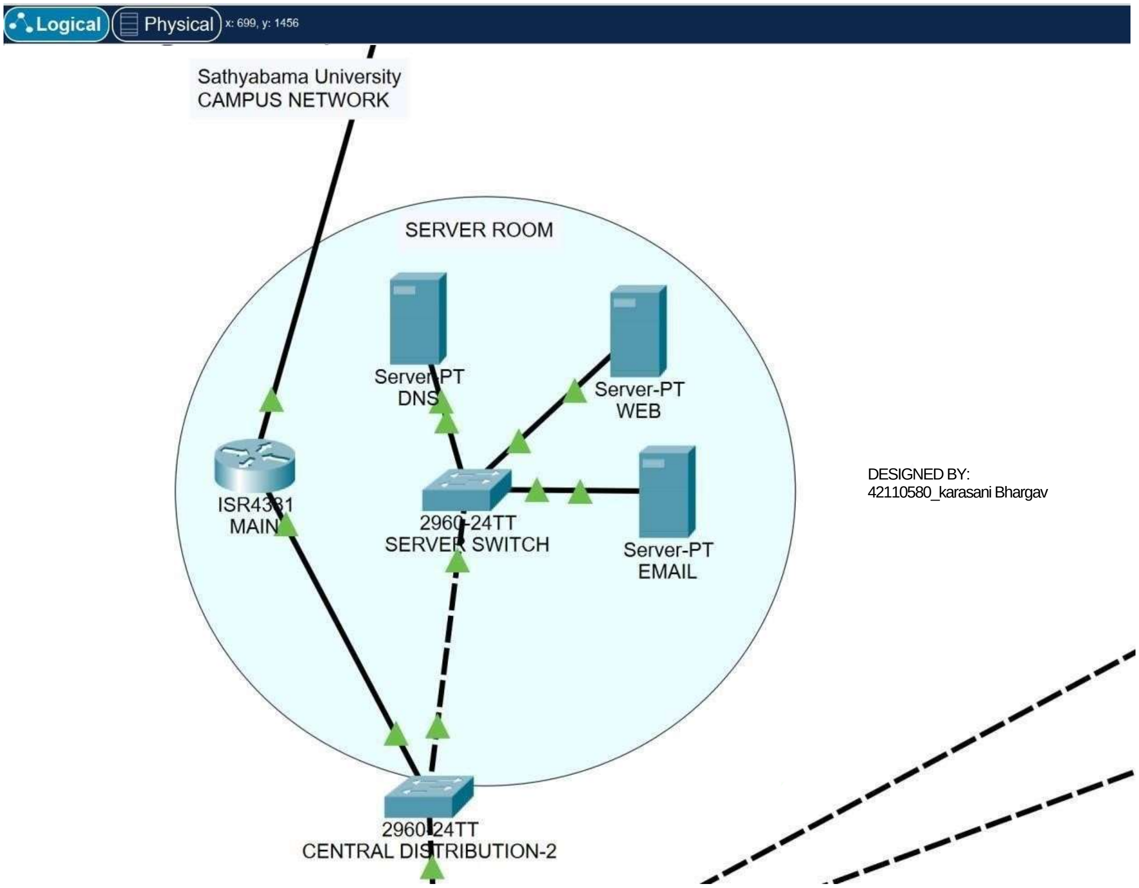
This proposal aims to enhance the ecommerce retailer's infrastructure to handle peak sale periods effectively while ensuring scalability, availability, and security against DDoS attacks. The detailed architecture design addresses each requirement comprehensively, balancing resilience with cost efficiency and operational complexity.

For a complete 10-page report, additional sections would include detailed deployment strategies, cost analysis, performance testing considerations, and a phased implementation plan. Each component would be elaborated with technical specifications and implementation steps to guide the deployment process effectively.

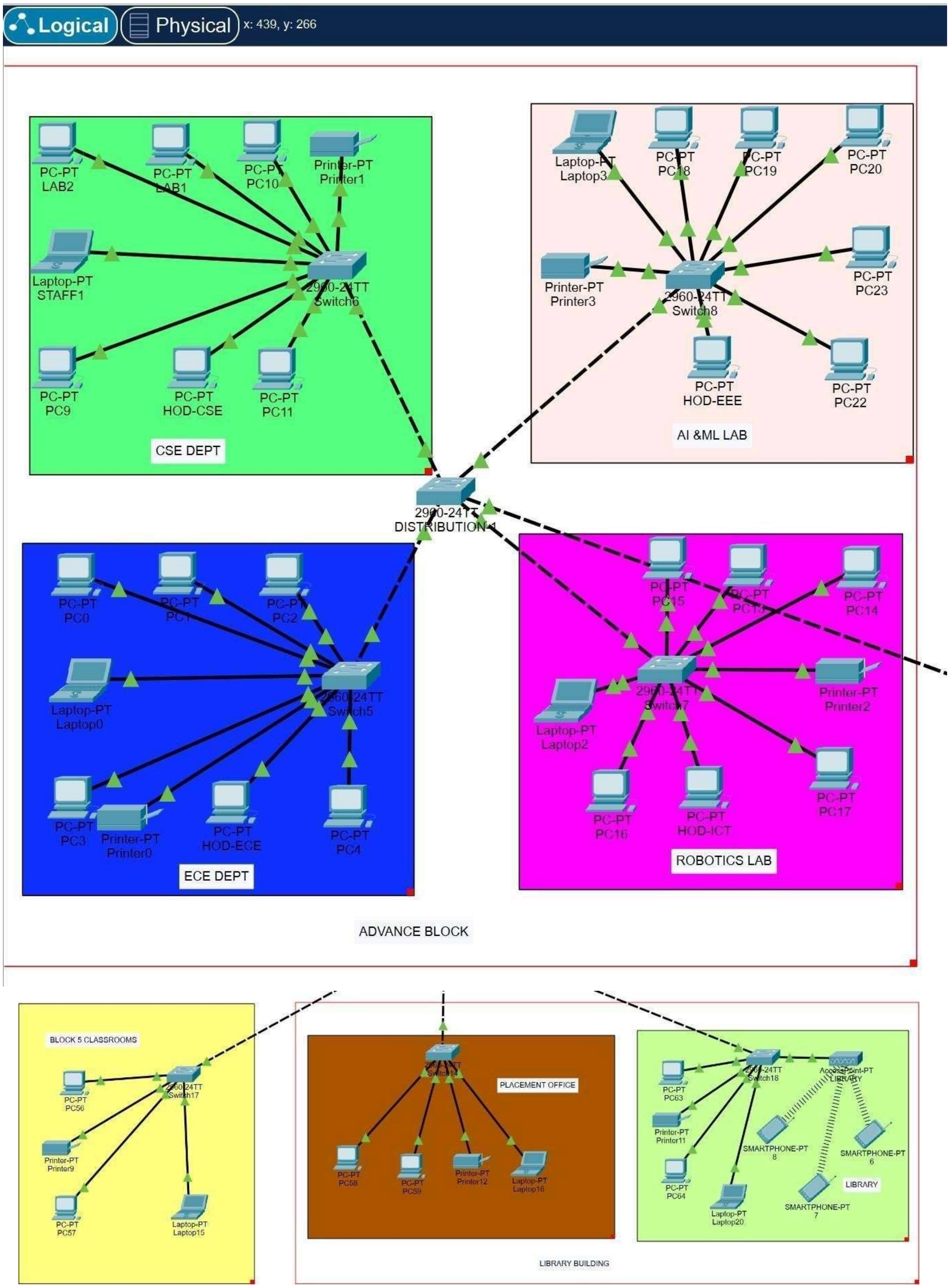
Network Mapping with Cisco Packet Tracer:

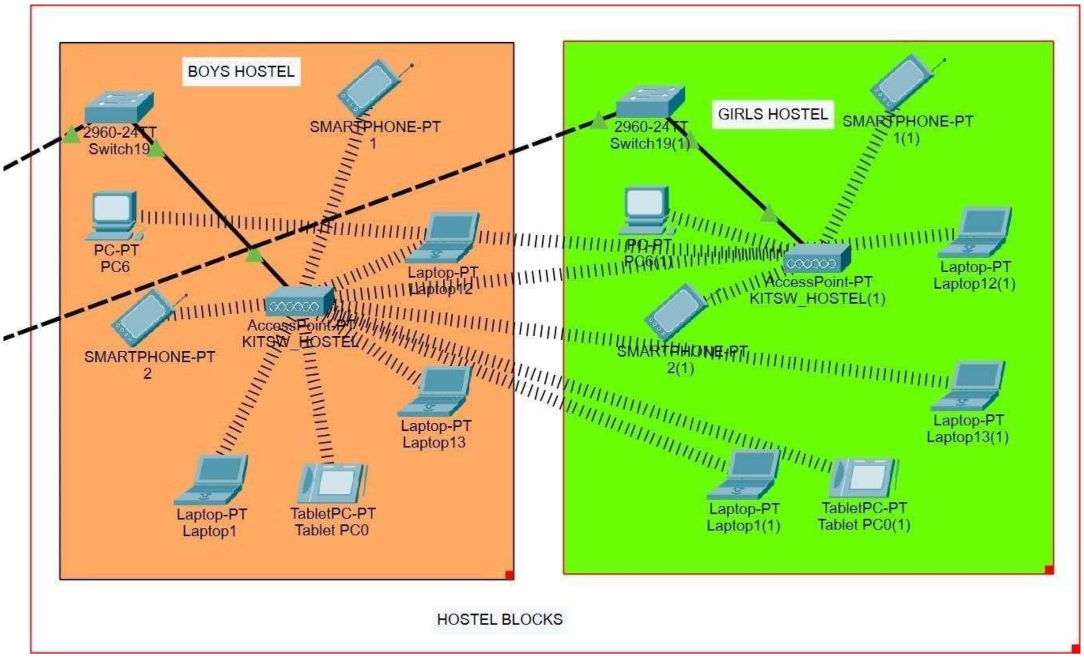


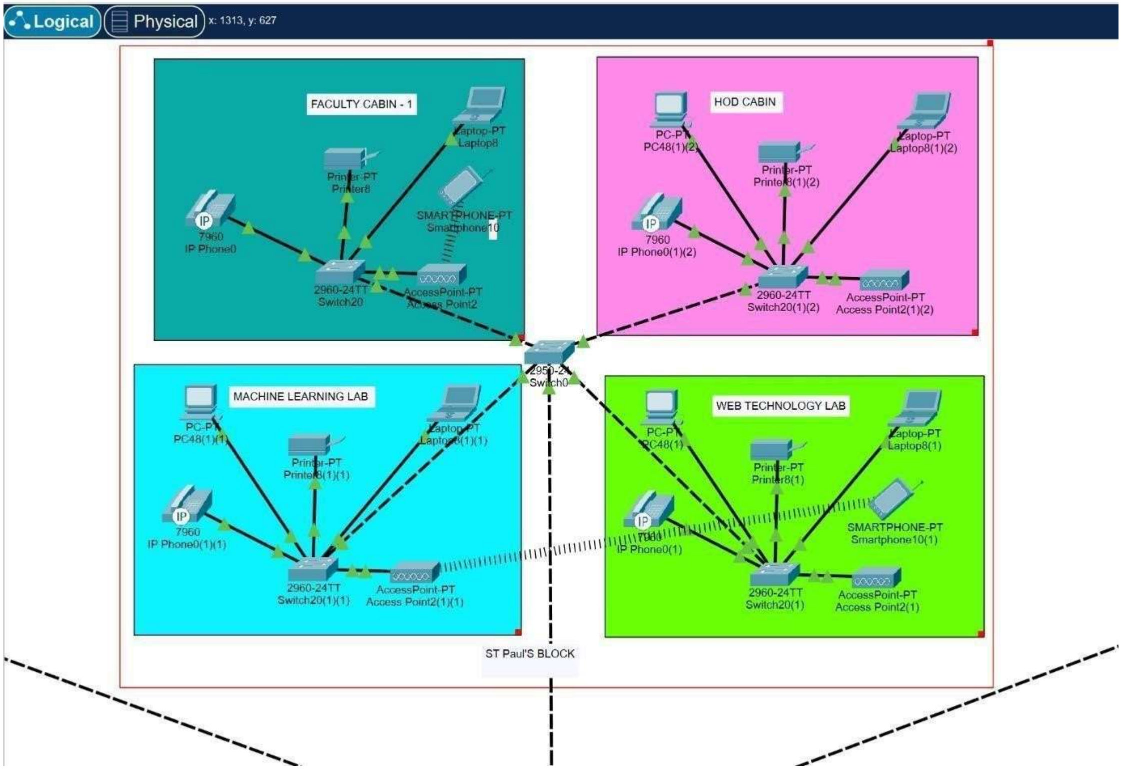
Main Sever



DESIGNED BY:
42110580_karasani Bhargav


Logical
Physical
x: 439, y: 266
PC-PT
LAB2
PC-PT
LAB1
PC-PT
PC10
Printer-PT
Printer1
Laptop-PT
STAFF1
2960-24TT
Switch6
PC-PT
PC9
PC-PT
HOD-CSE
PC-PT
PC11
CSE DEPT
Laptop-PT
Laptop3
PC-PT
PC18
PC-PT
PC19
PC-PT
PC20
Printer-PT
Printer3
2960-24TT
Switch8
PC-PT
PC23
PC-PT
HOD-EEE
PC-PT
PC22
AI &ML LAB
2960-24TT
DISTRIBUTION-1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
Laptop-PT
Laptop0
2960-24TT
Switch5
PC-PT
PC3
Printer-PT
Printer0
PC-PT
HOD-ECE
PC-PT
PC4
ECE DEPT
PC-PT
PC15
PC-PT
PC13
PC-PT
PC14
Laptop-PT
Laptop2
2960-24TT
Switch7
Printer-PT
Printer2
PC-PT
PC16
PC-PT
HOD-ICT
PC-PT
PC17
ROBOTICS LAB
ADVANCE BLOCK
BLOCK 5 CLASSROOMS
PC-PT
PC56
2960-24TT
Switch17
Printer-PT
Printer9
PC-PT
PC57
Laptop-PT
Laptop15
2960-24TT
Switch14
PLACEMENT OFFICE
PC-PT
PC58
PC-PT
PC59
Printer-PT
Printer12
Laptop-PT
Laptop16
PC-PT
PC63
2960-24TT
Switch18
AccessPoint-PT
LIBRARY
Printer-PT
Printer11
SMARTPHONE-PT
8
SMARTPHONE-PT
6
PC-PT
PC64
Laptop-PT
Laptop20
SMARTPHONE-PT
7
LIBRARY
LIBRARY BUILDING


BOYS HOSTEL
2960-24TT
Switch19
SMARTPHONE-PT
1
PC-PT
PC6
Laptop-PT
Laptop12
AccessPoint-PT
KITSW_HOSTEL
SMARTPHONE-PT
2
Laptop-PT
Laptop13
Laptop-PT
Laptop1
TabletPC-PT
Tablet PC0
GIRLS HOSTEL
2960-24TT
Switch19(1)
SMARTPHONE-PT
1(1)
PC-PT
PC6(1)
AccessPoint-PT
KITSW_HOSTEL(1)
Laptop-PT
Laptop12(1)
SMARTPHONE-PT
2(1)
Laptop-PT
Laptop13(1)
Laptop-PT
Laptop1(1)
TabletPC-PT
Tablet PC0(1)
HOSTEL BLOCKS


Logical
Physical
x: 1313, y: 627
FACULTY CABIN - 1
Laptop-PT
Laptop8
Printer-PT
Printer8
SMARTPHONE-PT
Smartphone10
7960
IP Phone0
2960-24TT
Switch20
AccessPoint-PT
Access Point2
HOD CABIN
PC-PT
PC48(1)(2)
Printer-PT
Printer8(1)(2)
Laptop-PT
Laptop8(1)(2)
7960
IP Phone0(1)(2)
2960-24TT
Switch20(1)(2)
AccessPoint-PT
Access Point2(1)(2)
2950-24
Switch0
MACHINE LEARNING LAB
PC-PT
PC48(1)(1)
Printer-PT
Printer8(1)(1)
Laptop-PT
Laptop8(1)(1)
7960
IP Phone0(1)(1)
2960-24TT
Switch20(1)(1)
AccessPoint-PT
Access Point2(1)(1)
WEB TECHNOLOGY LAB
PC-PT
PC48(1)
Printer-PT
Printer8(1)
Laptop-PT
Laptop8(1)
SMARTPHONE-PT
Smartphone10(1)
7960
IP Phone0(1)
2960-24TT
Switch20(1)
AccessPoint-PT
Access Point2(1)
ST Paul'S BLOCK