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 : Kandukuru Purandhar

AICTE Internship Student Registration ID) : STU662dda0fa41101714280975
Student ID (Enrolment number) : 42110567
Email : purandharkandukuru@gmail.com
Contact Info : +916303711457

Cyber Shield: Defending the network Problem Statement:

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:

Network Layout and Devices:

To effectively analyse the campus network, we start by understanding the existing network components and their interconnections:

1. **Core Routers**: These routers handle traffic between different campus segments and

external networks.

2. **Edge Routers**: They manage the connection between the campus network and the internet.
3. **Switches**: Located in various parts of the campus, switches manage local traffic within buildings or areas like dormitories, academic blocks, and administrative offices.
4. **Firewalls**: These devices are critical for protecting the network from unauthorized access by filtering incoming and outgoing traffic.
5. **Access Points (APs):** Provide wireless connectivity throughout the campus.
6. **Servers**: Host crucial services such as email, web applications, file storage, and databases.
7. **Intrusion Detection Systems (IDS):** Monitor network traffic for unusual or potentially harmful activity.

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

Attached 42110587_Kandukuru Purandhar_CyberSecurity.pkt [Link] file Where I have made the Network Mapping of my Sathyabama University Chennai Using Cisco Packet Tracer .

Using Cisco Packet Tracer, we can create a detailed map of the campus network:

- **Router Placement:** Place core and edge routers on the network map, showing their connections to switches and the internet.
- **Switch Placement:** Illustrate how switches connect to routers and endpoints, including computers, printers, and other devices.
- **Firewall Placement:** Position firewalls at strategic points, such as between the internal network and the internet, and between different network segments.
- **Access Points:** Show their locations and connections to switches.
- **Server Placement:** Map out servers and their connections to switches and routers.

2. **Security Controls:**
   - **Network Segmentation:** This involves dividing the network into smaller segments to improve security and performance. Common segmentation includes separating administrative, faculty, and student networks.
   - **Intrusion Detection Systems (IDS):** Analyze the existing IDS for its capabilities in detecting and responding to network threats.
   - **Firewalls:** Review the firewall rules and policies in place to ensure they are effectively protecting against unauthorized access and attacks.
   - **Authentication and Authorization:** Evaluate the mechanisms used for user authentication and authorization, such as LDAP, RADIUS, or Active Directory.

3. **Attack Surface Mapping:**

Identifying Potential Vulnerabilities:

- **Unauthorized Access:** Check for unsecured access points, weak passwords, and improper network segmentation.
- **Data Breaches:** Look for unprotected services or misconfigured firewall rules that might expose sensitive information.
- **Network Availability:** Assess the resilience of the network against potential disruptions or attacks.

Countermeasures:

- **Strengthen Authentication:** Implement multi-factor authentication (MFA) and enforce strong password policies.
- **Enhance Network Segmentation:** Use VLANs to separate different

user groups and services, minimizing the risk of cross-network attacks.

- **Upgrade IDS/IPS:** Deploy intrusion prevention systems (IPS) that can actively block
  malicious traffic.
- **Refine Firewall Rules:** Regularly update and review firewall rules to ensure they align with the latest security policies and best practices.

Conclusion:

The analysis of the existing campus network topology and the subsequent mapping using Cisco Packet Tracer reveals a comprehensive view of the current network infrastructure, including routers, switches, firewalls, and access points. The attack surface mapping exercise highlights potential vulnerabilities such as unauthorized access points, weak passwords, and insufficient network segmentation. By applying knowledge from cybersecurity principles, we have identified critical security controls currently in place and proposed countermeasures to address these risks. Enhancing network segmentation, refining firewall rules, and upgrading IDS/IPS systems are essential steps to mitigate identified vulnerabilities and strengthen overall network security.

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

Solution:

Designing a Hybrid Working Environment

1. Achieving Hybrid Access:

For Faculty Members:

- **Solution:** Use a Virtual Private Network (VPN) or secure remote access solutions to allow faculty members to connect to the college network from home and on-campus. The VPN should provide secure, encrypted access to faculty-specific resources.

For Students:

- **Solution:** Implement a secure portal that students can access using their personal devices. This portal should be accessible both on-campus and remotely, ensuring students can access necessary resources without exposing the campus network to public internet.

2. Network Security Products:

- **VPN Solutions:** Products like Cisco AnyConnect or OpenVPN provide secure access for faculty members working remotely.

- **Zero Trust Network Access (ZTNA):** Solutions such as Cisco Umbrella or Zscaler enforce strict access controls and verify user and device compliance before granting access to resources.

3. Updated Campus Network Topology:

Components Added:

- **VPN Gateways:** Ensure that faculty can securely access campus resources from remote locations.
- **ZTNA Systems:** Implement these to manage and enforce access controls for both faculty and students.
- **Enhanced Firewalls:** Protect internal resources by restricting access to authenticated and authorized users only.

Reasoning:

- **VPNs and ZTNA:** Provide secure and flexible access to internal resources, protecting against unauthorized access while ensuring usability for remote work.
- **Access Control Systems:** Manage and monitor access effectively, reducing the risk of data breaches and unauthorized access.

Risks and Advantages:

- **Risks:** Potential misconfigurations of VPNs or ZTNA systems could expose the network.
- **Advantages:** Improved security, controlled access, and enhanced flexibility for faculty and students.

Conclusion:

Designing a hybrid working environment for faculty and students involves implementing secure access solutions that ensure both groups can connect to campus resources from any location while maintaining network security. VPNs and Zero Trust Network Access (ZTNA) systems have been recommended to provide secure remote access for faculty and students. These solutions protect the campus network from unauthorized access while ensuring usability. The updated network topology incorporates VPN gateways and ZTNA systems, effectively balancing remote work flexibility with stringent access controls. The chosen approach mitigates risks associated with remote access and ensures that campus resources remain protected from public exposure.

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:

Implementing Web Content Restrictions

1. Achieving Content Filtering:

Solution: Deploy a Web Filtering Solution or DNS-based filtering service to control access to web content.

- **Web Filtering Solutions:** Products like Cisco Umbrella or Websense offer comprehensive content filtering capabilities, allowing administrators to define policies for web access based on categories.
- **DNS Filtering:** Services like OpenDNS can block access to undesirable sites by redirecting DNS requests.

2. Updated Network Topology:

Components Added:

- **Web Filter Appliance:** Positioned at the network edge to filter and control web traffic.
- **DNS Filtering Service:** Configured to manage and restrict access to inappropriate or noneducational content.

3. Reasoning and Policies:

Reasoning:

- **Web Filtering:** Provides granular control over accessible content, enhancing network security and productivity.
- **DNS Filtering:** Offers an additional layer of security by blocking access to known malicious sites and inappropriate content.

Policies:

- **Allow:** Access to educational, research, and institutional websites.

- **Block:** Access to social media, gaming sites, and other non-educational categories.

Conclusion Statement:

To address the issue of students misusing campus resources and accessing irrelevant sites, the implementation of web filtering and DNS-based filtering solutions provides a robust method for controlling web content access. Deploying web filter appliances and DNS filtering services ensures that only appropriate content is accessible, while blocking harmful or non-educational sites. The updated network topology with these new components allows for effective content management and enhances network security. The proposed policies clearly define allowed and blocked categories of web content, supporting a productive and secure network environment.

Cloud Security Problem

Statement:

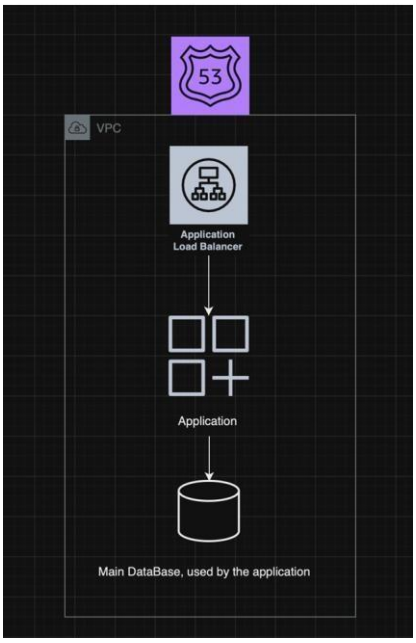
You have been hired as a cloud architect by a start-up. The start-up is an ecommerce retailer which has popular sale days on regional festivals or holidays.

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.



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:

Improving Cloud Architecture

1. Enhancing Scalability and Availability:

Solution:

- **Auto-Scaling:** Implement auto-scaling groups to automatically adjust the number of resources (e.g., servers) based on current traffic demands. This ensures that the system can handle traffic spikes during peak times.
- **Load Balancers:** Use load balancers to distribute incoming traffic across multiple servers, preventing any single server from becoming a bottleneck.
- **Database Replication:** Implement database replication to ensure high availability and quick recovery in case of database failures.

2. Revised Architecture:

Components Added:

- **Auto-Scaling Groups:** Automatically scale resources based on traffic.
- **Load Balancers:** Distribute traffic to multiple servers to ensure reliability and performance.
- **Database Backup Services:** Ensure backups are taken regularly and can be restored quickly in case of data corruption.
- **DDoS Protection Service:** Protect against Distributed Denial of Service (DDoS) attacks by filtering malicious traffic before it reaches your infrastructure.

3. Reasoning and Security Enhancements:

Reasoning:

- **Auto-Scaling and Load Balancing:** Address high traffic volumes efficiently and improve system resilience.

- **Database Replication and Backups:** Protect against data loss and ensure quick recovery.
- **DDoS Protection:** Mitigate the impact of large-scale attacks, ensuring continuous service availability.

4. DDoS Attacks and Mitigation:

Types of DDoS Attacks:

- **Volume-Based Attacks:** Flood the network with excessive traffic.
- **Protocol-Based Attacks:** Exploit weaknesses in network protocols.
- **Application Layer Attacks:** Target specific application vulnerabilities.

Mitigation:

- **Use DDoS Protection Services:** Employ services like Cloudflare or AWS Shield to absorb and mitigate attack traffic.

5. Vulnerabilities and Resilience:

Potential Vulnerabilities:

- **Service Overload:** Without proper scaling, high traffic can overwhelm servers.
- **Database Corruption:** Without adequate backup strategies, data loss can occur.

Solution Resilience:

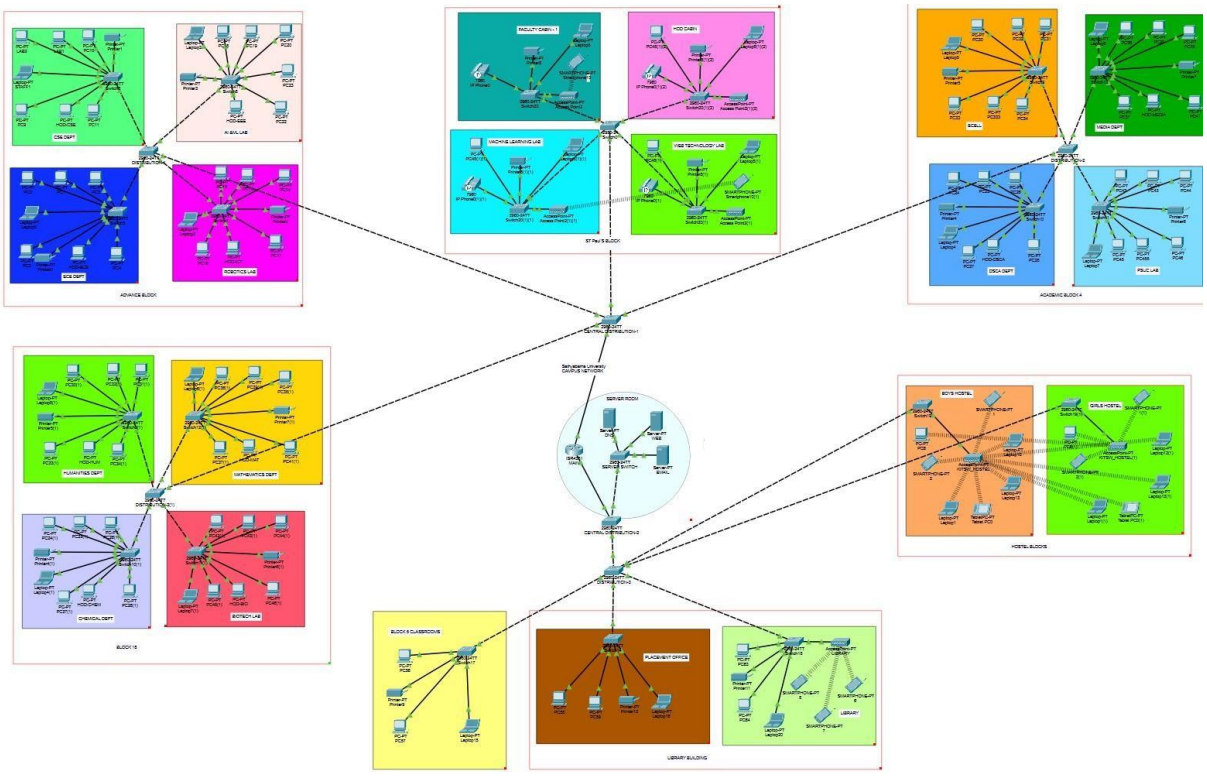
- **Scalable Design:** Ensures the system can handle traffic surges.
- **Backup Mechanisms:** Protect against data corruption and loss, allowing for quick restoration.

Conclusion Statement:

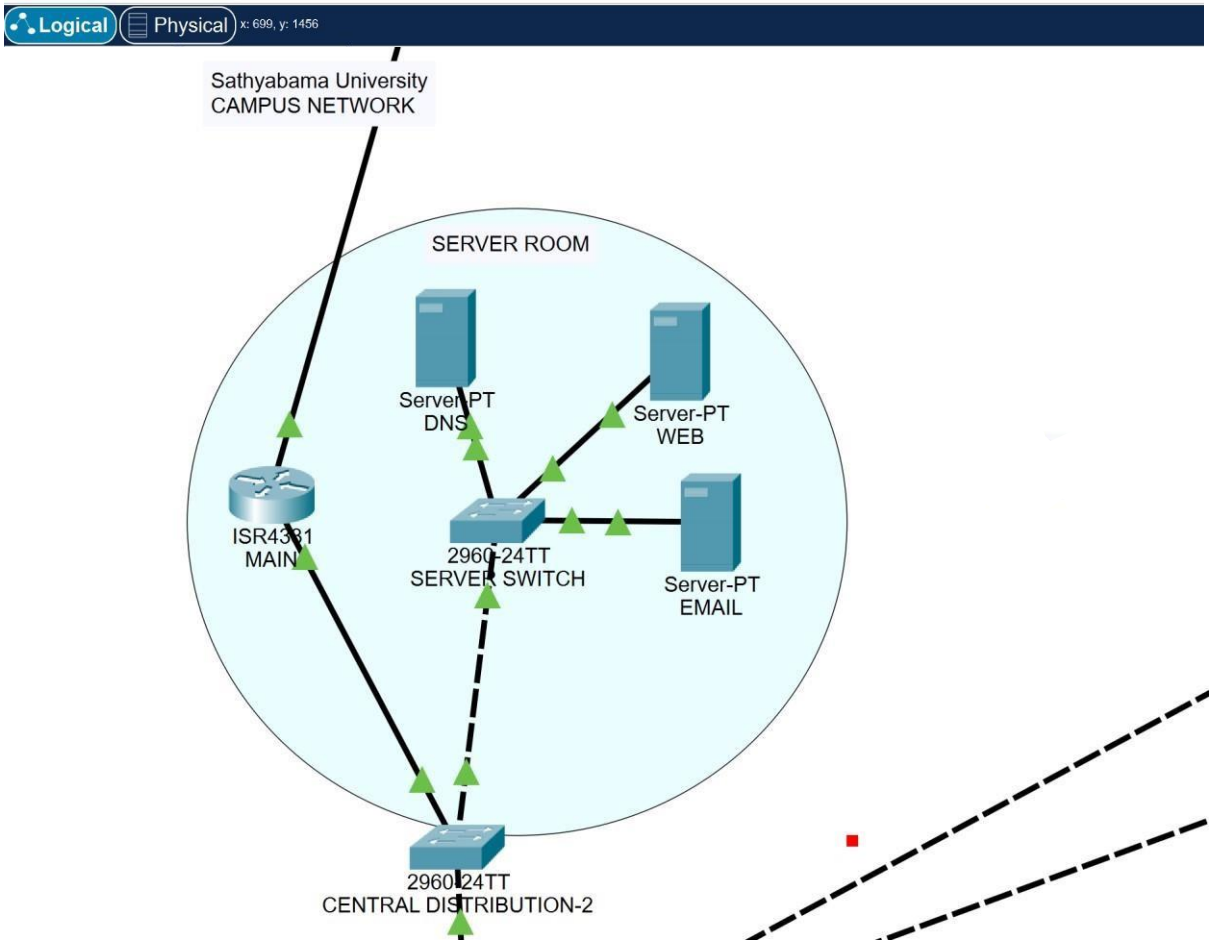
The revised cloud architecture for the e-commerce start-up addresses previous challenges by enhancing scalability, availability, and resilience against

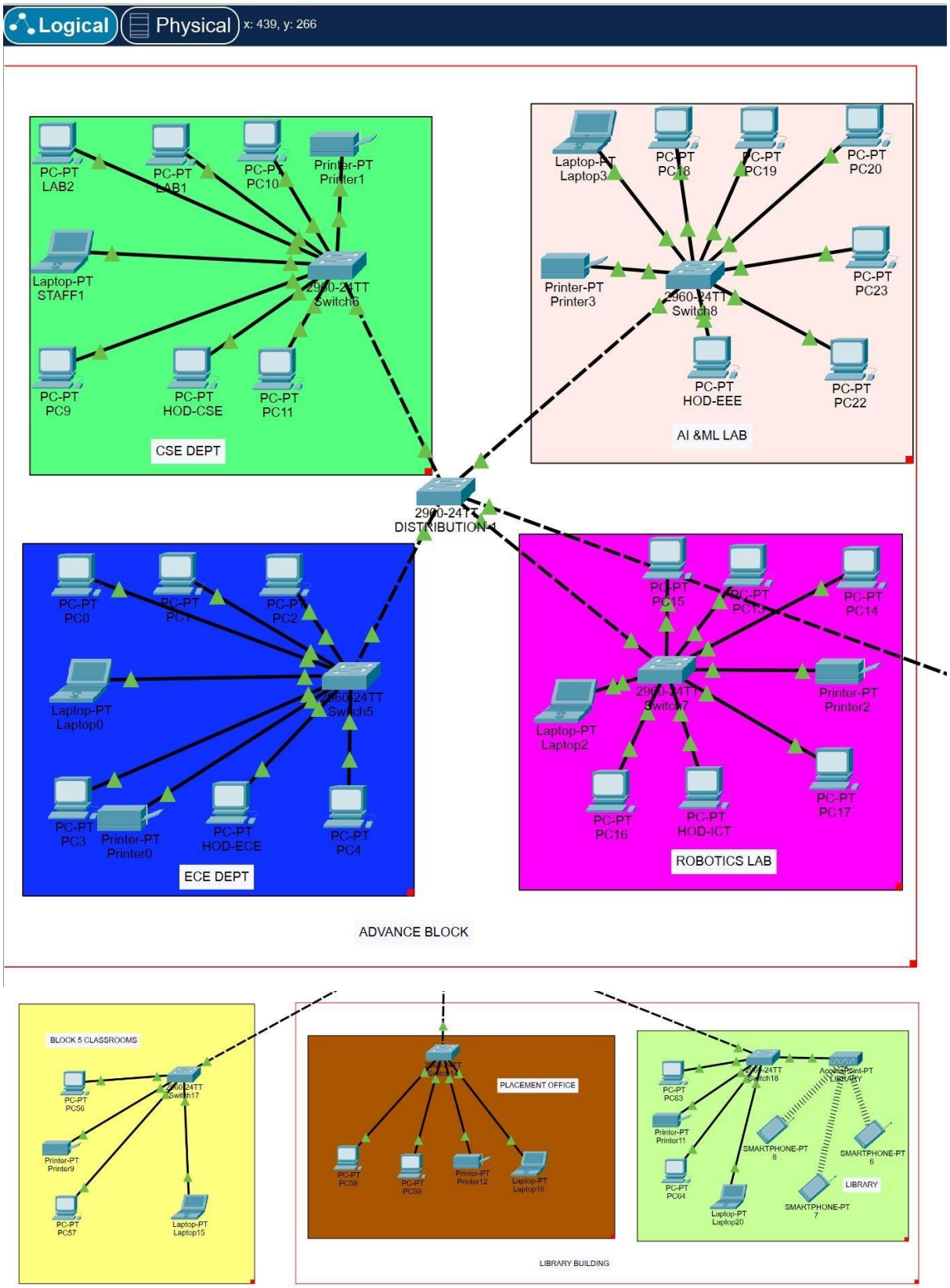
DDoS attacks. Implementing auto-scaling groups and load balancers ensures the system can handle high traffic volumes during peak sale periods without compromising performance. Database replication and backup services safeguard against data corruption and enable quick recovery. DDoS protection services provide an additional layer of defence against malicious traffic. This comprehensive approach ensures that the ecommerce platform remains operational, secure, and responsive during high-demand events, improving overall service reliability and customer satisfaction.

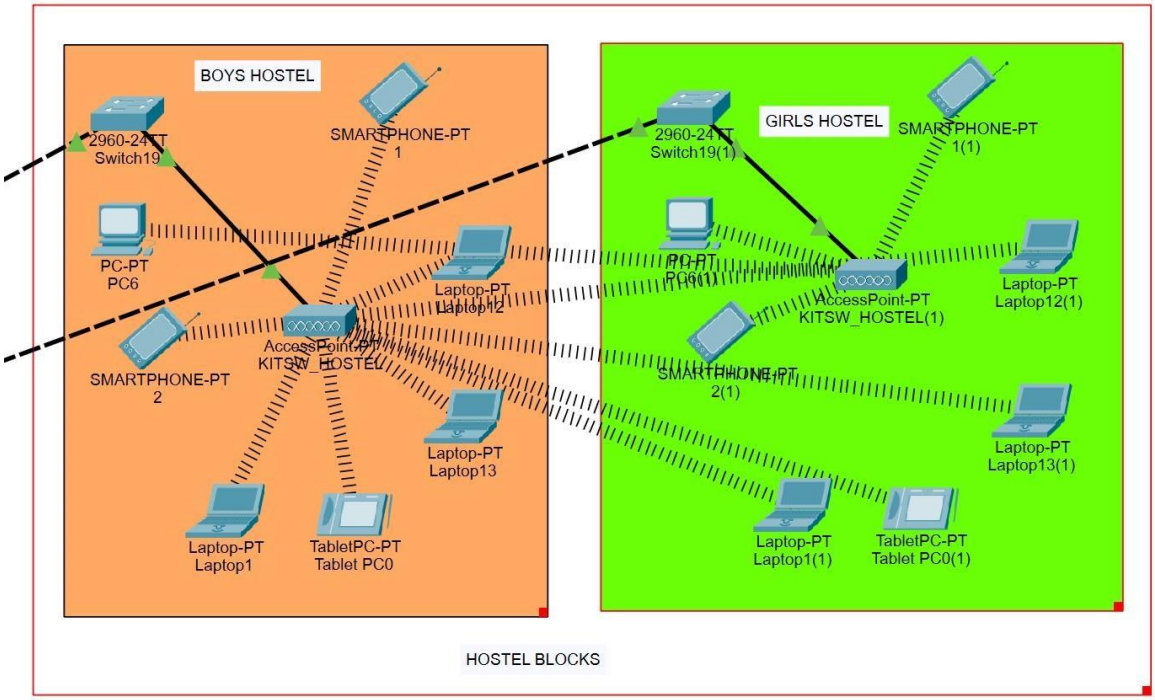
Network Mapping with Cisco Packet Tracer:

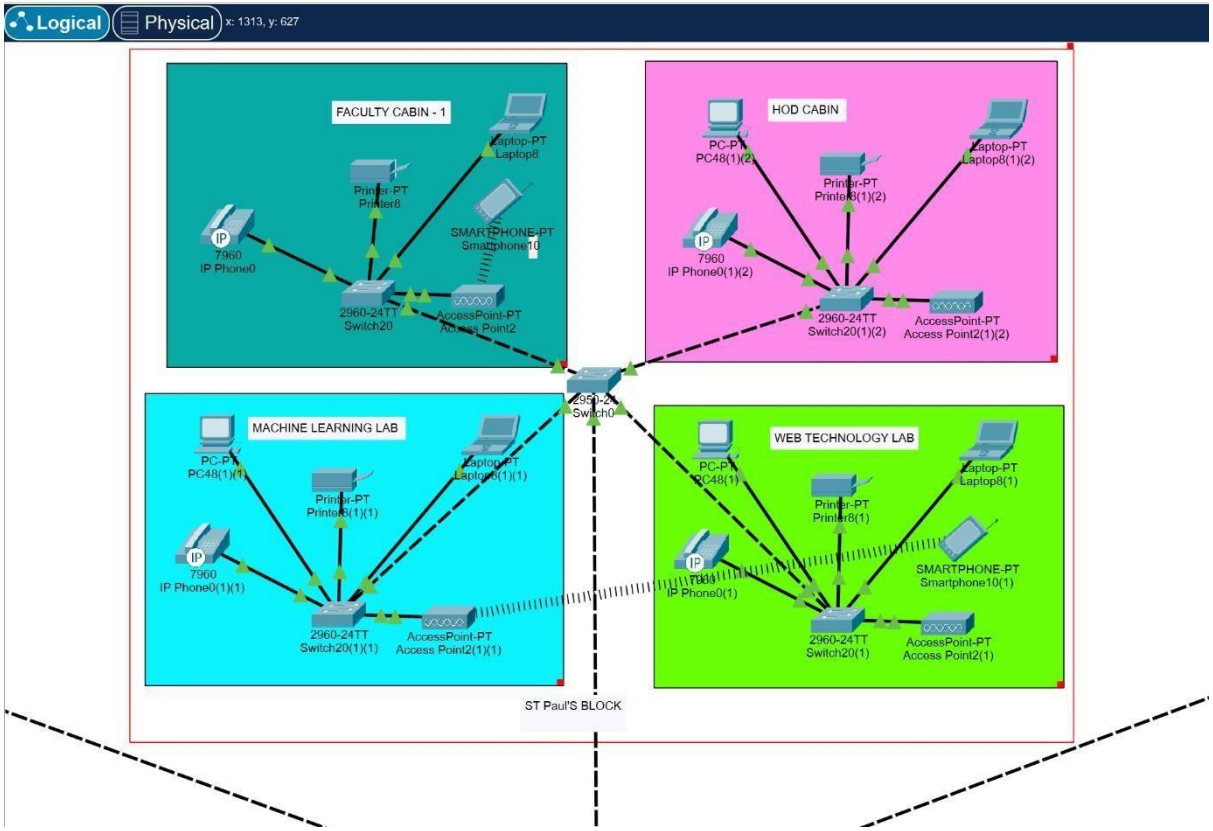


Main Sever


Logical
Physical
x: 699, y: 1456
Sathyabama University
CAMPUS NETWORK
SERVER ROOM
Server-PT
DNS
Server-PT
WEB
ISR4331
MAIN
2960-24TT
SERVER SWITCH
Server-PT
EMAIL
2960-24TT
CENTRAL DISTRIBUTION-2


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 PC14
2960-24TT Switch7
Printer-PT Printer2
Laptop-PT Laptop2
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
PLACEMENT OFFICE
PC-PT PC58
PC-PT PC59
Printer-PT Printer12
Laptop-PT Laptop16
PC-PT PC63
2960-24TT Switch18
Access-Point-PT LIBRARY
Printer-PT Printer11
SMARTPHONE-PT 8
SMARTPHONE-PT 6
PC-PT PC64
LIBRARY
Laptop-PT Laptop20
SMARTPHONE-PT 7
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
IP
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)
IP
7960
IP Phone0(1)(2)
2960-24TT
Switch20(1)(2)
AccessPoint-PT
Access Point2(1)(2)
MACHINE LEARNING LAB
PC-PT
PC48(1)(1)
Printer-PT
Printer8(1)(1)
Laptop-PT
Laptop8(1)(1)
IP
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)
IP
7960
IP Phone0(1)
SMARTPHONE-PT
Smartphone10(1)
2960-24TT
Switch20(1)
AccessPoint-PT
Access Point2(1)
ST Paul'S BLOCK