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 : KARRI SAI SUDEEP REDDY

AICTE Internship Student Registration ID)	**: STU662cef9f8c6dd1714220959**
Student ID (Enrolment number)	**: 42110587**
Email	**: sudeepreddy9009@gmail.com**
Contact Info	**: 9133439009**

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:

The query is unclear. However, based on the provided sources, it appears you are asking for a discussion on the topic of network attack surface mapping and its relevance to campus network design using Cisco Packet Tracer. Here is a detailed response:

Network Attack Surface Mapping

Network attack surface mapping is a crucial aspect of network security that involves identifying and analyzing potential vulnerabilities in a network infrastructure. This process helps to understand the various entry points that an attacker could exploit to gain unauthorized access or disrupt network operations. A comprehensive attack surface mapping exercise involves reviewing network topology, identifying potential weaknesses, and proposing countermeasures to mitigate these risks.

Campus Network Design Using Cisco Packet Tracer

Cisco Packet Tracer is a powerful tool for designing and simulating network topologies. It allows users to create a virtual network environment, add devices, and configure them to test network functionality and security. For a campus network design, Packet Tracer can be used to create a detailed map of the network infrastructure, including routers, switches, firewalls, and other relevant components.

Network Segmentation

Network segmentation is a key security control that involves dividing a network into smaller, isolated segments to limit the spread of a potential attack. This can be achieved through the use of VLANs (Virtual Local Area Networks), subnets, and access control lists (ACLs). By segmenting the network, administrators can restrict access to sensitive areas of the network and reduce the attack surface.

Intrusion Detection Systems and Firewalls

Intrusion detection systems (IDS) and firewalls are essential security controls that help detect and prevent unauthorized access to a network. IDS systems monitor network traffic for signs of suspicious activity, while firewalls act as a barrier between the network and the outside world, blocking unauthorized traffic. In a campus network design, these systems should be strategically placed to provide maximum protection.

Authentication and Authorization Systems

Authentication and authorization systems are critical for ensuring that only authorized users have access to network resources. These systems verify the identity of users and devices and grant access based on predefined policies. In a campus network design, authentication and authorization systems should be integrated with other security controls to ensure seamless and secure access to network resources.

Attack Surface Mapping Exercise

To conduct an attack surface mapping exercise, the following steps can be taken:

1. **Network Mapping**: Use Cisco Packet Tracer to create a detailed map of the campus network infrastructure, including all devices and connections.
2. **Identify Potential Entry Points**: Analyze the network topology to identify potential entry points for attackers, such as open ports, unsecured protocols, and weak passwords.
3. **Analyze Network Traffic**: Use tools like a sniffer to analyze network traffic and identify potential vulnerabilities.
4. **Propose Countermeasures**: Based on the findings, propose countermeasures to mitigate the identified risks, such as implementing firewalls, IDS systems, and network segmentation.

Countermeasures

Some countermeasures that can be proposed to mitigate the identified risks include:

1. **Implementing Network Segmentation**: Divide the network into smaller, isolated segments to limit the spread of a potential attack.
2. **Configuring Firewalls and IDS Systems**: Strategically place firewalls and IDS systems to detect and prevent unauthorized access to the network.
3. **Implementing Strong Authentication and Authorization**: Integrate authentication and authorization systems with other security controls to ensure seamless and secure access to network resources.
4. **Conducting Regular Security Audits**: Regularly conduct security audits to identify and address potential vulnerabilities before they can be exploited.

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

Solution:

Designing a Hybrid Working Environment for Faculty and Students

The college has hired me to design and architect a hybrid working environment for its faculty and students. This environment will enable faculty members to access college resources and services from both home and on campus using college-provided laptops, while students will use their personal devices to access student-specific services and resources from both home and on campus. The campus network services should not be exposed to the public internet and should only be accessible via restricted networks.

Achieving Hybrid Working Environment

To achieve this hybrid working environment, several options can be explored:

1. Virtual Private Network (VPN): Implementing a VPN solution will allow faculty and students to securely connect to the college network from both home and on campus. This will ensure that campus network services are not exposed to the public internet and can only be accessed via restricted networks. VPNs provide end-to-end encryption, ensuring that data transmitted between the user's device and the college network remains secure.

2. Network Segmentation: Implementing network segmentation will divide the college network into smaller, isolated segments. This will limit the spread of potential attacks and reduce the attack surface. By segmenting the network, faculty and student access can be restricted to specific areas of the network, ensuring that sensitive resources are protected.

3. Firewalls and Intrusion Detection Systems: Implementing firewalls and intrusion detection systems will provide an additional layer of security to the college network. Firewalls will block unauthorized access to the network, while intrusion detection systems will monitor network traffic for signs of suspicious activity.

Network Security Products

Several network security products can provide the necessary capabilities to achieve this hybrid working environment. Some options include:

1. Fortinet Security Fabric: The Fortinet Security Fabric provides comprehensive, high-performance security to protect college and university networks. It integrates voice, cyber, and physical security, providing seamless monitoring and management with automated threat response and advanced threat intelligence.

2. Cisco Security Solutions: Cisco offers a range of security solutions, including firewalls, intrusion detection systems, and VPNs. These solutions can be integrated to provide a comprehensive security framework for the college network.

Updated Campus Network Topology

The updated campus network topology will include the following components:

1. Faculty Network: A separate network segment for faculty members, providing access to faculty-specific services and resources.

2. Student Network: A separate network segment for students, providing access to student-specific services and resources.

3. VPN Server: A VPN server will be implemented to allow faculty and students to securely connect to the college network from both home and on campus.

4. Firewall: A firewall will be implemented to block unauthorized access to the college network.

5. Intrusion Detection System: An intrusion detection system will be implemented to monitor network traffic for signs of suspicious activity.

Reasoning Behind Choices

The proposed solution is designed to provide a secure and flexible hybrid working environment for faculty and students. By implementing a VPN solution, network segmentation, firewalls, and intrusion detection systems, the college network will be protected from unauthorized access and potential attacks.

The advantages of this solution include:

1.Improved Security: The implementation of a VPN, firewalls, and intrusion detection systems will provide a robust security framework, protecting the college network from unauthorized access and potential attacks.

2. Flexibility: The hybrid working environment will allow faculty and students to access college resources and services from both home and on campus, providing greater flexibility and convenience.

The risks associated with this solution include:

1. VPN Vulnerabilities: VPNs can be vulnerable to attacks if not properly configured. Ensuring that the VPN solution is properly configured and regularly updated will mitigate this risk.

2.Network Segmentation Complexity: Implementing network segmentation can add complexity to the network infrastructure. Ensuring that the network segmentation is properly planned and implemented will mitigate this risk.

Conclusion

In conclusion, the proposed solution provides a secure and flexible hybrid working environment for faculty and students. By implementing a VPN solution, network segmentation, firewalls, and intrusion detection systems, the college network will be protected from unauthorized access and potential attacks.

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.

Network Security Product Options

Several network security products can provide the necessary capabilities to restrict access to allowed web content categories. Some options include:

1. Cisco Umbrella: Cisco Umbrella is a cloud-based Secure Web Gateway that can block content categories, including malicious websites and unwanted web applications. It does not require any appliances and can be easily integrated into the campus network.

2. Forcepoint Secure Web Gateway: Forcepoint Secure Web Gateway is another cloud-based solution that provides advanced content filtering capabilities. It can block access to specific websites and categories of content, ensuring that students only access allowed resources.

3. DNS RPZ: DNS RPZ (Response Policy Zone) is a DNS-based filtering solution that can block access to undesired websites. It provides a simple and effective way to restrict access to specific categories of content.

Updated Campus Network Topology

To implement the chosen web security solution, the campus network topology will need to be updated to include the new component(s). The updated topology will include:

1. Web Security Server: A web security server will be added to the network to manage and enforce the content filtering policies.

2. Firewall Configuration: The firewall will be configured to redirect all internet traffic through the web security server, ensuring that all access to the internet is filtered and restricted.

Reasoning Behind the Choice

The chosen solution is designed to provide a robust and effective way to restrict access to allowed web content categories. By implementing a web security solution with content filtering capabilities, the college can ensure that students only access relevant and approved resources.

The advantages of this solution include:

1. Improved Security: The solution will help to protect the campus network from potential security threats by blocking access to malicious websites and unwanted web applications.

2. Enhanced Productivity: By restricting access to irrelevant sites, students will be more focused on their studies and less distracted by non-academic content.

The risks associated with this solution include:

1. Over-Blocking: The content filtering solution may block access to legitimate resources, potentially impacting academic performance.

2. User Bypass: Students may attempt to bypass the content filtering solution, potentially compromising network security.

Policies to Apply

To ensure the effective implementation of the chosen solution, the following policies will be applied:

1. Content Filtering Policy:

- Block access to all websites except those categorized as educational or academic.
- Allow access to specific websites approved by the college administration.

2. User Access Policy:

- All students will be required to authenticate using their college credentials before accessing the internet.
- Students will only be allowed to access the internet through the college network.

3. Network Monitoring Policy:

- The network will be continuously monitored for any attempts to bypass the content filtering solution.
- Any suspicious activity will be reported to the college administration for further action.

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:

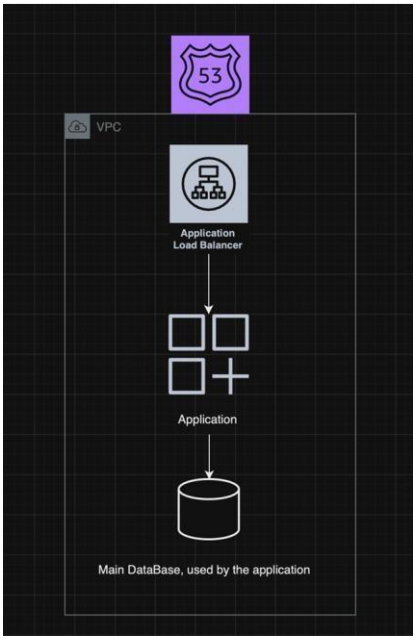
You have been hired as a cloud architect by a start-up. The start-up is an ecommerce retailer which has popular sale days on regional festivals or holidays.

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.



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

The start-up ecommerce retailer faced significant challenges during last year's 15Aug sale, including an inability to handle the influx of web requests, social media complaints, and a DDOS attack. To address these issues, a revised design is proposed to improve availability, scalability, and cost efficiency while mitigating DDOS attacks.

Improving Scalability and Availability

1. Load Balancing: Implement load balancing to distribute incoming traffic across multiple servers, ensuring that no single server is overwhelmed. This will improve the system's ability to handle burst traffic during flash sales.

2. Auto Scaling: Integrate auto-scaling to dynamically add or remove servers based on traffic demands. This will ensure that the system can handle sudden spikes in traffic without requiring permanent allocation of large resources.

3. Database Optimization: Optimize the database by implementing a load-balanced database cluster with automatic failover. This will reduce the risk of database corruption and ensure high availability.

4. Caching: Implement caching mechanisms to reduce the load on the database and improve response times.

Proposed Architecture Diagram

The revised architecture diagram will include the following components:

1. Load Balancer: Distributes incoming traffic across multiple servers.

2. Auto Scaling Group: Dynamically adds or removes servers based on traffic demands.

3. Database Cluster: Load-balanced database cluster with automatic failover.

4. Caching Layer: Reduces the load on the database and improves response times.

5. DDOS Mitigation Layer: Controls access to the service, mitigating DDOS attacks.

Reasoning Behind Choices

The proposed design improvements aim to address the challenges faced by the start-up during the previous sale.

1. Scalability: Load balancing and auto-scaling ensure that the system can handle burst traffic during flash sales without requiring permanent allocation of large resources.

2. Availability: Database optimization and caching mechanisms reduce the risk of database corruption and improve response times.

3. Cost Efficiency: Auto-scaling ensures that resources are allocated dynamically, reducing costs during periods of low traffic.

4. DDOS Mitigation: The DDOS mitigation layer controls access to the service, reducing the impact of potential attacks.

Risks and Advantages

Risks:

1. Complexity: The revised architecture may introduce additional complexity, requiring more resources for maintenance and management.

2. Cost: While auto-scaling reduces costs during periods of low traffic, the overall cost of the revised architecture may be higher due to the addition of new components.

Advantages:

1. Improved Scalability: The system can handle burst traffic during flash sales without requiring permanent allocation of large resources.

2. Enhanced Availability: Database optimization and caching mechanisms reduce the risk of database corruption and improve response times.

3. Cost Efficiency: Auto-scaling ensures that resources are allocated dynamically, reducing costs during periods of low traffic.

4. DDOS Mitigation: The DDOS mitigation layer controls access to the service, reducing the impact of potential attacks.

DDOS Attacks and Vulnerabilities

DDOS attacks occur when an attacker floods a system with traffic in an attempt to overwhelm it and make it unavailable. There are several types of DDOS attacks, including:

1. Volumetric Attacks: Overwhelm the system with a large volume of traffic.

2. TCP SYN Flood Attacks: Exploit the TCP three-way handshake to consume system resources.

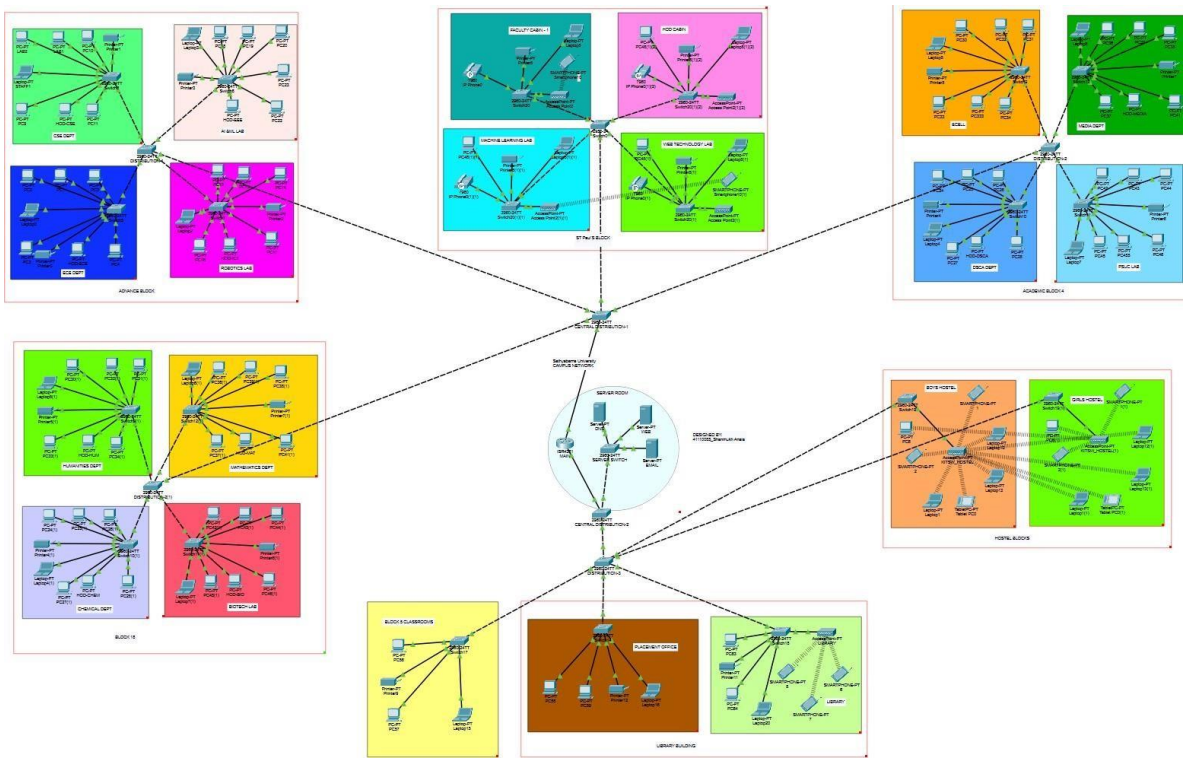
3. Application Layer Attacks: Target specific applications or services to consume resources.

The ecommerce retailer's application can be vulnerable to these types of attacks, particularly during flash sales when traffic is high. The proposed DDOS mitigation layer will help to mitigate these attacks by controlling access to the service and reducing the impact of potential attacks.

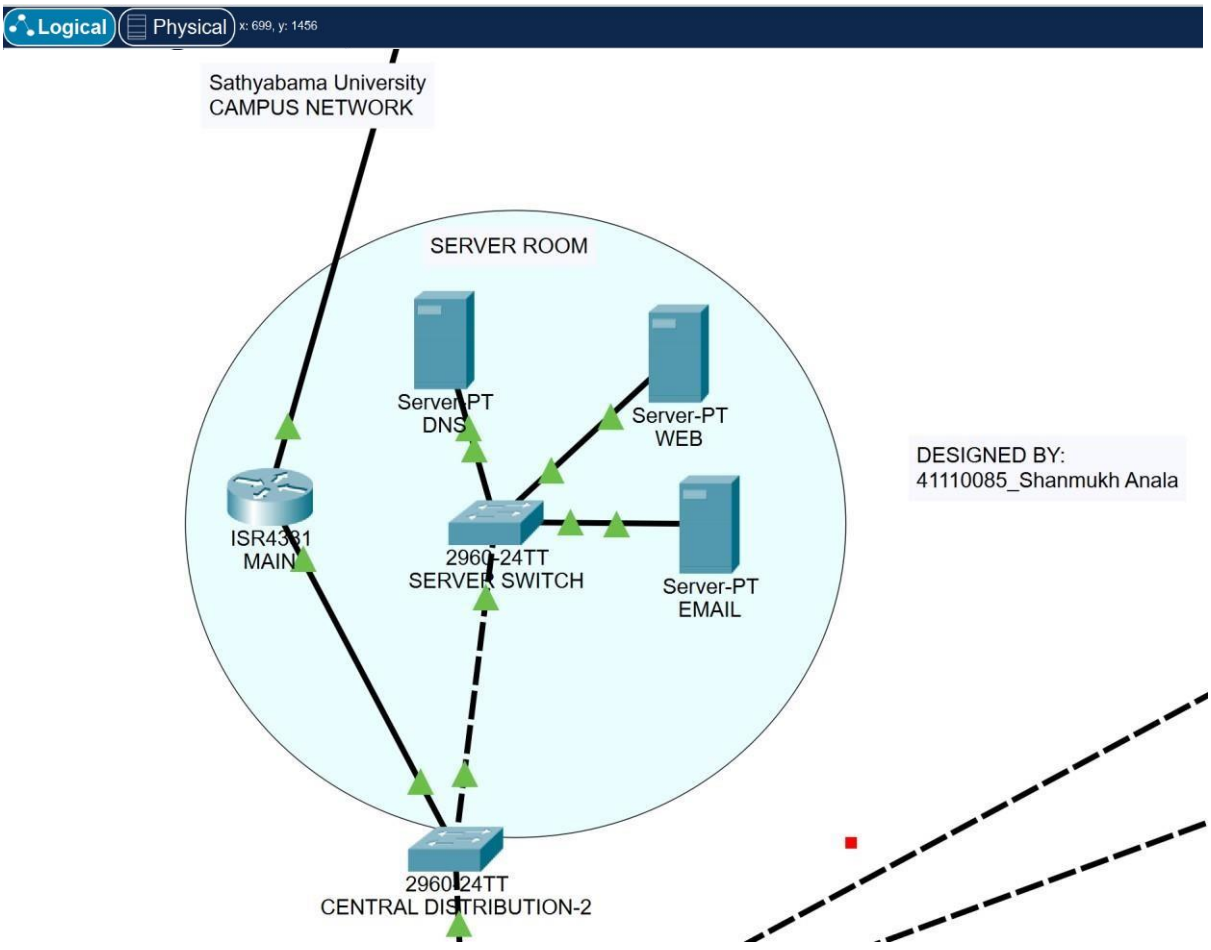
Conclusion:

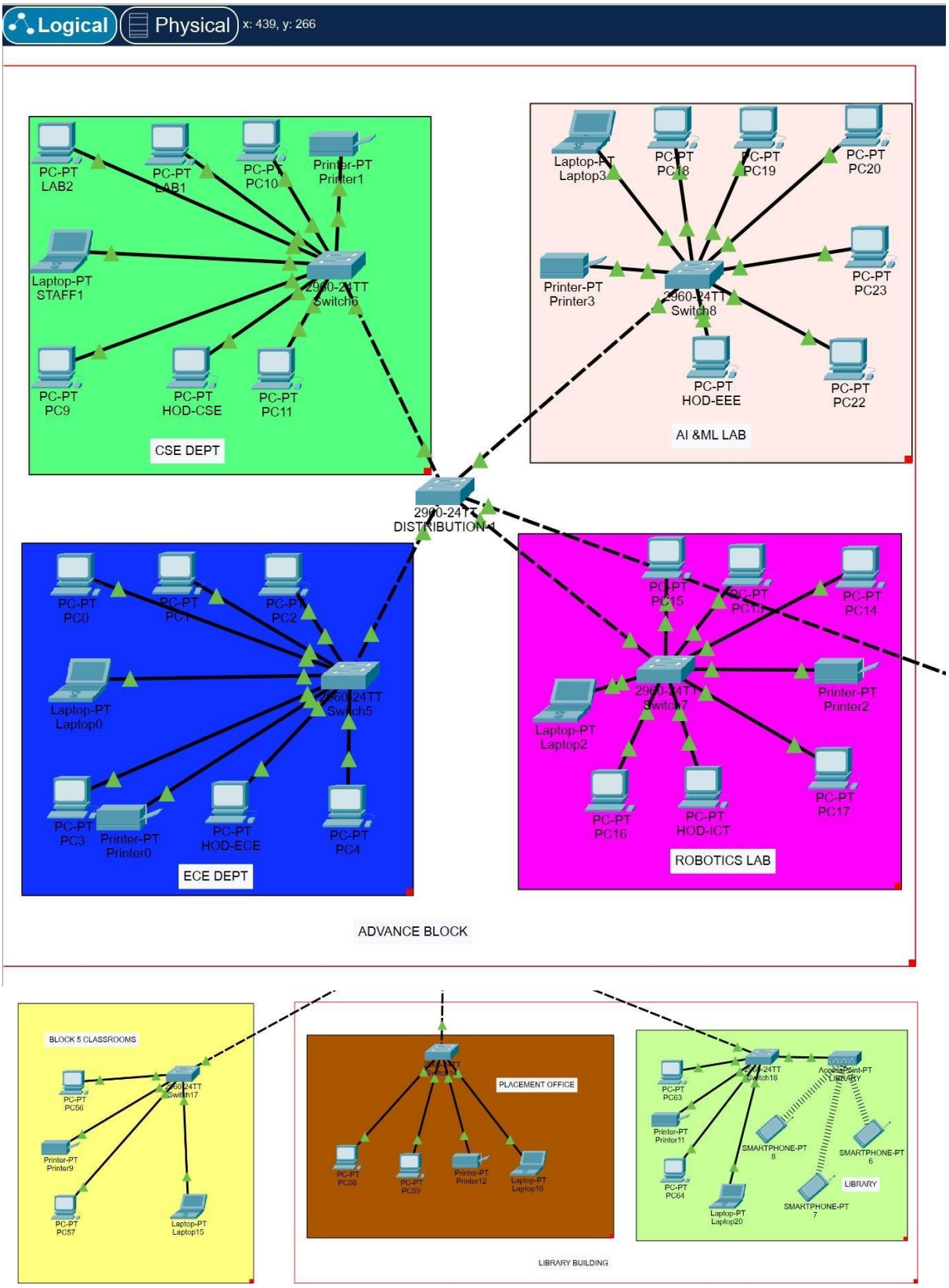
The revised architecture diagram incorporates load balancing, auto-scaling, database optimization, caching, and a DDOS mitigation layer to improve scalability, availability, and cost efficiency while mitigating DDOS attacks. This design will help the ecommerce retailer to better handle burst traffic during flash sales and reduce the risk of database corruption and DDOS attacks.

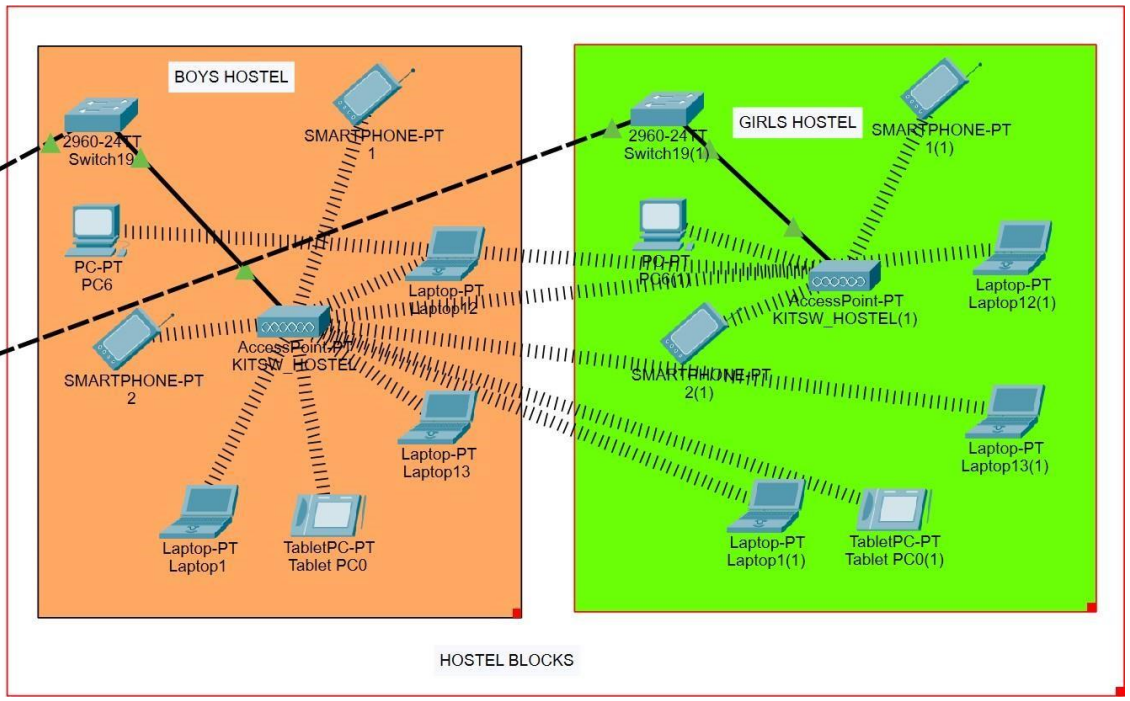
Network Mapping with Cisco Packet Tracer:

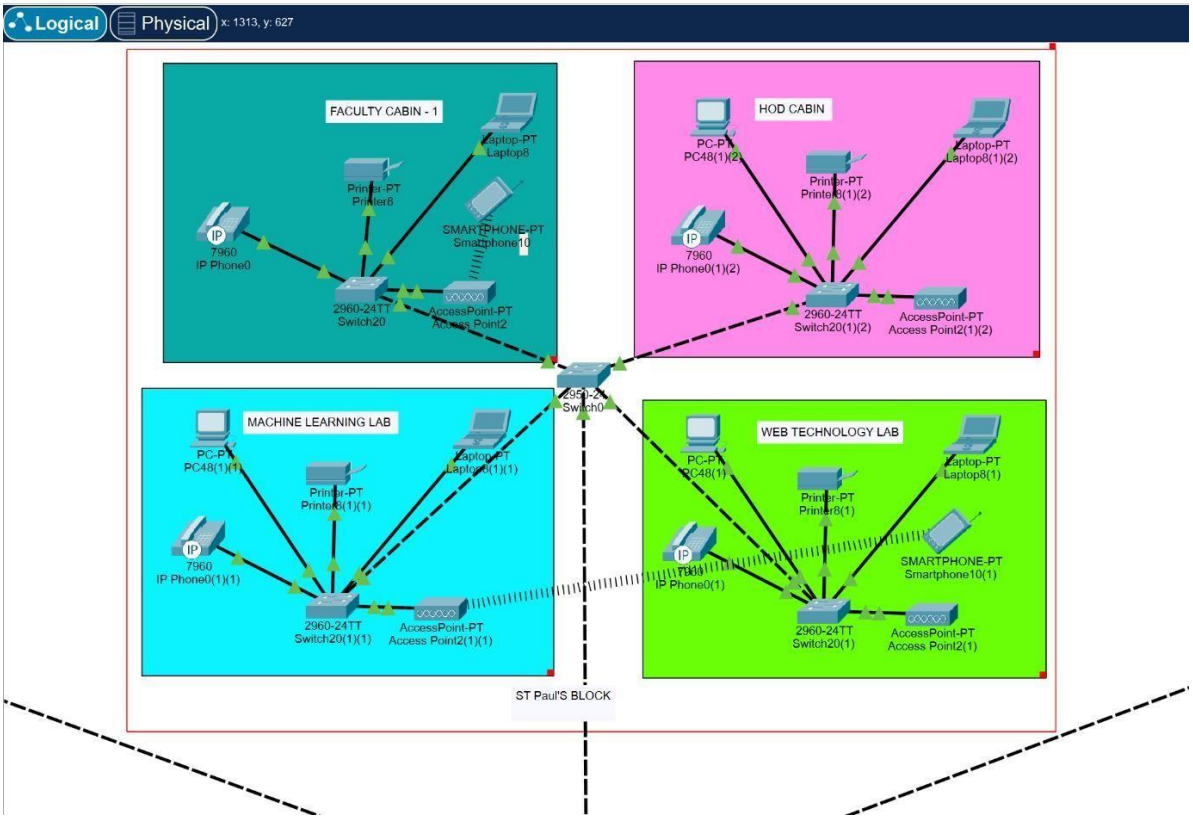


Main Sever


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
DESIGNED BY:
41110085_Shanmukh Anala
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
2960-24TT Switch17
PC-PT PC56
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
2960-24TT Switch18
Access Point-PT LIBRARY
PC-PT PC63
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
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)
7960
IP Phone0(1)
SMARTPHONE-PT
Smartphone10(1)
2960-24TT
Switch20(1)
AccessPoint-PT
Access Point2(1)
ST Paul'S BLOCK