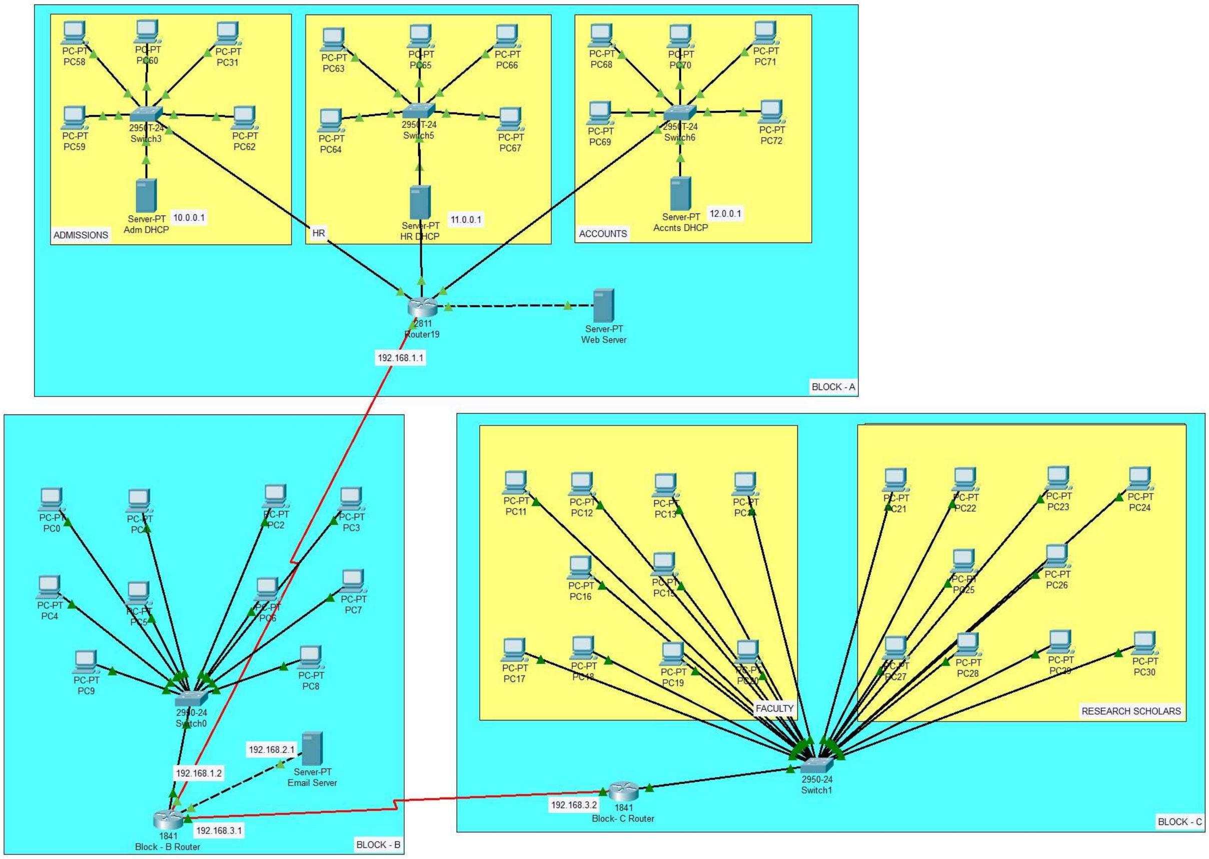
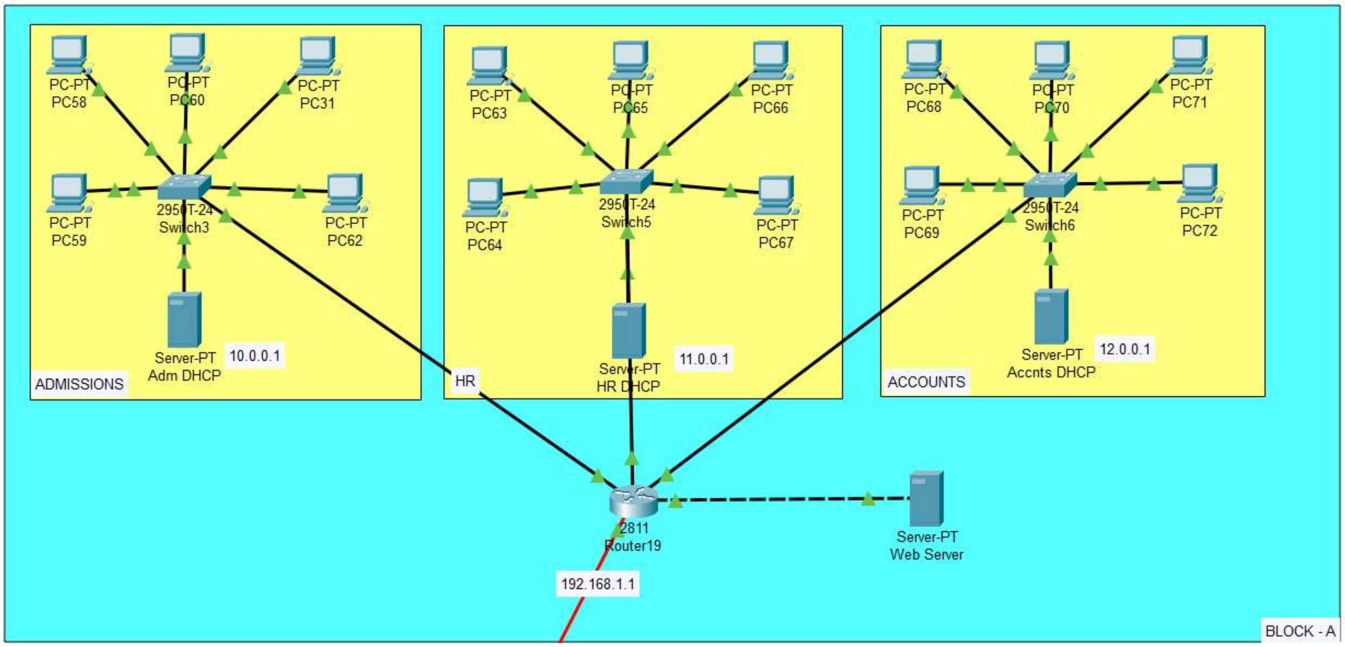
Security Assessment

Below is the network topology that consists of 3 blocks and systems in it interconnected which consists of a web server in Block-A and an email server in Block-B and the routers of all three blocks are connected through serial ports.



We will go through block by block and analyze the components involved, security risks and their mitigations.

Block - A



Block A consists of three departments (Admissions, HR and Accounts) which the network is segmented into 3 parts where one system of respective department should be inaccessible to the system in other departments.

It consists if components like PCs, Router, A Web Server and DHCP servers configured for every department systems.

Security Risk : Unauthorized Access

There is a security risk here where a system from one department can access the system in other departments. This leads to the exposure of information where if a person from HR department is accessing Accounts.

Proposed Solution

Apart from the respective department systems, other department systems should not be accessible.

We can achieve this by using VLANs and access control lists.

> VLAN stands for "Virtual Local Area Network." It is a technology used in computer networks to logically divide a single physical local area network (LAN) into multiple virtual LANs. These virtual LANs operate as separate entities.

> Access Control Lists (ACLs) are a fundamental security feature used in computer networks to control and manage the flow of traffic between devices. ACLs are employed primarily in routers and firewalls to permit or deny specific types of traffic based on defined rules and conditions. These rules act as filters, determining what traffic can pass through the network and what traffic should be blocked.

Steps (In Packet Tracer):

- Create VLANs

```
Switch-A(config)# vlan 10
Switch-A(config-vlan)# name Admissions

Switch-B(config)# vlan 20
Switch-B(config-vlan)# name HR

Switch-C(config)# vlan 30
Switch-C(config-vlan)# name Accounts
```

- Assign ports to VLANs

```
Switch-A(config)# interface fastethernet 0/0
Switch-A(config-if)# switchport mode access
Switch-A(config-if)# switchport access vlan 10

Switch-B(config)# interface fastethernet 0/1
Switch-B(config-if)# switchport mode access
Switch-B(config-if)# switchport access vlan 20

Switch-C(config)# interface fastethernet 1/0
Switch-C(config-if)# switchport mode access
Switch-C(config-if)# switchport access vlan 30
```

- Configure the router

```
Router(config)# interface fastethernet 0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# 10.0.0.1 255.0.0.0
Router(config)# interface fastethernet 0/0.20
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# 11.0.0.1 255.0.0.0

Router(config)# interface fastethernet 0/0.30
Router(config-subif)# encapsulation dot1q 30
Router(config-subif)# 12.0.0.1 255.0.0.0
```

- Create Access Control Lists with the respective IP addressess

```
Router(config)# access-list 100 deny 11.0.0.1 0.0.0.0 12.0.0.1 0.0.0.0
Router(config)# access-list 100 permit ip any any
```

- Apply ACL to VLAN interfaces

```
Router(config)# interface fastethernet 0/0.10
Router(config-if)# ip access-group 102 in

Router(config)# interface fastethernet 0/0.20
Router(config-if)# ip access-group 101 in

Router(config)# interface fastethernet 0/0.30
Router(config-if)# ip access-group 100 in
```

- Save the configuration and we mitigated the security risk of unauthorized accessing of systems of one department to the system of other department.

Security Risk : Web Server Security Risks

Department systems can access the web as the web server is functioning.

There are certain security risks possible :

- `Insecure Configuration` - Incorrectly configured web servers can expose sensitive information or grant unauthorized access to files or directories
- `DDoS Attacks` - Web servers can be targeted with Distributed Denial of Service (DDoS) attacks, where multiple compromised devices flood the server with traffic, overwhelming

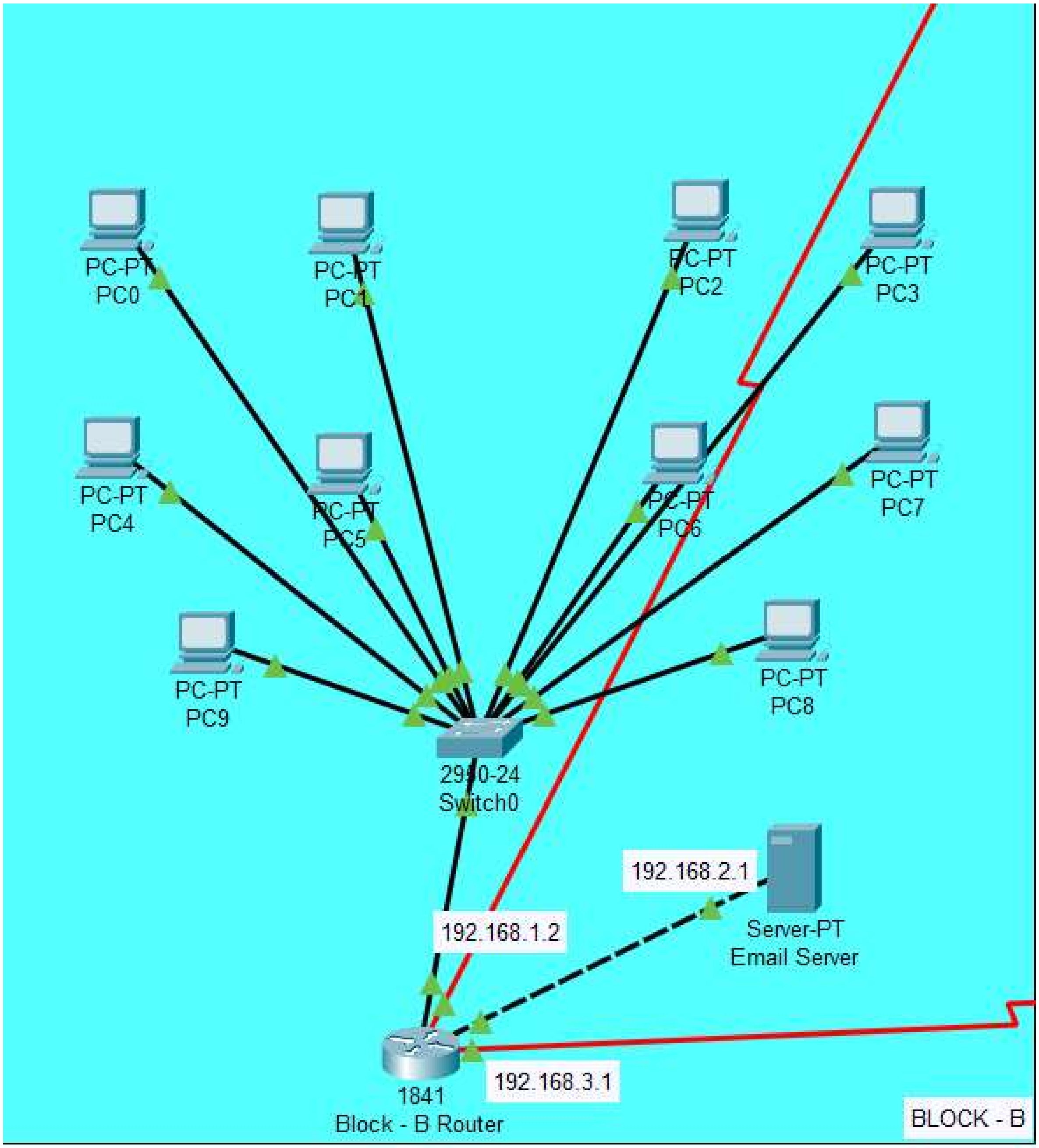
its resources and making it inaccessible to legitimate users.

- `SQL Injection` - If the web server interacts with a database and is not properly secured, attackers can manipulate the database through maliciously crafted SQL queries.
- `Cross-Site Scripting (XSS)` - XSS attacks occur when malicious scripts are injected into web pages, allowing attackers to steal sensitive information or hijack user sessions.
- `Server Misconfiguration` - Misconfigurations in the server software or operating system settings can expose unnecessary services or open unnecessary ports, providing potential entry points for attackers.
- `Insecure File Uploads` - If the web server allows users to upload files without proper validation, attackers can upload malicious files that can lead to code execution or data leakage.

Proposed Solutions

- `Secure Configuration` - Review and adjusting the server configuration to minimize exposure of sensitive information, disable unnecessary services and ports, and implement secure protocols like HTTPS.
- `Strong Authentication` - Enforcing strong password policies and implementing multi-factor authentication (MFA) for added security.
- `Web Application Firewall (WAF)` - Deploying a WAF to protect web applications from common attacks, such as SQL injection, XSS, and CSRF.
- `File Upload Validation` - Validating and restrict file uploads to prevent malicious files from being uploaded to the server.
- `Data Encryption` - Using encryption protocols (SSL/TLS) to protect data transmitted between the web server and clients.

Block - B



In this block, there are systems interconnected and there's a Email server in it.

Possible security risks are :

Security Risk : Email Phishing

Employees could fall victim to phishing emails or websites, leading to stolen credentials or malware infection.

Several factors contribute to the prevalence of email phishing like Social Engineering, Ease of Execution, Anonymity, Compromised credentials and Impersonation of trusted entities etc.

Proposed Solution

- `Email Security Gateway` - Implementing an email security gateway solution that includes spam filters, antivirus scanning, and anti-phishing measures
- `Domain-based Message Authentication, Reporting, and Conformance (DMARC)` - DMARC validates the authenticity of email senders and can instruct email servers on how to handle suspicious emails
- `Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)` - Configuring SPF and DKIM on the email server to verify the legitimacy of incoming emails and prevent domain spoofing.
- `Attachment Scanning` - Utilizing attachment scanning solutions to check email attachments for malware and malicious content before they reach users.

Security Risk : Denial of Service (DoS) Attacks

Attackers might attempt to overwhelm the email server, router, or other systems with a flood of traffic, causing a denial of service for legitimate users.

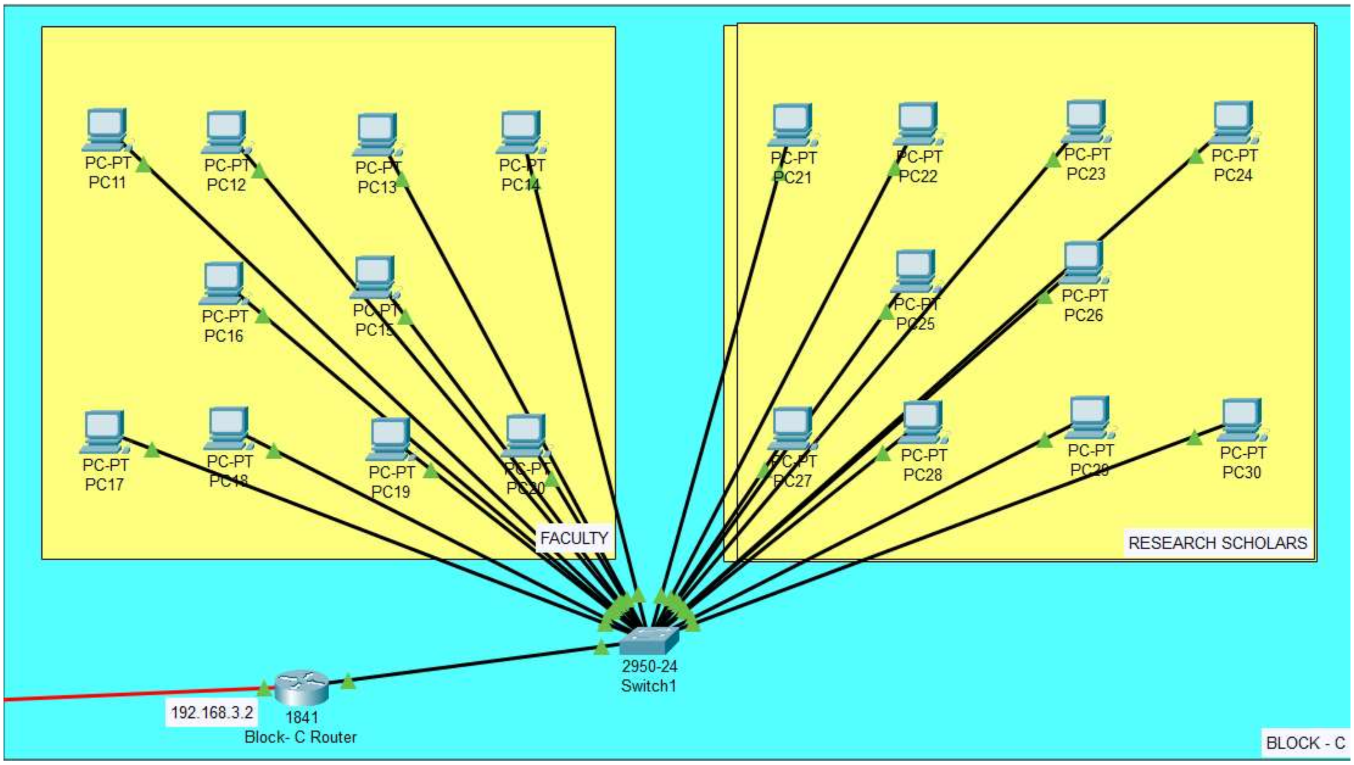
Denial of Service (DoS) is a cyber attack where an attacker overwhelms a target's resources, making its services or website inaccessible to legitimate users. It aims to disrupt availability and functionality.

Proposed Solution

- `Bandwidth Management` - Implementing Quality of Service (QoS) policies on the router to prioritize critical traffic over non-essential traffic. This helps prevent the network from becoming overwhelmed during a DoS attack
- `Ingress and Egress Filtering` - Configuring the router to perform ingress and egress filtering to block packets with spoofed source IP addresses. This helps prevent attackers from using IP address spoofing in their attacks.
- `Rate Limiting` - Enabling rate limiting on the router and switches to limit the number of packets allowed per second from individual IP addresses or network segments. This can help mitigate the impact of low-scale DoS attacks.
- `Load Balancers` - Deploying load balancers in front of critical services, including the email server, to distribute incoming traffic evenly across multiple servers. This helps

distribute the load during a DoS attack.

Block - C



Block C consists of two departments (Faculty & Research Scholars) and interconected to a router.

Possible security risks are

Security Risk : Brute Force Attack

Weak passwords on the systems, email server, or router could be susceptible to brute force attacks, where attackers try numerous password combinations to gain access. Attackers might also use social engineering techniques to trick employees into revealing sensitive information or granting access to their systems or the network.

Proposed Solution

- `Strong Password Policy` - Passwords to be of sufficient length and complexity, including a mix of uppercase and lowercase letters, numbers, and special characters.

- `Account Lockout Policy` - Implementing an account lockout policy that temporarily locks out user accounts after a certain number of failed login attempts.
- `Two-Factor Authentication (2FA)` - This adds an extra layer of security by requiring a second form of authentication, such as a one-time code sent to the user's mobile device
- `Rate Limiting` - Rate limiting restricts the number of login attempts from a single IP address or user within a specific time period, preventing brute force attacks.
- `IP Whitelisting/Blacklisting` - Maintaining a list of trusted IP addresses (whitelisting) that are allowed to access critical systems. Block or limit access from suspicious or unauthorized IP addresses (blacklisting).
- `Implementing CAPTCHA` - Implementing CAPTCHA on login pages to prevent automated scripts from repeatedly attempting login.

Security Risk : Unauthorized Access

Systems in Block - C are categorized into two seperate departments same as like in Block - A.

Thus, unauthorized access takes place here too which the proposed solution is already discussed at Block-A mitigations.

Thus, college campus network topology is created and discussed about the security risks and their proposed solutions with mitigations.