CYBER SHIELD: Defending the Network

Part 1: University Campus Topology/Network Analysis and Security Analysis.

TASKS:

TASK 1: Campus Network analysis

1. Network Topology
    - **Main Campus Router**: Placed at the centre of the University layout, serving as the primary routing device.
    - **Hostel Router:** Connects to the main campus router using the serial port.
    - **Cloud Router:** This connects the main campus router with the cloud router with a serial port. It connects to the EMAIL server.
    - **Main Campus Switch:** Connected to the main campus router and this switch is an L3 switch which connects to several other floors in the main buildings.
    - **Hostel Switch:** It is also an L3 switch which connects the hostel router to the several hostel blocks on the campus. This switch is again connected to other switches through copper cross-over wires.
    - **iBus Centre:** This is the centre in the campus where it is connected to wireless access points which helps students to connect their PCs, smartphones and laptops with WPE encryption and password protection.
2. Network Segmentation
    - The Network is segmented into four main areas:

1) Main Building: Which consists of different floors serving their purpose in the network.
2) Hostel Area: This connects all the campus hostel blocks.
3) iBus Campus/Hostel/Wifi: This is responsible for providing wifi all over the campus.
4) Cloud Server: It contains Email-Server.

3. Security Systems not in place

1) Access Control: It is not implemented and is up to mark.
2) FireWalls: Not mentioned in the existing topology.
3) Port-Security: It helps from unauthorized access into the network making the network more vulnerable.
4) Switches Security: There is no password set to access the switches so that no unauthorised access takes place.

4. Security Systems in Place

Wireless Encryption: WPE is used for wifi as of now though it is outdated and will be updated by the end of this task.

Passwords: Wireless Wifi requires a password to connect.

TASK 2: Network Mapping:

- **Main Campus Router**: Placed at the centre of the University layout, serving as the primary routing device.

- **Hostel Router:** Connects to the main campus router using the serial port.
- **Cloud Router:** This connects the main campus router with the cloud router with a serial port. It connects to the EMAIL server.
- **Main Campus Switch:** Connected to the main campus router and this switch is an L3 switch which connects to several other floors in the main buildings.
- **Hostel Switch:** It is also an L3 switch which connects the hostel router to the several hostel blocks on the campus. This switch is again connected to other switches through copper cross-over wires.
- **iBus Centre:** This is the centre in the campus where it is connected to wireless access points which helps students to connect their PCs, smartphones and laptops with WPE encryption and password protection.

TASK 3: Attack Surface Mapping

1. Identified Vulnerabilities and Weaknesses:

- **Weak Wireless Encryption:** The use of WPE encryption is highly vulnerable to attacks.
- **Lack of Port-Security:** No port-security systems in place to prevent unauthorized access and protect the network.
- **Basic Access Control:** Only password protection for wireless access points, no robust authentication and authorization systems.

2. Potential Entry Points for Cyber-Attacks:

- **Wireless Networks:** Weak encryption (WPE) makes wireless access points easy targets for unauthorized access.

- **Unmonitored Network Segments:** Lack of VPNs and port-security leaves network segments exposed to potential threats.
- **Unauthorized Access:** Insufficient access control mechanisms could allow unauthorized users to connect to the network.

Deliverables

1. Network Topology Diagram:

(Visual representation of the existing infrastructure in Cisco Packet Tracer, depicting the placement of routers, switches, wireless access points, and connected devices.)

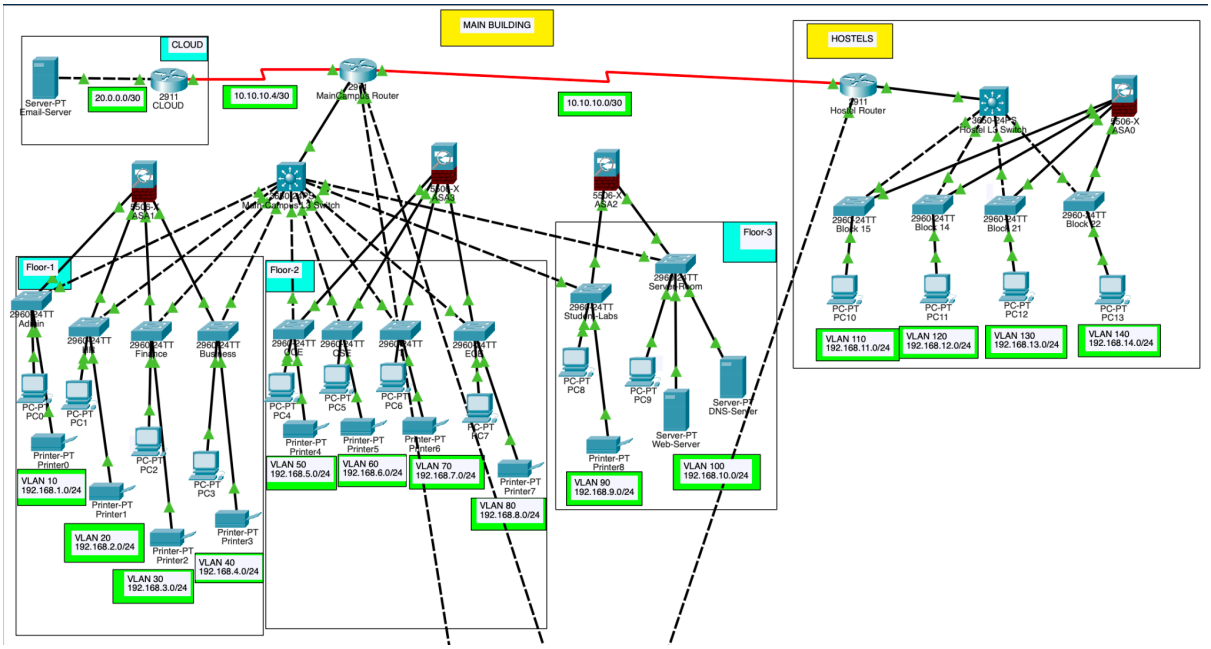
2. Security Assessment Report:

Security Risks:

- **Weak Wireless Encryption:** WPE is highly vulnerable to attacks.
- **Lack of IDS and Firewalls:** No mechanisms in place to monitor and protect the network.
- **Basic Access Control:** Only password protection for wireless access points.

Proposed Solutions and Countermeasures:

- **Upgrade Wireless Security:** Implement WPA2 encryption for all wireless access points to enhance security.
- **Deploy ACLs and Port-Security:** Implement Access Control Lists and Port-Security to protect the network from potential threats.
- **Regular Security Audits:** Conduct periodic security audits and vulnerability assessments to identify and address potential weaknesses in the network.



Part-2: Hybrid Working Environment design for both teachers and students.

TASK-1: Explore options for achieving secure Hybrid Network access

1) Hierarchical Network Design:

- Core Routers and Multilayer switches and Access Switches: Implementing a Hierarchical model is crucial as this ensures efficient Data Flow and management. Core Routers will connect to multilayer switches and these switches connect the access switches.

2) VLAN and Subnetting:

- Allocating specific VLAN and subnets to each department to manage the network traffic securely and efficiently.

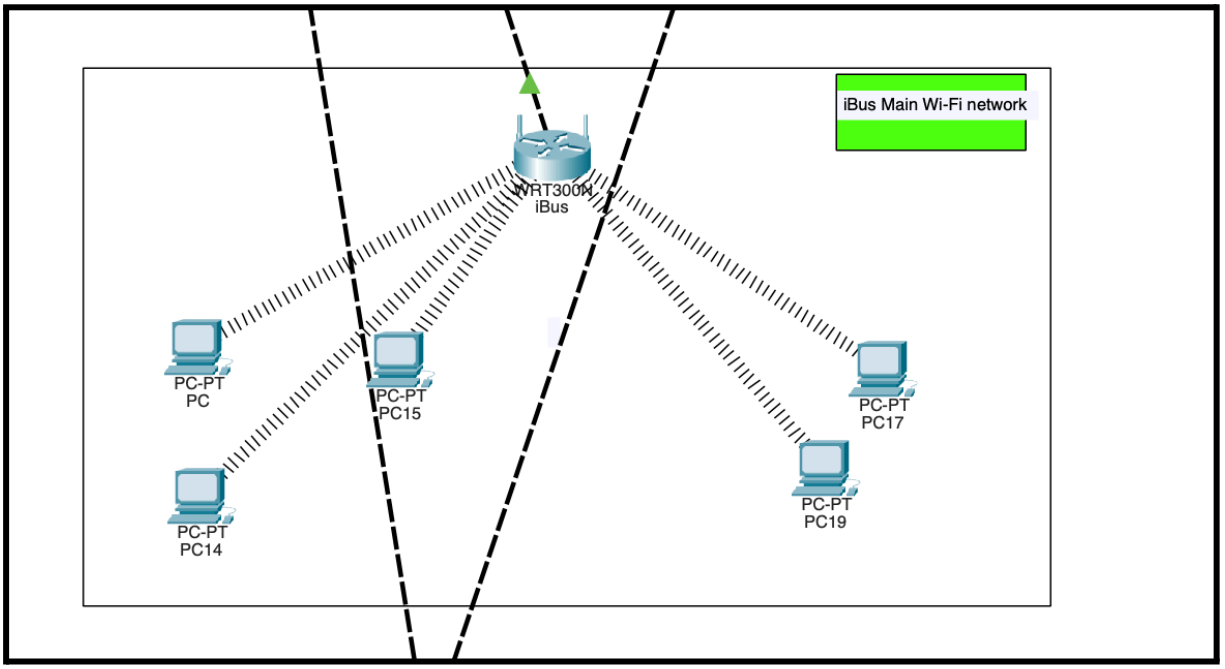
3) Security Measures:

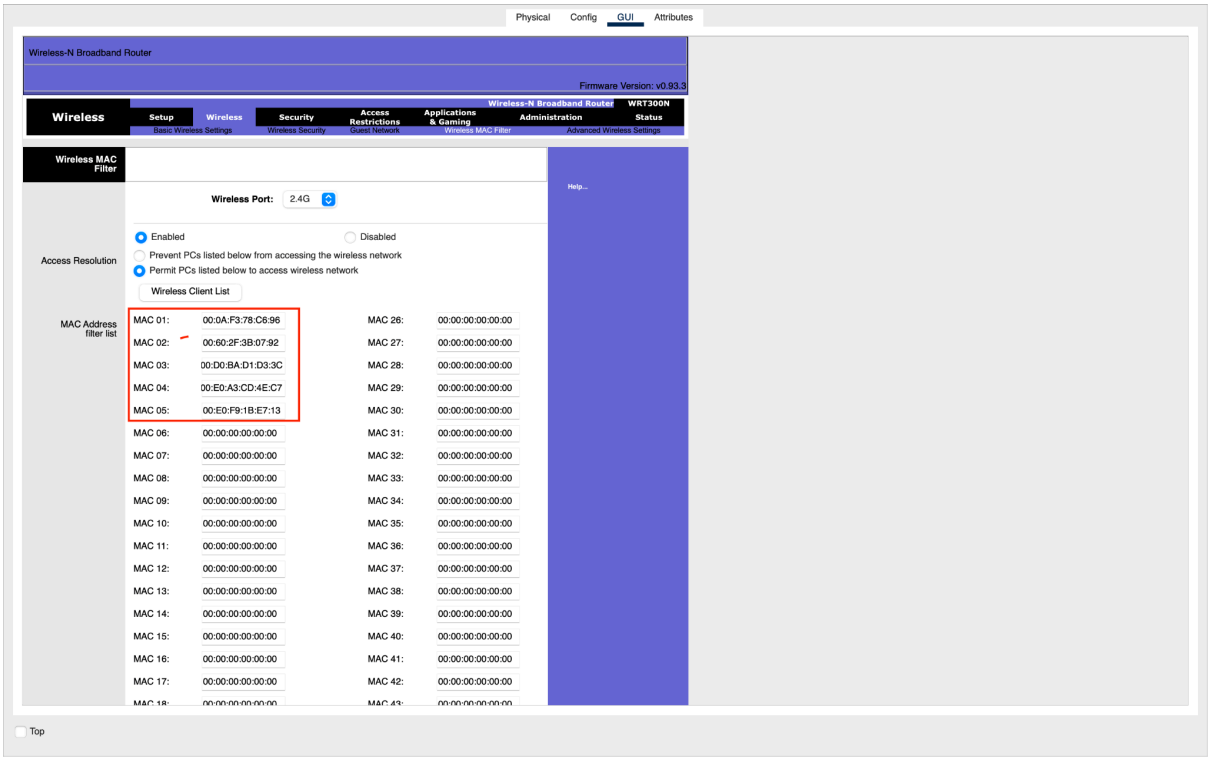
- **Access Control Lists(ACLs):** Configure ACLs to restrict access to sensitive areas and services, ensuring that only authorized users can access specific resources.
- **Port-Security:** Enforce port-security measures to prevent unauthorized devices from connecting to the network, safeguarding against potential breaches.

```
admin#show port-security interface fastEthernet 0/2
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Restrict
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 0
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0000.0000.0000:0
Security Violation Count    : 0

admin#
```

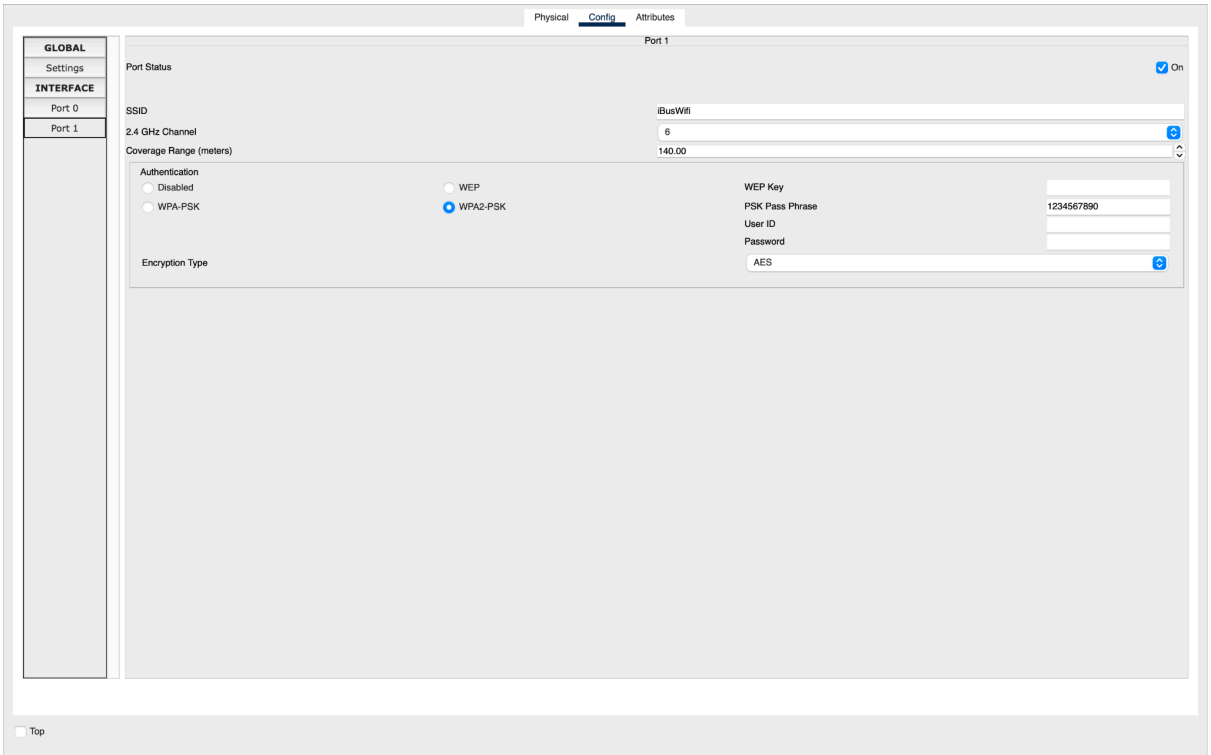
4) Separate Wi-Fi Networks:

- **iBus Main Campus Network:** This will ensure that only faculty can connect to the network by denying all the other MAC addresses in the network.

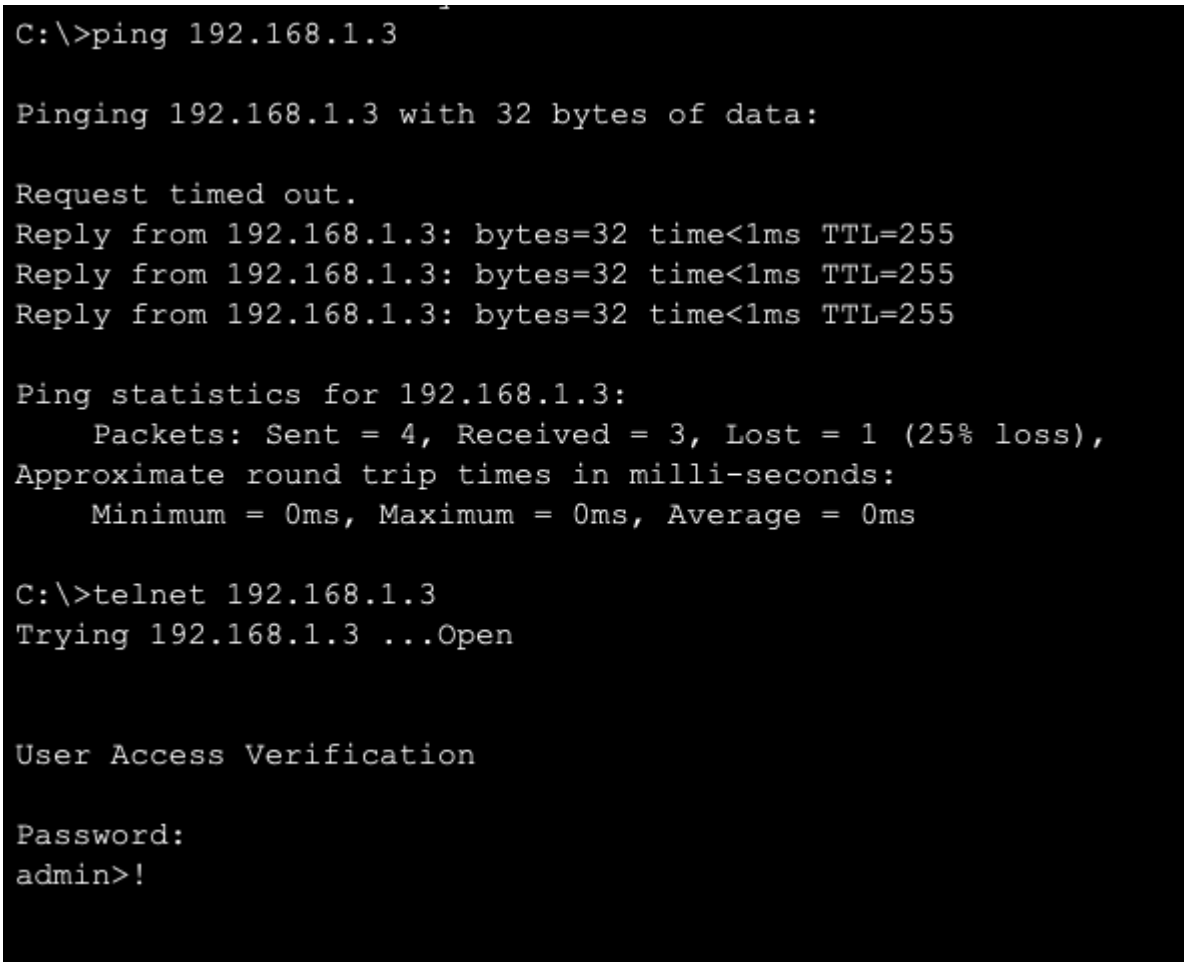




- **iBus Main/Hostel Network:** This uses WEP2 encryption to help all the devices of the students and the faculty to connect to the network and work in a hybrid mode.



5) Telnet access: As Port security is already in place Telnet access is given to the faculty to access the router directly from the PCs.



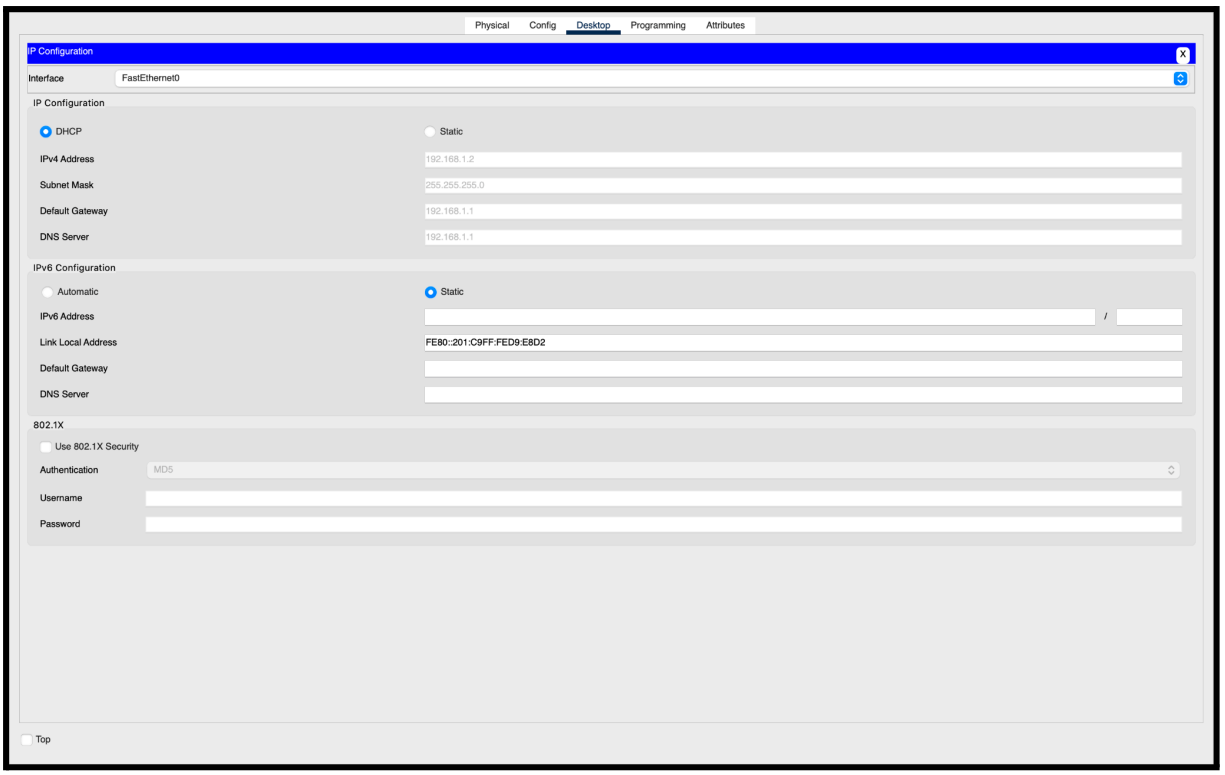
6) DHCP Configuration: Establish DHCP Configuration for dynamic IP address allocation. Assign static IP addresses to critical devices to ensure stability.

7) Monitoring and Testing:

1) **Network Monitoring Tools:** Integrate advanced monitoring tools to track performance and security in real time.
2) **Comprehensive Testing:** Conduct thorough testing of communication channels, DHCP services, ASA(FireWall) connectivity, and security measures to ensure effectiveness.

TASK-2: Update the Campus Network Topology with New Components

1) Network Design and Topology Implementation:
    - Detailed Network Topology: Developed a comprehensive topology outlining the placement of routers, switches, and servers.
    - Core Routers and Switches: Configured core routers, multilayer switches, and access switches to optimize network performance and management.
2) VLANs and Subnetting Configuration:
    - VLAN Allocation: Planned and implemented VLAN allocations for each department to ensure scalability and efficiency.
    - VLAN Implementation: Applied VLAN configurations on respective switches to manage and isolate traffic.
3) Security Measures Implementation (ACLs, Port-Security):
    - Access Control Lists: Defined stringent ACLs to control user access and protect sensitive resources.
    - Port-Security: Set up port-security measures to prevent unauthorized access to network ports.
4) DHCP Implementation:
    - Established and configured DHCP for dynamic IP address allocation. Shown below image will give us an idea and confirmation about DHCP configuration in all the PCs in the network.



5) Network Monitoring Tool Implementation:

- Monitoring Tools: Deployed advanced monitoring tools for real-time performance and security tracking.
- Proactive Issue Resolution: Ensured proactive identification and resolution of potential network issues.

TASK-3: Explain the Reason Behind Choices and Detail the Risks and Advantages

Reasoning Behind Choices:

1) Hierarchical Network Design: A hierarchical model ensures efficient data management, scalability, and redundancy, enhancing overall network performance and reliability.

2) VLANs and Subnetting: VLANs and subnets provide secure traffic segmentation and efficient network management, reducing the risk of unauthorized access and improving performance.
3) Security Measures: ACLs, and port-security measures ensure robust protection against unauthorized access, data breaches, and other security threats.
4) DHCP Configuration: DHCP facilitates dynamic IP address allocation, ensuring efficient management and connectivity of devices.
5) Telnet Access: This will help so much time as switches, and routers of respective departments are accessed through the respective PC without any unauthorised access.
6) Separate Wi-Fi: Allowing only faculty MAC addresses will help us ensure that only authorised members are accessing the network and they are not misusing it.
7) Monitoring and Testing: Advanced monitoring tools and comprehensive testing ensure continuous performance tracking and security, allowing proactive issue resolution

RISKS and ADVANTAGES:

1) Advantages:
    - Enhanced Security: Robust security measures (ACLs, FireWalls, port-security) protect against unauthorized access and data breaches, ensuring data confidentiality, integrity, and availability.
    - Operational Efficiency: Streamlined communication, dynamic IP allocation, and efficient routing improve overall network efficiency.
    - Cost-Efficiency: Internal management of the network infrastructure reduces reliance on third-party services, lowering operational costs.

- Reliability: Redundancy strategies and a hierarchical design increase network reliability and ensure continuous availability.

2) Risks:

- Complexity: Implementing a hierarchical network design with multiple security measures can be complex and may require advanced technical expertise.
- Initial Cost: Initial setup costs for advanced hardware and monitoring tools can be high, although long-term savings and efficiency gains will offset this.
- Maintenance: Ongoing maintenance and updates are required to ensure security and performance, demanding regular attention and resources.

By implementing this comprehensive methodology, the college will establish a secure and efficient hybrid working environment for faculty and students, ensuring seamless access to resources and services both on-campus and remotely.

Part-3: Web Content Filtering for Campus Network

To address the issue of students misusing campus resources by accessing irrelevant websites, I have implemented a solution to restrict access to specific categories of web content. Below are the detailed steps and configurations used to achieve this, aligned with the tasks and deliverables outlined in the problem statement.

Task 1: Explore Network Security Product

To restrict access to only allowed categories of web content, I explored several network security products. After thorough research, I selected Cisco's Content Filtering features within the Cisco IOS. This method leverages Access Control Lists (ACLs) and Policy Maps to block access to specific websites by IP address or domain name.

Network Security Product: Cisco IOS with Content Filtering

Capabilities:

- Blocks access to specific websites by IP or domain name.
- Configurable using ACLs.
- Integrates with existing network infrastructure.

Task 2: Update Campus Network Topology with New Component(s)

I updated the existing campus network topology to include content filtering capabilities. This involved configuring the core router with ACLs to enforce web content restrictions.

Task 3: Explain Reasoning Behind Choice

Reasoning:

1) Risks Addressed: The primary risk addressed is the misuse of campus network resources for accessing irrelevant or potentially harmful websites.
2) Advantages:
    - Cost-Effective: Utilizes existing Cisco IOS features without the need for additional hardware.
    - Scalable: Easy to update and manage as new websites need to be blocked.
    - Effective: Directly blocks traffic at the network level, ensuring compliance with access policies.

Task 4: Write the Policies

The following are the policies applied to block access to specific websites, demonstrated with examples for Facebook and YouTube.

Step-by-Step Configuration

Step 1: Create an Access Control List (ACL) to Deny HTTP Traffic to Specific Sites

I created an extended ACL to block HTTP traffic to the IP addresses of the websites we want to restrict. For demonstration purposes, I have chosen the IP addresses 31.13.71.36 (facebook.com) and 172.217.10.78 (youtube.com).

hostels(config)# ip access-list extended BLOCK-SOCIAL-SITES

hostels(config-ext-nacl)# deny tcp any host 31.13.71.36 eq www

hostels(config-ext-nacl)# deny tcp any host 172.217.10.78 eq www

hostels(config-ext-nacl)# permit ip any any

hostels(config-ext-nacl)# exit

Step 2: Create a Class Map to Match the ACL

Next, I created a class map to match traffic defined by our ACL.

hostels(config)# class-map match-all BLOCK-SITES

hostels(config-cmap)# match access-group name BLOCK-SOCIAL-SITES

hostels(config-cmap)# exit

Step 3: Create a Policy Map to Drop the Traffic

I then created a policy map to specify the action to take on the matched traffic. In this case, I drop the traffic by using the police command, which rate-limits and drops the traffic

hostels(config)# policy-map WEB-BLOCK

hostels(config-pmap)# class BLOCK-SITES

hostels(config-pmap-c)# police rate 32000 conform-action drop exceed-action drop

hostels(config-pmap-c)# exit

Step 4: Apply the Policy Map to the Interface

Finally, I applied the policy map to the outbound traffic on the interface facing the Internet.

hostels(config)# interface GigabitEthernet 0/0

hostels(config-if)# service-policy output WEB-BLOCK

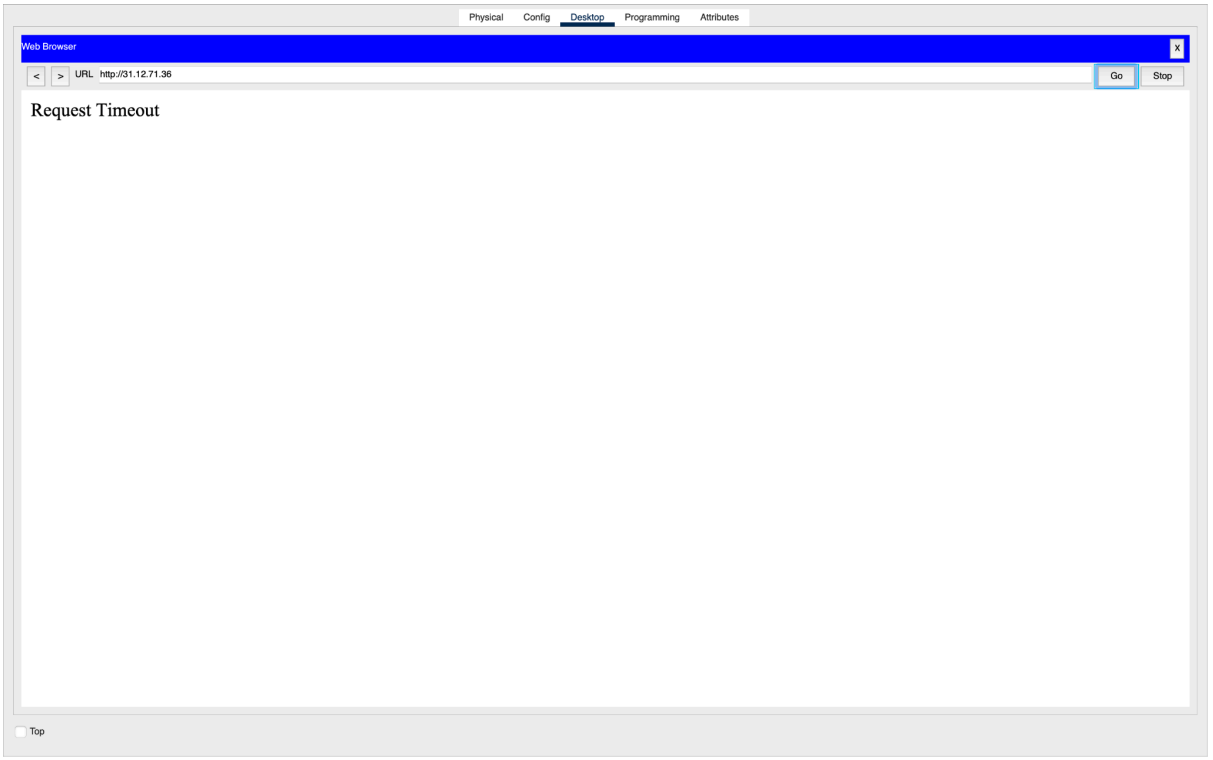
hostels(config-if)# exit

```
hostels(config)#ip access-list extended BLOCK-SOCIAL-SITES
hostels(config-ext-nacl)#deny tcp any host 31.13.71.36 eq www
hostels(config-ext-nacl)#deny tcp any host 172.217.10.78 eq www
hostels(config-ext-nacl)#permit ip any any
hostels(config-ext-nacl)#exit
hostels(config)#class-map match-all BLOCK-SITES
hostels(config-cmap)#match access-group name BLOCK-SOCIAL-SITES
hostels(config-cmap)#exit
hostels(config)#policy-map WEB-BLOCK
hostels(config-pmap)#class BLOCK-SITES
```

```
hostels(config-pmap-c)#exit
hostels(config-pmap)#interface GigabitEthernet 0/0
hostels(config-if)#service-policy output WEB-BLOCK
hostels(config-if)#exit
hostels(config)#exit
hostels#
```

```
User Access Verification

Password:

hostels>en
Password:
hostels#show policy-map interface GigabitEthernet 0/0
 GigabitEthernet0/0

  Service-policy output: WEB-BLOCK

    Class-map: BLOCK-SITES (match-all)
      44 packets, 14608 bytes
      5 minute offered rate 260 bps, drop rate 0 bps
      Match: access-group name BLOCK-SOCIAL-SITES
      Queueing
        Output Queue: Conversation 265
        Bandwidth 0 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      24 packets, 7764 bytes
      5 minute offered rate 159 bps, drop rate 0 bps
      Match: any

hostels#show policy-map
  Policy Map WEB-BLOCK
    Class BLOCK-SITES
hostels#show access-lists BLOCK-SOCIAL-SITES
Extended IP access list BLOCK-SOCIAL-SITES
    deny tcp any host 31.13.71.36 eq www
    deny tcp any host 172.217.10.78 eq www
    permit ip any any

hostels#show class-map
 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all BLOCK-SITES (id 1)
   Match access-group name BLOCK-SOCIAL-SITES
hostels#
```

VERIFICATION



CONCLUSION:

By Following all the tasks above I have configured the network to block access to hostels for social websites like FaceBook and YouTube. This solution leverages existing network security features and enhances the overall security posture of the campus network.

OVERALL CONCLUSION:

Overall by following all the parts and tasks I have successfully configured the network in many ways for it to be robust and secure.

CLOUD SECURITY

Tasks & Deliverables

1) Improving Scalability and Availability

Scalability Improvements:

- Auto-Scaling Groups: Implement auto-scaling groups for application servers. This ensures the system can automatically scale up during high traffic and scale down during low traffic, optimizing resource usage and costs. Auto-scaling policies will be defined based on CPU usage, request rates, and other relevant metrics.
- Elastic Load Balancer (ELB): Use an Elastic Load Balancer to distribute incoming traffic across multiple instances, improving availability and fault tolerance. This helps balance the load efficiently, preventing any single instance from becoming a bottleneck.

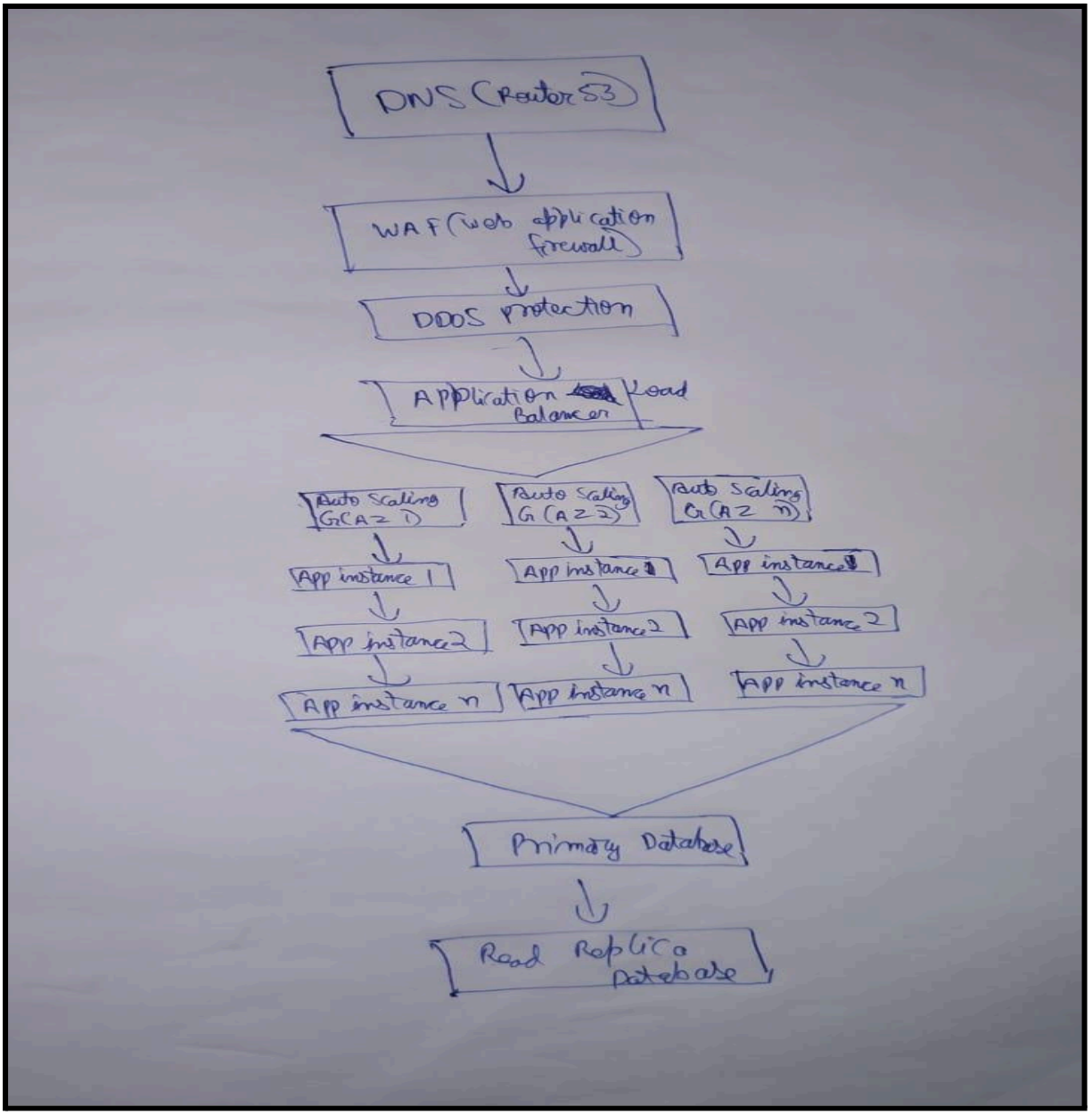
Availability Improvements:

- Multi-AZ Deployment: Deploy application servers and databases across multiple Availability Zones (AZs) to ensure high availability and fault tolerance. In the event of an AZ failure, traffic can be redirected to instances in another AZ, ensuring continuous service availability.
- Database Replication: Implement a read replica and failover mechanism for the database to ensure high availability and quick recovery in case of a primary database failure. The read replica can also help balance read traffic, reducing the load on the primary database.

Cost Efficiency:

- Spot Instances: Utilize spot instances for non-critical tasks to reduce costs. Spot instances are significantly cheaper than on-demand instances, although they can be terminated by the cloud provider with little notice.
- Auto-Scaling Policies: Define auto-scaling policies to adjust the number of instances based on demand. This ensures cost efficiency during non-peak times while still providing the necessary resources during peak traffic.

2) New Diagram with Proposed Design Improvements



3) Explanation:

- **Auto-Scaling Gatherings:**

  Advantages:

  Automatically changes assets because of traffic, guaranteeing ideal execution and cost-effectiveness.

  Provides a consistent client experience by keeping up with administration levels during busy times.

  Risks:

  Misconfigured auto-scaling approaches could prompt over or under-provisioning, influencing execution or causing superfluous expenses.

- **Versatile Burden Balancer (ELB):**

  Advantages:

  Distributes traffic proficiently, giving adaptation to internal failure and high accessibility.

  Prevents any single example from turning into a bottleneck.

  Risks:

  Single weak spot while possibly not appropriately arranged, however, moderated by multi-AZ sending.

- **Multi-AZ Organization**:

  Advantages:

Ensures high accessibility and fiasco recuperation abilities.

Increases adaptation to non-critical failure by circulating examples across various geological areas.

- **Cost Effectiveness:**

  Advantages:

  Reduces functional expenses by utilizing spot occurrences and enhancing asset use.

  Ensures assets are apportioned effectively founded on request.

  Risks:

  Spot examples can be ended by the cloud supplier, so they ought to be utilized for non-basic assignments.

4) Research on DDOS Attacks:

DDOS (Distributed-Denial Of Service) attacks are usually done due to botnets, traffic overload and vulnerability exploitation.

Types of DDoS Attacks:

1. Volume-Based Attacks:
   - UDP Flood: Involves sending a large number of UDP packets to random ports on a host, causing the host to check for the application listening at that port and reply with an ICMP "Destination Unreachable" message. This process consumes bandwidth and server resources.

- ICMP Flood: Also known as Ping Flood, this attack involves sending a large number of ICMP Echo Request (ping) packets to the target, overwhelming the target's bandwidth and preventing legitimate traffic from reaching the host.
- DNS Amplification: Involves sending DNS requests with a spoofed source IP address (the target's IP address) to open DNS servers. The servers reply to the target with large DNS responses, overwhelming the target with traffic.

2. Protocol Attacks:
   - SYN Flood: Exploits the TCP handshake process by sending a large number of SYN requests to a server, but not completing the handshake. This leaves open connections on the server, consuming resources and potentially leading to a denial of service.
   - Ping of Death: Sends malformed or oversized packets to the target, causing buffer overflow and potential system crashes.
   - Smurf Attack: Involves sending ICMP Echo Requests with a spoofed source IP address (the target's IP) to a network broadcast address. All devices on the network reply to the target, overwhelming it with traffic.
3. Application Layer Attacks:
   - HTTP Flood: Sends a large number of HTTP requests to the target's web server, often exploiting resource-intensive operations (like searching a database or loading large files) to exhaust server resources.
   - Slowloris: Sends HTTP requests very slowly, consuming server resources by keeping connections open and exhausting the server's connection pool.
   - DNS Query Flood: Involves sending a high volume of DNS requests to a DNS server, overwhelming its processing capacity and preventing legitimate DNS queries from being resolved.

5) Vulnerability and Resilience Strategies

- Potential Vulnerabilities:

· Volume-Based Attacks: Can overwhelm network bandwidth, causing service outages.

· Protocol Attacks: Can exploit weaknesses in network protocols, leading to disruptions.

· Application Layer Attacks: Can exhaust server resources, causing slowdowns or crashes.

- Resilience Strategies:

· Web Application Firewall (WAF): Protects against application layer attacks by filtering malicious traffic and blocking common attack patterns.

· DDoS Protection Service: Uses cloud provider's DDoS protection services to detect and mitigate DDoS attacks, ensuring continuous service availability.

· Rate Limiting: Controls the number of requests from a single IP address, preventing any one user from overwhelming the system.

· Traffic Analysis: Continuously monitors traffic patterns to detect and respond to anomalies, enabling proactive defence against attacks.

- Advantages:

· Improved Availability: Multi-AZ deployment and database replication ensure high availability and quick recovery, minimizing downtime and service disruptions.

· Enhanced Scalability: Auto-scaling groups and ELB handle burst traffic efficiently, providing a seamless user experience during peak times.

· Increased Security: WAF, DDoS protection, and rate limiting mitigate the risk of attacks, ensuring a secure environment for both users and the application.

- Risks:

· Configuration Complexity: Properly configuring and managing the new components requires expertise, and misconfigurations could lead to vulnerabilities or inefficiencies.

· Cost Implications: Additional resources and services may increase costs, though these can be optimized by using scaling policies and cost-effective instance types.

By implementing these improvements, the start-up will be better prepared to handle high traffic during sales events and mitigate potential DDoS attacks, ensuring a reliable and secure shopping experience for customers.