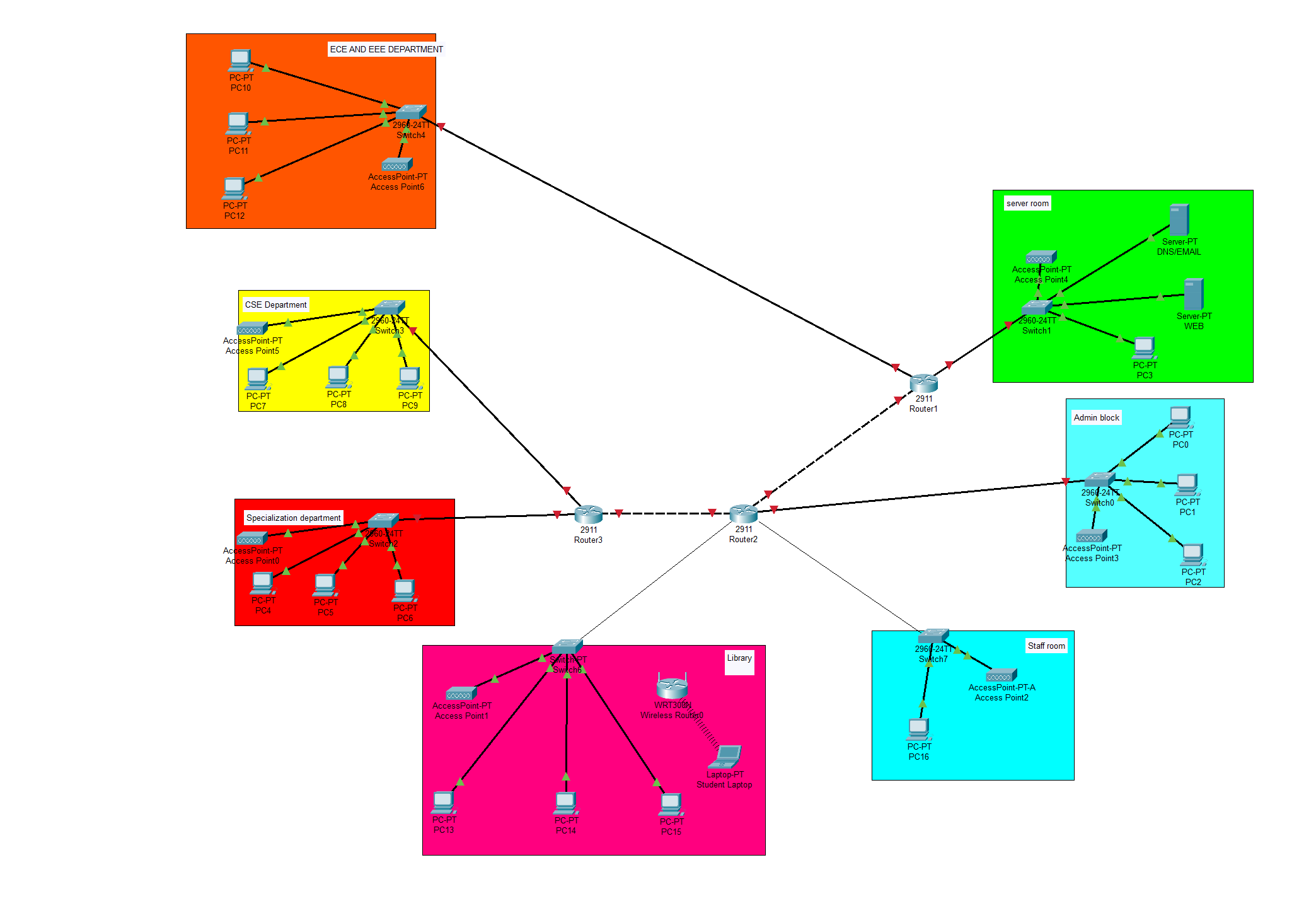
**Cisco Virtual Internship Program 2025**

**Cyber Shield: Defending the Network - Complete Project Report**

**PART 1: SECURITY ASSESSMENT REPORT  
Network Topology Diagram:  
**

**Network Analysis Overview**

After analyzing our college network topology, I found several departments connected through a basic router setup. The network has different zones like ECE/EEE Department, CSE Department, Specialization Department, Library, Server Room, Admin Block, and Staff Room. Each department has its own switch connecting multiple PCs and wireless access points.

**Current Network Segmentation**

The network is divided into different colored zones representing departments, but there's no real security segmentation. All departments connect directly to the main routers (Router1, Router2, Router3) without any filtering between them. This creates what we learned in class as a "flat network" where once someone gets access, they can potentially reach any other department.

**Trust Zones Identified**

Based on the topology, I can see these trust zones:

* **Public Zone**: Library and general student areas
* **Academic Zone**: ECE/EEE, CSE, and Specialization departments
* **Administrative Zone**: Admin Block and Staff Room
* **Critical Zone**: Server Room with main servers

The problem is all these zones trust each other completely with no barriers.

**Security Controls Assessment**

**What I Found:**

* Basic wireless access points in each department (good for connectivity)
* Switches and routers for network connectivity
* Servers in dedicated server room
* No firewalls visible between departments
* No intrusion detection systems shown
* No access control lists or authentication servers visible

**Major Security Gaps:**

1. **No perimeter security** - Direct connection between departments
2. **Flat network design** - Lateral movement is very easy
3. **No wireless security** - Access points don't show any authentication
4. **Missing monitoring** - No way to detect unusual network activity
5. **Server exposure** - Server room directly connected without protection

**Attack Surface Analysis**

**High Risk Areas:**

* **Wireless networks**: Students could potentially access any department's network through weak wireless security
* **Flat design**: An attacker in one department can easily move to others
* **Server room**: Critical servers are not properly isolated
* **No monitoring**: Attacks could go undetected for long time

**Likely Attack Scenarios:**

* Student brings infected laptop, malware spreads across departments
* Unauthorized wireless access leads to data theft
* Someone accesses admin systems from student areas
* No way to track who accessed what and when

**Risk-Based Countermeasures**

**High Priority (Must Fix):**

1. **Add firewalls** between main network zones
2. **Implement VLANs** to separate departments logically
3. **Secure wireless networks** with WPA2/WPA3 and proper authentication
4. **Isolate server room** with dedicated firewall

**Medium Priority:**

1. Install basic intrusion detection system
2. Set up network access control for device authentication
3. Implement logging for network activities
4. Create separate networks for students vs faculty

**Policy Changes Needed:**

* Students should not access administrative networks
* Guest network should be completely separated
* Server access should be restricted to IT staff only
* All network access should be logged and monitored

**Budget-Friendly Implementation**

Understanding that college budgets are tight, I suggest starting with:

1. Configure existing switches for VLAN separation (no extra cost)
2. Add one firewall between critical zones (moderate cost)
3. Improve wireless security settings (no extra cost)
4. Use free tools for basic network monitoring

**Part 1 Conclusion**

The current network works for basic connectivity but has serious security weaknesses. The flat design and lack of access controls make it vulnerable to various attacks. With some strategic changes and minimal investment, we can significantly improve security without disrupting normal operations.

Main recommendation: Start with network segmentation using VLANs and add at least one firewall to protect critical systems.

**PART 2: HYBRID ACCESS TECHNICAL DOCUMENTATION  
Network Topology Diagram:  
A diagram of a computer network

AI-generated content may be incorrect.**

**Project Overview**

After the security assessment, I was asked to design a hybrid access system that allows faculty to work from home while keeping students' access secure on campus. The main requirement was that internal services should never be directly exposed to the internet.

**Network Segmentation Design**

**User Role-Based Segmentation:**

**Faculty Network:**

* Dedicated VLAN for faculty devices
* Higher privilege level for accessing research databases and internal services
* Secure remote access through VPN when working from home
* Access to both academic and administrative resources

**Student Network:**

* Separate VLAN with restricted access
* Limited to educational resources and internet
* No access to faculty systems or administrative networks
* Controlled through access policies

**Chosen Technology Solution**

**Primary Solution: VPN (Virtual Private Network)**

I chose VPN as the main remote access solution because:

* It's cost-effective for a college budget
* Creates encrypted tunnel for secure communication
* Works well with existing router infrastructure
* Faculty are familiar with VPN clients

**Implementation in Network:**

* Added VPN-capable firewall/router near the network core
* Remote faculty devices connect through encrypted VPN tunnel
* VPN server authenticates users before granting access
* All remote traffic goes through campus security controls

**Authentication Flow**

**For Remote Faculty:**

1. Faculty member starts VPN client on home device
2. VPN client connects to campus VPN server
3. Server checks username/password against authentication database
4. If valid, encrypted tunnel is created
5. Faculty device gets campus network access as if on-site
6. All internet traffic can go through campus or split tunnel for better performance

**For On-Campus Users:**

1. Device connects to appropriate wireless network (faculty or student)
2. Captive portal asks for login credentials
3. Authentication server verifies access level
4. User gets network access based on their role

**Internal Service Protection**

**Security Measures:**

* VPN server acts as gateway - no direct internet exposure of internal services
* Firewall rules prevent unauthorized access between faculty and student networks
* Internal services like file servers, research databases only accessible through campus network
* Even remote faculty must connect through VPN to access these services

**Network Topology Updates**

**Key Changes Made:**

* Added firewall between main router and internal network
* Implemented VPN server capability
* Created remote access zone for managing external connections
* Set up policy enforcement points at network boundaries

**Traffic Flow:**

* Internet → Router → Firewall → VPN Processing → Internal Network
* Remote users must authenticate at VPN layer before accessing anything internal

**Risk Assessment**

**Risks Addressed:**

* **Data interception**: VPN encryption protects remote communications
* **Unauthorized access**: Authentication required before network entry
* **Internal exposure**: No direct internet access to internal services
* **Network segmentation**: Faculty and students kept in separate zones

**Remaining Risks:**

* VPN client security depends on faculty device security
* Need to monitor VPN connections for unusual activity
* Bandwidth limitations during peak usage
* Single point of failure if VPN server goes down

**Use Cases Covered**

**Faculty Working from Home:**

* Access to research databases and academic tools
* Secure connection to campus file servers
* Ability to manage course materials remotely
* Safe access to administrative systems when needed

**Students on Campus:**

* Access to educational resources and internet
* Connection to academic portals and lab systems
* Restricted from accessing faculty and admin systems
* Monitored usage for policy compliance

**Fallback Strategies**

**If VPN Fails:**

* Faculty can use secure web portals for critical applications
* Emergency access through controlled remote desktop solutions
* Temporary expansion of on-campus faculty network access
* Mobile hotspot policies for critical situations

**If Network Congestion:**

* Split tunneling allows non-sensitive traffic to bypass VPN
* Quality of Service (QoS) prioritizes academic traffic
* Load balancing across multiple internet connections if available

**Advantages of This Design**

1. **Security**: All remote access is encrypted and authenticated
2. **Simplicity**: Uses familiar VPN technology
3. **Cost-effective**: Leverages existing infrastructure
4. **Scalable**: Can add more VPN users as needed
5. **Flexible**: Supports various devices and operating systems

**Part 2 Conclusion**

The hybrid access design successfully balances security and usability. Faculty get secure remote access to all necessary resources while internal services remain protected from direct internet exposure. The VPN-based approach is practical for our college environment and provides a solid foundation for future enhancements.

**PART 3: WEB ACCESS POLICY AND FILTERING FRAMEWORK  
Network Topology Diagram:  
A diagram of a computer network

AI-generated content may be incorrect.**

**Problem Background**

After implementing the hybrid network, we started getting complaints about students streaming videos during lectures, downloading torrents in computer labs, and bypassing basic restrictions using browser extensions and proxies. The administration needed a smart filtering solution that controls access without blocking legitimate academic research.

**Filtering Technology Comparison**

**DNS-Based Filtering:**

* *Advantages*: Easy to set up, low resource usage, works on all devices
* *Disadvantages*: Easy to bypass with alternative DNS servers, limited granular control
* *Best for*: Basic blocking of known bad domains

**Layer 7 Firewall Filtering:**

* *Advantages*: Deep packet inspection, application-aware, hard to bypass
* *Disadvantages*: More expensive, requires more processing power
* *Best for*: Comprehensive control with detailed policies

**Proxy-Based Filtering:**

* *Advantages*: Good balance of control and cost, detailed logging, content inspection
* *Disadvantages*: Can slow down browsing, requires client configuration
* *Best for*: Medium-sized networks like ours

**Client-Side Enforcement:**

* *Advantages*: Works even outside campus network
* *Disadvantages*: Students can disable or bypass easily
* *Best for*: Additional layer, not primary solution

**Chosen Solution: Hybrid Approach**

I recommend combining **Proxy-based filtering** as primary method with **DNS filtering** as backup, because:

* Proxy gives us detailed control and logging
* DNS filtering catches bypass attempts
* Cost-effective for college budget
* Can handle both HTTP and HTTPS traffic

**User Group Access Policies**

**Students (Most Restrictive)**

**During Class Hours (8 AM - 5 PM, Monday-Friday):**

* ✅ **ALLOWED**: Educational websites, research databases, library resources, email
* ✅ **LIMITED**: News websites (max 30 min/day), educational YouTube videos
* ❌ **BLOCKED**: Social media, gaming sites, streaming services, file sharing, adult content

**After Hours & Weekends:**

* ✅ **ALLOWED**: All educational content plus limited social media
* ⏰ **TIME LIMITED**: Social media (2 hours/day), streaming (1 hour/day)
* ❌ **ALWAYS BLOCKED**: Torrents, inappropriate content, security threats

**Faculty (Moderate Restrictions)**

**All Times:**

* ✅ **ALLOWED**: Academic and research sites, professional social media, educational streaming
* ⏰ **BANDWIDTH LIMITED**: Personal streaming during peak hours (9 AM - 5 PM)
* ❌ **BLOCKED**: File sharing networks, inappropriate content, security threats
* 🔍 **MONITORED**: All activity for security purposes only

**Administrative Staff (Least Restrictive)**

**All Times:**

* ✅ **ALLOWED**: Most business and educational content
* ❌ **BLOCKED**: Only known malicious sites, inappropriate content
* 🔍 **MONITORED**: Bandwidth usage and security threats

**Guest Network (Heavily Restricted)**

**All Times:**

* ✅ **ALLOWED**: Basic web browsing, email
* ⏰ **TIME LIMITED**: 2 hours per day, 500 MB data limit
* ❌ **BLOCKED**: Social media, streaming, downloads, file sharing

**Policy Enforcement Logic**

**Time-Based Rules Implementation:**

IF (current\_time BETWEEN 08:00 AND 17:00) AND (weekday) THEN

apply\_strict\_student\_policy()

ELSE IF (current\_time BETWEEN 17:00 AND 23:00) THEN

apply\_relaxed\_student\_policy()

ELSE

apply\_minimal\_access\_policy()

**Content Category Rules:**

STUDENT\_BLOCKED\_CATEGORIES = [

"social\_media", "gaming", "streaming", "file\_sharing",

"adult\_content", "proxy\_services"

]

FACULTY\_LIMITED\_CATEGORIES = [

"personal\_streaming", "non\_work\_social\_media"

]

**Bandwidth Management:**

* Students: 10 Mbps during class, 25 Mbps after hours
* Faculty: 50 Mbps always, unlimited for research
* Admin: 100 Mbps for business needs
* Guests: 5 Mbps maximum

**Network Implementation**

**Components Added:**

* **Web Filtering Server**: Handles proxy filtering and policy enforcement
* **Log Server**: Stores access logs and generates reports
* **DNS Server**: Provides DNS-based blocking as secondary layer

**Traffic Flow:**

1. User requests website
2. Request goes to Web Filtering Server
3. Server checks user group and current time
4. Applies appropriate policy rules
5. Either allows, blocks, or rate-limits the request
6. Logs all activity to Log Server

**Bypass Prevention Strategies**

**Common Bypass Methods & Countermeasures:**

**VPN Services:**

* Block known VPN provider IPs and domains
* Monitor for VPN-like traffic patterns
* Educational campaign about policy violations

**Proxy Websites:**

* Maintain updated list of proxy sites
* Block categories containing proxy services
* Use keyword filtering for new proxy sites

**DNS Changes:**

* Block external DNS queries at firewall level
* Force all devices to use campus DNS servers
* Monitor DNS traffic for tunneling attempts

**Mobile Hotspots:**

* Policy education about personal device usage
* WiFi signal monitoring in labs (where appropriate)
* Data usage reporting to identify excessive mobile usage

**Logging and Monitoring**

**Information Logged:**

* User identity and device information
* Websites accessed and time stamps
* Blocked attempts and reasons
* Bandwidth usage per user
* Policy violation attempts

**Alert Triggers:**

* Multiple policy violations by same user
* Attempts to access blocked categories repeatedly
* Unusual bandwidth usage patterns
* Suspected bypass attempts
* Malware or phishing site access attempts

**Reporting:**

* Daily summary of blocked content by category
* Weekly user activity reports for departments
* Monthly bandwidth usage analysis
* Violation reports for administration review

**Policy Intent and Educational Approach**

**Primary Goals:**

* Maintain academic focus during class hours
* Prevent network abuse and excessive bandwidth usage
* Protect users from malicious content
* Comply with legal requirements for educational institutions

**Educational Component:**

* Clear communication of policies to all users
* Regular reminders about appropriate usage
* Digital citizenship training for students
* Faculty guidance on academic freedom vs. policy compliance

**Enforcement Philosophy:**

* Progressive discipline: warning → restriction → escalation
* Focus on education rather than punishment
* Consider academic needs and research requirements
* Regular policy review and updates based on feedback

**Advantages of This Framework**

1. **Flexible**: Different rules for different users and times
2. **Educational**: Balances control with learning opportunities
3. **Scalable**: Can adjust rules based on network capacity
4. **Transparent**: Clear policies communicated to users
5. **Reasonable**: Allows legitimate academic and personal use

**Part 3 Conclusion**

This framework provides comprehensive web access control while respecting the educational mission of the institution and the legitimate needs of faculty and students.

**OVERALL PROJECT SUMMARY**

This three-part cybersecurity project demonstrates a comprehensive approach to securing a college campus network:

**Part 1** identified critical security vulnerabilities in the existing flat network design and provided practical recommendations for improvement within budget constraints.

**Part 2** implemented a secure hybrid access solution using VPN technology that enables remote faculty access while maintaining security boundaries and protecting internal services.

**Part 3** established a balanced web filtering framework that controls inappropriate usage while preserving academic freedom and research capabilities.

The complete solution transforms an insecure campus network into a properly segmented, monitored, and controlled environment that supports both educational objectives and cybersecurity requirements. The implementation prioritizes cost-effectiveness and practical deployment suitable for educational institutions with limited IT resources.