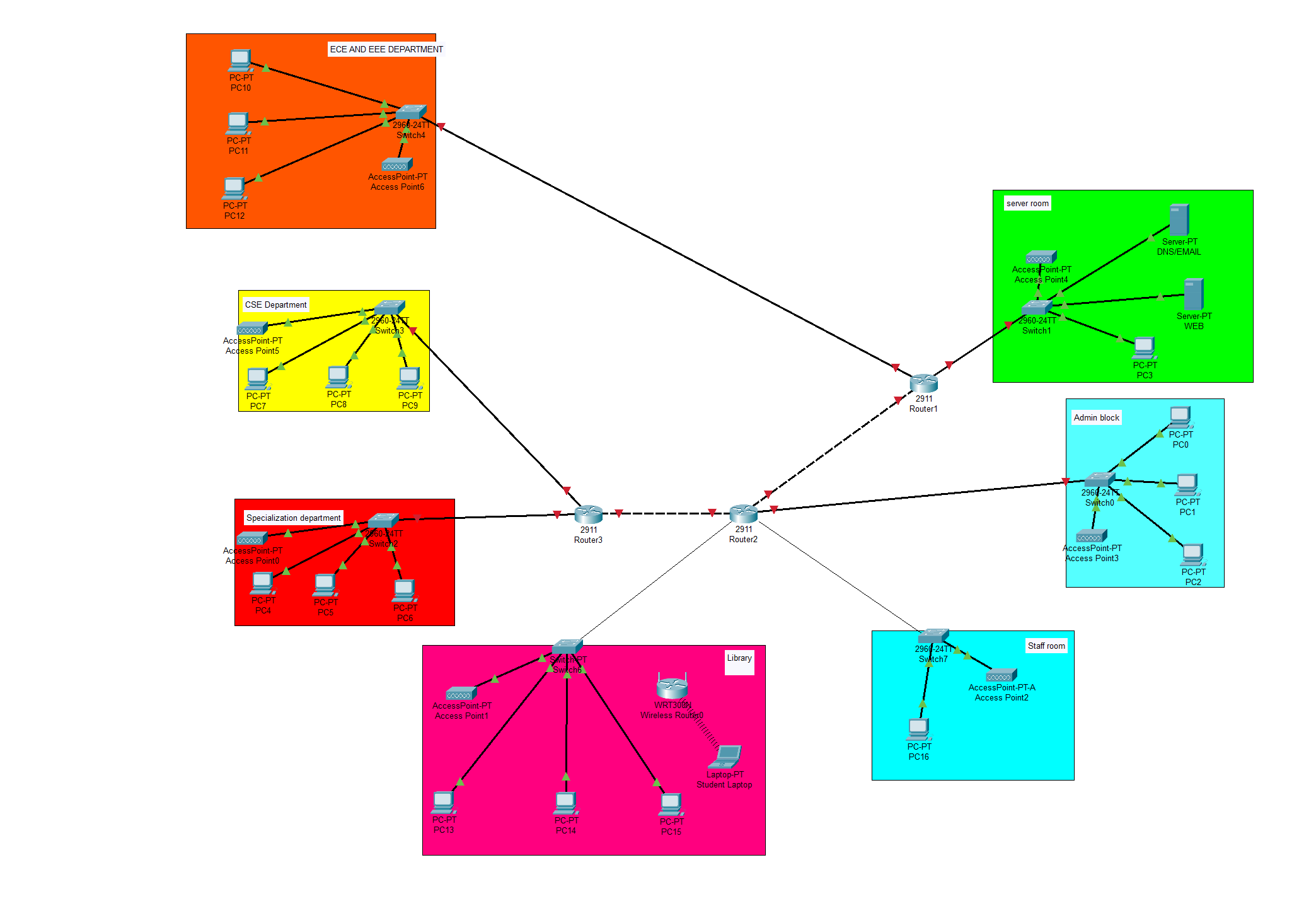
**Security Assessment Report - College Campus Network  
Network topology diagram:  
**

**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

**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.