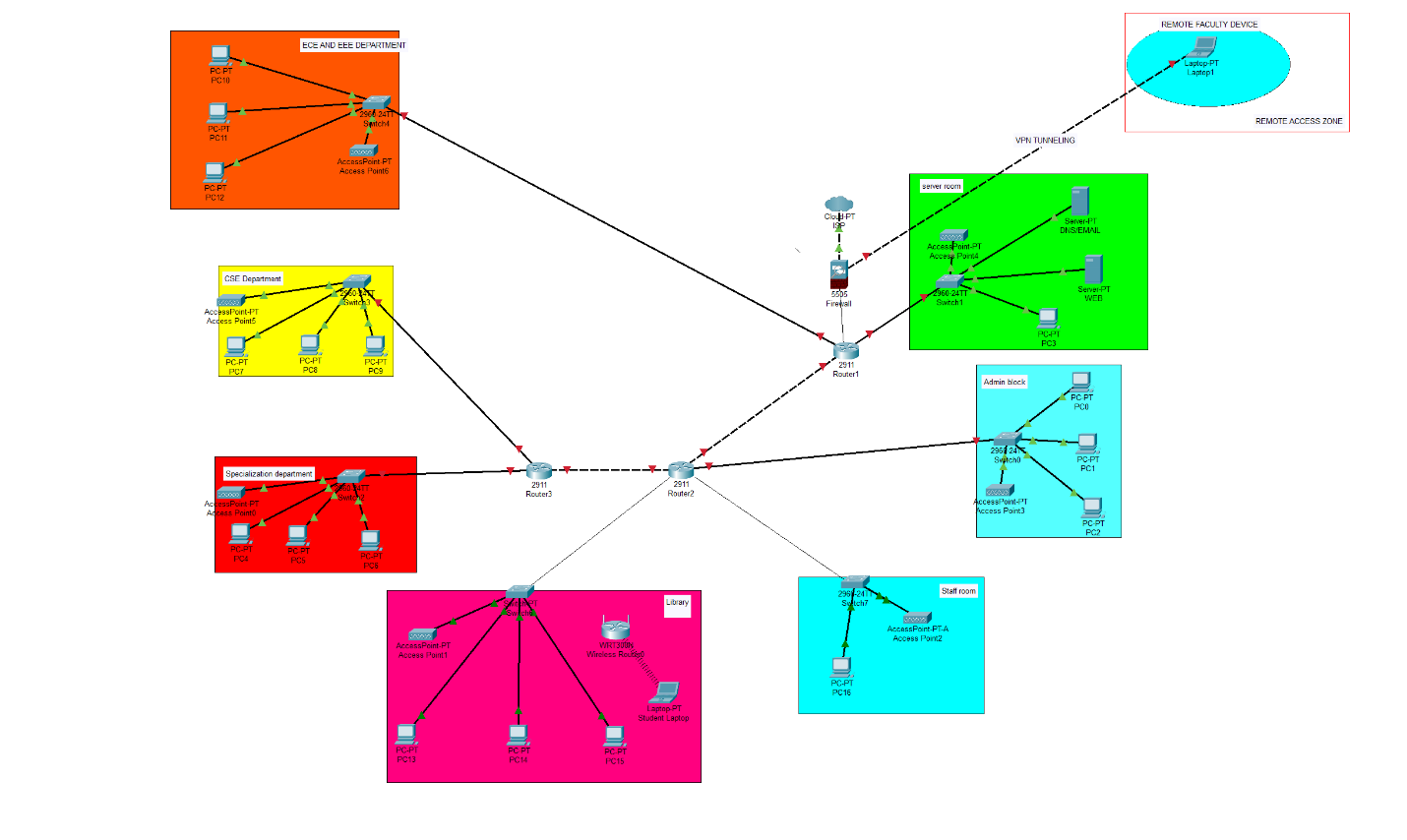
**Hybrid Access Network Architecture - Technical Documentation  
Network Topology Diagram:  
**

**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

**Future Improvements**

When budget allows, consider:

* Multi-factor authentication for VPN access
* More sophisticated access control based on device health
* Additional VPN servers for redundancy
* Network access control for device compliance checking

**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.