Virtual Internship Program 2025

PART 1:

Cyber Shield: Defending the network

1) Scope & Context

The project was conducted in the environment of ABES Institute of Technology

(ABESIT), which consists of a single main campus serving approximately 500-700 active users daily. The network supports a mix of students, faculty, administrative staff, and guests, and must handle a wide range of applications such as e-learning portals, campus management systems, research collaboration, and high-speed Internet access.

The infrastructure includes:

- Academic blocks, computer laboratories, administrative offices, and residential areas (faculty/student hostels).
- Both wired LAN and wireless WLAN (Wi-Fi) connectivity.
- Centralized core switching and routing infrastructure providing inter-VLAN communication.
- Access to the public Internet through an edge router connected to an ISP.

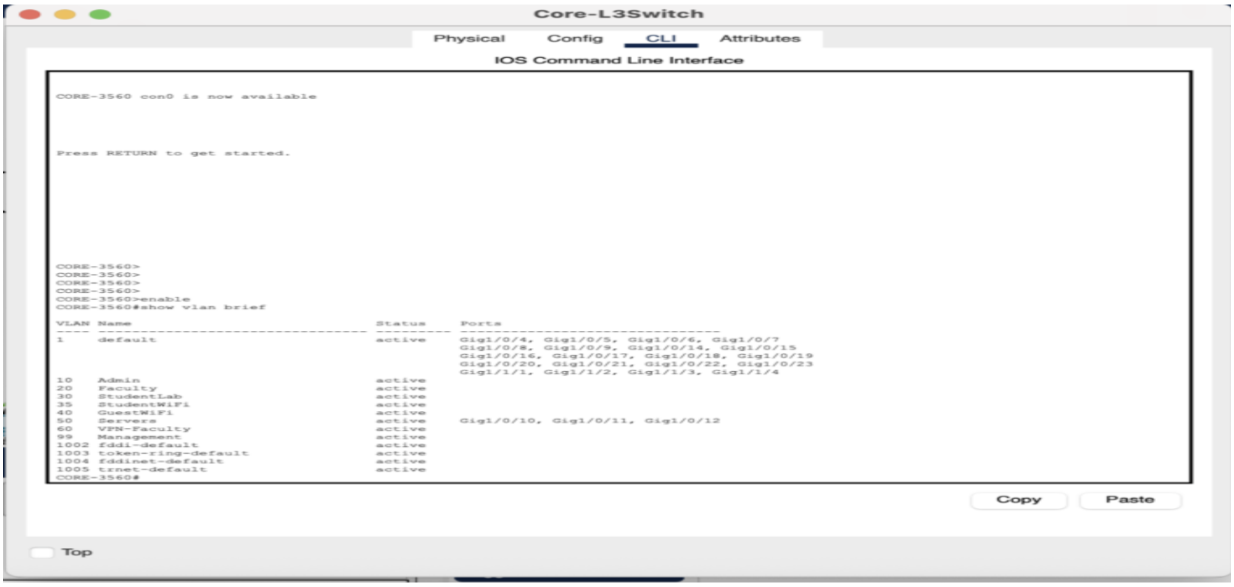
Tools

To simulate, analyze, and secure this campus network, the following tools and technologies were used:

- Cisco Packet Tracer v8.x - for virtual simulation of the entire campus topology.
- Cisco IOS-based devices - including Layer 3 switches, Layer 2 access switches, routers, and WRT-300N wireless access points.
- Configuration commands - CLI-based setup for VLANs, routing, ACLs, and device hardening.
- Basic monitoring tools - Syslog (for logging), Ping/Traceroute (for connectivity testing), and NAT for external Internet access.

2. Logical Segmentation (Trust Zones)

Zone	VLAN	Subnet	Gateway	Purpose
Admin/IT	10	10.10.10.0/24	10.10.10.1	Network mgmt & sysadmin
Faculty	20	10.10.20.0/24	10.10.20.1	Faculty devices, internal apps
Student Labs	30	10.10.30.0/24	10.10.30.1	Lab desktops
Student Wi-Fi	35	10.10.35.0/24	10.10.35.1	BYOD student access
Guest Wi-Fi	40	10.10.40.0/24	10.10.40.1	Internet-only access
Servers/DMZ	50	10.10.50.0/24	10.10.50.1	AD/LDAP, LMS, DB, Git
VPN-Faculty (opt)	60	10.10.60.0/24	10.10.60.1	IP phones or VPN lab
Mgmt/OOB	99	10.10.99.0/24	10.10.99.1	SSH, SNMP, Syslog, NTP



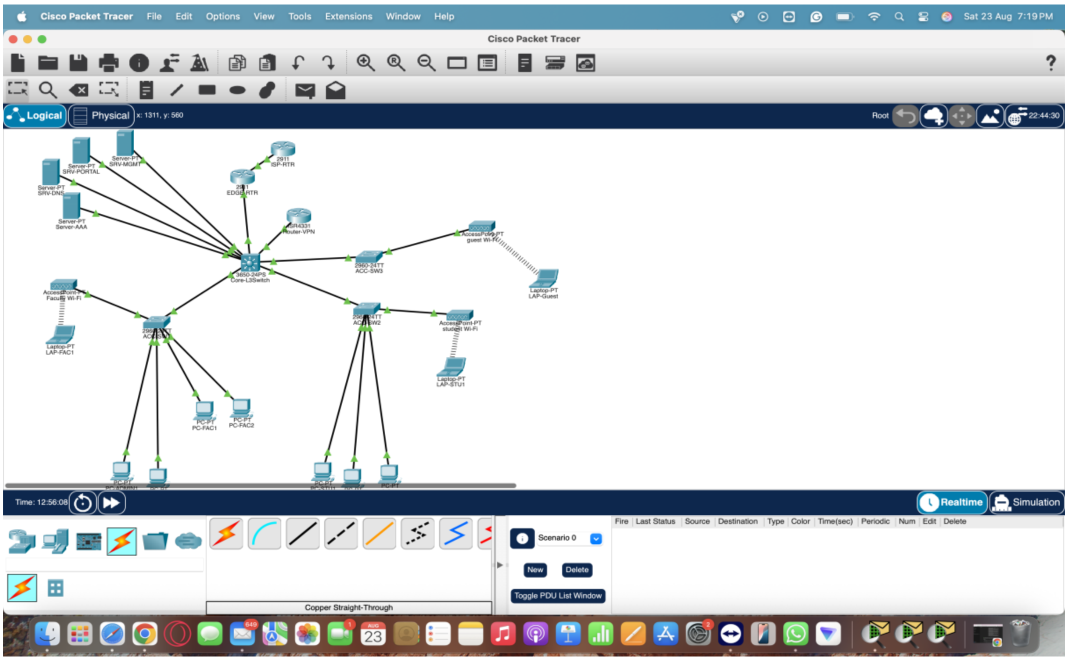
```
CORE-3560 con0 is now available




Press RETURN to get started.









CORE-3560>
CORE-3560>
CORE-3560>
CORE-3560>
CORE-3560>enable
CORE-3560#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/4, Gig1/0/5, Gig1/0/6, Gig1/0/7
                                                Gig1/0/8, Gig1/0/9, Gig1/0/14, Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23
                                                Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
10   Admin                            active
20   Faculty                          active
30   StudentLab                       active
35   StudentWiFi                      active
40   GuestWiFi                        active
50   Servers                          active    Gig1/0/10, Gig1/0/11, Gig1/0/12
60   VPN-Faculty                      active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
CORE-3560#
```

Shows `vlan brief` output showing VLANs and assignments.

Explanation: Each VLAN isolates traffic by user type or function. Management VLAN is out-of-band to protect critical devices. Optional VPN VLAN ensures faculty remote access doesn't mix with student traffic.

3. Physical Topology Overview

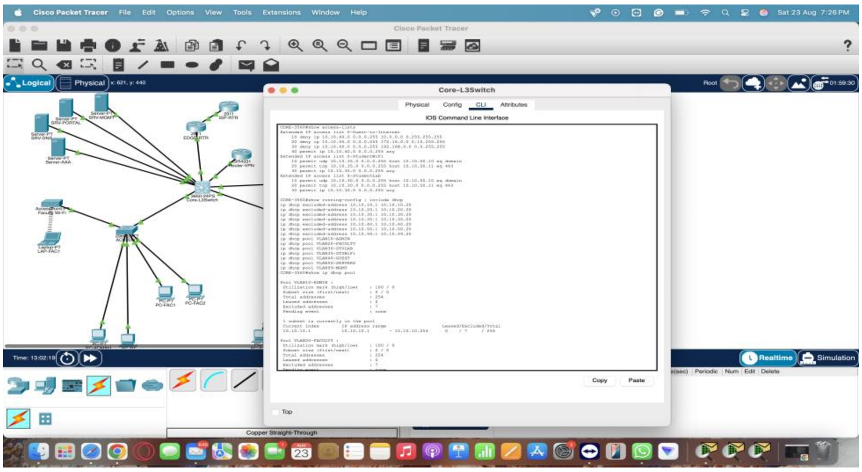
- **ISP Edge / NGFW → Core L3 Switch → Distribution Switches → Access Switches & APs**
- **Server/DMZ** connected to core/firewall with ACLs
- **Wireless LAN Controller / APs** trunked to core; SSIDs mapped to VLANs



Packet Tracer topology diagram with device labels, VLAN coloring, and SVI gateways.

4. Device Inventory & Security Controls

Device Type	Device	Location	Security Controls
Edge	Router / NGFW	Edge rack	NAT, IPS, ACLs, logging
Core	L3 Switch	DC	SVIs, ACLs, DHCP snooping
Dist	L2/L3 Switch	Buildings	Port security, BPDU guard, storm ctrl
Wireless	AP/WLC	Labs/Classrooms	WPA2/3-Enterprise, 802.1X
Servers	AD/LDAP, LMS, DB	Server Room	MFA, regular patching, logging
Mgmt	Syslog/NTP	DC	Centralized logging, NTP sync

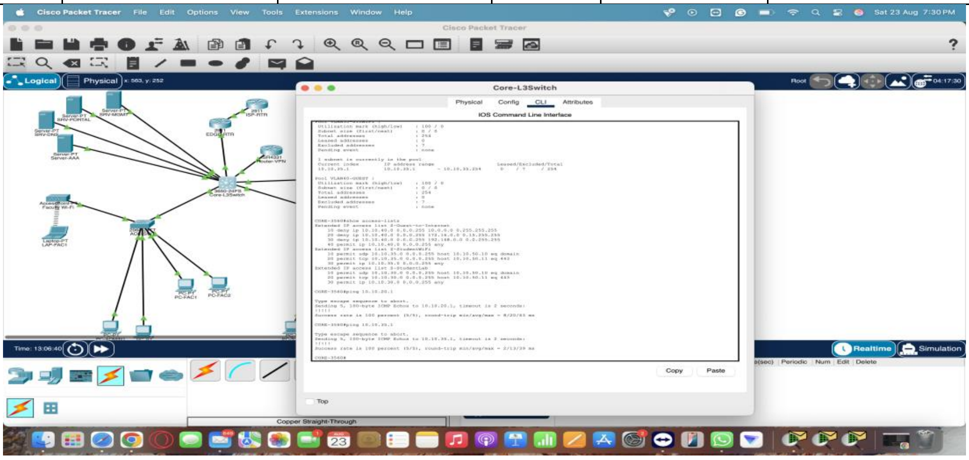


```
CORE-3560#show access-lists
Extended IP access list Z-Guest-to-Internet
    10 deny ip 10.10.40.0 0.0.0.255 10.0.0.0 0.255.255.255
    20 deny ip 10.10.40.0 0.0.0.255 172.16.0.0 0.15.255.255
    30 deny ip 10.10.40.0 0.0.0.255 192.168.0.0 0.0.255.255
    40 permit ip 10.10.40.0 0.0.0.255 any
Extended IP access list Z-StudentWiFi
    10 permit udp 10.10.35.0 0.0.0.255 host 10.10.50.10 eq domain
    20 permit tcp 10.10.35.0 0.0.0.255 host 10.10.50.11 eq 443
    30 permit ip 10.10.35.0 0.0.0.255 any
Extended IP access list Z-StudentLab
    10 permit udp 10.10.30.0 0.0.0.255 host 10.10.50.10 eq domain
    20 permit tcp 10.10.30.0 0.0.0.255 host 10.10.50.11 eq 443
    30 permit ip 10.10.30.0 0.0.0.255 any

CORE-3560#show running-config | include dhcp
ip dhcp excluded-address 10.10.10.1 10.10.10.20
ip dhcp excluded-address 10.10.20.1 10.10.20.20
ip dhcp excluded-address 10.10.30.1 10.10.30.20
ip dhcp excluded-address 10.10.35.1 10.10.35.20
ip dhcp excluded-address 10.10.40.1 10.10.40.20
ip dhcp excluded-address 10.10.50.1 10.10.50.20
ip dhcp excluded-address 10.10.99.1 10.10.99.20
ip dhcp pool VLAN10-ADMIN
ip dhcp pool VLAN20-FACULTY
ip dhcp pool VLAN30-STULAB
ip dhcp pool VLAN35-STUWIFI
ip dhcp pool VLAN40-GUEST
ip dhcp pool VLAN50-SERVERS
ip dhcp pool VLAN99-MGMT
CORE-3560#show ip dhcp pool

Pool VLAN10-ADMIN :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 7
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.10.10.1           10.10.10.1       - 10.10.10.254      0     / 7     / 254

Pool VLAN20-FACULTY :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 7
```

Device configurations showing ACLs, DHCP pools, and SVI setups.

5. Attack Surface Mapping

Finding	Evidence	Likelihood (L)	Impact (I)	Priority	Recommended Mitigation
Flat student VLAN	No ACLs	4	4	16	Inter-VLAN ACLs
Guest Wi-Fi → RFC1918	Traceroute	3	5	15	Guest egress ACLs
Weak Wi-Fi auth	PSK	4	3	12	802.1X / RADIUS
No centralized logs	None configured	3	4	12	Deploy Syslog/NTP
Default creds	`cisco/cisco`	2	5	10	AAA + SSH, change passwords



```
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 7
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.10.35.1           10.10.35.1       - 10.10.35.254      0     / 7     / 254

Pool VLAN40-GUEST :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 7
 Pending event                  : none


CORE-3560#show access-lists
Extended IP access list Z-Guest-to-Internet
    10 deny ip 10.10.40.0 0.0.0.255 10.0.0.0 0.255.255.255
    20 deny ip 10.10.40.0 0.0.0.255 172.16.0.0 0.15.255.255
    30 deny ip 10.10.40.0 0.0.0.255 192.168.0.0 0.0.255.255
    40 permit ip 10.10.40.0 0.0.0.255 any
Extended IP access list Z-StudentWiFi
    10 permit udp 10.10.35.0 0.0.0.255 host 10.10.50.10 eq domain
    20 permit tcp 10.10.35.0 0.0.0.255 host 10.10.50.11 eq 443
    30 permit ip 10.10.35.0 0.0.0.255 any
Extended IP access list Z-StudentLab
    10 permit udp 10.10.30.0 0.0.0.255 host 10.10.50.10 eq domain
    20 permit tcp 10.10.30.0 0.0.0.255 host 10.10.50.11 eq 443
    30 permit ip 10.10.30.0 0.0.0.255 any

CORE-3560#ping 10.10.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/20/43 ms

CORE-3560#ping 10.10.35.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.35.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/13/39 ms

CORE-3560#
```

ACL hit counters, ping tests, and Wireshark evidence.

Assigning risk priorities helps focus on high-impact vulnerabilities first. Inter-VLAN ACLs and strong Wi-Fi security prevent unauthorized lateral movement.

6. Recommendations

Immediate (0–2 weeks):

- Enforce inter-VLAN ACLs
- Enable DHCP snooping, DAI, port security
- Centralize logs on Syslog/NTP server

Near Term (1–2 months):

- WPA2/3-Enterprise with RADIUS
- MFA for admin accounts
- Regular patching and vulnerability scans

Mid Term (Quarter):

- Deploy IDS/IPS
- NAC (802.1X) for wired networks
- Security awareness training for staff/students

Part-2

Hybrid Access Network Design

1. Problem Context

Theory:
Modern campuses require **secure hybrid access** because faculty often need to work remotely while maintaining access to sensitive internal services. Students and guests, however, only need restricted campus or internet access. Exposing internal apps directly to the internet increases **attack surface**, creating risk for data breaches, ransomware, or lateral movement attacks.

Security Principles Applied:

- **Least Privilege:** Faculty only get access to apps they need; students and guests are isolated.
- **Zero-Trust:** Never trust devices by default; verify identity, device, and session context before allowing access.
- **Segmentation:** VLANs and ACLs logically isolate traffic to reduce risk.

2. Network Segmentation for Hybrid Access

Segmentation reduces attack propagation. Each VLAN acts as a **trust zone**:

- **Faculty VPN VLAN (10.10.20.0/24):** Only faculty devices, including remote VPN clients, can access internal servers. Split tunneling ensures bandwidth efficiency while keeping internal app traffic secure.
- **Student VLAN (10.10.35.0/24):** Only campus Wi-Fi; blocked from sensitive internal VLANs to enforce security boundaries.
- **Guest VLAN (10.10.40.0/24):** Internet-only access prevents exposure to internal resources, even if devices are compromised.

Zone	Users	VLAN/Subnet	Access Type
Faculty VPN	Faculty	20 / 10.10.20.0/24	Remote VPN, split tunneling
Student Wi-Fi	Students	35 / 10.10.35.0/24	Campus Wi-Fi only
Guest	Guests	40 / 10.10.40.0/24	Internet-only

ACL Implementation: ACLs enforce **policy-driven access**, blocking student/guest traffic to sensitive VLANs while allowing faculty remote access. This ensures **micro-segmentation**, a key principle in modern cybersecurity frameworks.

3. Secure Access Technologies

VPN (SSL/IPSec):

- Encrypts traffic between remote faculty and internal resources.
- Provides **confidentiality, integrity, and authentication**, ensuring data cannot be intercepted in transit.

SASE / Cloud Gateway (Optional):

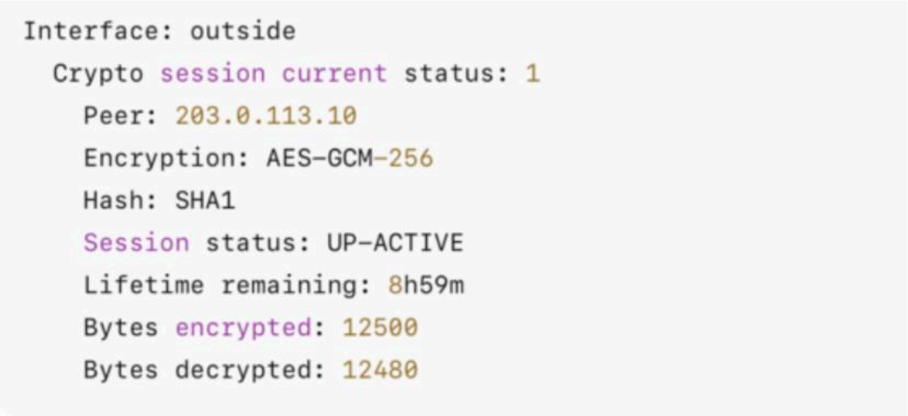
- Cloud-based security that extends campus policies to remote users.
- Provides **secure access to SaaS apps** without exposing the internal network.

Identity-Aware Proxy:

- Enables **application-level access** instead of full network access.
- Reduces risk if a device is compromised; only authorized apps are accessible.

Split Tunneling:

- Balances **security and efficiency**: internal app traffic goes through VPN; internet traffic goes direct.
- Theory: Reduces network congestion while maintaining secure internal connectivity.



```
Interface: outside
  Crypto session current status: 1
    Peer: 203.0.113.10
    Encryption: AES-GCM-256
    Hash: SHA1
    Session status: UP-ACTIVE
    Lifetime remaining: 8h59m
    Bytes encrypted: 12500
    Bytes decrypted: 12480
```

VPN configuration in Packet Tracer or ASA device.

4. Trust Model & Authentication

Authentication:

- RADIUS / AD ensures users are verified centrally.
- **MFA (Multi-Factor Authentication)** provides an extra layer, mitigating stolen credential attacks.

Authorization:

- VLAN and ACL restrictions enforce **role-based access**.

- Ensures students cannot access servers or admin VLANs.

Control Flow Theory:

- VPN terminates at the edge firewall or VPN gateway.
- Traffic is filtered and forwarded according to policies, creating a **controlled access path**.

Internal Apps Access:

- Only via internal VLAN or identity-aware proxy.
- Theory: Limits exposure, enforcing **principle of minimal attack surface**.

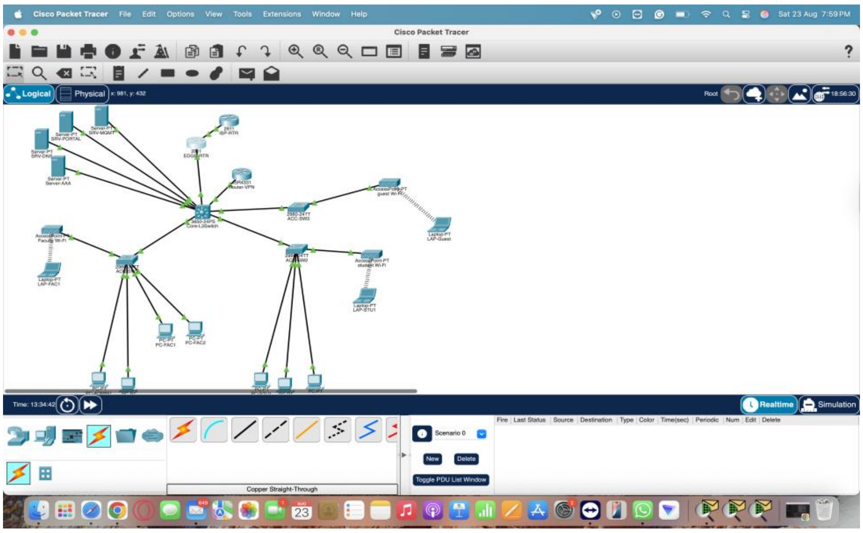
5. Topology Diagram

A hierarchical hybrid topology ensures:

- Clear **traffic flow** from external to internal zones.
- **Isolation** of student and guest networks from sensitive VLANs.
- Encrypted VPN tunnels maintain confidentiality and integrity for remote faculty.

Key flows:

- Edge Firewall → VPN Gateway → Core Switch → VLANs / Servers
- Students → Campus Wi-Fi → VLAN 35 only
- Guests → Internet via NAT



PT topology diagram showing remote access paths and ACLs.

6. Risk Assessment & Fallback

Risk	Likelihood	Impact	Mitigation
VPN misconfiguration	3	5	Test tunnels, backup configs
Unauthorized access	2	5	MFA + ACL enforcement

Risk	Likelihood	Impact	Mitigation
Network congestion	3	3	QoS policies, bandwidth monitoring
App unavailability	2	4	Redundant servers, load balancing

7. Recommendations

- Deploy SSL/IPSec VPN for faculty
- Integrate identity-aware proxy for sensitive apps
- Implement split tunneling cautiously
- Monitor all remote access traffic via Syslog/NMS

8. Deliverables

1. VLAN, ACL, and routing tables (Screenshots 1–4)
2. Packet Tracer topology diagrams (Screenshots 2, 6)
3. VPN / Edge configurations (Screenshot 5)
4. Syslog / monitoring logs

Appendix: Sample Config Snippets

Inter-VLAN ACL Example:

```
ip access-list extended STUDENT_ACL
 permit ip 10.10.35.0 0.0.0.255 any
 deny ip 10.10.35.0 0.0.0.255 10.10.20.0 0.0.0.255
```

VPN Tunnel Example (ASA):

```
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
crypto map VPN-MAP 10 match address VPN-ACL
crypto map VPN-MAP 10 set peer 203.0.113.1
crypto map VPN-MAP 10 set transform-set VPN-SET
```

DHCP Pool Example:

```
ip dhcp pool STUDENT_WIFI
 network 10.10.35.0 255.255.255.0
 default-router 10.10.35.1
 dns-server 8.8.8.8
```

Syslog Example:

```
logging 10.10.99.5
logging trap informational
```

Part 3:
Web Access Policy & Smart Filtering

1. Problem Context

Scenario:
After hybrid access is rolled out, students are abusing network privileges by streaming videos during lectures, torrenting files, and bypassing restrictions using proxies or browser extensions.

Goal:
Design a **smart, enforceable web access policy framework** that:

- Differentiates access by user type (students, faculty, guests)
- Varies rules by time (class hours, weekends)
- Blocks only unwanted content while allowing legitimate research
- Monitors usage and reports violations

Security Principles Applied:

- **Least Privilege Access:** Users can access only content required for their role.
- **Context-Aware Filtering:** Policies adapt based on identity, time, or device.
- **Defense-in-Depth:** Multiple layers of filtering (DNS, L7 firewall, proxies) reduce circumvention.

2. Comparison of Filtering Solutions

Solution Type	How it Works	Pros	Cons	Recommended Use
DNS-Based Filtering	Blocks access at domain resolution level	Lightweight, cloud-based, easy to deploy	Can be bypassed via alternative DNS, doesn’t inspect HTTPS fully	Quick filtering of social media, gaming, malicious domains
Layer 7 (Application) Firewall	Inspects traffic at application layer; can block HTTP/S apps by category	Granular control, can block streaming, torrents	Needs more resources, complex rules	Enforce policies by content type and time
Proxy-Based Filtering	Routes traffic through proxy, can inspect URLs, cache, and log requests	Detailed logging, authentication possible, can enforce time-based rules	Single point of failure, adds latency	For student VLANs, faculty optional

Client-Side Enforcement	Endpoint software enforces rules on device	Works off-network, hard to bypass for managed devices	Needs deployment on every device, can be disabled by users	Supplementary, optional for faculty/staff laptops

Recommendation: Combine **DNS filtering + L7 firewall/proxy** for maximum coverage with minimal user backlash. Client-side enforcement is optional for managed lab devices.

3. Policy Design

3.1 By User Group

User Group	Allowed Content	Restricted Content	Enforcement Layer
Faculty	All educational apps, research, SaaS	Streaming, gaming optional	L7 Firewall / Proxy
Students	Educational portals, LMS, research databases	Social media (during lectures), video streaming, torrents	L7 Firewall + DNS filtering + proxy
Guests	Internet-only, casual browsing	Internal resources, high-bandwidth apps	L7 Firewall / NAT rules

3.2 By Time

Time Period	Policy Logic
Class Hours	Restrict video, gaming, torrents; allow LMS, research sites
Weekends / Off Hours	Relax restrictions; monitor usage
Night / Maintenance	Minimal access for backups, testing

3.3 Content Categorization

- Use **predefined URL categories** (social media, adult, gaming, streaming, P2P).
- Map categories to policies by user group and time.

4. Enforcement Mechanisms

Network Components:

- **L7 Firewall / UTM Appliance:** Blocks traffic by URL category, time, or user identity.
- **DNS Filtering Service:** Blocks domains before DNS resolution.
- **Proxy Server (optional):** Captures logs, enforces authentication, caches allowed content.
- **Syslog/NMS:** Collects logs, triggers alerts on policy violations.

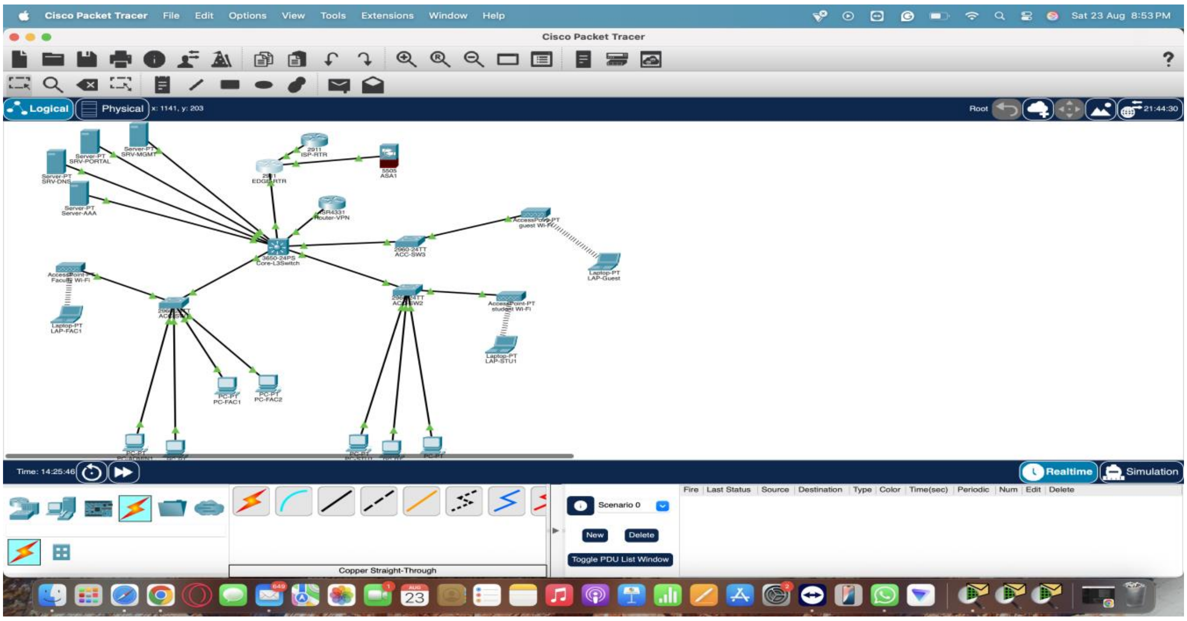
Pseudo-Policy Example:

Student VLAN (10.10.35.0/24)
  Time: 09:00-16:00
    Block: social media, video streaming, torrents
    Allow: LMS, research portals
  Time: 16:00-22:00
    Allow: social media, video streaming (non-disruptive)
Faculty VLAN (10.10.20.0/24)
  Allow all except P2P torrents
Guest VLAN (10.10.40.0/24)
  Allow: Internet only
  Block: internal VLANs, high-bandwidth apps

Monitoring & Logging:

- Log every access attempt, allowed or blocked, for auditing.
- Detect circumvention attempts (VPN/proxy bypass, browser extension).
- Trigger alerts to NMS/Syslog server for repeated violations.

5. Topology Update



- Add **filtering appliance or cloud DNS** in **edge network**:
    - Traffic from student and guest VLANs passes through L7 firewall or proxy.
    - Faculty VPN traffic inspected optionally for policy compliance.
- Maintain **core routing to servers**, preserving internal segmentation.
- Annotate topology with filtering appliance and traffic paths.

6. Advantages of This Approach

- **Granular control:** Policies vary by user, time, content.
- **Minimized backlash:** Students can still access legitimate resources.
- **Circumvention detection:** Logs and alerts identify unauthorized methods.
- **Scalable:** Can add new users, devices, or content categories easily.
- **Compliance-ready:** Supports audits and reporting requirements.

7. Deliverables

- **Updated PT Topology Diagram:** Shows filtering appliance and traffic flow.
- **Web Access Policy Document:** Natural language or pseudo-policy (as above).
- **Overview:** Explains intent, enforcement logic, and advantages.
- **Logs / Monitoring Output:** Sample logs from proxy/DNS/firewall showing blocked and allowed traffic (simulated).