Zhanxing (Harrison) Guo

Professor Talia Q

Principles of Information Systems Security

March 2025

ABC Company Secure Network Design

1. Introduction 3

2. Trust Zones Classification 3

3. VLAN Allocation Summary 4

4. User Role Classification and Access Control 5

5. Server Risk Management Table 7

6. Logging and Auditing Strategy 9

7. Cloudflare and Public Service Access Control 10

8. Network Topology 11

9. Departmental VLAN Plan 12

10. Security Architecture Overview 22

11. Secure Wireless Access 23

12. VPN Remote Access 23

13. Web Access Security 23

14. ACL Matrix (Access Policy) 24

15. Configuration Appendix 25

16. Additional Technical Notes 27

17. Conclusion 28

18. Works Cited 28

1. Introduction

This report presents a secure and scalable enterprise network infrastructure for ABC Company. The design prioritizes access control, VLAN segmentation, authentication, and auditing. It integrates a layered defense approach with firewall inspection, identity-based policies, and secure remote access using VPN. This project expands upon a previously submitted networking assignment (CIS-192), enhancing it to reflect security engineering best practices.

2. Trust Zones Classification

The ABC Company network is segmented into distinct trust zones to enforce layered security:

- **Trusted Internal Zone**: Includes all internal departmental VLANs (e.g., IT, Development, Finance). These are protected by the internal firewall and are not directly accessible from outside.
- **DMZ (Demilitarized Zone)**: Hosts semi-public services such as the anonymous CVS, external web server, mail server, and VPN server. This zone is accessible externally but highly restricted by firewall policies.
- **Anonymous / External Zone**: Represents unknown internet users, VPN clients, and untrusted endpoints. All access is restricted, monitored, and must traverse the firewall and authentication processes.

This classification allows strict control over who can talk to whom and ensures external users are isolated from the trusted core.

3. VLAN Allocation Summary

VLAN ID	Subnet	Department	Access Purpose
1001	192.168.10.0/24	Development	Internal + CVS Access
1002	192.168.13.0/24	Sales	Web Access Only
1003	192.168.12.0/24	IT	Full Admin Rights
1004	192.168.15.0/24	Cafeteria	Wireless Only
1005	192.168.14.0/24	Support	Shared App Access
1006	192.168.11.0/24	Finance	Internet + Mail Access
20	192.168.20.0/24	Wireless Users	Authenticated via WLC
40	192.168.40.0/24	Voice/Phones	Isolated VoIP Network

VLAN ID	Subnet	Department	Access Purpose
100	192.168.100.0/27	DMZ	Public Servers

User access is tightly coupled with VLAN assignment, firewall policy, and authentication mechanisms. Wireless users are dynamically assigned to appropriate VLANs via WLC and, in enterprise settings, RADIUS + AD integration enables identity-based segmentation. VPN users are filtered via ACL and MFA policy, allowing only Dev staff to reach internal resources like the CVS server.

4. User Role Classification and Access Control

To enforce a principle of least privilege, all users on the network are categorized based on their roles and granted only the minimum access necessary to perform their duties. The following table outlines each user type, their access level, permitted systems, and access control enforcement.

User Type	Privilege Level	Permitted Resources	Access Control Mechanism
Developers	Medium-High	Internal CVS, Dev VLAN, VPN Access	Firewall ACL, VPN SPLIT Tunnel
System Admins	Highest	All Internal VLANs, ASA, Switches, WLC	Full Access, Local Auth + SSH
Testers	Medium	Read-Only CVS, Dev VLAN	ACL + VLAN Segmentation
Finance Staff	Medium	Internet, Mail Server	ACL-permitted TCP ports only
Sales Team	Low	Internet Only	Isolated VLAN, Firewall block on internal
Wireless Guests	Very Low	Internet only via NAT	WLC VLAN Mapping + Firewall default deny

User Type	Privilege Level	Permitted Resources	Access Control Mechanism
VPN Dev Users	Medium	CVS Server only	VPN ACLs, MFA enforced
External Users	None (Anonymous)	Public Web, Anonymous CVS (DMZ only)	NAT + Firewall DMZ ACL

5. Server Risk Management Table

The following table outlines major internal and DMZ servers, their associated security concerns, administrative ownership, and implemented controls.

Server	**Potential Risks**	**Who Can Manage It**	**Security Controls Applied**
Internal CVS	Source code theft, tampering	Dev Leads, IT Admins	VPN + ACL, access only from Dev VLAN
Anonymous CVS (DMZ)	Malware injection, DoS abuse	System Admin	Firewall isolation, read-only restrictions
Internal Web Server	XSS, internal data leaks	IT Admin	Internal-only access, ACL enforced
External Web Server	Defacement, exploitation, DDoS	Admin via Cloudflare	TLS enforced, Cloudflare WAF, public ACL
Mail Server (DMZ)	Spam relay, phishing, mail theft	IT Admin	SMTP ACLs, virus scanning, port filtering
VPN Server (DMZ)	Credential brute-force, unauthorized entry	System Admin	MFA, restricted tunnel ACL, login auditing

Server	**Potential Risks**	**Who Can Manage It**	**Security Controls Applied**
DNS Server (DMZ)	Poisoning, hijacking, service abuse	IT Admin	Port 53 restricted, logged queries
WLC (Internal)	Rogue AP control, VLAN leaks	System Admin	Centralized auth, static VLAN mapping
Syslog Server	Tamper of audit trails, false event injection	IT Admin (read-only ops)	Secure storage, internal-only access

Each server is categorized not only by function, but also by risk level and required protections. Internal servers are firewalled and hidden from external access. DMZ servers are publicly accessible but tightly regulated. Roles are clearly separated to ensure accountability and minimize insider threat.

6. Logging and Auditing Strategy

A centralized logging system is essential to detect and respond to policy violations, misconfigurations, or intrusions. The ABC Company network implements a logging and auditing mechanism across key components:

- **Firewall Logs**: All inbound, outbound, and denied traffic is logged by the ASA firewall and sent to the internal syslog server (192.168.12.100).
- **VPN Logs**: Successful and failed login attempts are captured. Login patterns are monitored to detect brute-force attacks or misuse.
- **WLC Logs**: Wireless login activity is tracked, and rogue AP detection is enabled (planned).
- **Switch Port Security Logs**: Interface shutdown events (due to violations) are logged.
- **Syslog Server**: Aggregates logs from ASA, WLC, and switches for centralized auditing. Only IT Admins have read-only access.

```
! ASA logging config
logging enable
logging trap informational
logging host inside-2 192.168.12.100
! Optional email alert integration (simulated)
logging mail alerts@abccompany.local severity warning
```

7. Cloudflare and Public Service Access Control

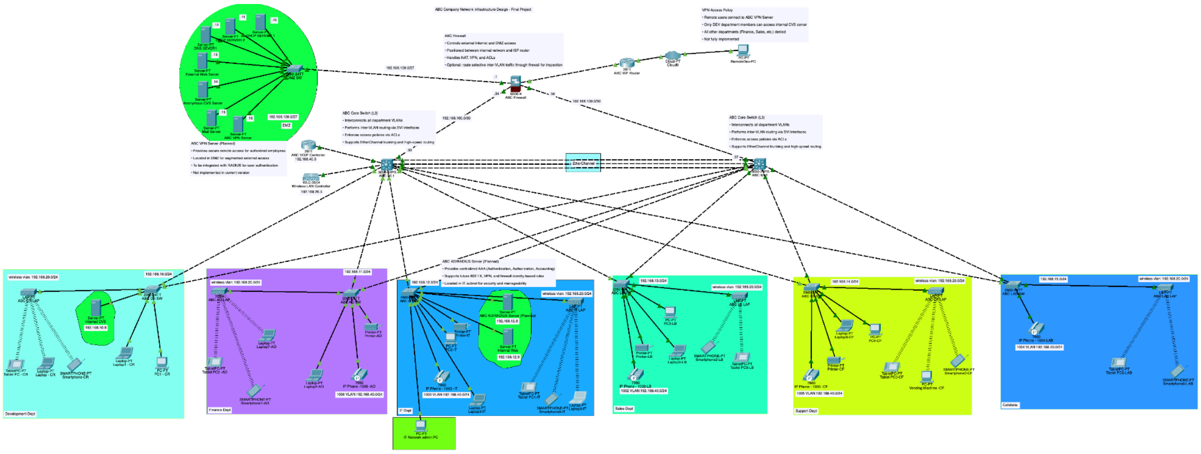
To protect public-facing services while maintaining availability, the network utilizes a Cloudflare-based perimeter defense strategy for the DMZ. This includes:

- **TLS Enforcement**: All HTTP requests are automatically redirected to HTTPS at the Cloudflare edge. TLS certificates are issued and managed via Cloudflare.

- **Web Application Firewall (WAF)**: Cloudflare's WAF filters suspicious requests, blocks known attack signatures (SQL injection, XSS), and mitigates bot scans.
- **Rate Limiting & DDOS Mitigation**: Incoming traffic is throttled per IP to prevent flood or brute-force attacks on public endpoints such as abc.com and cvs.abc.com.
- **Port Restrictions**: Only ports **80** and **443** are accessible externally. All other ports are closed at the ASA firewall.
- **Origin IP Masking**: Real server IPs are hidden behind Cloudflare proxy, reducing exposure of the DMZ layer.
- **Geo-blocking (Optional)**: Traffic from high-risk countries can be geofenced at the CDN level.

This setup ensures that public access is secure, encrypted, and filtered before any packet reaches the internal DMZ. The use of Cloudflare not only reduces the risk of web-based attacks, but also offloads bandwidth and TLS processing from the internal firewall and server infrastructure.

8. Network Topology



ABC Company Network Infrastructure Design - Final Project

ABC Firewall
- Controls external Internet and DMZ access
- Positioned between internal network and ISP router
- Handles NAT, VPN, and ACLs
- Optional: route selective inter-VLAN traffic through firewall for inspection

VPN Access Policy
- Remote users connect to ABC VPN Server
- Only DEV department members can access internal CVS server
- All other departments (Finance, Sales, etc.) denied
- Not fully implemented

ABC VPN Server (Planned)
- Provides secure remote access for authorized employees
- Located in DMZ for segmented external access
- To be integrated with RADIUS for user authentication
- Not implemented in current version

ABC Core Switch (L3)
- Interconnects all department VLANs
- Performs inter-VLAN routing via SVI interfaces
- Enforces access policies via ACLs
- Supports EtherChannel trunking and high-speed routing

ABC Core Switch (L3)
- Interconnects all department VLANs
- Performs inter-VLAN routing via SVI interfaces
- Enforces access policies via ACLs
- Supports EtherChannel trunking and high-speed routing

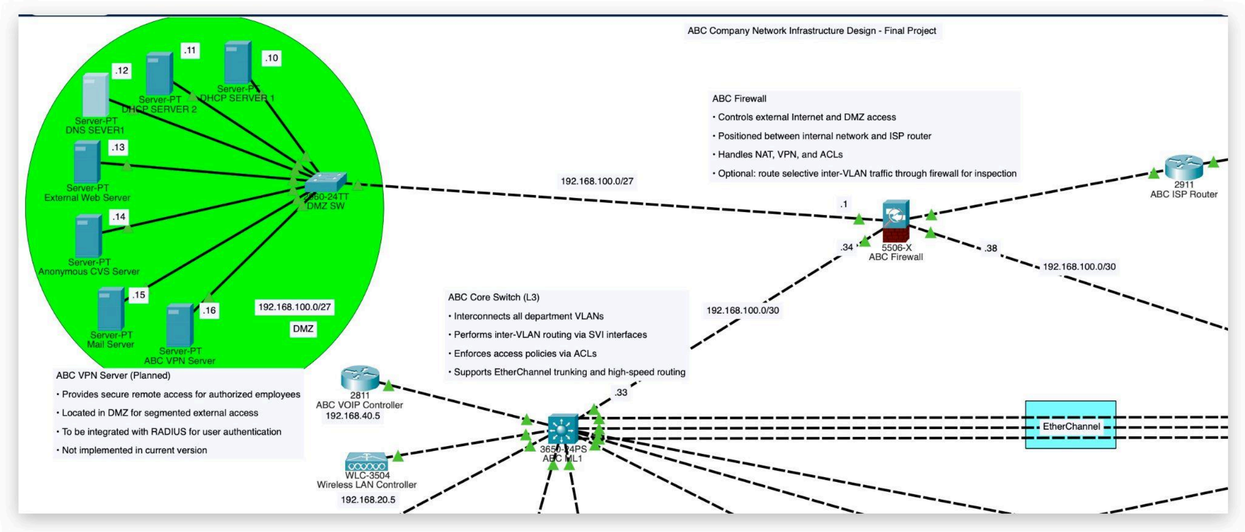
ABC AD/RADIUS Server (Planned)
- Provides centralized AAA (Authentication, Authorization, Accounting)
- Supports future 802.1X, VPN, and firewall identity-based rules
- Located in IT subnet for security and manageability

Figure 1 shows the complete logical layout of ABC Company's enterprise network, including departmental VLANs, firewall segmentation, and DMZ.

---

9. Departmental VLAN Plan

Departmental Segments Overview:



ABC Company Network Infrastructure Design - Final Project

ABC Firewall

- Controls external Internet and DMZ access
- Positioned between internal network and ISP router
- Handles NAT, VPN, and ACLs
- Optional: route selective inter-VLAN traffic through firewall for inspection

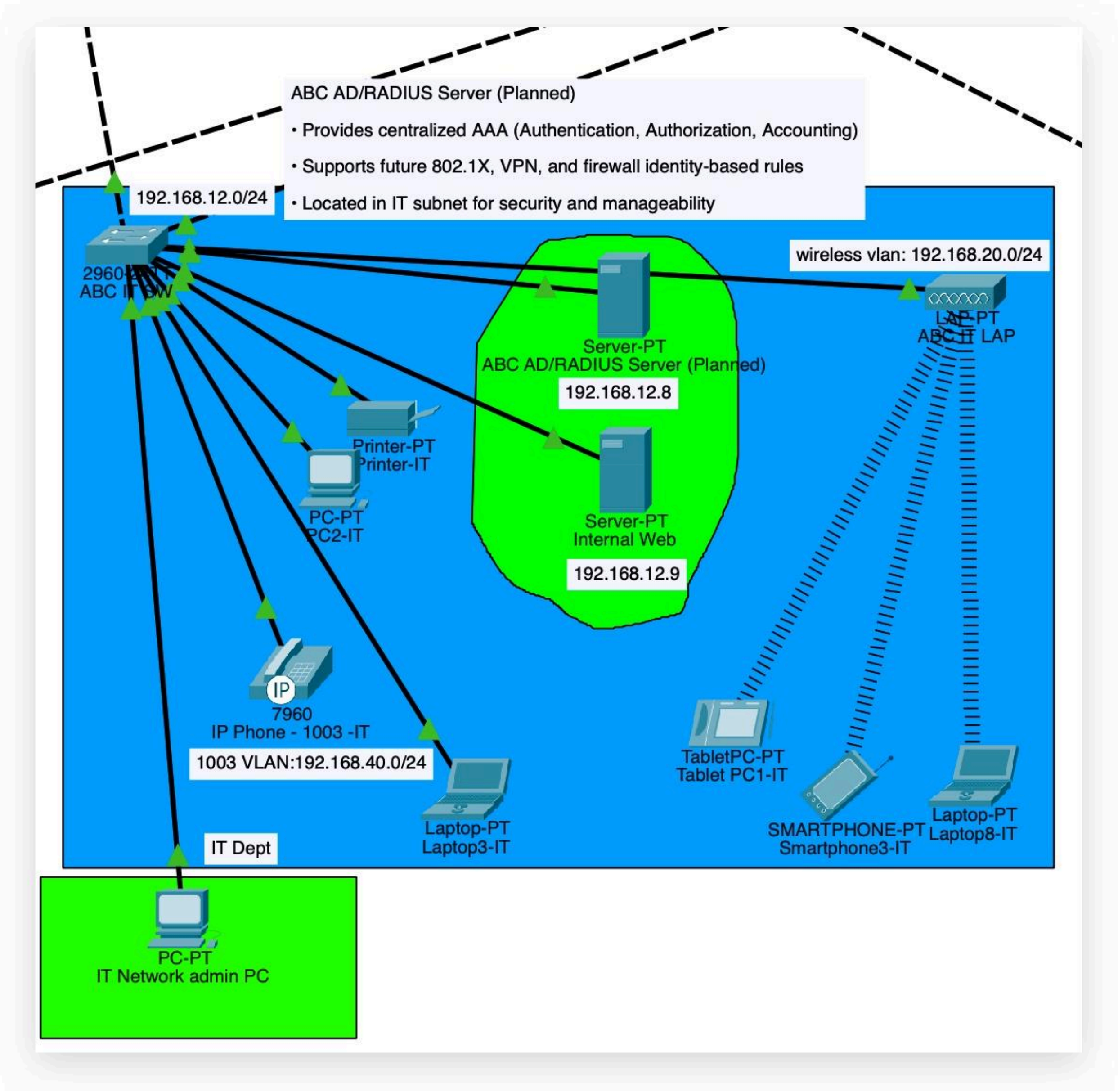
ABC Core Switch (L3)

- Interconnects all department VLANs
- Performs inter-VLAN routing via SVI interfaces
- Enforces access policies via ACLs
- Supports EtherChannel trunking and high-speed routing

ABC VPN Server (Planned)

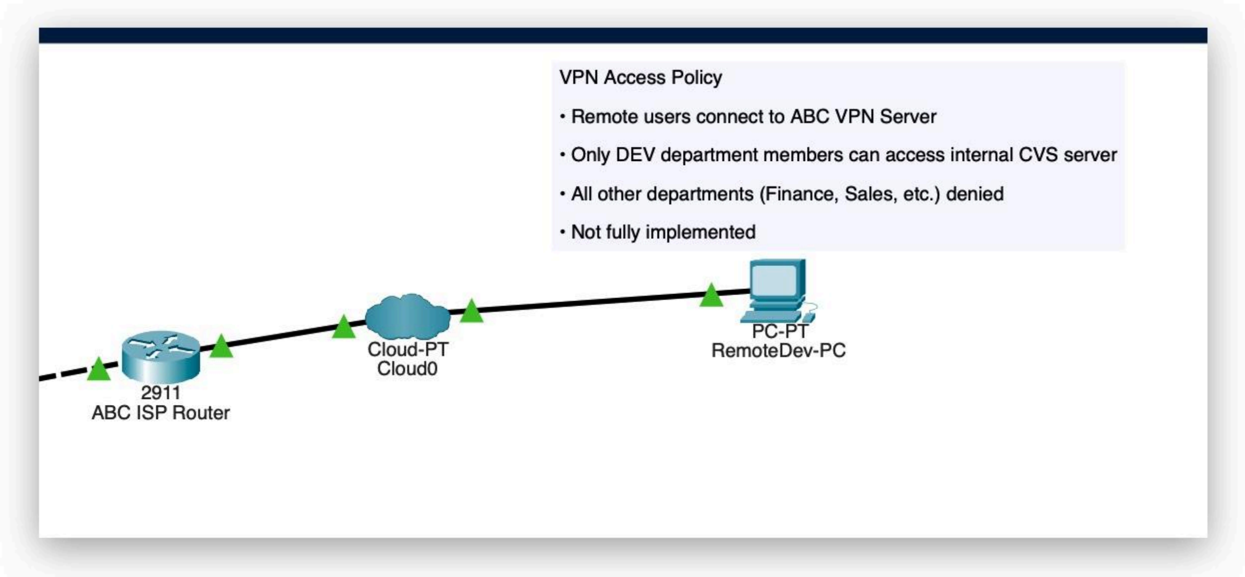
- Provides secure remote access for authorized employees
- Located in DMZ for segmented external access
- To be integrated with RADIUS for user authentication
- Not implemented in current version

Figure 2 VLAN 100 is assigned the subnet 192.168.100.0/27 and designated as the DMZ (Demilitarized Zone). It hosts all semi-public services such as the external web server, mail server, VPN gateway, and anonymous CVS. Traffic to and from this zone is strictly controlled by the ASA firewall. No direct access is allowed between DMZ and trusted internal VLANs without explicit inspection and permission.


ABC AD/RADIUS Server (Planned)

- Provides centralized AAA (Authentication, Authorization, Accounting)
- Supports future 802.1X, VPN, and firewall identity-based rules
- Located in IT subnet for security and manageability

Figure 3 IT VLAN 1003 includes the AD/RADIUS servers used for central identity and AAA.



VPN Access Policy

- Remote users connect to ABC VPN Server
- Only DEV department members can access internal CVS server
- All other departments (Finance, Sales, etc.) denied
- Not fully implemented

Figure 4 ***Remote VPN Access Design***

This diagram illustrates the remote VPN access path for ABC Company. RemoteDev-PC connects to the internal network via the ABC VPN server through the internet and cloud gateway. Only members of the Development department are allowed to access internal resources (e.g., the CVS server) via split-tunnel VPN. All other users from different departments such as Sales or Finance are denied access after authentication. This setup enforces strict access control and implements the principle of least privilege.

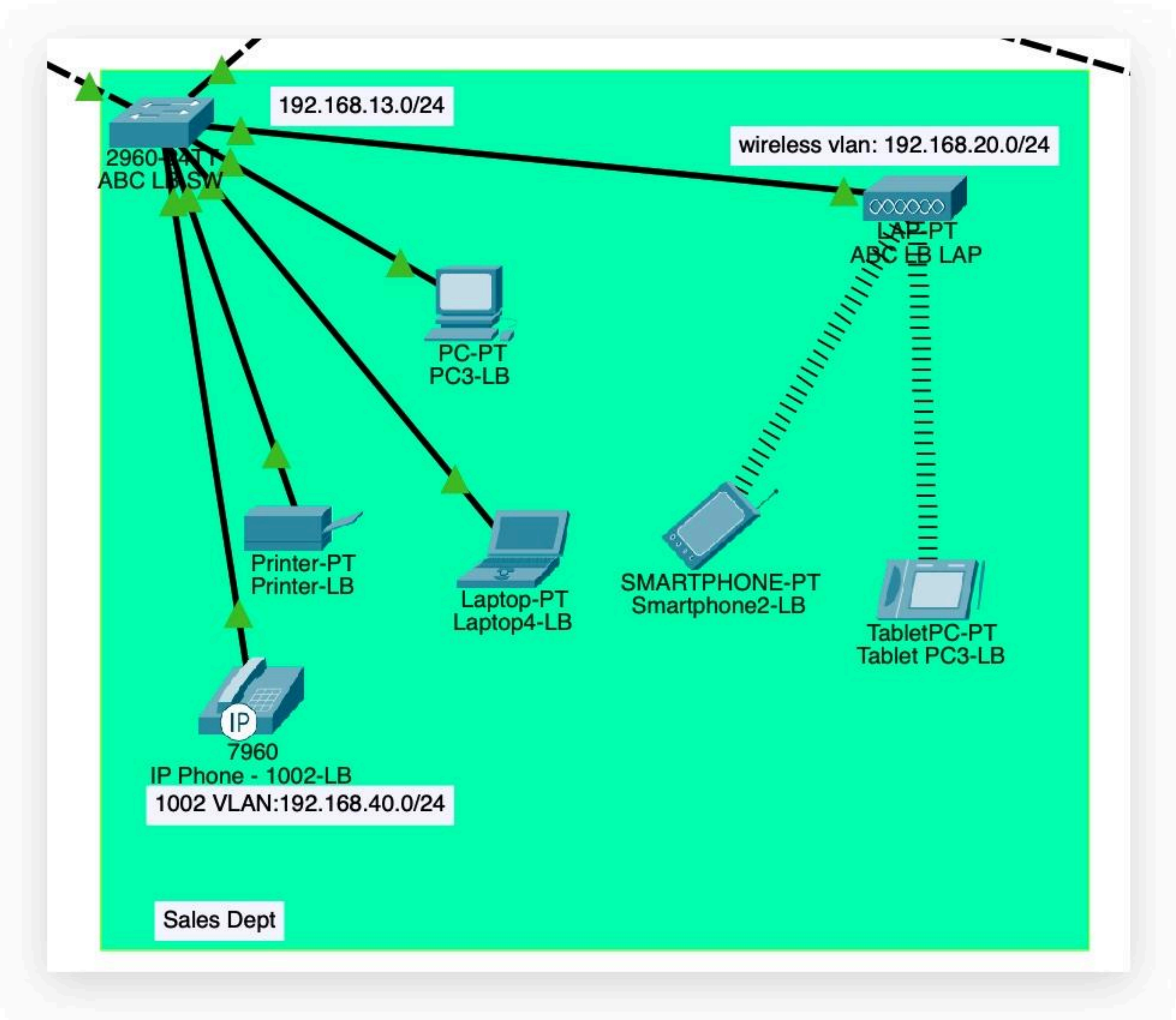


Figure 5 Sales VLAN 1002 is internet-only with no access to internal IT systems.

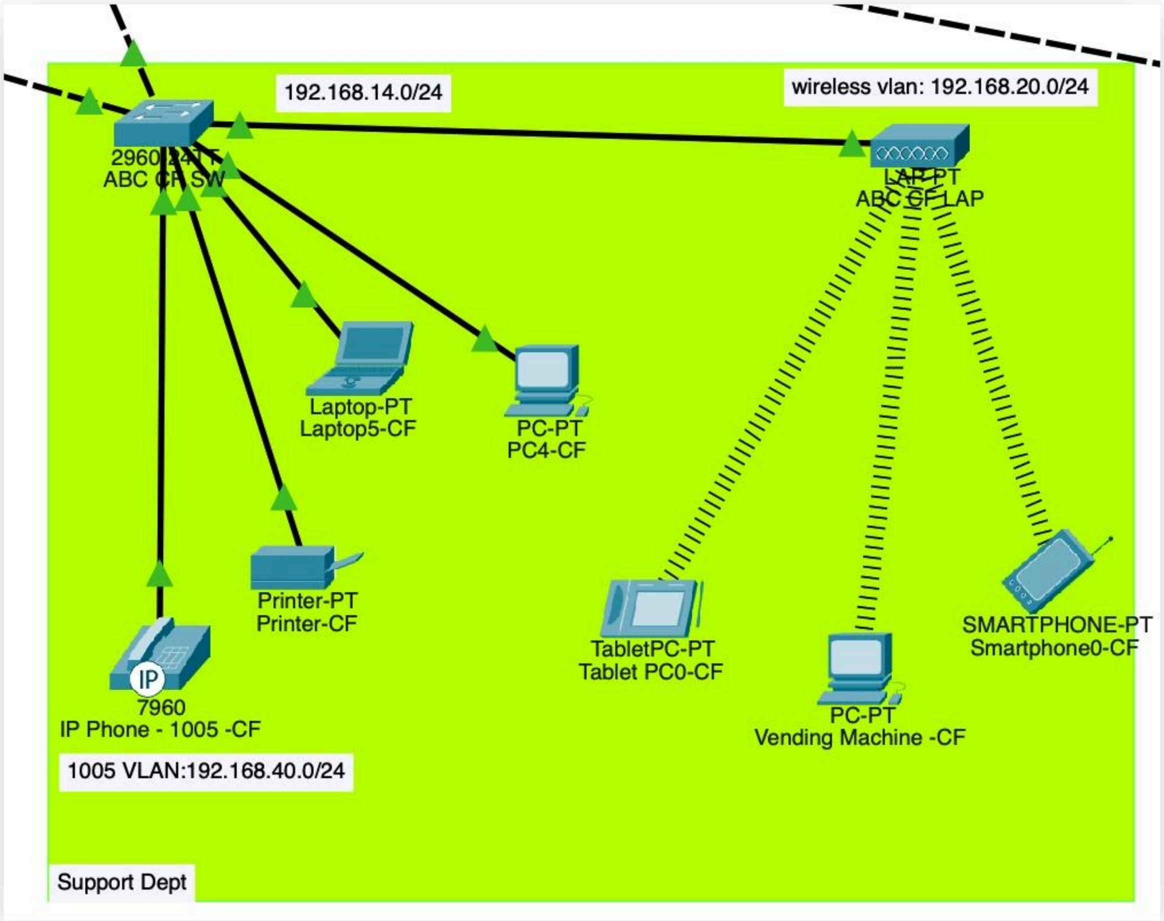


Figure 6 Support VLAN 1005 serves shared technical support staff.

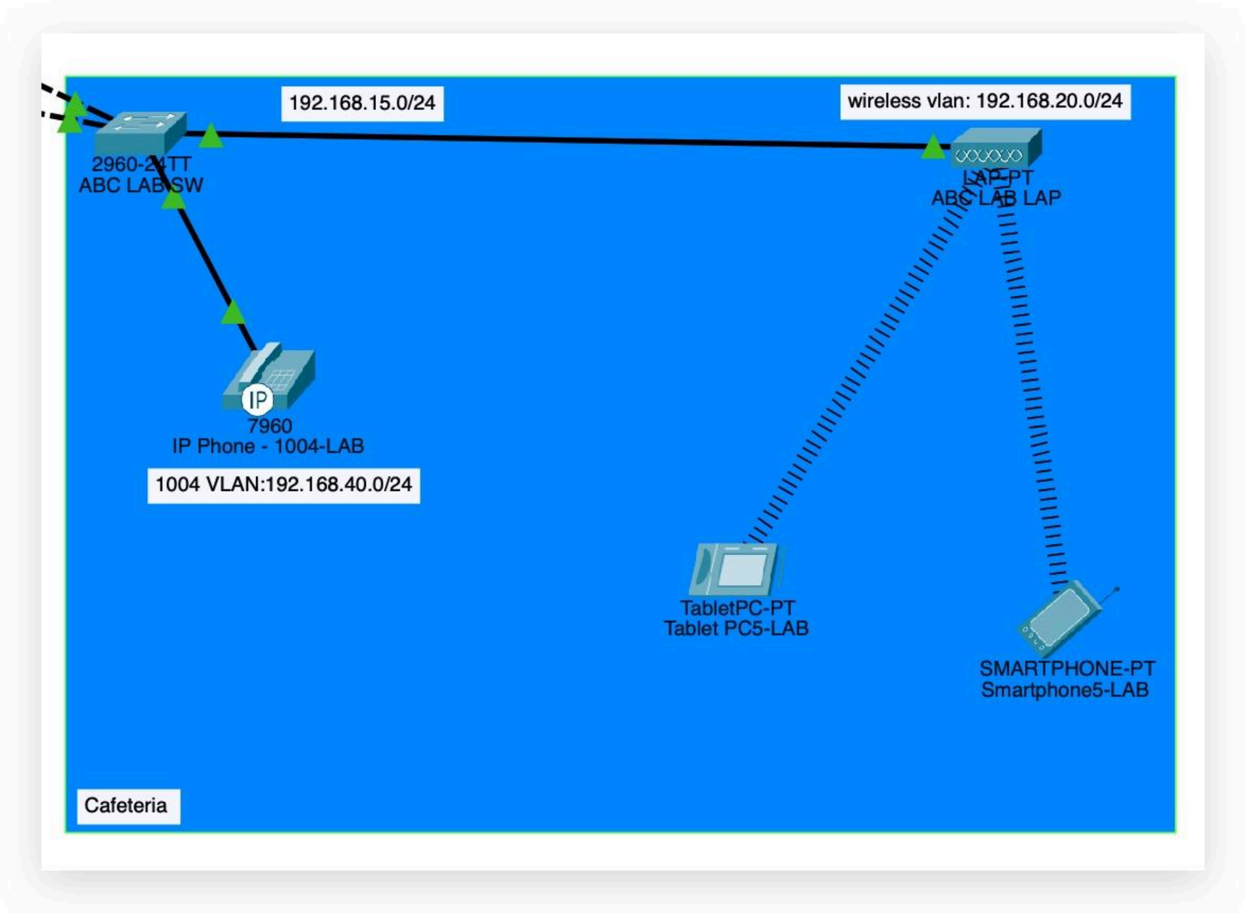


Figure 8 Cafeteria VLAN 1004 has restricted guest Wi-Fi and limited access.

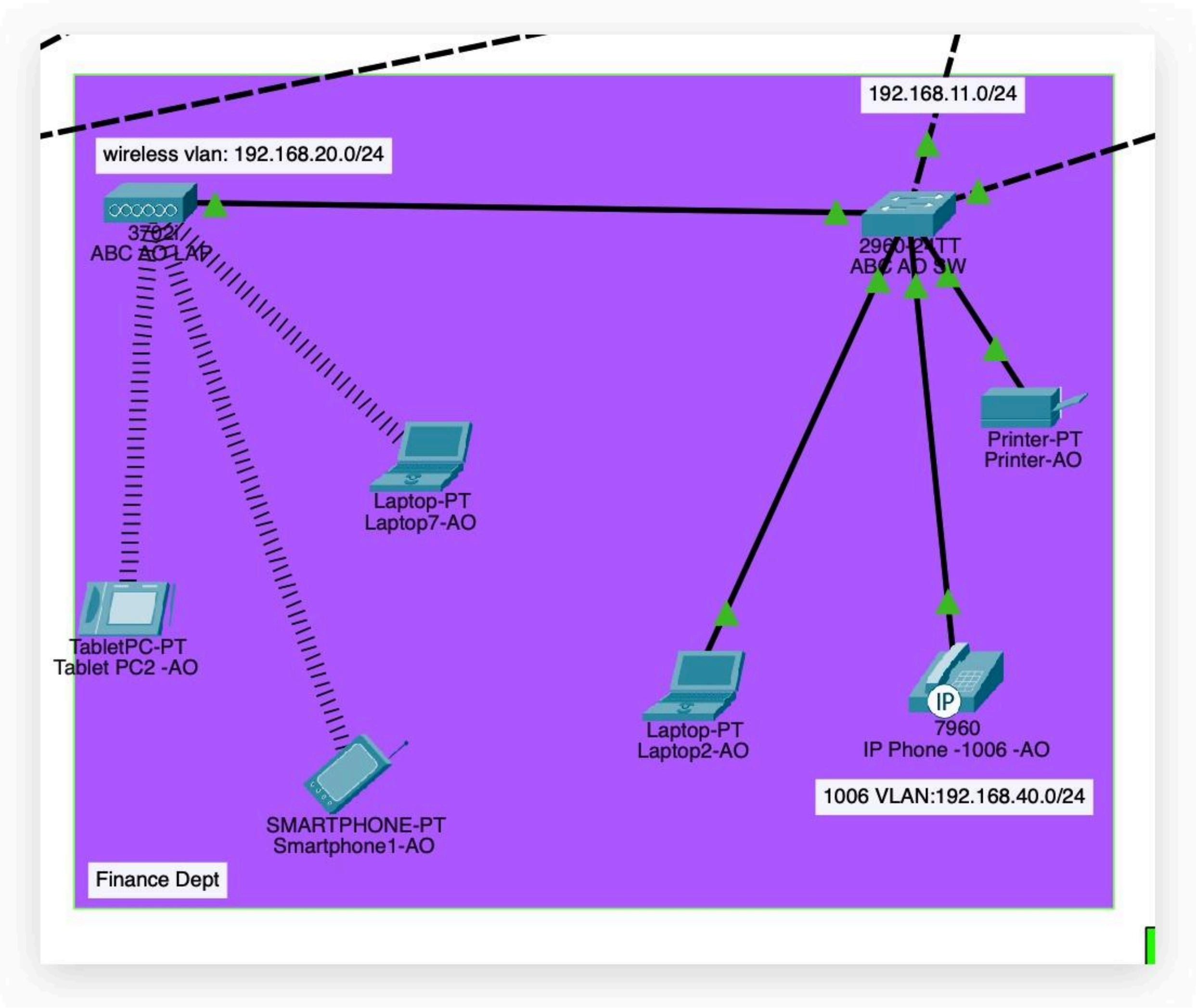


Figure 9 Finance VLAN 1006 is isolated and only allowed outbound email and selected access.

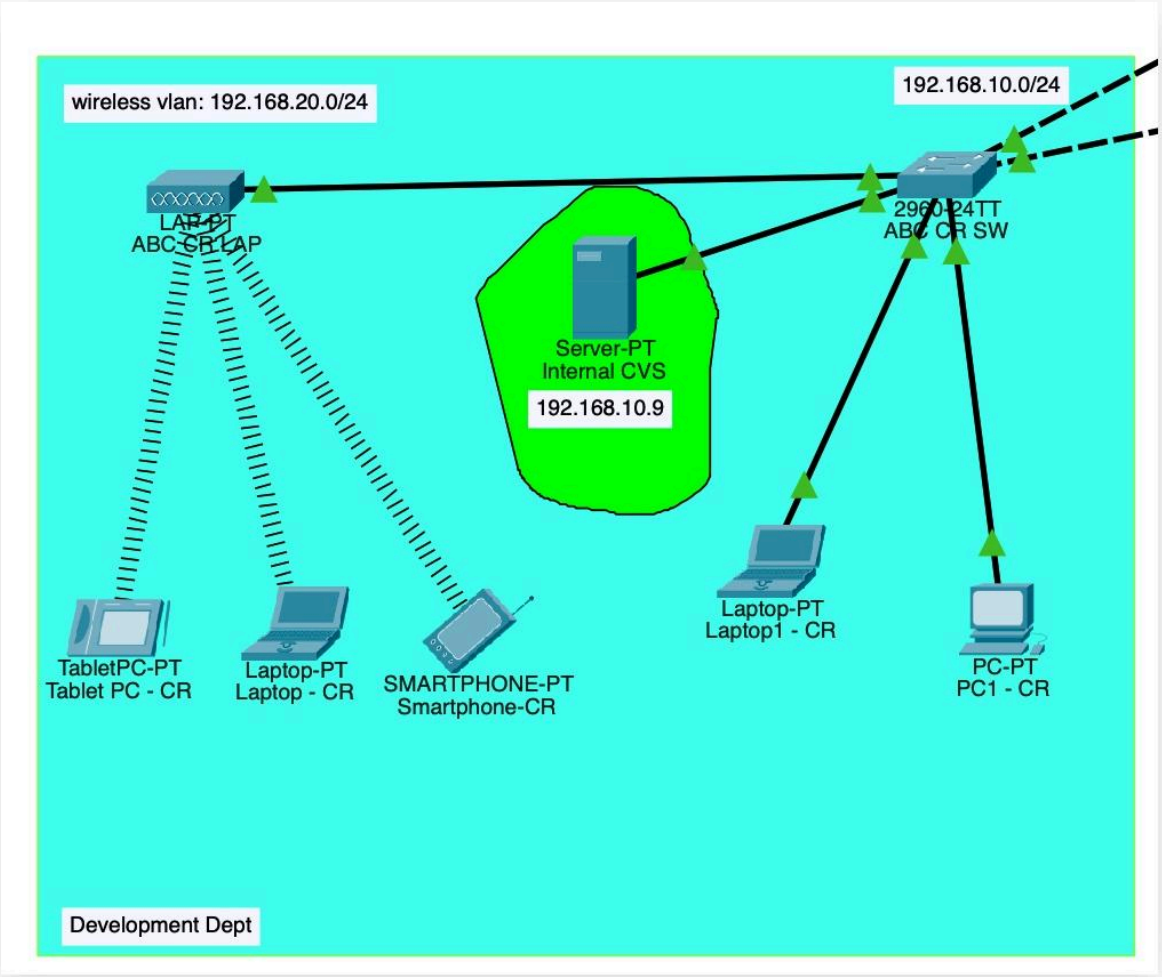


Figure 10 Dev Dept uses VLAN 1001 and hosts the internal CVS server. Access is controlled via firewall ACL.

VLAN ID	***Subnet***	***Department***	***Access Type***
1001	*192.168.10.0/24*	*Development*	*Internal CVS, Internet*
1002	*192.168.13.0/24*	*Sales*	*Limited Internet Only*
1003	*192.168.12.0/24*	*IT*	*Full Admin Access*
1004	*192.168.15.0/24*	*Cafeteria*	*Internet Only*
1005	*192.168.14.0/24*	*Support*	*Access to Shared Tools*
1006	*192.168.11.0/24*	*Finance*	*Internet + Limited Internal*
20	*192.168.20.0/24*	*Wireless Users*	*Controlled by WLC*
40	*192.168.40.0/24*	*IP Phone*	*VLAN Isolation*
100	*192.168.100.0/27*	*DMZ Zone*	*External Services*

101	*192.168.100.0/30*	*Core <-> Firewall*	*Transit Link*
102	*192.168.100.0/30*	*Firewall <-> ISP*	*Transit Link*

10. Security Architecture Overview

This diagram illustrates how internal traffic is routed to the firewall for policy enforcement before reaching DMZ services or the internet. ABC's security model follows a multi-layered design:

- **VLAN Isolation**: All departments are separated with inter-VLAN routing disabled by default. Specific routes are enforced via firewall policies.
- **Firewall-Centric Routing**: Internal cross-VLAN traffic is routed via the Layer 3 switch but handed off to the firewall for inspection, logging, and control. This allows selective approval (e.g., Dev to CVS, IT to Internal Web).
- **Least-Privilege Principle**: Department access is restricted to only necessary internal or external resources.
- **Wireless Access Control**: All wireless connections are authenticated through the centralized Wireless LAN Controller. Per-user access rules are enforced through the firewall. Future upgrades will use RADIUS + AD for role-based control.
- **AAA Authentication**: ABC AD/RADIUS server is planned for VPN, 802.1X, and wireless user identity management.

11. Secure Wireless Access

- Wireless LAN Controller (192.168.20.5) manages all LAPs across departments.
- Each user connects with unique credentials assigned to their department.
- Current deployment uses local user validation; future plan includes AD + RADIUS.
- Firewall will enforce access control per identity.

12. VPN Remote Access

RemoteDev-PC connects via VPN to the firewall, and is authenticated using multi-factor credentials. Only Dev users are allowed to access the internal CVS server.

- VPN Server (192.168.100.16) located in DMZ.
- MFA required: Password + SMS/AuthApp token.
- Only authorized Dev staff can access the internal CVS server (192.168.10.9).
- Other departments denied post-authentication via ACL.

Example ACL:

```
access-list VPN_SPLIT extended permit tcp any host 192.168.10.9 eq 443
access-list VPN_SPLIT extended deny ip any 192.168.11.0 255.255.255.0
```

13. Web Access Security

- All public-facing servers (e.g., www.abc.com) are protected by Cloudflare CDN.
- HTTPS enforced; HTTP redirected automatically.
- Protection against DDoS and malicious scanning.

---

14. ACL Matrix (Access Policy)

Source Dept	Destination	Allowed	Notes
Development	Internal CVS	✅	Required for version control
Finance	Internal Web / CVS	❌	Not permitted
IT	All servers	✅	Admin privileges
Sales	Internal resources	❌	Limited to web only
Wireless	Internet via NAT only	✅	No internal subnet access
VPN Dev	Internal CVS	✅	MFA protected
VPN Others	Any internal resource	❌	Blocked by VPN ACLs

15. Configuration Appendix

Note on Supplementary Files: To maintain readability in this report, only critical configuration snippets are included in the Configuration Appendix. Full configuration files for the ASA firewall and Layer 3 core switch, as well as the complete Cisco Packet Tracer topology (FinalProject-CIS221.pkt), are submitted separately with this report. These files provide detailed command-level implementation to support the logical design discussed herein.

A1 – ASA Firewall: ACL + VPN + NAT

```
! VPN ACL: Only Dev users can access CVS server
access-list VPN_SPLIT extended permit tcp any host 192.168.10.9 eq 443
access-list VPN_SPLIT extended deny ip any 192.168.11.0 255.255.255.0
access-list VPN_SPLIT extended deny ip any 192.168.13.0 255.255.255.0


! Object NAT for CVS server (public access)
object network obj_CVS
 host 192.168.10.9
 nat (inside,outside) static interface service tcp 443 443


! Syslog logging setup
logging enable
logging trap informational
logging host inside-2 192.168.12.100
```

A2 – L3 Core Switch: VLAN + ACL Example

```
ip access-list extended BLOCK-FINANCE-TO-DEV
 deny ip 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255
 permit ip any any

interface Vlan11
 ip access-group BLOCK-FINANCE-TO-DEV in

! Default route to ASA
ip route 0.0.0.0 0.0.0.0 192.168.100.34
```

A3 – HSRP (Redundancy for Core Switch)

```
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby 1 ip 192.168.10.1
 standby 1 priority 120
 standby 1 preempt
```

A4 – Wireless LAN Controller / RADIUS (Planned)

```
! Wireless Users → VLAN 20
interface vlan 20
 ip address 192.168.20.5 255.255.255.0
```

```
! (Planned) Radius Server Integration
radius-server host 192.168.12.8 auth-port 1812 acct-port 1813 key CIS221
aaa new-model
aaa authentication login default group radius local
```

16. Additional Technical Notes

1. **VoIP VLAN Isolation**

Voice VLAN (ID: 40) is isolated from data VLANs to ensure Quality of Service (QoS) and prevent interference. This separation leverages VLAN's inherent broadcast domain isolation, reducing latency and jitter in voice traffic.

2. **Wireless Access Precision via RADIUS + AD**

While this simulation uses WLC with local user authentication, in a real enterprise environment, a centralized RADIUS server combined with Active Directory (AD) enables fine-grained access control. Users and even computers can be dynamically assigned to VLANs based on group membership, MAC address, device posture, or security clearance. This not only strengthens authentication but also simplifies network policy enforcement across mobile and wireless devices.

3. **High Availability Design – Switch Redundancy & Firewall Control**

The system employs dual Layer 3 switches configured in a load-balancing and failover pair. This ensures high availability of routing services and network continuity in the event of hardware failure. Inter-VLAN traffic is routed through the firewall, allowing centralized control, logging, and policy enforcement. This architecture balances security (firewall inspection) with availability (switch redundancy) and performance (localized L2 switching).

17. Conclusion

This enhanced network design adheres to CIS-221-AB1 security principles, including identity enforcement, traffic auditing, VLAN isolation, and secure remote access. While several components (e.g., VPN, RADIUS) are marked as future implementations, the architecture is designed with best practices in mind. This project transforms a prior L2-focused topology into a modern secure enterprise framework.

“Security is not a feature, but a posture.”

18. Works Cited

Whitman, Michael E., and Herbert J. Mattord. *Principles of Information Security*. 7th ed., Cengage Learning, 2022.

Cisco. “Configure ASA Firewalls: CLI and Security Contexts.” Cisco Documentation, 2023, https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config.html?dtid=osscdc000283&linkclickid=srch.

Cisco. “Configure Layer 3 Switches and VLAN Routing.” Cisco Networking Academy, 2023, https://www.netacad.com/courses/packet-tracer.

Cloudflare. “Introduction to Cloudflare and Security Controls.” Cloudflare Docs, 2024, https://developers.cloudflare.com/fundamentals/security.