ParkShield: Secure, Segmented Campus Network Architecture

Subtitle: A MultiVLAN, DMZFirst Design with Centralized Services and DefenseinDepth
Course: *Cybersecurity]*
Instructor: *Sananda*
Institution: *Becode Bruxelles*
Date of Submission: *31-08-2025*
Repository: vestersly/ParkShield-Network-Architecture: Secure, Segmented Campus Network Architecture featuring a DMZ-first policy and Layer 3 ACL enforcement.

Project Team & Roles

- **Sylvester** — Team Lead & Documentation
- **Julien** — Firewall & Security Policy (DMZ + ACLs)
- **Viktor** — Authentication Services (RADIUS – Phase 2)
- **Harold** — Application Services (Mail & File Servers – Phase 2)
- **Yurii** — Core Network Implementation (L2/L3, DHCP, DNS)

This jury edition spotlights scope, rationale, metrics, and verifiable tests. All configuration snippets are reproducible in Packet Tracer and/or GNS3.

Executive Summary

This project delivers a **secure, segmented campus network** for a multidepartment environment (“the Park”). The design implements **layered security** via VLAN segmentation, a **DMZfirst policy**, and **centrally managed core services** (DNS, DHCP). The solution emphasizes **operational resilience**, **futurereadiness**, and **clear governance** of eastwest and northsouth traffic using ACLs and a dedicated DMZ.

Outcomes & Impact

- **Security:** Attack surface reduction through VLAN isolation, DMZ controls, device hardening, and leastprivilege ACLs.
- **Reliability:** Redundant paths (where applicable), standard STP settings, and faulttolerant IP addressing scheme.
- **Scalability:** Consistent L2/L3 templates and modular VLAN plan for frictionless growth.
- **Auditability:** Test plan with pass/fail criteria; change, backup, and monitoring procedures.

Key KPIs

- ✅ InterVLAN latency < 2 ms (campus)
- ✅ 100% success on core functional tests (DHCP/DNS reachability, server access per policy)
- ✅ 0 policy violations in ACL test matrix (negative test suite)

1. Introduction & Requirements

1.1 Project Team and Responsibilities

- **Sylvester (Team Lead & Documentation):** Coordinates milestones, integrates deliverables; authors this jury report, cost analysis, and test plans.
- **Julien (Firewall & Security Policy):** Designs DMZ policy and stateful/ACL rules; validates segmentation and northsouth controls.
- **Viktor (RADIUS – Phase 2):** Designs centralized authentication; allocates addressing and integration points for future wireless/VPN.
- **Harold (App Services – Phase 2):** Plans mail and file services deployment; defines capacity and service dependencies.
- **Yurii (Core Network):** Implements L2/L3, VLANs, trunks, SVIs, DHCP pools, and DNS; ensures baseline hardening.

1.2 Scope

- **In Scope (Phase 1):** Core & access switching, VLAN segmentation, interVLAN routing, DHCP/DNS, DMZ policy via ACLs, remoteuser simulation, security hardening, test & validation, and documentation.
- **Phase 2 (Planned):** RADIUS AAA, production mail/file servers, iSCSI storage segment, optional firewall appliance/ASA replacement for L3 ACLs.

1.3 Assumptions

- Packet Tracer used for simulation; IOS feature parity assumed as documented.
- No public Internet connectivity required for jury demo; “Remote Users” modeled as a dedicated VLAN/subnet.
- Single core switch with room to add a second for HA in future.

1.4 Success Criteria

- Segmentation enforced; only approved flows pass (per ACL matrix).
- All clients receive DHCP and resolve names via DNS.
- DMZ hosts reachable only via permitted services from specific VLANs.
- Documentation is reproducible, with configs stored in VCS.

2. Architecture Overview

2.1 Logical Topology

Core: L3 switch (SVIs, DHCP/DNS hosting or relays).
Access Layer: Six 2960class switches (departmental VLAN access).
Edge/DMZ: Server segment for shared services (DNS/DHCP now; Mail/File later).
Optional Security Appliance: ASA or L3 ACLs on the core (current build uses L3 ACLs; ASA kept as an extension path).

Note: Standardize trunk **native VLAN 99** (Black_Hole) across all trunk links to prevent VLAN 1 exposure and stop nativeVLAN mismatch.

2.2 VLAN & Subnet Plan (Final Mapping)

VLAN	Name	Subnet	Gateway (SVI)	Notes
10	Management/Admin	192.168.10.0/24	192.168.10.1	IT & admin clients
20	Study	192.168.20.0/24	192.168.20.1	Students/Lab
30	Production	192.168.30.0/24	192.168.30.1	Production users
40	Support_1	192.168.40.0/24	192.168.40.1	Support team zone 1
50	Support_2	192.168.50.0/24	192.168.50.1	Support team zone 2
60	DMZ	192.168.60.0/24	192.168.60.1	DNS/DHCP now; Mail/File later
70	AAA/Storage (Rsv)	192.168.70.0/24	192.168.70.1	Reserved for RADIUS / iSCSI (Phase 2)
80	Remote Users	10.10.10.0/24	10.10.10.1	Simulated remote subnet
99	Black_Hole	N/A	—	Native on trunks; not routed

If your current .pkt uses a different mapping, adapt SVI IPs and pools accordingly—the policy and tests remain valid.

2.3 Device Inventory & Roles

- **Core L3 Switch:** InterVLAN routing (SVIs), DHCP server or relay, DNS hosting (lab), ACL enforcement.
- **Access Switches (x6):** Dept VLAN access; trunks to core; PortFast on edge ports.
- **Servers (DMZ):** DNS, DHCP (or DHCP relay from core), future Mail/File.
- **Remote PC(s):** In VLAN 80 to validate edge policy.

3. Implementation Design

3.1 Layer 2 (Switching)

- **Trunks:** `switchport mode trunk`, `switchport trunk native vlan 99`, `switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99`
- **Edge Ports:** `switchport mode access`, `switchport access vlan <X>`, `spanning-tree portfast`

- **STP:** PVST default; ensure no VLAN 1 traffic on trunks; VLAN 99 not used for users.

3.2 Layer 3 (SVIs & Routing)

SVIs on core: `Vlan10..Vlan80` with gateway IPs per §2.2.
Static default not required in campus; add if ASA/edge router is used for upstream traffic.

3.3 IP Services

- **DHCP (on Core or DMZ server):** Scopes for VLANs 10–50 & 80. DMZ servers typically **static**; reserve or exclude appropriate ranges.
- **DNS:** Authoritative zone for `park.local` (lab). A records for servers; optional PTRs. Clients receive DNS via DHCP option.
- **NTP:** Core as client to a simulator or manual clock set; propagate to servers.

3.4 Authentication (Phase 2)

- RADIUS server in VLAN 70 with IP `192.168.70.10` (reserved).
- AAA on network devices (SSH + local fallback).
- Future: 802.1X on access ports; WPA2Enterprise for WLAN.

3.5 Security Controls (DMZ & ACLs)

- **Principle:** Allow only required services from leastprivileged sources. Block all else.
- **Placement:** Extended ACLs applied inbound on **SVIs** closest to source, or on routed DMZ interface.

ACL Policy Matrix (excerpt)

Source VLAN	Destination	Service	Action	Rationale
10 (Mgmt)	60 (DMZ DNS)	UDP/TCP 53	Permit	Admin clients resolve names
20 (Study)	60 (DMZ DNS)	UDP/TCP 53	Permit	Students resolve names
30 (Prod)	60 (DMZ DNS)	UDP/TCP 53	Permit	Production resolve names
Any (10–50)	60 (DMZ DHCP)	UDP 67/68	Permit	DHCP relay if server in DMZ
10–50	60 (Mail)	TCP 25/587/993 (Phase 2)	Permit	Client ↔ Mail (future)
Any	Any	Any	Deny	Default explicit deny

If an ASA is available, mirror these policies with security levels / ACLs on the ASA. In the Phase 1 build, enforcement occurs on the L3 core.

3.6 Remote User Simulation (VLAN 80)

- Validate that **remote users** (10.10.10.0/24) cannot reach internal VLANs except permitted public services in DMZ (e.g., HTTP/HTTPS to a test web host in VLAN 60).

3.7 Resilience & Growth

- Modular VLAN numbering; /24 per segment.
- Clear templates to autoprovision additional access switches.
- Reserved VLAN 70 for AAA/Storage to be activated without renumbering.

4. Configuration Templates (Packet Tracer–Ready)

Replace bracketed values with your actual interface/VLAN numbers. Save "golden" templates in VCS.

4.1 Core L3 Switch (Baseline)

```
! Hostname & hardening
hostname CORE-L3
no ip domain-lookup
service password-encryption

! VLANs
vlan 10 name MANAGEMENT
vlan 20 name STUDY
vlan 30 name PRODUCTION
vlan 40 name SUPPORT_1
vlan 50 name SUPPORT_2
vlan 60 name DMZ
vlan 70 name AAA_STORAGE
vlan 80 name REMOTE
vlan 99 name BLACK_HOLE

! Trunk to Access (examples)
interface Fa0/2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99
!
interface Fa0/3
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99

! SVIs
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
 no shut
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
 no shut
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
 no shut
interface Vlan40
```

```
 ip address 192.168.40.1 255.255.255.0
 no shut
interface Vlan50
 ip address 192.168.50.1 255.255.255.0
 no shut
interface Vlan60
 ip address 192.168.60.1 255.255.255.0
 no shut
interface Vlan70
 ip address 192.168.70.1 255.255.255.0
 no shut
interface Vlan80
 ip address 10.10.10.1 255.255.255.0
 no shut

ip routing

! DHCP (example pools)
ip dhcp excluded-address 192.168.10.1 192.168.10.49
ip dhcp pool VLAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 192.168.20.1 192.168.20.49
ip dhcp pool VLAN20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 192.168.30.1 192.168.30.49
ip dhcp pool VLAN30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 192.168.40.1 192.168.40.49
ip dhcp pool VLAN40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 192.168.50.1 192.168.50.49
ip dhcp pool VLAN50
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 10.10.10.1 10.10.10.49
ip dhcp pool VLAN80
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 dns-server 192.168.60.10

! Example DMZ DNS server
! Assign static IP 192.168.60.10/24 on the server NIC

! ACLs (apply closest to source)
ip access-list extended ACL_VLAN10_OUT
 permit udp 192.168.10.0 0.0.0.255 host 192.168.60.10 eq 53
 permit tcp 192.168.10.0 0.0.0.255 host 192.168.60.10 eq 53
```

```
 deny   ip any any log
!
interface Vlan10
 ip access-group ACL_VLAN10_OUT in
!
! Duplicate per VLAN with least-privilege rules

line con 0
 logging synchronous
line vty 0 4
 transport input ssh
 login local
!
username admin privilege 15 secret 9 adminSecret

end
write memory
```

```
! Hostname & hardening
hostname CORE-L3
no ip domain-lookup
service password-encryption

! VLANs
vlan 10 name MANAGEMENT
vlan 20 name STUDY
vlan 30 name PRODUCTION
vlan 40 name SUPPORT_1
vlan 50 name SUPPORT_2
vlan 60 name DMZ
vlan 70 name AAA_STORAGE
vlan 80 name REMOTE
vlan 99 name BLACK_HOLE

! Trunk to Access (examples)
interface Fa0/2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99
!
interface Fa0/3
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99

! SVIs
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
 no shut
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
```

```
 no shut
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
 no shut
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
 no shut
interface Vlan50
 ip address 192.168.50.1 255.255.255.0
 no shut
interface Vlan60
 ip address 192.168.60.1 255.255.255.0
 no shut
interface Vlan70
 ip address 192.168.70.1 255.255.255.0
 no shut
interface Vlan80
 ip address 10.10.10.1 255.255.255.0
 no shut

ip routing

! DHCP (example pools)
ip dhcp excluded-address 192.168.10.1 192.168.10.49
ip dhcp pool VLAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 192.168.20.1 192.168.20.49
ip dhcp pool VLAN20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 192.168.30.1 192.168.30.49
ip dhcp pool VLAN30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 192.168.40.1 192.168.40.49
ip dhcp pool VLAN40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.60.10
!
```

```
ip dhcp excluded-address 192.168.50.1 192.168.50.49
ip dhcp pool VLAN50
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
 dns-server 192.168.60.10
!
ip dhcp excluded-address 10.10.10.1 10.10.10.49
ip dhcp pool VLAN80
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 dns-server 192.168.60.10

! Example DMZ DNS server
! Assign static IP 192.168.60.10/24 on the server NIC

! ACLs (apply closest to source)
ip access-list extended ACL_VLAN10_OUT
 permit udp 192.168.10.0 0.0.0.255 host 192.168.60.10 eq 53
 permit tcp 192.168.10.0 0.0.0.255 host 192.168.60.10 eq 53
 deny   ip any any log
!
interface Vlan10
 ip access-group ACL_VLAN10_OUT in
!
! Duplicate per VLAN with least-privilege rules

line con 0
 logging synchronous
line vty 0 4
 transport input ssh
 login local
!
username admin privilege 15 secret 9 adminSecret

end
write memory
```

Access Switch (PerVLAN Template)

```
hostname ACCESS-<N>
no ip domain-lookup

vlan 99 name BLACK_HOLE
vlan <X> name <SEGMENT>

interface Fa0/1
```

```
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99

interface range Fa0/2 - 24
 switchport mode access
 switchport access vlan <X>
 spanning-tree portfast

line con 0
 logging synchronous
end
write memory
```

(Optional) ASA/Edge Policy (Concept)

If using an ASA, mirror the ACL matrix with outside/inside/DMZ interfaces, and enable inspection as needed. For Packet Tracer builds without ASA, enforce at the L3 core via SVIs (as above).

5. DNS & DHCP Design

- **DNS Zone:** `park.local`
  - `dns1.park.local` → 192.168.60.10
  - `mail.park.local` → 192.168.60.20 (Phase 2)
  - `files.park.local` → 192.168.60.30 (Phase 2)
- **DHCP Strategy:** Dynamic for client VLANs (10–50, 80); static for DMZ servers; 50IP exclusion at top of each subnet for infra.

6. Security Architecture

6.1 Threat Model (Summary)

- **Untrusted user hosts** laterally moving without segmentation → **VLAN isolation + ACLs**.
- **Service exposure** (DNS, future mail/file) → **DMZ placement + allowlist**.
- **Device compromise → baseline hardening, SSHonly, encrypted secrets**.
- **Misconfig (native VLAN 1) → Blackhole VLAN 99** on all trunks.

6.2 Device Hardening Checklist

- Disable unused services; `no cdp run` where appropriate on untrusted edges.
- Exec timeouts; privilege 15 only for admins; banner; encrypted passwords.
- NTP & consistent timezone; config backups to secured repo.

7. Test & Validation Plan (DemoReady)

Functional Tests

1. **DHCP**: Clients in VLANs 10/20/30/40/50/80 receive correct IP, GW, DNS.
2. **DNS**: `ping dns1.park.local` and name resolution works from each client VLAN.
3. **Segmentation**: Hosts cannot reach other VLANs (ICMP) unless explicitly allowed.
4. **DMZ Access**: Only permitted services (e.g., DNS) reachable; others blocked.

Negative/Security Tests

- From VLAN 20, attempt `telnet 192.168.60.10 25` → **DENY**.
- From VLAN 80 (Remote), attempt to ping VLAN 10 gateway → **DENY**.
- Trunk native VLAN mismatch intentionally created → STP/ACL logs confirm block.

Performance

- IntraVLAN ping `<1 ms`; InterVLAN `<2 ms` inside campus.

Test Matrix (Excerpt)

Test ID	Source	Destination	Protocol/Port	Expect
T01	VLAN10 Client	192.168.60.10	UDP 53	PASS
T02	VLAN20 Client	192.168.60.10	TCP 53	PASS
T03	VLAN80 Client	192.168.10.1	ICMP	DENY
T04	VLAN30 Client	192.168.60.20	TCP 587 (Phase 2)	PASS

8. Operations: Monitoring, Backup, Change

- **Monitoring:** Enable syslog to a DMZ syslog host (Phase 2) or console logs for lab. Track ACL hits.
- **Backups:** `copy running-config tftp:` to a secured server; commit to VCS with tags.
- **Change Control:** Use semantic versions (v1.0 = Phase 1 GA). Change tickets for ACL edits.

9. Bill of Materials (Indicative)

Item	Qty	Notes
L3 Core Switch (PT)	1	InterVLAN routing & services
2960 Access Switch	6	Dept access
Servers (PT)	2–3	DNS/DHCP now; Mail/File later
PCs (PT)	as needed	Per VLAN tests
ASA (Optional)	1	Phase 2 stateful edge

In production, include support contracts, licenses, and redundant power. In Packet Tracer, focus on logical completeness and testability.

10. Risks & Mitigations

- **Risk:** Misaligned trunk native VLAN → **Mitigation:** All trunks fixed to 99; audit `show interfaces trunk` on both ends.
- **Risk:** Overpermissive ACLs → **Mitigation:** Default deny; change control; log counters.
- **Risk:** Single core switch → **Mitigation:** Roadmap for dualcore (HSRP/VRRP) in Phase 3.

11. Future Enhancements (Roadmap)

- **AAA/RADIUS (VLAN 70)** for device login and 802.1X.
- **Mail & File Servers** in DMZ with TLS; dedicated reverse proxy if Internetfacing.
- **Storage (iSCSI)** in VLAN 70 with ACL pinholes from authorized servers only.
- **High Availability:** Second core + dynamic routing; redundant links (EtherChannel).
- **Observability:** Central syslog/SIEM; NetFlow for traffic analytics; SNMPv3.

.

Appendix A – Full ACL Examples (Per VLAN)

```
ip access-list extended ACL_VLAN20_OUT
 permit udp 192.168.20.0 0.0.0.255 host 192.168.60.10 eq 53
 permit tcp 192.168.20.0 0.0.0.255 host 192.168.60.10 eq 53
 deny ip any any log
!
interface Vlan20
 ip access-group ACL_VLAN20_OUT in
```

(Replicate for VLANs 30/40/50/80 with exact leastprivilege rules. For future mail/file, add specific ports and hosts.)

Appendix B – Sample DNS Zone (park.local)

```
$ORIGIN park.local.
@       IN SOA  dns1.park.local. admin.park.local. (
                20250818 ; serial
                7200     ; refresh
                3600     ; retry
                1209600  ; expire
                3600 )   ; minimum
        IN NS   dns1.park.local.
dns1    IN A    192.168.60.10
mail    IN A    192.168.60.20
files   IN A    192.168.60.30
```

```
$ORIGIN park.local.
@     IN SOA  dns1.park.local. admin.park.local. (
          20250818 ; serial
          7200    ; refresh
          3600    ; retry
          1209600  ; expire
          3600 )  ; minimum
      IN NS  dns1.park.local.
dns1   IN A   192.168.60.10
mail   IN A   192.168.60.20
files  IN A   192.168.60.30
```

Appendix C – Demo Script (5–7 minutes)

1. **Show VLANs & trunks:** `show vlan brief`, `show interfaces trunk` (native 99 aligned).
2. **Show SVIs & routing:** `show ip interface brief`, `show ip route`.
3. **DHCP & DNS:** Release/renew on a client; resolve `dns1.park.local`.
4. **Policy in action:** From VLAN 20, allow DNS; block SMTP to DMZ.
5. **Remote VLAN 80 isolation:** Ping internal gateways → denied.
6. **ACL hits:** `show access-lists` to display counters increasing.

Project Cost Estimate & Justification Report

Project Title: Secure and Scalable Network Infrastructure for Park Operations

Prepared For: The Project Evaluation Jury [Or Client Name, e.g., "Park Management Board"]

Prepared By: [Your Name/Your Consulting Company Name, e.g., "SecureNet Solutions & Consulting"]

Date: August 16, 2025

Version: 1.0

---

1. Executive Summary

This document provides a detailed cost estimation for the successful design, implementation, and deployment of the new network infrastructure. The project's scope encompassed a complete overhaul of the existing network, creating a secure, segmented, and highly manageable environment to support all operational departments.

The total estimated investment for this project is $126,627.50. This figure is inclusive of all hardware, software licensing, and professional labor required to move from the initial analysis phase to a fully tested and operational network.

This investment provides a robust and scalable network foundation that directly addresses all project requirements, including departmental segmentation, centralized DHCP/DNS services, and a secure DMZ architecture. The costs outlined represent a strategic investment in the organization's security posture, operational efficiency, and future technological growth.

---

2. Project Scope and Deliverables

The costs detailed below are for the complete delivery of the following key infrastructure and services:

- User Base: Network infrastructure supporting 43 workstations across five distinct departmental VLANs.
- Server Infrastructure: A secure server VLAN hosting 5 physical servers (DNS, DHCP, iSCSI, RADIUS, and one spare/FTP).
- Security: A fully configured DMZ with a dedicated server, protected by a granular Access Control List (ACL) on the core router.
- Physical Infrastructure: A centralized network rack with professional cabling and power management.

• Professional Services: End-to-end project services including consultation, design, implementation, testing, and documentation.

---

3. Detailed Cost Breakdown

The total project cost is broken down into three primary categories: Hardware & Materials, Software & Licensing, and Labor & Professional Services.

3.1. Hardware & Material Costs

This category includes all physical components required to build the network. Prices are estimated based on 2025 market rates for new, enterprise-grade equipment suitable for a small-to-medium business environment.

Item	Model/Description	Qty	Unit Cost	Total Cost	Justification
Core Switch/Router	Cisco Catalyst 9300 Series (Layer 3)	1	$6,500.00	$6,500.00	The heart of the network; provides high-performance inter-VLAN routing.
Access Switches	Cisco Catalyst 9200 Series (Layer 2)	7	$2,800.00	$19,600.00	Provides secure, reliable connectivity for all end devices in each VLAN.
Servers	Dell PowerEdge R450 or similar (incl. RAID, redundant PSU)	5	$4,500.00	$22,500.00	Enterprise-grade servers to reliably host critical network services.
Workstations	Dell OptiPlex / HP EliteDesk Business Desktop	43	$950.00	$40,850.00	Standardized business PCs for all 43 users across the five departments.
Network Rack	Standard 42U Server Cabinet with vertical cable managers	1	$1,200.00	$1,200.00	Centralizes all network hardware for security and ease of management.
UPS (Power Supply)	Rackmount 3000VA Uninterruptible Power Supply	1	$1,800.00	$1,800.00	Provides clean power and short-term backup for all servers and switches.
Cabling Infrastructure	Per-port cost (Cat6a cable, patch panel port, faceplate)	48	$175.00	$8,400.00	Professional, certified cabling for all 43 PCs and 5 servers ("drops").
Patch Cables	Assorted lengths of Cat6a patch cords	100	$7.50	$750.00	For connections between patch panels and switches, and PCs to faceplates.
Subtotal Hardware				$101,600.00	

3.2. Software & Licensing Costs

This category covers the necessary operating system licenses for the servers.

Item	Description	Qty	Unit Cost	Total Cost	Justification
Server Operating System	Windows Server 2025 Standard (per core)	5	$1,250.00	$6,250.00	Licensed OS for each of the five physical servers.
Subtotal Software				$6,250.00	

3.3. Labor & Professional Services Costs

This is the most critical component, covering the time and expertise required to design, deploy, and verify the entire solution. A blended rate of $125/hour is used for network engineering labor.

Phase	Description	Estimated Hours	Rate/Hour	Total Cost
Phase 1: Consultation & Field Study	Initial meetings, requirements gathering, site survey, analysis of existing infrastructure.	16 hours	$125.00	$2,000.00
Phase 2: Project Analysis & Design	Developing the logical/physical topology, IP addressing scheme, VLAN strategy, and security policies.	24 hours	$125.00	$3,000.00
Phase 3: Implementation	Racking and cabling hardware, physical installation, and applying all base configurations to switches.	32 hours	$125.00	$4,000.00
Phase 4: Service Configuration	Deployment and configuration of DHCP pools, DNS records, and the security ACL.	20 hours	$125.00	$2,500.00
Phase 5: Testing & Verification	Rigorous end-to-end testing of all network functions, services, and security rules.	16 hours	$125.00	$2,000.00
Phase 6: Documentation & Reporting	Creation of detailed network diagrams, configuration backups, and this final project report.	12 hours	$125.00	$1,500.00
Subtotal Labor		120 hours		$15,000.00

---

4. Grand Total Cost Summary

This section summarizes all costs to provide a final project total. A standard 10% contingency is added to cover unforeseen challenges or scope adjustments.

Category	Total Cost

Hardware & Material Costs $101,600.00

Software & Licensing Costs $6,250.00

Labor & Professional Services $15,000.00

Subtotal $122,850.00

Contingency (10%) $12,285.00

PROJECT GRAND TOTAL $135,135.00

---

5. Assumptions and Exclusions

This cost estimate is based on the following assumptions and exclusions:

- Assumptions: All work will be performed during standard business hours. The physical site (server room, offices) is ready for installation with adequate power and cooling.

- Exclusions: This estimate does not include taxes, internet service provider (ISP) fees, ongoing support or maintenance contracts, application software for workstations, or major structural modifications to the building.

---

6. Conclusion

The total projected investment of $135,135.00 provides a modern, secure, and professionally-managed network infrastructure. This new system directly addresses the critical needs for departmental separation and security while providing a scalable foundation that will support the organization's operational needs for years to come. This project should be considered a vital and valuable investment in the organization's technological future.