ParkShield: Secure, Segmented Campus Network Architecture

A comprehensive multi-VLAN design with DMZ-first approach, centralized services, and defense-in-depth security for campus environments.

Project Team & Scope

1

Sylvester — Team Lead & Documentation

Coordinates milestones, integrates deliverables, authors jury report, cost analysis, and test plans.

2

Julien — Firewall & Security Policy

Designs DMZ policy and stateful/ACL rules; validates segmentation and north-south controls.

3

Yurii — Core Network Implementation

Implements L2/L3, VLANs, trunks, SVIs, DHCP pools, and DNS; ensures baseline hardening.

4

Viktor & Harold — Phase 2 Services

Viktor: RADIUS authentication; Harold: Mail & File Servers deployment.

Phase 1 includes core & access switching, VLAN segmentation, inter-VLAN routing, DHCP/DNS, DMZ policy via ACLs, remote-user simulation, security hardening, testing, and documentation.

Executive Summary

This project delivers a secure, segmented campus network for a multi-department environment ("the Park"). The design implements layered security via VLAN segmentation, a DMZ-first policy, and centrally managed core services (DNS, DHCP).

The solution emphasizes operational resilience, future-readiness, and clear governance of east-west and north-south traffic using ACLs and a dedicated DMZ.

<2ms

Inter-VLAN Latency

Campus-wide performance

100%

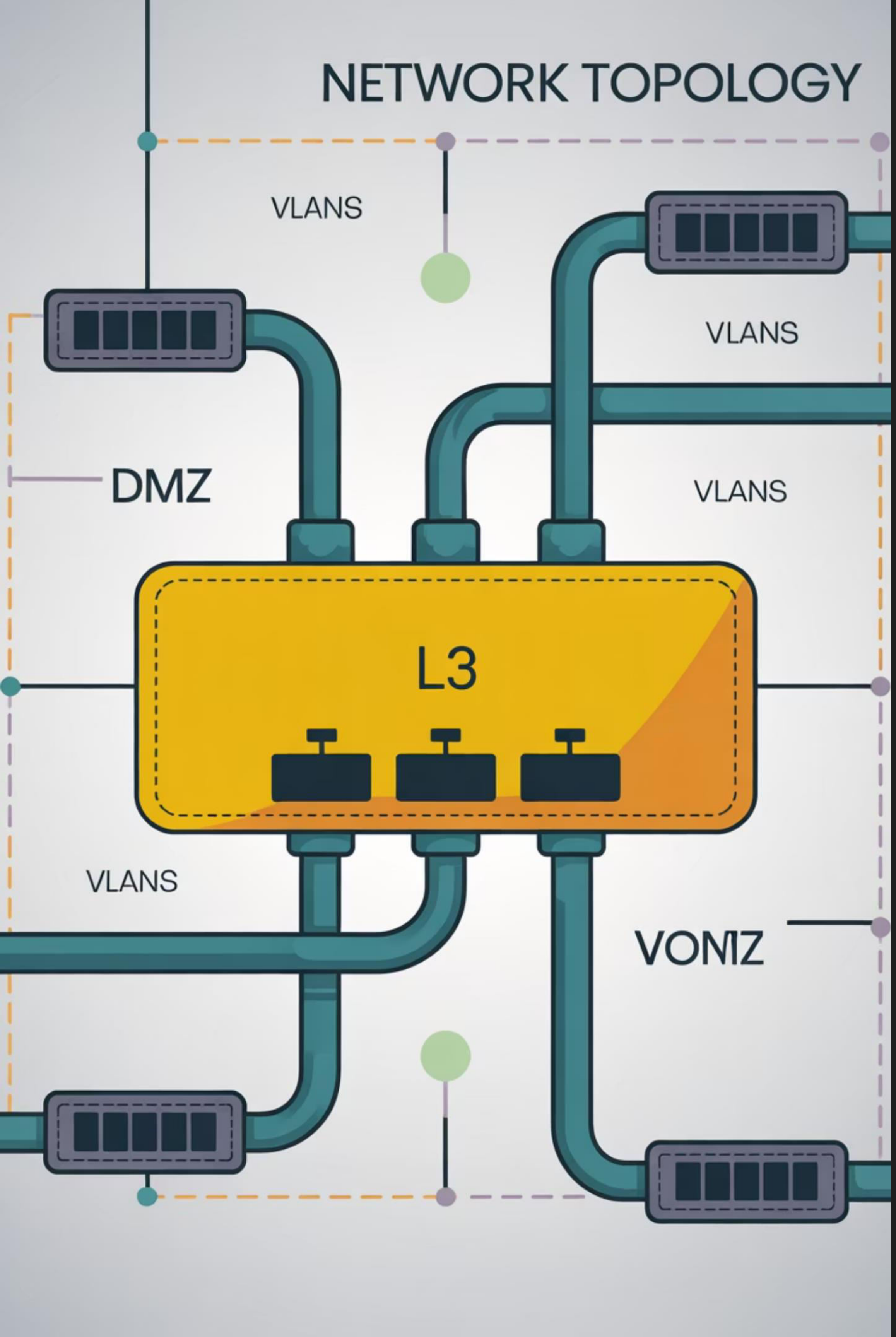
Core Tests

DHCP/DNS reachability

0

Policy Violations

In ACL test matrix



Network Architecture Overview

Core Layer

L3 switch with SVIs, DHCP/DNS hosting or relays

Access Layer

Six 2960-class switches for departmental VLAN access

Edge/DMZ

Server segment for shared services (DNS/DHCP now; Mail/File later)

Security

L3 ACLs on core (current); ASA as extension path (future)

All trunk links standardized with native VLAN 99 (Black_Hole) to prevent VLAN 1 exposure and stop native-VLAN mismatch.

VLAN & Subnet Plan

VLAN	Name	Subnet	Gateway (SVI)
10	Management/Admin	192.168.10.0/24	192.168.10.1
20	Study	192.168.20.0/24	192.168.20.1
30	Production	192.168.30.0/24	192.168.30.1
40	Support_1	192.168.40.0/24	192.168.40.1
50	Support_2	192.168.50.0/24	192.168.50.1
60	DMZ	192.168.60.0/24	192.168.60.1
70	AAA/Storage (Rsv)	192.168.70.0/24	192.168.70.1
80	Remote Users	10.10.10.0/24	10.10.10.1
99	Black_Hole	N/A	—

Security Architecture

Threat Model

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

ACL Policy Matrix (Excerpt)

Source VLAN	Destination	Service	Action
10 (Mgmt)	60 (DMZ DNS)	UDP/TCP 53	Permit
20 (Study)	60 (DMZ DNS)	UDP/TCP 53	Permit
Any (10–50)	60 (DMZ DHCP)	UDP 67/68	Permit
Any	Any	Any	Deny

Default explicit deny policy with least-privilege access control enforced at the source.

Implementation Highlights

Layer 2 (Switching)

Trunks with native VLAN 99, edge ports with PortFast, PVST default with no VLAN 1 traffic on trunks

Layer 3 (Routing)

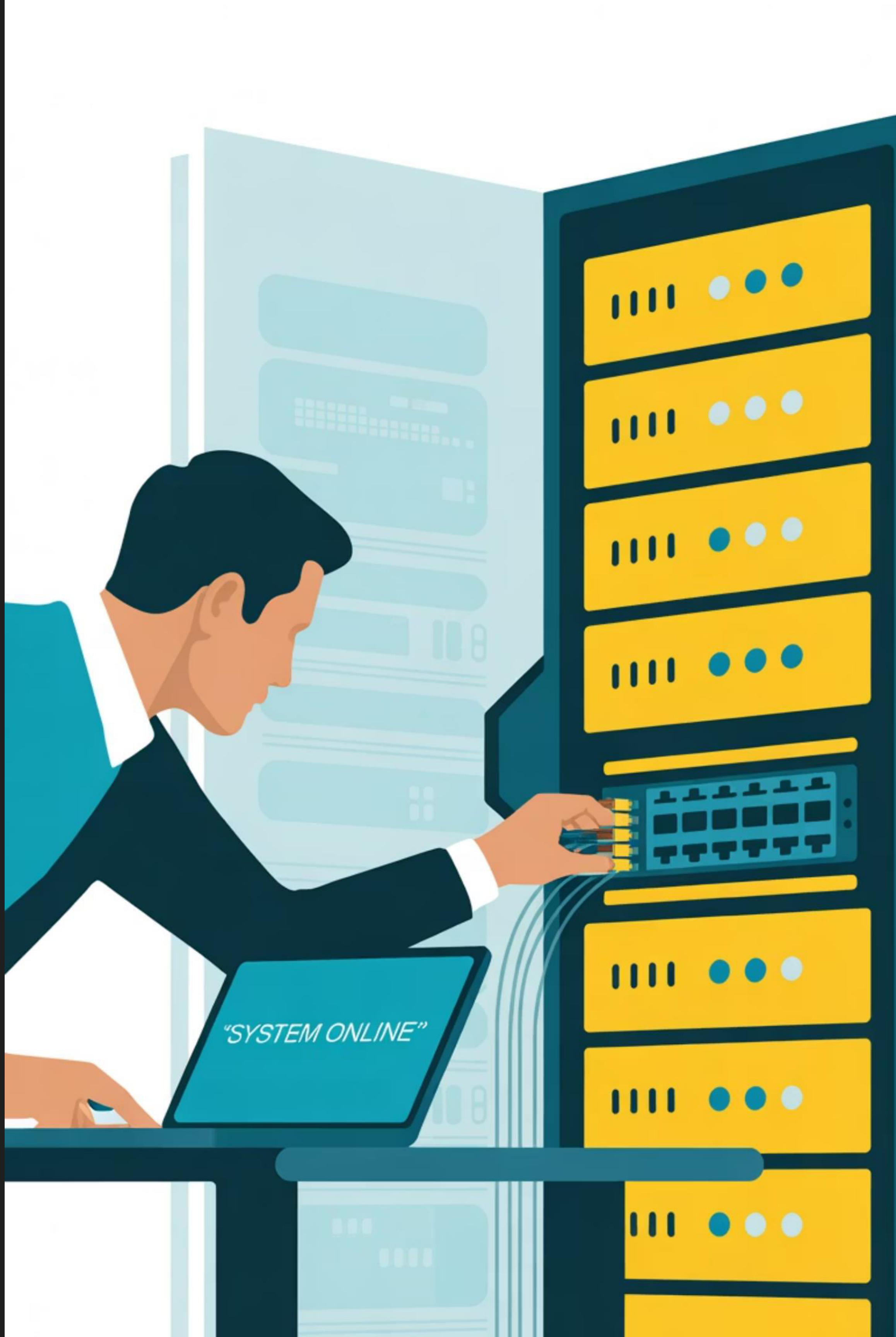
SVIs on core for VLANs 10-80 with gateway IPs per subnet plan

IP Services

DHCP scopes for VLANs 10-50 & 80, DNS zone for park.local with server records

Security Controls

Extended ACLs applied inbound on SVIs closest to source



Testing & Validation

Functional Tests

- DHCP: Clients in all VLANs receive correct IP, GW, DNS
- DNS: Name resolution works from each client VLAN
- Segmentation: Hosts cannot reach other VLANs unless explicitly allowed
- DMZ Access: Only permitted services reachable; others blocked

Negative/Security Tests

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

Performance metrics: Intra-VLAN ping <1 ms; Inter-VLAN <2 ms inside campus.

Project Costs & Future Roadmap

Project Cost Summary

Category	Total Cost
Hardware & Materials	$32,550.00
Software & Licensing	$600.00
Labor & Services	$9,000.00
Contingency (10%)	$4,215.00
GRAND TOTAL	**$46,365.00**

Future Enhancements

- AAA/RADIUS (VLAN 70) for device login and 802.1X
- Mail & File Servers in DMZ with TLS
- Storage (iSCSI) in VLAN 70 with ACL pinholes
- High Availability: Second core + dynamic routing
- Observability: Central syslog/SIEM; NetFlow for analytics

Key Takeaways

Defense in Depth

VLAN isolation, DMZ controls, device hardening, and least-privilege ACLs reduce attack surface

Operational Resilience

Redundant paths, standard STP settings, and fault-tolerant IP addressing scheme

Verifiable Security

Test plan with pass/fail criteria; change, backup, and monitoring procedures

Future-Ready Design

Consistent L2/L3 templates and modular VLAN plan for frictionless growth

ParkShield delivers a comprehensive, secure network architecture that balances security, functionality, and scalability for campus environments.