Home Lab Network Upgrade Documentation

1. Executive Summary

This document outlines the current-state architecture and planned upgrade of my home lab environment. The goal of this upgrade is to transition from a flat LAN design to an enterprise-style segmented network using VLANs, Layer 3 switching, access control lists (ACLs), and enhanced firewall policies. This design aligns with real-world enterprise networking and cybersecurity best practices.

2. Current-State Architecture

The current home lab operates on a single flat network with basic security controls. While functional, this design limits segmentation, scalability, and internal security enforcement.

Current Network Topology:

- ISP Modem → ISP Router
- ISP Router → TP-Link ER605 (Double NAT)
- ER605 → TP-Link Managed Switch
- Switch → Patch Panel → End Devices

Current Devices and Services:

- TP-Link ER605 acting as gateway and firewall
- TP-Link managed switch
- Raspberry Pi 5 running Pi-hole DNS
- Intel N150 mini-PC running TrueNAS with 1TB external SSD
- TP-Link Archer A8 in Access Point mode
- Patch panel with labeled Ethernet runs
- HDMI splitter and portable monitor for Raspberry Pi and TrueNAS
- 6U 10-inch wall-mounted rack housing core equipment (AP mounted externally for signal optimization)

Current Network Characteristics:

- Single LAN subnet: 192.168.50.0/24
- No VLAN segmentation
- Basic port security
- Basic firewall rules on ER605
- Limited internal traffic control

3. Limitations of Current Design

- No internal network segmentation
- All devices share the same broadcast domain
- Limited ability to restrict east–west traffic

- Security controls primarily focused on the network edge
- Reduced realism for enterprise networking and security practice

4. Target-State Architecture (Post-Upgrade)

The upgraded home lab will follow an enterprise-style layered network design. The ER605 will remain the perimeter firewall, while a Cisco Catalyst 3560 will provide inter-VLAN routing and internal traffic enforcement.

Target Network Topology:

- ISP Modem → ISP Router
- ISP Router → TP-Link ER605 (Perimeter Firewall / NAT)
- ER605 → Cisco Catalyst 3560 (Layer 3 Core Switch)
- Cisco 3560 → Patch Panel → End Devices and Servers

5. VLAN and IP Addressing Plan

- VLAN 10 – User / Homelab / Wireless Access
  Subnet: 192.168.10.0/24

- VLAN 50 – DNS / Infrastructure Services
  Subnet: 192.168.50.0/24

- VLAN 80 – Active Directory Practice Environment
  Subnet: 192.168.80.0/24

6. Routing and Switching Design

- Cisco Catalyst 3560 will host SVIs for each VLAN
- Inter-VLAN routing enabled on the 3560
- Access ports assigned per VLAN
- Trunk link between ER605 and Cisco 3560
- Default route on the 3560 pointing to the ER605

7. Security Design and Controls

Inter-VLAN Access Control (Cisco 3560):

- No direct communication between VLANs by default
- Only DNS traffic permitted across VLANs
- DNS responses allowed from VLAN 50 (Pi-hole) to other VLANs
- ACLs applied inbound on SVI interfaces following least-privilege principles
- Port security enforced on access ports

Perimeter Firewall Policy (ER605):

- Stateful firewall enforcement for north–south traffic
- Deny inbound WAN traffic by default

- Block vulnerable or unnecessary outbound ports (e.g., Telnet, SMB, unused services)
- Allow only required outbound traffic
- Maintain double NAT configuration for ISP compatibility

8. Expected Outcomes

- Improved internal security through segmentation
- Reduced attack surface and lateral movement risk
- Realistic enterprise-style networking environment
- Improved troubleshooting visibility and control
- Strong foundation for Active Directory and security testing labs

9. Future Enhancements

- Expand IDS/IPS monitoring
- Centralized logging and alerting
- Configuration backup and automation
- Migration to additional virtualization platforms
- Advanced firewall rule tuning and auditing

10. Conclusion

This upgrade represents a significant step toward an enterprise-aligned home lab environment. By implementing VLANs, ACLs, and layered security controls, the lab will serve as a practical platform for networking, cybersecurity, and systems administration skill development.