Prepared By:

AGHA ESSA KHAN

Date: Thursday, july 20, 2025

SECURE RESEARCH LAB INFRASTRUCTURE

"A VLAN-Based Secure Infrastructure with SSH, ACLs, and Wireless Protection"

Abstract

This project demonstrates the design and implementation of a secure, enterprise-style research laboratory network using Cisco Packet Tracer. The infrastructure is segmented into VLANs for Researchers, Students, Admins, Servers (DMZ), and Wi-Fi zones. Security measures include MAC binding, SSH-only administrative access, WPA2-AES Wi-Fi with MAC filtering, Access Control Lists (ACLs), and DMZ firewall simulation. Additionally, RIP and OSPF routing protocols are configured to coexist, simulating a realistic ISP-backed network.

Objective:

To build a segmented, security-hardened lab that enforces role-based access, restricts unauthorized communication, and ensures secure administration and wireless connectivity in a simulated enterprise environment.

Network Layout & Zones

Block	Description	Devices
A	Researchers (IP + MAC Binding)	5 PCs
B	Students (Rate-Limited VLAN)	5 PCs
C	Admin (SSH-Only Access)	2 PCs
D	Server Room (DMZ)	3 Servers
E	Wi-Fi Zone (WPA2 + MAC Filtering)	2 Laptops
External	Internet (Cloud Simulation)	1 Router + ISP Cloud

Total Devices:

12 PCs, 2 Laptops, 3 Servers, 2 Switches, 1 Wireless Router, 1 Cisco Router, 1 ISP Cloud

VLAN Design

VLAN ID	Department	IP Range
10	Researchers	192.168.10.0/24
20	Students	192.168.20.0/24
30	Admin	192.168.30.0/24
40	Servers (DMZ)	192.168.40.0/24

VLAN ID	Department	IP Range
50	Wi-Fi Zone	192.168.50.0/24

Key Security Features

i. **Segmentation:** Five VLANs isolating Researchers, Students, Admins, Servers, and Wi-Fi.
ii. **ACLs:**Researchers restricted to File Server access only.
iii. Students blocked from HTTP/SSH while ICMP is allowed.
iv. **SSH-Only Admin Access:** Enforced domain, local login, and VTY line encryption.
v. **Wireless Protection:** WPA2-AES, SSID securelabwifi, and MAC filtering.
vi. **DMZ Simulation:** Servers isolated and accessible only through ACL-controlled firewall rules.
vii. **Routing:** Router-on-a-Stick inter-VLAN routing with both RIP and OSPF to test coexistence.
viii. **ISP Simulation:** Static default route towards 200.200.200.1 (Cloud ISP).

Testing & Validation

Security Goal	Status
Students blocked from researcher resources	✅
Admin access via SSH only	✅
Wireless secure with WPA2 + MAC filter	✅
Unauthorized MAC rejected from Wi-Fi	✅
DMZ servers isolated from internal VLANs	✅
ACLs enforcing restrictions properly	✅
Inter-VLAN routing functional	✅

Tested using:

Ping, SSH sessions, Wi-Fi **association**, ACL deny checks, server reachability from external cloud.

Conclusion

The **Secure Research Lab Infrastructure** successfully replicates an enterprise-grade network environment with layered security. By combining VLAN segmentation, ACL-based firewalling, SSH-only admin access, WPA2-AES wireless protection, and simulated ISP connectivity, this project validates strong defensive design principles. The coexistence of RIP and OSPF demonstrates adaptability in protocol configuration. Overall, this design ensures **confidentiality, integrity, and availability** across different network segments while preparing a scalable model for future extensions.