Enterprise Network Design & Security Project

Type: Academic Project
Tool: Cisco Packet Tracer
Field: Cyber Forensics / Network Security
Student: Fakhr Aldin Alkhatib
University: Fırat University
Year: 2026

---

1. Project Overview

This project focuses on designing and securing a small-scale enterprise network using Cisco Packet Tracer. The goal was to apply networking and security fundamentals in a simulated environment, emphasizing secure communication, access control, and attack mitigation techniques relevant to cyber forensics and incident analysis.

---

2. Network Architecture

The network topology includes:

- Multiple end devices segmented into VLANs
- Layer 2 and Layer 3 switches
- Routers enabling inter-VLAN routing
- Centralized network services (DHCP, NAT)

Key design goals:

- Network segmentation
- Controlled access between departments
- Secure routing and traffic flow

---

3. Implemented Technologies

- TCP/IP addressing and subnetting
- VLAN configuration and trunking
- Inter-VLAN routing
- OSPF routing protocol
- NAT / PAT
- Secure remote management using SSH

---

4. Security Controls Applied

The following security mechanisms were implemented and tested:

- Access Control Lists (ACLs) to restrict unauthorized traffic
- Port Security to limit MAC address usage
- DHCP Snooping to prevent rogue DHCP attacks
- Dynamic ARP Inspection (DAI) to mitigate ARP spoofing
- Basic network hardening techniques

---

5. ARP Spoofing Analysis

The project included analysis of the ARP protocol and its vulnerabilities. ARP spoofing risks were studied, and mitigation techniques such as DHCP Snooping and DAI were applied to reduce the attack surface within the simulated network.

---

6. VPN Considerations

VPN concepts were studied and documented. Due to Cisco Packet Tracer limitations, full VPN implementation was not possible; however, real-world VPN deployment principles and expected behavior were analyzed and explained.

---

7. Limitations

- Simulation environment limitations
- No real packet capture from live systems
- VPN implementation constrained by tool capabilities

These limitations were documented to reflect real-world differences between simulations and production environments.

---

8. Conclusion

This project demonstrates foundational skills in enterprise network design and security, as well as an understanding of attack mitigation and forensic relevance within networked environments.
