



**KONYA FOOD AND AGRICULTURE UNIVERSITY  
FACULTY OF ENGINEERING AND ARCHITECTURE  
COMPUTER ENGINEERING DEPARTMENT**

**COMP 3800**

## **SUMMER INTERNSHIP REPORT**

**Mehmet Emre KAYACAN  
212010020011**

Performed at  
**Süleyman Demirel Üniversitesi  
Bilgi İşlem Daire Başkanlığı**

**04.08.2025 - 29.08.2025**

## Table of Contents

1. Abstract .....	3
2. Introduction .....	3
3. Company Information .....	4
4. Work Done .....	5
4.1. Network Infrastructure Projects .....	5
4.2. Virtual Machine and Firewall Configuration .....	6
4.3. Field Service and Technical Support.....	7
4.4. Advanced Python Scripting for Network Automation .....	8
5. Conclusion.....	9
6. References .....	10
7. Questionnaire .....	10
Work focus .....	10
Courses that are useful to your internship .....	10
Target Industry.....	10
Team Profile .....	11
The Joel Test: 12 Steps to Better Code .....	11
8. Appendices .....	12
Appendix A – Python Network Automation Script (Snippet) .....	12
Appendix B – Example VLAN Configuration (HP2626 Switch CLI).....	13
Appendix C – Firewall Rule Example (OpnSense).....	13

# 1. Abstract

During my summer internship at Süleyman Demirel University Information Technology Department, I worked in the Network and System Administration unit from August 4 to August 29, 2025. My main activities included network infrastructure setup, VLAN configuration using HP2626 switches, virtual machine installation with firewall implementations using OpnSense, and providing technical support across the university campus. I gained practical experience in network troubleshooting, cable management, and system administration. This internship enhanced my understanding of enterprise-level network operations and strengthened my interest in pursuing a career in network engineering and cybersecurity.

---

## 2. Introduction

I completed my summer internship at Süleyman Demirel University Information Technology Department, specifically within the Network and System Administration unit. Süleyman Demirel University is a major state university that requires robust IT infrastructure to support thousands of students, faculty, and staff members. I chose this institution for my internship because I wanted to gain experience in a government organization and observe corporate-level IT operations in an educational environment.

During my three-week internship, I primarily focused on network infrastructure management, virtual machine configuration, firewall security implementations, and field service support. The work involved hands-on experience with enterprise networking equipment, security protocols, and troubleshooting real-world network issues across the university campus.

This report is organized into four main sections. Following this introduction, the second section provides detailed information about the organization and my work environment. The third section describes the technical work I performed, including network projects, system configurations, and field service activities. Finally, the conclusion summarizes my learning outcomes and how this experience relates to my academic studies at Konya Food and Agriculture University.

### 3. Company Information

**Organization:** Süleyman Demirel University Information Technology Department

**Address:** Süleyman Demirel University, Isparta, Turkey

**Department:** Network and System Administration Unit

**Supervisor Information:**

Name: Kadir Sümer

Position: Computer Engineering Faculty Member & Staff, Network and System Administration Unit

Education Background:

- Bachelor's Degree: Computer Engineering, Süleyman Demirel University (2019)
- Master's Degree: Computer Engineering (Thesis), Süleyman Demirel University (2019)

**Team Composition:**

The Network and System Administration Unit consists of 10 members, 7 Computer Engineering graduates and 3 Computer Engineering students:

- 1 Faculty Member & Staff (Kadir Sümer)
- 6 Full-time Computer Engineering Personnel
- 1 Part-time Technical Staff
- 2 Summer Interns (including myself)

**Team Members:**

- Sinan Ece (Part-time Technical Staff)
- Furkan Özdemir (Summer Intern)

**Department Focus and Resources:**

The department manages the entire IT infrastructure of Süleyman Demirel University, including network connectivity, server management, security systems, and technical support services. The hardware resources include enterprise-level switches (HP2626 series), routers, firewalls, servers, and various networking equipment. The department utilizes both physical and virtual environments, with extensive use of virtualization technologies for testing and production systems.

**Software and System Environment:**

The department operates with a mixed environment of Linux distributions (Ubuntu, Rocky Linux), Windows systems, and specialized network management tools. The team frequently works with virtualization platforms, network monitoring software, and security management systems to maintain university-wide IT services.

## 4. Work Done

### 4.1. Network Infrastructure Projects

#### **HP2626 Switch Configuration and VLAN Implementation**

One of my primary responsibilities involved configuring HP2626 enterprise switches and implementing VLAN (Virtual Local Area Network) segmentation. I utilized multiple connection methods to access the switches, including console cable connections for initial setup, SSH for remote management, and Telnet for legacy system compatibility. This multi-protocol approach provided comprehensive understanding of network device management techniques.

Using Command Line Interface (CLI) commands, I created three distinct VLANs to serve different organizational functions. The first VLAN was designated for management purposes (Yönetim\_Departmanı), the second for software development activities, and the third maintained default configuration settings for general network access. Each VLAN required specific configuration parameters including VLAN ID assignment, port membership configuration, and inter-VLAN routing policies.

The configuration process involved both trunk and access port setups. Trunk ports were configured to carry traffic for multiple VLANs between switches, while access ports were assigned to specific VLANs for end-user device connectivity. I learned to implement proper VLAN tagging protocols and understand the IEEE 802.1Q standard for VLAN identification across network infrastructure.

#### **Advanced Cable Infrastructure Management**

The most challenging aspect of physical infrastructure work involved CAT7 cable installation and termination across multiple campus locations. A complex project required installing network connectivity to a new office space, which involved running CAT7 cables from the central switch location to individual office rooms. The installation process required terminating both ends of each cable - one end connecting to the switch infrastructure and the other end providing RJ45 connectivity within office spaces.

#### **Network Diagnostics and Troubleshooting Methodology**

Network troubleshooting followed a systematic approach beginning with physical layer verification. Using RJ45 cable testers, I learned to verify cable integrity, pin-out configuration, and signal continuity before proceeding to higher-level diagnostics. When cables tested successfully, troubleshooting progressed to switch port analysis, examining port status, VLAN assignments, and traffic flow patterns.

The final diagnostic step involved log analysis from central management systems, reviewing system events, error messages, and network performance metrics to identify root causes of connectivity issues. This structured approach ensured efficient problem resolution while minimizing network downtime.

## 4.2. Virtual Machine and Firewall Configuration

### **Comprehensive Virtualization Environment**

I designed and implemented a complex virtual machine environment using VirtualBox, creating seven distinct virtual machines with specific resource allocations and networking configurations. The Ubuntu-based infrastructure consisted of four specialized virtual machines: a management server, a web application server, and a database server, plus one additional Ubuntu instance for testing purposes. Each Ubuntu VM received identical resource allocation of 4GB RAM, 25GB hard disk space, and 2 CPU cores to ensure consistent performance across the virtual infrastructure.

The OpnSense firewall virtual machine required different specifications optimized for network security operations: 2GB RAM, 12GB hard disk space, and 1 CPU core. Additionally, two Rocky Linux virtual machines were configured with 4GB RAM, 25GB disk space, and 2 CPU cores each for specialized Linux administration tasks and cross-platform compatibility testing.

### **Advanced OpnSense Firewall Implementation**

Using OpnSense's web-based management interface, I implemented comprehensive security policies governing inter-VM communication and external network access. The firewall configuration established a DMZ (Demilitarized Zone) architecture, providing secure network segmentation between internal systems and external networks.

Specific firewall rules were configured to control traffic flow between the management Ubuntu system, web server Ubuntu instance, and database Ubuntu server. Protocol-specific rules were implemented to allow necessary services while blocking potentially malicious traffic. For example, the database server was configured to accept connections only from the web server on specific database ports (typically 3306 for MySQL or 5432 for PostgreSQL), while denying all other inbound connections.

The internal network design utilized private IP addressing schemes with all virtual machines connected through OpnSense as the central gateway and security enforcement point. NAT (Network Address Translation) rules were configured to enable controlled outbound internet access while maintaining internal network security.

### **Advanced Linux System Administration**

The Rocky Linux virtual machines provided opportunities to work with enterprise-grade Linux distributions commonly used in corporate environments. I gained experience with systemd service management, package management using DNF, and security configuration specific to Red Hat-based distributions. Additionally, IPTables configuration on both Ubuntu and Rocky Linux systems provided hands-on experience with Linux-native firewall management, complementing the OpnSense appliance-based security approach.

## 4.3. Field Service and Technical Support

### **Complex Campus Infrastructure Projects**

Field service responsibilities involved providing technical support across multiple university facilities including the Information Technology Department, Engineering Faculty, Arts and Sciences Faculty, and various administrative buildings. Each location presented unique networking challenges requiring different technical approaches and equipment configurations.

The most complex field service project involved complete network infrastructure installation for a new office space. This project required comprehensive planning, including network topology design, cable routing through building infrastructure, switch port allocation, and VLAN assignment coordination. The installation process involved both physical cable installation and logical network configuration to ensure proper connectivity and security compliance.

### **Systematic Network Troubleshooting in Production Environments**

Field troubleshooting followed established protocols beginning with physical layer verification using specialized testing equipment. RJ45 cable testers were used to verify wire continuity, proper pin assignments, and cable integrity before investigating higher-level network issues. When physical connectivity was confirmed, troubleshooting progressed to switch-level diagnostics including port status verification, VLAN configuration validation, and traffic flow analysis.

Advanced troubleshooting involved accessing central network management systems to review system logs, error messages, and performance metrics. This comprehensive approach enabled identification of issues ranging from simple cable problems to complex network configuration conflicts, ensuring efficient problem resolution across diverse campus networking environments.

## 4.4. Advanced Python Scripting for Network Automation

### **Comprehensive Network Monitoring Solution**

I developed a sophisticated Python script comprising approximately 200 lines of code, completed within a 30-minute development timeframe. The script utilized multiple Python libraries including socket for network connectivity testing, subprocess for system command execution, and psutil for system resource monitoring, providing comprehensive network analysis capabilities.

The script's primary functions included automated ping testing to verify network connectivity between virtual machines, bandwidth monitoring to assess network performance, and interface status checking to ensure proper network adapter configuration. The ping testing component implemented systematic connectivity verification across all virtual machines, generating detailed reports of network reachability and response times.

Interface status monitoring provided real-time information about network adapter states, including IP address assignments, subnet configurations, and connection status for each virtual machine. The bandwidth monitoring functionality measured network throughput between systems, identifying potential performance bottlenecks and providing data for network optimization decisions.

This automation script demonstrated the integration of programming skills with network administration tasks, showcasing how software development expertise can enhance system administration efficiency and provide valuable network management capabilities in enterprise environments.



## 5. Conclusion

My summer internship at Süleyman Demirel University Information Technology Department provided valuable practical experience in network administration and system management. The work I completed included network infrastructure configuration, virtual machine setup, firewall security implementation, field service support, and automation script development.

### **Key Learning Outcomes:**

- Practical experience with enterprise networking equipment including HP2626 switches
- Understanding of VLAN configuration and network segmentation principles
- Hands-on experience with Linux system administration and virtualization technologies
- Knowledge of firewall configuration using OpnSense and IPTables
- Field service skills and real-world troubleshooting experience
- Integration of programming skills with network management tasks

**Skills Acquired:** The internship significantly enhanced my technical skills in network administration, which complements the theoretical knowledge gained from my Computer Networks course at Konya Food and Agriculture University. The practical experience with tools like VirtualBox, Wireshark, Cisco Packet Tracer, and various Linux distributions provided concrete understanding of concepts previously learned in academic settings.

**Career Impact:** This internship experience has significantly influenced my career direction. The hands-on work with network infrastructure and security systems has increased my interest in network engineering and cybersecurity fields. Compared to my previous focus on software development, I found network administration more engaging and aligned with my professional interests. This experience will guide my future academic choices and career planning toward network engineering and cybersecurity specialization.

The combination of theoretical knowledge from university courses and practical experience from this internship has provided a solid foundation for my future career in computer engineering, with a specific focus on network and security systems.

## 6. References

1. Süleyman Demirel Univ., *IT Dept. Internal Docs & Training Materials*
  2. Kurose, J. F., & Ross, K. W., *Computer Networking: A Top-Down Approach*, 8th Ed., Pearson, 2020
  3. HP, *ProCurve 2626 Switch Configuration Guide*
  4. OpnSense, *Firewall Configuration & Management Docs*
  5. Konya Food & Agriculture Univ., *Computer Networks Course Materials*
- 

## 7. Questionnaire

### Operating Systems Used

☒ Windows ☒ Linux ☐ Mac OS ☐ Other:

### Programming Languages Used

☒ Python ☐ C ☐ C++ ☐ Java ☐ C# ☐ Matlab ☐ R ☐ JavaScript ☐ Ruby ☐ PHP ☐ SQL ☐ Swift ☐ Kotlin ☐ Other:

### Work focus

☐ Web application development ☐ Game development  
☐ Desktop application development ☐ Data science  
☐ Mobile application development ☐ Software testing  
☐ Embedded development ☒ Security and Network  
☐ Database oriented development ☐ Other:

### Courses that are useful to your internship

☒ Introduction to Programming (with Python) ☐ Programming Languages  
☐ C Programming ☐ Software Engineering  
☐ Data Structures (with C++) ☐ Computer Organization  
☐ Object Oriented Programming (with Java) ☐ Design and Analysis of Algorithms  
☐ Database Management Systems ☒ Computer Networks  
☐ Other 1: ☐ Other 2:

### Target Industry

☒ Government ☐ Defense ☐ Medical ☐ Entertainment ☐ Telecom  
☐ E-commerce ☒ Education ☐ Finance ☐ Agriculture ☐ Other:

## Team Profile

- Number of engineers: 6
- Number of scientists (i.e. Mathematician): 0
- Number of other workers: 1
- High school graduate count: 1
- University graduate count: 6
- MS graduate count: 2
- PhD graduate count: 1

## The Joel Test: 12 Steps to Better Code

- Do you use source control? Yes
- Can you make a build in one step? Yes
- Do you make daily builds? Partially - for critical systems
- Do you have a bug database? Yes - ticket system for IT support
- Do you fix bugs before writing new code? Yes
- Do you have an up-to-date schedule? Yes
- Do you have a spec? Yes - for network configurations
- Do programmers have quiet working conditions? Yes
- Do you use the best tools money can buy? Partially - budget constraints
- Do you have testers? Yes - extensive testing before deployment
- Do new candidates write code during their interview? Not applicable - mainly system admin roles
- Do you do hallway usability testing? Yes - informal testing with end users

## 8. Appendices

### Appendix A – Python Network Automation Script (Snippet)

```
import socket, subprocess, psutil

# Ping Test Function
def ping(host):
    result = subprocess.run(["ping", "-c", "4", host],
                             stdout=subprocess.PIPE)
    return result.stdout.decode()

# Network Interface Status
def get_interfaces():
    interfaces = psutil.net_if_addrs()
    for iface, addrs in interfaces.items():
        print(f"Interface: {iface}")
        for addr in addrs:
            print(f"    {addr.address}")

# Example usage
print(ping("8.8.8.8"))
get_interfaces()
```

This Python script was developed during the internship to automate network connectivity checks, bandwidth monitoring, and interface status reporting across the virtual machine environment.

## Appendix B – Example VLAN Configuration (HP2626 Switch CLI)

```
configure terminal
vlan 10
    name "Management_Department"
    untagged 1-10
    exit
vlan 20
    name "Software_Development"
    untagged 11-20
    exit
vlan 30
    name "General_Access"
    untagged 21-24
    exit
write memory
```

This configuration demonstrates VLAN segmentation using HP ProCurve 2626 switches, including VLAN ID assignment, port membership, and persistence across reboots.

---

## Appendix C – Firewall Rule Example (OpnSense)

```
Action: Allow
Source: 192.168.10.0/24
Destination: 192.168.20.5
Port: 3306 (MySQL)
Protocol: TCP
Description: Allow web server to access database server
```

This firewall rule restricts database access to only the web server, enhancing security by denying all other inbound connections.