DIU Campus Area Network System

Submitted By

Student Name	Student ID
Md. Sabbir Hosen Hamim	0242310005101803
Md. Robiul Karim	0242310005101534
Mehedi Islam Miazi Sami	0242310005101582
Abir Karmoker	0242310005101004
Kh. Atia Rahman	0242310005101623

MINI LAB PROJECT REPORT

This Report Presented in Partial Fulfillment of the course **CSE322: Computer Networks Lab in the Computer Science and Engineering Department**

GitHub: https://github.com/sabbirhamim/DIU-Campus-Area-Network

DAFFODIL INTERNATIONAL UNIVERSITY

Dhaka, Bangladesh

April 13, 2025

DECLARATION

We hereby declare that this lab project has been done by us under the supervision of **Amir Sohel, Sr. Lecturer**, Department of Computer Science and Engineering, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere as lab projects.

Submitted To:

Amir Sohel
Sr. Lecturer
Department of Computer Science and Engineering
Daffodil International University

Submitted by

<table>
<tr><td colspan="2">Md Sabbir Hosen Hamim
0242310005101803
Dept. of CSE, DIU</td></tr>
<tr><td>Md Robiul Karim
0242310005101534
Dept. of CSE, DIU</td><td>Mehedi Islam Miazi Sami
0242310005101582
Dept. of CSE, DIU</td></tr>
<tr><td>Abir Karmoker
0242310005101004
Dept. of CSE, DIU</td><td>Kh. Atia Rahman
0242310005101623
Dept. of CSE, DIU</td></tr>
</table>

COURSE & PROGRAM OUTCOME

The following course have course outcomes as following:

Table 1: Course Outcome Statements

CO's	Statements
CO1	**Understanding Network Fundamentals** Demonstrate a comprehensive understanding of networking principles, including the architecture, components, and functions of campus area networks (CAN).
CO2	**Network Design and Implementation** Apply theoretical knowledge to design, configure, and implement a secure and efficient campus area network that meets institutional requirements.
CO3	**Protocols and Communication** Analyze and apply appropriate communication protocols and routing strategies to optimize network performance in a campus environment.
CO4	**Security Management** Identify and address potential security vulnerabilities within a campus area network by implementing effective security measures and policies.

Table 2: Mapping of CO, PO, Blooms, KP and CEP

CO	PO	Blooms	KP	CEP
CO1	PO1	C2,A2, P2	K2, K3,K4,K8	EP1, EP4
CO2	PO3	C3, A3, P3	K2,K3,K4, K6, K8	EP1, EP2,EP7
CO3	PO5	C3	K6	EP4

The mapping justification of this table is provided in section **4.3.1**, **4.3.2** and **4.3.3**.

Table of Contents

Chapter 1

Introduction

1.1 Introduction

The Campus Area Network System is a solution that facilitates seamless and secure communication between different buildings and departments within a campus environment. It is larger than a Local Area Network (LAN) but smaller than a Wide Area Network (WAN), typically covering an area that spans several kilometers, such as a university, research institution, or business park.

The system is designed to provide various services, such as internet connectivity, data sharing, communication systems (email, VoIP, etc.), and access to central resources (like file servers, databases, and applications). The Campus Area Network uses a combination of networking hardware like switches, routers, and fiber optic cables to create a high-performance and scalable network environment.

Key Features: High-Speed Connectivity: Ensures fast and reliable communication between Devices and users within the campus. Centralized Management: Provides network administrators with the ability to monitor, configure, and troubleshoot the network from a central location.

Security: Implements security measures like firewalls, intrusion detection systems, and authentication protocols to protect against unauthorized access.

Scalability: Can easily accommodate additional devices and users as the campus grows.

Wireless Access: Supports Wi-Fi networks for mobile devices, enabling users to stay connected throughout the campus.

1.2 Motivation

Enhanced Communication and Collaboration: Universities and campuses have a diverse group of people students, faculty, staff who need seamless access to resources, emails, online learning platforms, and other communication tools. A Campus Area Network (CAN) ensures smooth connectivity among these groups, fostering improved collaboration.

Centralized Network Management: A CAN allows the institution's IT team to centrally manage resources, troubleshoot issues, and monitor network performance, ensuring that connectivity is always optimal and secure.

Cost Efficiency: By implementing a CAN, a campus can optimize its infrastructure and reduce costs associated with external internet access and data management. Shared resources across the campus network improve the overall cost-effectiveness.

Scalability: The network should be adaptable to future needs. As campuses grow in terms of students, devices, and technology, a CAN can be designed to scale up without major overhauls.

Security and Data Protection: A dedicated CAN helps in enforcing security protocols tailored to educational environments. This ensures protection against cyber threats, data breaches, and unauthorized access.

Support for Emerging Technologies: With the increasing use of IoT, smart devices, and cloud-based applications, a well-designed CAN supports the integration of emerging technologies, enhancing the learning and operational capabilities of the campus.

Student and Faculty Experience: Providing fast, reliable internet and access to online educational tools improves the learning experience, while also enabling teachers and staff to perform their administrative and academic roles more efficiently.

1.3 Objectives

- The Design and Implementation: To design and implement a robust campus network that connects various buildings, departments, and resources within a defined campus area, ensuring fast, secure, and reliable communication.

- Scalability and Flexibility: Ensure the network is scalable to accommodate future growth, including adding new buildings, departments, or services without significant restructuring.

- High-Speed Connectivity: Provide high-speed internet access for students, faculty, and staff for academic and administrative purposes, supporting a wide range of applications and services.

- Network Security: Develop and implement security protocols to protect the network from unauthorized access, data breaches, and cyber threats, ensuring data confidentiality, integrity, and availability.

- Resource Sharing: Facilitate the sharing of resources like printers, file servers, and databases across the campus, improving collaboration and reducing operational costs.

- Wi-Fi Coverage: Provide comprehensive wireless coverage across the campus, enabling mobile access to the network from anywhere within the designated areas.

- Management and Monitoring: Establish a network monitoring and management system for real-time tracking of network performance, troubleshooting, and ensuring minimal downtime.

- Cost Efficiency: Implement cost-effective solutions in terms of hardware, software, and infrastructure to provide high-quality services while maintaining budget constraints.

- User Support and Maintenance: Develop a plan for ongoing user support, network maintenance, and upgrades to ensure the system continues to meet the needs of the campus community.

- Compliance with Standards: Ensure that the campus network follows industry standards and complies with regulations regarding privacy, data protection, and accessibility.

1.4 Feasibility Study

Technical Feasibility: This section assesses whether the technology required for the campus network system is available and feasible to implement. It covers:

Network infrastructure: wiring, routers, switches, firewalls, and access points. Network design and architecture (e.g., topology, bandwidth requirements).

Compatibility with existing systems or software on the campus. Security requirements (e.g., data encryption, access control).

Economic Feasibility: This involves estimating the financial costs and comparing them with the potential benefits. It includes:

Initial setup costs (hardware, software, and installation). Operational costs (maintenance, power consumption, support).

Cost-benefit analysis: evaluating if the system will provide sufficient value for the investment.

Operational Feasibility: This section looks at whether the system will function as needed in real-world conditions. It includes:

The usability of the network for students, faculty, and administrative staff. How easy it will be to maintain the system (e.g., troubleshooting, updates). The scalability of the network as the campus grows.

Legal and Regulatory Feasibility: This evaluates any legal issues or compliance requirements related to privacy, security, and data protection, such as:

Data protection regulations (e.g., GDPR, FERPA). Local laws regarding IT infrastructure and networking. Licensing of software and hardware.

Schedule Feasibility: This assesses the timeline for implementing the system, including:

Project milestones (design, installation, testing, and deployment). Any dependencies (e.g., external vendors or infrastructure work).

1.5 Gap Analysis

Gap Define Current Network Infrastructure:

Map out the current network components: routers, switches, wireless access points, servers, etc.
Evaluate the existing network capacity (bandwidth, coverage, etc.). Assess current technologies (e.g., Ethernet, Wi-Fi standards, fiber optics). Identify current security features (firewalls, encryption, etc.).

Determine Desired Network State:
Define the goals and objectives for the campus network (e.g., higher bandwidth, wider coverage, better security, IoT support). Set performance targets (e.g., 10Gbps throughput, 99.9% uptime). Plan for future scalability (e.g., more users, additional buildings). Ensure the network aligns with academic, research, and administrative needs.

Identify Gaps:

- **Technology Gaps:** Are there outdated or insufficient technologies in the current system? (e.g., older Wi-Fi standards, insufficient fiber optic links).
- **Capacity Gaps:** Is the current network capacity insufficient for expected traffic or future needs? (e.g., lack of bandwidth, network congestion).
- **Security Gaps:** Are there vulnerabilities in the current network security infrastructure? (e.g., outdated firewalls, lack of encryption).
- **Management Gaps:** Is the network management system inadequate? (e.g., manual configuration vs. automated management tools).
- **Coverage Gaps:** Are there areas on campus with poor or no coverage? (e.g., remote buildings, parking lots).

1.6 Project Outcome

Improved Connectivity: A robust and high-speed network connecting various buildings, departments, and devices across the campus.

- **Enhanced Communication**: Facilitating communication among students, staff, and faculty through various tools and platforms.
- **Network Security:** Implementing strong security measures to protect data and ensure privacy across the network.
- **Cost-Effective Infrastructure**: A cost-efficient network system that meets the campus's needs without excessive maintenance or resource consumption.
- **Scalability:** A network designed to be scalable for future expansion and increased demand.
- **Optimized Network Performance:** Achieving minimal downtime, fast data transfer, and reliable service for users across the campus.
- **Comprehensive Feasibility Analysis:** A detailed gap analysis, risk assessment, and recommendation for the network’s improvement and sustainability.

Chapter 2

Proposed Methodology/Architecture

2.1 Requirement Analysis & Design Specification

This section identifies and defines the functional and non-functional requirements of the Campus Area Network (CAN) system. It's crucial to gather stakeholder input (such as from students, faculty, and network administrators) to ensure that the network meets everyone's needs.

Functional Requirements:

These are the specific features the system must provide to users.

- **Connectivity**: Reliable internet and intranet connectivity across all campus buildings and outdoor areas.
- **Security**: Secure access to the network, including user authentication and authorization, firewalls, encryption for data transmission, etc.
- **Performance**: High-speed internet, minimal downtime, low-latency connections.
- **Scalability**: The ability to add new devices, buildings, and users as the campus grows.
- **Monitoring and Management**: Tools for network administrators to monitor bandwidth usage, detect faults, and ensure network health.
- **Access Control**: Role-based access to network resources (students, faculty, and staff).
- **Bandwidth Management**: Quality of Service (QoS) to prioritize traffic for different services (e.g., video conferencing, academic research) based on priority.
- **Non-Functional Requirements:** These address the quality and constraints of the network.
- **Reliability**: High availability, ensuring that the network is operational 24/7 with minimal downtime.
- **Redundancy**: Backup links and equipment to ensure continuous network operation in case of failure.
- **Security**: Protection from unauthorized access, malware, and data breaches.

2.1.1 Overview

The A Campus Area Network (CAN) is a network of interconnected systems within a defined geographical area, such as a university, college, or corporate campus. It provides reliable communication services between buildings, departments, and individuals within the campus. The main goal of a CAN is to ensure high-speed data transfer, secure connectivity, and seamless communication among all users and devices.

This project aims to design, implement, and evaluate a robust and efficient **Campus Area Network**

System that can meet the specific needs of a university or similar institution. The system will be designed to handle the increasing demand for internet access, data sharing, communication, and digital resources. Additionally, it will ensure scalability, security, and reliability to accommodate future technological advancements and growing user requirements.
Key features of the proposed system include:

- **High-speed internet access** for students, faculty, and staff.
- **Wi-Fi coverage** across the campus, enabling connectivity from various locations.
- **Centralized management system** for monitoring network performance and security.
- **Redundancy and fault tolerance** to minimize downtime.
- **Security protocols** to protect data and prevent unauthorized access.

Through this project, the goal is to deliver a **future-proof network solution** that enhances the overall educational and administrative experience while supporting modern technologies like cloud computing, IoT (Internet of Things), and multimedia streaming.

2.1.2 Proposed Methodology/ System Design

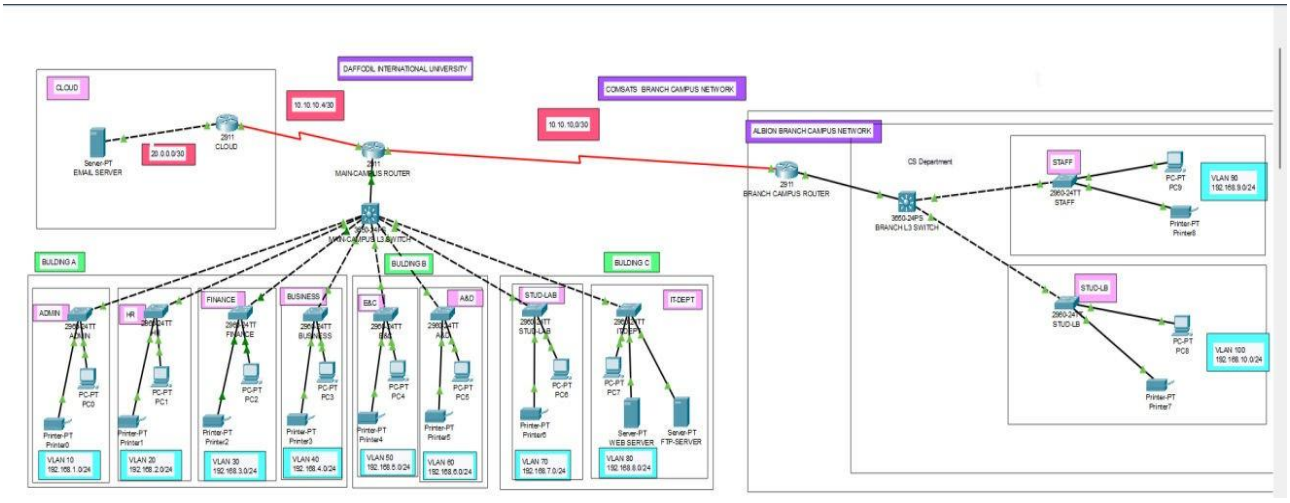
The Campus Area Network (CAN), the design typically involves several components such as:

- **Core Network**: High-speed backbone connecting all buildings, routers, and switches.
- **Access Layer**: Devices like switches and wireless access points that provide network access to users.
- **Edge Devices**: Computers, laptops, and smartphones that connect to the network.
- **Servers**: Hosting services like file storage, DNS, email, and web services.
- **Security Devices**: Firewalls, intrusion detection systems (IDS), and monitoring tools.

The diagram could include the following elements:

1. A central router or core switch acting as the backbone.
2. Multiple building-level switches or wireless access points connecting end-user devices.
3. Servers in a data center or server room connected to the core switch.
4. Firewall for external internet access and security.

2.1.3 UI Design



2.2 Overall Project Plan

The Project Phases:

Phase 1: Feasibility Study & Requirement Analysis (1-2 weeks)
- Conduct gap analysis and requirements gathering.
- Define system objectives and scope.

Phase 2: System Design & Architecture (2-3 weeks)
- Develop the system design, network layout, and UI design.
- Identify hardware/software requirements.

Phase 3: Development (4-6 weeks)
- Backend development: Database setup, network configurations, server- side logic.
- Frontend development: UI creation and integration with backend.

Phase 4: Testing & Deployment (2 weeks)
- Conduct system testing (unit tests, integration tests, and performance testing).
- User acceptance testing.
- Deployment on the campus network.

Phase 5: Maintenance & Documentation (Ongoing)
- Provide system support and regular updates.
- Documentation of the system architecture, UI, and network configurations.

Resources:
- **Team Members**: Developers, UI/UX designers, network specialists, and testers.
- **Tools & Software**: Development IDEs, network simulation tools, version control systems (e.g., Git), testing frameworks.

Timeline:
- Set milestones for each phase.
- Allocate time for meetings, reviews, and adjustments.

Risk Management:
- Identify potential risks such as delays, technical challenges, or resource shortages.
- Define mitigation strategies for each risk.

Budget:
- Estimate costs for hardware (network devices, servers) and software (licenses, tools).
- Account for staffing, testing, and deployment expenses

Chapter 3

Implementation and Results

3.1 Implementation

The Network Design: Explain the architecture, topology (e.g., star, ring, bus), and components used (e.g., routers, switches, cables, servers).

Hardware and Software: Specify the hardware (servers, routers, switches,
Workstations) and software (network management tools, configuration scripts, operating systems) used.

Configuration: Outline the step-by-step process of configuring the network, such as IP addressing schemes, subnetting, routing protocols (e.g., OSPF, RIP), and security measures (firewalls, encryption).

Integration: Discuss how different parts of the network are integrated (e.g., linking buildings, connecting workstations to the server).

Challenges and Solutions: Address any challenges faced during implementation (e.g., hardware limitations, connectivity issues) and how they were resolved**.**

3.2 Performance Analysis

Tests Bandwidth and Latency: Measure the network's speed, latency, and throughput. Discuss factors affecting these, such as distance between devices, router performance, and network traffic.

- **Network Load**: Analyze the network's performance under varying loads. Simulate different numbers of users or devices to test its scalability.
- **Packet Loss and Jitter**: Measure packet loss and jitter to assess the network's reliability and quality of service.
- **Security Performance:** Test the security measures (e.g., firewall rules, encryption) and their impact on performance.

3.3 Results and Discussion

The Comparison with Expectations: Compare actual results with expected outcomes, highlighting any discrepancies.

- **Network Performance**: Discuss how well the network performed under different conditions. Did it meet the desired performance goals?

- **Optimization and Improvements**: Suggest areas for optimization, such as upgrading hardware, fine-tuning configurations, or adding redundancy for better reliability.

- **Lessons Learned**: Share insights gained from the project and how the experience could inform future network designs or improvements.

.

Chapter 4

Engineering Standards and Mapping

4.1 Impact on Society, Environment and Sustainability

4.1.1 Impact on Life

The implementation of a Campus Area Network (CAN) system can significantly enhance the daily life of students, faculty, and staff by providing seamless internet connectivity across campus. It can improve communication, access to educational resources, and overall digital infrastructure. By facilitating online learning, virtual collaboration, and efficient administrative services, the CAN system can foster a more engaged and informed community. Additionally, it can support research initiatives, making it easier to access online libraries, databases, and software applications essential for academic success.

4.1.2 Impact on Society & Environment

The CAN system's impact on society is multifaceted. On one hand, it can bridge the digital divide by providing reliable internet access to underserved areas of campus, especially in regions where access to technology is limited. On the environmental front, a well-designed CAN system can contribute to the reduction of paper waste, as more services and communications move online. Moreover, integrating energy- efficient infrastructure, such as low-power switches and devices, can help minimize the environmental footprint. However, there could also be negative effects such as increased energy consumption from the network equipment and the potential for electronic waste as technology upgrades are made.

4.1.3 Ethical Aspects

Ethically, the deployment of a CAN system must consider issues related to data privacy and security. It's essential to ensure that personal data of students, faculty, and staff is protected and that the network is not used for surveillance without consent. The ethical use of technology should also address concerns about the digital divide ensuring equitable access to resources and preventing any group from being disadvantaged due to the lack of access to technology. Additionally, the development and maintenance of the system should prioritize transparency in decision-making processes and ensure that all stakeholders are informed and involved in discussions about how the network is used.

4.1.4 Sustainability Plan

A sustainability plan for the CAN system should address both environmental and operational longevity. Environmentally, the network should employ energy-efficient technologies, such as low-power network equipment, renewable energy sources (like solar panels), and recycling programs for electronic waste. From an operational perspective, sustainability includes ensuring that the network infrastructure is scalable and adaptable to future technological advancements. Regular maintenance, updates to software and hardware, and user training will help keep the system running smoothly. Furthermore, the system should aim to reduce overall operational costs through energy saving.

.

4.2 Project Management and Team Work

The project was developed through collaborative teamwork, with clear roles assigned for front-end development, back-end coding, testing. Regular standup meetings ensured smooth communication and progress.

4.3 Complex Engineering Problem

4.3.1 Mapping of Program Outcome

The project outcome aligns with the program's objectives by integrating modern web technologies to create a robust and scalable system. The solution meets user expectations for both the customer-facing application and restaurant management.

Table 4.1: Justification of Program Outcomes

PO's	**Justification**
PO1	Networking principles concepts, and functions of campus area networks.
PO2	Network Design and Implementation
PO3	Protocols and Communication

4.3.2 Complex Problem Solving

In this section, we will map engineering activities with respect to the DIU Campus Area Network System project. These activities include aspects such as resource management, level of interaction, innovation, societal impact, and familiarity with the technologies used.

Knowledge profile and rational thereof-

Table 4.2: Mapping with complex problem solving.

EP1 Dept of Knowledge	**EP2** Range of Conflicting Requirements	**EP3** Depth of Analysis	**EP4** Familiarity of Issues	**EP5** Extent of Applicable Codes	**EP6** Extent Of Stakeholder Involvement	**EP7** Inter-dependence
Core technologies include networking principles, including the architecture, components, and functions of campus area networks (CAN).	Apply theoretical knowledge to design, configure, and implement a secure and efficient campus area network	Apply appropriate communication protocols and routing strategies to optimize network performance in a campus environment	Familiar challenges such as address potential security vulnerabilities within a campus area network	The project adhered to Protocols and Communication	Involvement of users, efficient campus area network that meets institutional requirements	Smooth interaction implementing effective security measures and policies.

4.3.3 Engineering Activities

In this section, provide a mapping with engineering activities. For each mapping add subsections to put rationale (Use Table 4.3).

Table 4.3: Mapping with complex engineering activities.

EA1 Range of resources	**EA2** Level of Interaction	**EA3** Innovation	**EA4** Consequences for society and environment
Understanding Network Fundamentals .	Users Network Design and Implementation	Real-time Protocols and Communication	Security Management

Chapter 5

Conclusion

5.1 Summary

The In this section, we provide an overview of the Campus Area Network (CAN) system, its purpose, and key findings from our study. Summarize the primary objectives, design, and the results of our feasibility study, highlight:

- **Objective:** The goal of implementing a Campus Area Network to support efficient communication, data sharing, and internet access within a campus environment.

- **Key Findings:** Insights into the technical, financial, and operational feasibility of the network system.

- **System Design:** Overview of the chosen architecture, such as network topology (e.g., star, bus, or hybrid), protocols, and hardware/software components.

- **Impact:** The benefits such as improved connectivity, scalability, and support for educational and administrative functions.

.

5.2 Limitation

The limitations or challenges we encountered during the design and implementation phases of the project. Some examples could include:

a. **Budget Constraints:** Limited financial resources could affect the quality or extent of network infrastructure.

b. **Scalability:** Potential limitations in scaling the system as the campus grows in terms of users or devices.

c. **Technical Challenges:** Difficulties with integration of different hardware, software, or protocols across the network.

d. **Security Concerns:** Ensuring data privacy, secure communication, and protection against cyber threats.

e. **Environmental Constraints:** Physical limitations of the campus space (e.g., building layout or environmental factors like weather for outdoor equipment).

5.3 Future Work

Looking ahead, we should focus on potential improvements, upgrades, or extensions to the **Campus Area Network** in the future. These could include:

a. **Network Expansion:** Exploring the addition of more access points, upgrading cables, or introducing new technologies (e.g., Wi-Fi 6, 5G integration).

b. **Improved Security Measures:** Implementing advanced encryption methods, firewalls, and intrusion detection systems.

c. **IoT Integration:** Future integration of Internet of Things (IoT) devices for smart classrooms, buildings, and campus management.

d. **Cloud Integration:** Potential use of cloud-based services for data storage, backup, and disaster recovery.

e. **Sustainability:** Focusing on energy-efficient network components and renewable energy sources for powering network infrastructure.

References

[1] Kurose, J. F., & Ross, K. W. *Computer networking: A top-down approach*. Pearson Education, 2017. [Online]. Available: https://www.pearson.com/store/p/computer-networking/P100000753400

[2] Stallings, W. *Data and computer communications*. Pearson Education, 2017. [Online]. Available: https://www.pearson.com/store/p/data-and-computer-communications/P100000751678

[3] Cisco. *Campus Area Network (CAN)*. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collaboration/endpoints/campus-area-network-can.html

[4] IEEE 802 Standards. *Explore relevant IEEE 802 standards related to local and metropolitan area networks*. [Online]. Available: https://standards.ieee.org/

[5] Symantec. *Campus Network Security Guide*. [Online]. Available: https://www.broadcom.com/products/cyber-security

[6] NIST. *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology, n.d. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final