Synopsis Report: Manufacturing Plant Network

Project Title: Design and Implementation of a Secure and Scalable Network Infrastructure for a Manufacturing Plant.

Group Number: 03

Project Team:

- Amal Antony Alex – FET-BCD-2023-27-020
- Swosti Sanhita Jena - FET-BCD-2023-27-022
- Chidananda Sashank Bhuyan - FET-BCD-2023-27-025
- Chiranjibi Dash - FET-BCD-2023-27-026

Mentors:

- **Internal Mentor:** Dr. Chinmaya Kumar Nayak
- **External Mentor:** Ms. Neha Bagle
- **Faculty:** Faculty of Engineering & Technology, Sri Sri University, Cuttack

---

1. Abstract

This project focuses on designing a hierarchical, scalable, and secure network for a manufacturing plant. The proposed network follows a **three-layer model** (Core, Distribution, Access) to ensure high availability and performance. The **segmentation** of the plant into Production, Engineering, Corporate, Storage, DMZ, and Guest zones is achieved using VLANs. Critical **security measures** such as firewalls, intrusion prevention, and access control lists (ACLs) protect against cyber threats targeting industrial control systems (OT). The objective is to create a resilient network that facilitates seamless data flow and real-time communication.

---

2. Introduction

- **Domain:** Scalable network design for manufacturing plants.

- **Problem Statement:** Securely integrating diverse units (Assembly, QC, Logistics, Admin) with real-time monitoring.
- **Importance:** Ensures operational efficiency, cybersecurity, and future scalability.
- **Approach:**
    - **Hierarchical Network Design:** Core, Distribution, and Access layers.
    - **Security Measures:** VLAN segmentation, firewalls, and OT security.

---

3. Literature Review

- Studies on hierarchical network design in industrial environments.
- Use of VLANs for segmentation in secure industrial networks.
- Importance of cybersecurity in OT and IoT-based networks.

---

4. Objectives

- Develop a **comprehensive network** for the manufacturing plant.
- Implement **VLANs** for secure communication.
- Enable **real-time monitoring** to detect and resolve issues.
- Ensure **high availability** with redundancy mechanisms.
- **Protect OT systems** from industrial cyber threats.

---

5. Motivation

- **Interconnected systems** are essential for manufacturing efficiency.
- **Increasing cyber threats** necessitate strong security measures.
- **Scalability** is key for accommodating future growth.
- Provides hands-on experience in **network design and security**.

---

6. Problem Statement

Develop a **scalable and secure** network for a manufacturing plant integrating:

- Assembly, Quality Control, Logistics, and Administration.
- VLAN segmentation for IoT devices, SCADA systems, and enterprise networks.
- **Real-time monitoring** and **protection against cyber threats** in OT systems.

---

7. Work Plan & Timeline

Phase	Tasks	Duration
Phase 1	Research & Literature Review	2-3 Weeks
Phase 2	Network Design & Planning	2-3 Weeks
Phase 3	VLAN, IP Configuration, Routing & Security	4-5 Weeks
Phase 4	Testing & Documentation	2-3 Weeks
Phase 5	Final Submission	March 31, 2025

---

8. Conclusion

This project presents a **real-world** network design solution that enhances **security, scalability, and efficiency** in a manufacturing plant. VLAN segmentation, routing protocols, and security measures improve performance while **real-time monitoring minimizes downtime**. The design is **future-ready**, supporting technological advancements.

---

9. Future Scope

- **AI-driven network analytics** for failure prediction and bandwidth optimization.

- **5G-enabled IoT** devices for ultra-low latency communication.
- **IPv6 adoption** for long-term scalability.
- **Blockchain authentication** for secure vendor interactions.
- **Biometric-based network access control (NAC)** for enhanced security.
- **Cloud-native SD-WAN** for dynamic traffic management.
- **Digital twin technology** for network simulation and optimization.

---

10. References

1. Mwansa, G., Ngandu, M. R., & Dasi, Z. S. (2024). Enhancing Practical Skills in Computer Networking: Evaluating the Unique Impact of Simulation Tools, Particularly Cisco Packet Tracer, in Resource-Constrained Higher Education Settings. Education Sciences, 14(10), 1099.
2. Das, B. J., Chidambaram, V., & Palanidoss, S. (2023, November). Packet tracer for smart home networks and real-world monitoring. In AIP Conference Proceedings (Vol. 2946, No. 1). AIP Publishing.
3. Malanchini, I., Michailow, N., Agostini, P., Ali-Tolppa, J., Hock, D., Kasparick, M., ... & Zhou, Q. (2023). Convergence of Manufacturing and Networking in Future Factories. arXiv preprint arXiv:2312.08708.
4. Lindenschmitt, D., Mertes, J., Schellenberger, C., Schmitz, M., Han, B., Aurich, J. C., & Schotten, H. D. (2023, October). 6G Underlayer Network Concepts for Ultra Reliable and Low Latency Communication in Manufacturing. In European Wireless 2023; 28th European Wireless Conference (pp. 26-30). VDE.
5. Allison, J. (2022, July). Simulation-based learning via cisco packet tracer to enhance the teaching of computer networks. In Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1 (pp. 68-74).
6. Cisco Networking Cisco Networking Academy. (2020). Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7). Pearson Education, Limited.
7. Kurose, J. F., & Ross, K. W. (2007). Computer networking: A top-down approach edition. Addision Wesley.

8. Coleman, D. D., & Westcott, D. A. (2014). CWNA: Certified wireless network administrator official study guide: Exam CWNA-106. John Wiley & Sons.