NetworkWeaver: A Centralized Network Control and Monitoring Platform Using SNMP and APIs

M.J. Arenas, W.F. Basilio, R.A. Dela Cruz, R.J. Umali Wesleyan University - Philippines
Email: {arenas.mariusjose, renzaarondc}@gmail.com

I. Introduction

Modern network environments, especially in SMEs and educational institutions, face increasing complexity due to distributed infrastructure and limited IT resources. Manual configuration and fragmented monitoring tools often lead to inefficiencies, increased risk of misconfiguration, and delayed incident response. In the Philippines, these challenges are compounded by unique local factors such as frequent power disruptions and variable ISP reliability. There is a growing demand for solutions that unify monitoring and configuration into a single, accessible platform, reducing operational overhead and improving network resilience.

NetworkWeaver addresses these needs by providing a centralized dashboard for real-time monitoring and template-driven configuration management. The platform is designed to be hardware-agnostic, leveraging standard protocols (SNMP, REST API) to support a wide range of network devices without requiring specialized SDN hardware. This paper outlines the system's design, situates it within local and international research, and proposes an evaluation plan for its initial deployment.

In addition, A. I. Al-Khateeb and N. A. A. Al-Juboori (2023), in their publication "Design and implement a real-time network traffic management system using SNMP protocol," detail the development of a centralized system that leverages SNMP for real-time monitoring and traffic management [1]. Their findings highlighted significant improvements in fault detection, resource allocation, and overall network performance, emphasizing the importance of centralized platforms for efficient modern network operations.

According to Bladegrass Technologies (2025), in their report "Industry-Wide Network Hardware Configuration Plan for BPO Hubs," the deployment of standardized, centrally managed configuration plans across large enterprise networks in the Philippines, particularly in BPO hubs, provides significant advantages in network resilience, security compliance, and operational efficiency [2]. The report emphasizes the importance of unified configuration and monitoring strategies for addressing the diverse challenges faced by Philippine enterprise environments. This directly supports the rationale for centralized network management platforms.

According to S. Domingo et al. (2021), in their study "Real-time Remote Monitoring and Security System for a Local Area Network," the development and evaluation of a real-time remote monitoring system for local area networks in the Philippines demonstrated that unified dashboards and remote control capabilities significantly improve usability and operational effectiveness compared to proprietary solutions [3]. The system was evaluated using surveys and statistical analysis, showing higher satisfaction and control capability among IT staff, and was recommended for Management Information System departments.

A study by S. Zhuo et al. (2023), "Design of the Network Security Architecture for Philippine Smart Campuses," analyzed the network security framework of Philippine smart campuses and identified the need for robust monitoring and configuration to ensure data integrity and operational continuity [4]. The research integrates situational awareness and zero-trust technologies to enhance network reliability, further supporting the adoption of centralized monitoring solutions.

S. Lee et al. (2014), in their article "Network Monitoring: Present and Future," discuss the evolution of network monitoring tools, emphasizing the shift toward centralized, automated solutions using SNMP, REST APIs, and AI-driven analytics for improved efficiency and scalability [5].

In "Design and Implementation of Bandwidth Monitoring, Line Aggregation of VoIP" T. Oo and A.D. Africa (2019) implemented a Cacti-based monitoring system for Cisco devices, demonstrating the use of SNMP for real-time device status and network health tracking [6]. The research highlights the importance of synchronized configuration and monitoring for effective network management.

According to R. Villalobos et al. (2021), in their study "Design and Implementation of Network Monitoring System for Campus Infrastructure Using Software Agents," a multi-agent system for network monitoring was proposed, using SNMP and software agents to optimize data collection and reduce latency [7]. The system improved real-time monitoring and resource management in large-scale campus networks.

1. Describe the challenges faced by modern network environments, such as distributed infrastructure complexity, limited IT resources, and unique local factors impacting network reliability.
2. Implement a hardware-agnostic system supporting SNMP and REST APIs.
3. Develop real-time monitoring dashboards and configuration templates.
4. Evaluate system performance in virtual lab environments simulating SME and campus networks.
5. Assess user usability and operational efficiency improvements.

II. Methodology

A. Agile Software Development Life Cycle (SDLC)

This project follows the Agile Software Development Life Cycle (SDLC), a flexible, iterative approach that emphasizes collaboration, adaptability, and continuous improvement.

B. Pilot Deployment: Virtual Lab Environment

The pilot deployment of NetworkWeaver will be conducted within a virtual lab environment, leveraging advanced network emulation platforms such as EVE-NG and GNS3. These tools are widely recognized for their ability to simulate complex network topologies and support multi-vendor device emulation, making them ideal for rigorous testing of monitoring and centralized configuration systems.

The virtual lab will consist of simulated routers, switches, and firewalls configured to mimic real-world SME and campus network environments. Devices will be interconnected to form multiple segments, allowing for the testing of monitoring accuracy, configuration deployment, and fault recovery scenarios. SNMP agents and REST API endpoints will be enabled on all virtual devices to facilitate seamless integration with the NetworkWeaver platform.

Key scenarios to be evaluated include device onboarding, real-time status monitoring, alert generation, template-based configuration deployment, and rollback. Metrics such as alert detection rate, configuration success rate, and system response times will be collected for quantitative analysis. Usability feedback will be gathered from participants interacting with the platform in the simulated environment.

C. Project Design

The following are the web development tools and technologies that will be used in developing NetworkWeaver.

1) Node.js and Python (Polyglot Backend): The backend of NetworkWeaver will utilize a polyglot approach, combining Node.js and Python to maximize flexibility and performance. Node.js will be responsible for the monitoring subsystem, handling SNMP polling, REST API integrations, and real-time data streams due to its event-driven architecture and efficient handling of concurrent connections. Python will be used for automation and configuration management, leveraging its robust libraries for network automation and scripting complex workflows.

2) React.js(Frontend): The frontend will be developed using React.js, a modern JavaScript library for building responsive and dynamic user interfaces. React.js enables the creation of interactive dashboards, real-time alert panels, and intuitive configuration forms, enhancing the user experience for network administrators.

3) DynamoDB (Database): For data storage, DynamoDB will be used as a fully managed NoSQL database service. It is chosen for its scalability, high availability, and ability to efficiently store time-series monitoring data, configuration logs, and user actions.

4) WireGuard (VPN): WireGuard will be implemented to establish secure VPN tunnels between the orchestrator and managed network devices. WireGuard is selected for its simplicity, strong cryptographic design, and efficient performance, ensuring secure and reliable communication for both monitoring and configuration tasks.

D. Research Locale

This study will be conducted using a virtual laboratory environment set up with advanced network emulation platforms, specifically EVE-NG and GNS3. These tools enable simulation of the network conditions and operational scenarios typical of small-to-medium enterprises (SMEs) and educational campuses in the Philippines. The virtual lab, hosted on local infrastructure, allows the construction of network topologies that reflect the diversity of Philippine network environments, including multi-segment LANs, WAN links, and VPN-secured remote sites.

The use of EVE-NG and GNS3 enables controlled, repeatable testing of the NetworkWeaver platform's monitoring and configuration features, supporting dynamic scenarios, multi-vendor device emulation, and automated workflows. This setup allows researchers to simulate real-world challenges such as intermittent connectivity, device heterogeneity, and heightened security requirements commonly encountered in Philippine organizations (S.Domingo et al., 2024; Bladegrass Technologies, 2025).

By leveraging a virtualized environment with EVE-NG and GNS3, the study ensures that the evaluation of NetworkWeaver is both rigorous and relevant to the needs of local IT practitioners, while providing a safe and flexible platform for iterative development and testing.

E. Sampling Method

For the purpose of this research, a purposive sampling method will be applied, specifically targeting participants and network scenarios that best represent the intended use cases of NetworkWeaver. The following criteria will be used for sample selection:

1. Participants should be network engineering students or IT professionals with basic to intermediate experience in network monitoring and configuration.

2. The virtual lab environment will simulate typical Philippine SME and campus network topologies, including multi-segment LANs, WAN links, and VPN-secured remote sites.

3. Devices and scenarios will be chosen to reflect common challenges such as intermittent connectivity, device heterogeneity, and security requirements.

4. Participants must be able to access the virtual lab and perform monitoring and configuration tasks using the NetworkWeaver platform.

III. Statistical Treatment

To evaluate the effectiveness and usability of the Network-Weaver platform, both descriptive and inferential statistical methods will be employed. The following approaches will be used to analyze the data collected from the virtual lab environment:

A. Descriptive Statistics

The mean, standard deviation, and frequency counts will be used to summarize key metrics such as alert detection rate, configuration success rate, system response times, and usability scores. These statistics will provide an overview of the platform's performance and user experience.

B. Paired t-test

To compare operational metrics (e.g., time to detect issues, time to apply configurations) before and after the introduction of the NetworkWeaver platform, a paired t-test will be used if the data is normally distributed. If the data does not meet normality assumptions, the Wilcoxon signed-rank test will be applied. This approach follows the analysis methods used by Domingo et al. (2021).

C. System Usability Scale (SUS) Analysis

The mean and confidence intervals for SUS scores will be calculated to assess the perceived usability of the platform among participants.

References

[1] A. I. Al-Khateeb and N. A. A. Al-Juboori, "Design and implement a real-time network traffic management system using SNMP protocol," *Eastern-European Journal of Enterprise Technologies*, vol. 6, no. 123, pp. 68-77, 2023. [Online].

[2] Bladegrass Technologies, "Industry-Wide Network Hardware Configuration Plan for BPO Hubs," 2025. [Online].

[3] S.Domingo, N.Guererro, and A. Acoba, "Real-time Remote Monitoring and Security System for a Local Area Network," *IIARI Journal of Interdisciplinary Research*, 2021. [Online].

[4] Y. Yuhong, S. Zhuo, and R. Monreal "Design of the Network Security Architecture for Smart Campus in the Philippines," *Journal of Knowledge and Learning in Smart Technology*, 2023. [Online].

[5] S. Lee, K. Levanti, and H. Kim, "Network Monitoring: Present and Future," *Computer Networks*, 2014. [Online].

[6] T. Oo, and A.D. Africa, 'Design and Implementation of Bandwidth Monitoring, Line Aggregation of VoIP " *International Journal of Advanced Trends in Computer Science and Engineering*, 2019. [Online].

[7] R. Villalobos, E. Triana, H. Ceballos, and J. Triviño "Design and Implementation of Network Monitoring System for Campus Infrastructure Using Software Agents," in *Proceedings of the International Conference on Computer, Communication, and Control*, 2021. [Online].