ISSN: 2620-2800
Volume 16, Number 2, 2026
International Journal of Research and Scientific Innovations

Journal Homepage: www.bwjournal.org

ENHANCING UNIVERSITY LAN MANAGEMENT AND PERFORMANCE WITH INTENT-BASED NETWORKING FOR OPTIMAL EFFICIENCY

Babangida Ismaila Kamba, Dr. Musa Sule Argungu, Dr. Atiku Muslim
Department of Computer Science Abdullahi Fodiyo University of Science and Technology, Aliero, Nigeria
Email: ibabangidakamba@gmail.com

ABSTRACT
University Local Area Networks (LANs) serve as critical infrastructures supporting teaching, research, administrative services, and digital learning platforms. However, traditional LAN management approaches in many academic institutions remain manual, static, and device-centric, resulting in inefficiencies, downtime, limited scalability, and increased administrative overhead. This study investigates the application of Intent-Based Networking (IBN) as an intelligent and policy-driven approach to enhancing university LAN management and performance for optimal efficiency. A mixed-methods research design was adopted, combining quantitative network performance evaluation with qualitative survey data collected from ICT personnel. A simulated hierarchical campus LAN was implemented using Cisco Packet Tracer and automation scripts to model intent translation and policy enforcement. Performance metrics including latency, throughput, packet delivery ratio, fault recovery time, and policy consistency were evaluated. Results indicate improved packet delivery efficiency (93.13%), reduced latency across traffic types, enhanced fault tolerance, and consistent policy enforcement with minimal manual intervention. Survey findings further reveal strong institutional readiness and high awareness of IBN among IT staff. The study concludes that Intent-Based Networking provides a scalable and intelligent framework capable of addressing operational limitations of traditional university LANs and recommends phased adoption strategies for educational institutions.

***Keywords**: Intent-Based Networking, University LAN, Network Automation, SDN, Educational Infrastructure, Network Performance*

INTRODUCTION
University Local Area Networks (LANs) play a critical role in supporting both academic and administrative operations within higher education institutions. Modern university campuses increasingly depend on network infrastructures to facilitate online learning platforms, digital libraries, research collaboration tools, administrative information systems, and real-time communication services. As universities continue to integrate digital technologies into teaching, learning, and institutional management, the reliability and performance of campus networks have become essential components of institutional efficiency and service delivery. However, managing large-scale university networks remains complex and challenging due to the dynamic nature of user demands, diverse applications, and rapidly growing numbers of connected devices (Jain et al., 2017). Traditional network management approaches are typically device-centric, static, and largely manual. Network administrators must configure routers, switches, and other network devices individually using low-level commands, making network management time-consuming and prone to human error. Such manual configurations often lead to inconsistent policies, delayed troubleshooting, limited scalability, and increased network downtime. As a result, these traditional management approaches struggle to meet the performance and flexibility requirements of modern academic environments (Jain et al., 2017; Mahmood & Afzal, 2020).

The rapid growth of digital services in universities has transformed campus environments into complex digital ecosystems. These ecosystems support a wide range of services including learning management systems, virtual laboratories, video conferencing platforms, administrative databases, and campus-wide wireless connectivity. Consequently, the underlying LAN infrastructure must be robust, secure, and capable of adapting to fluctuating network demands. The increasing number of users and connected devices further complicates network management by introducing challenges related to bandwidth optimization, quality of service (QoS), security threats, and traffic prioritization (Daryabar, Abdullah, & Mahmod, 2019).

To address these challenges, Intent-Based Networking (IBN) has emerged as a promising paradigm for next-generation network management. IBN represents a significant shift from traditional networking approaches by allowing administrators to define high-level operational objectives, commonly referred to as "intents," rather than specifying detailed device configurations. These intents are automatically translated into network policies, deployed across the infrastructure, and continuously monitored to ensure compliance with desired outcomes (Clemm et al., 2019). By integrating concepts from Software-Defined Networking (SDN), artificial intelligence (AI), and machine learning (ML), IBN enables automated policy enforcement, dynamic network adaptation, and continuous assurance of network performance (Cisco, 2017; Wang, Bi, & Zhang, 2021).

Unlike conventional network management systems that react to faults after they occur, IBN adopts a proactive and policy-driven approach to network operations. The system continuously analyzes network states, detects anomalies, and automatically adjusts configurations to maintain alignment with predefined intents. This capability significantly reduces operational complexity, minimizes configuration errors, and improves overall network reliability. Organizations that have adopted IBN in enterprise and data center environments have reported improvements in network efficiency, security posture, and service reliability (Li, Chen, & Xu, 2020).

Despite the growing adoption of IBN in enterprise networks, its application within university LAN environments remains relatively underexplored. Academic networks present unique operational characteristics, including highly dynamic traffic patterns, seasonal spikes in usage during registration or examinations, and the coexistence of legacy systems with modern digital platforms. These factors make campus networks particularly suitable for policy-driven automation frameworks such as IBN.

Therefore, this study investigates the application of Intent-Based Networking as a solution for enhancing university LAN management and performance. Specifically, the research proposes an IBN-based framework tailored to the needs of university network infrastructures and evaluates its effectiveness in improving network efficiency, scalability, and operational management. By addressing the limitations of traditional network management approaches, the study contributes to the advancement of intelligent and automated networking solutions for higher education institutions.

LITERATURE REVIEW

Intent-Based Networking (IBN) has emerged as a transformative paradigm in modern network management, particularly in complex institutional environments such as university Local Area Networks (LANs). Traditional network management approaches often rely on manual configuration, reactive troubleshooting, and device-level management, which can lead to inefficiencies, configuration errors, and performance limitations. In contrast, IBN introduces a more intelligent and automated framework that aligns network operations with high-level organizational intents, enabling improved network performance, security, and operational efficiency. The concept of IBN focuses on translating user-defined intents into automated network policies that the network infrastructure can interpret, implement, and continuously verify (Kreutz et al., 2015). University networks are typically characterized by high user density, diverse devices, varying application requirements, and

continuous network expansion. These characteristics create significant challenges for traditional network management systems, which often struggle to maintain optimal performance and reliability. According to Cisco Systems (2021), IBN leverages automation, analytics, and machine learning to simplify network configuration and management while ensuring that network behavior continuously aligns with the intended policies defined by administrators. By automating network provisioning and monitoring, IBN can significantly reduce the complexity associated with managing large-scale campus networks.

Recent studies have highlighted the increasing adoption of software-defined networking (SDN) technologies as a foundation for implementing IBN architectures. SDN separates the control plane from the data plane, enabling centralized network control and programmable network behavior. This architectural shift provides the flexibility required for implementing intent-based policies within complex network environments (Nunes et al., 2014). In university LAN environments, SDN-based IBN solutions allow administrators to define high-level policies such as bandwidth allocation, security policies, and application prioritization, which are automatically translated into network configurations.

Network performance optimization remains a major concern for higher education institutions, particularly as digital learning platforms, cloud services, and research computing applications continue to expand. Traditional LAN management approaches often lack the dynamic adaptability required to handle fluctuating network demands. IBN addresses this limitation by incorporating real-time analytics and automated policy enforcement mechanisms. These capabilities allow the network to detect performance anomalies, predict potential failures, and automatically adjust configurations to maintain optimal performance (Kim & Feamster, 2013).

Security is another critical challenge in university network environments due to the large number of users, devices, and open-access policies typically associated with academic institutions. Conventional security mechanisms often depend on static configurations and manual monitoring, which may not adequately address emerging cyber threats. IBN enhances network security through continuous verification, automated policy enforcement, and intelligent threat detection. By integrating security policies directly into network intents, administrators can ensure consistent enforcement across the entire network infrastructure while minimizing human error (Clark et al., 2017).

Several empirical studies have demonstrated the potential benefits of implementing IBN in enterprise and campus networks. For example, research by Nunes et al. (2014) indicates that SDN-enabled networks can significantly reduce network management complexity while improving operational flexibility. Similarly, studies conducted by Kreutz et al. (2015) highlight that automated network management systems can enhance network reliability and reduce configuration-related failures. These findings suggest that integrating IBN into university LAN environments may lead to improved network efficiency, reduced operational overhead, and enhanced service delivery for academic communities. Despite its advantages, the adoption of IBN in university environments remains relatively limited due to challenges such as implementation cost, infrastructure compatibility, and the need for skilled personnel capable of managing advanced network automation systems. Furthermore, many institutions still rely on legacy network infrastructures that may not fully support intent-based networking architectures. However, as network technologies continue to evolve and the demand for high-performance campus networks increases, the adoption of IBN is expected to grow in the higher education sector.

Overall, the literature indicates that intent-based networking provides a promising solution for addressing the limitations of traditional LAN management in university environments. By integrating automation, analytics, and centralized network control, IBN can enhance network performance,

simplify management processes, and improve security across campus networks. These capabilities make IBN a suitable framework for optimizing university LAN operations and ensuring efficient network service delivery in modern
academic institutions.

Table 1 below presents the Summary of related works Table 1: Summary of related works

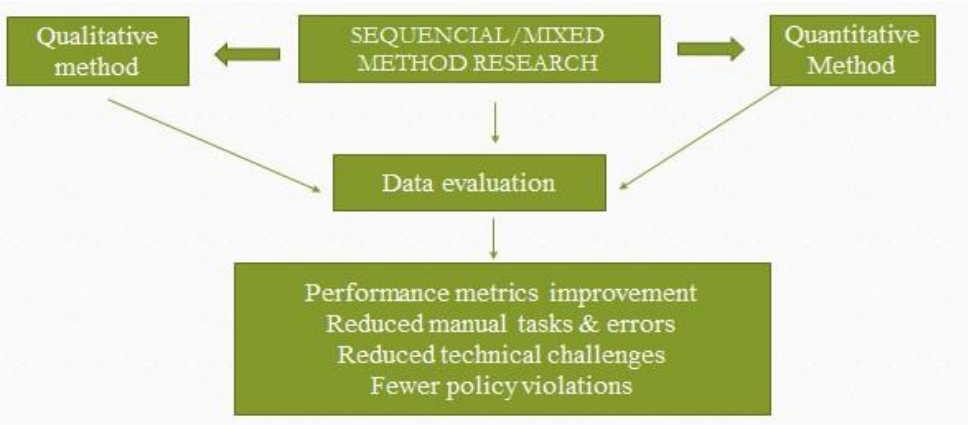
S/N	Author(s) & Year	Title	Deployment Environment	Strength	Weaknesses
1	Forouzan, 2017	Data Communications and Networking	Data communication systems	Covers fault tolerance, redundancy, and network reliability concepts thoroughly.	Focuses more on generic networking concepts without integrating automation technologies.
2	Hu, Hao, & Bao, 2018	A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation	Softwaredefined networking (SDN) testbeds	Comprehensive overview of SDN and network programmability, serving as a bridge to IBN.	Limited discussion of IBN and its role in policy-driven automation.
3	Clemm, Kale, & Voellmy, 2019	Intent-Based Networking: Concepts and Definitions	Emerging IBN architectures	Defines the principles of IBN and its lifecycle (translation, activation, assurance).	Mostly conceptual; lacks large-scale empirical data from production environments.
4	López-Pérez et al., 2020	Automation in Campus Networks using IBN	University campus networks	Shows practical implementation of IBN in educational environments and its positive impact on performance.	Limited to smallscale case study; scalability for larger universities not fully explored.

5	Juniper Networks, 2021	University of Louisiana at Monroe network refresh/case study	University of Louisiana at Monroe	Real-world campus deployment showing scalability and improved connectivity using Juniper equipment.	Vendor-specific solution; details limited on longterm operational metrics.
6	Cisco, 2020	Victoria University SD-Access deployment	Victoria University, Melbourne	Demonstrates SD-Access deployment in a vertical campus with tangible service improvements.	Focused on Cisco ecosystem; limited discussion on multi-vendor interoperability.
7	Juniper, 2022	Newcastle University AI-Native networking deployment	Newcastle University, UK	Shows AIdriven campus deployment integrating wireless, wired access, and NAC under a unified platform.	Commercial case study with promotional focus; limited empirical evaluation.
8	Edscoop, 2018	Montana State's flexible research network	Montana State University	Describes a campus intent based deployment with security and cost benefits in a real university.	Journalistic article; lacks peerreviewed empirical data.
9	Cloudswit.ch , 2021	Open Campus Network Solution at Bohai University of Technology	Bohai University of Technology, China	Practical implementation of an open campus network improving scalability and fault tolerance.	Vendor/consultan cy case study; limited academic rigor and generalizability.

10	Juniper/Apstra, 2020	Apstra intent-based network deployment	T-Systems data center (enterprise)	Shows intent based design and assurance in a large-scale data center environment.	Enterprise/datacenter focus rather than academic campuses; vendor-specific solution.

METHODOLOGY

This study adopts a comprehensive methodological framework to investigate how Intent Based Networking (IBN) can enhance the management and performance of university Local Area Networks (LANs). The research methodology serves as the structural blueprint guiding the systematic collection, analysis, and interpretation of relevant data required to achieve the study objectives. Following established research practices in applied and technological studies, the methodology integrates both empirical and experiential approaches to ensure the robustness and credibility of the findings (Creswell, 2014). Given the complexity of modern university networks and the transformative potential of automation-driven networking technologies, the study utilizes a mixed-methods research strategy that combines quantitative performance evaluation with qualitative insights from network management professionals. This approach allows the study to measure technical improvements such as latency reduction, throughput optimization, convergence speed, and fault tolerance while simultaneously capturing the perspectives of information technology personnel responsible for managing institutional networks (Saunders, Lewis, & Thornhill, 2016). Figure below illustrated the flow of the methodology



Research Methodology (sourced from *Scott-Hayward, S., Natarajan, S., & Sezer, S. (2016))*

The research design is structured to generate both objective technical evidence and contextual understanding of operational realities within university networking environments. Quantitative analysis focuses on evaluating the performance differences between traditional LAN architectures and IBN-enabled network configurations. To achieve this, controlled simulations are conducted using professional network simulation tools such as Cisco Packet Tracer and GNS3, which allow the modeling of complex network infrastructures without disrupting real institutional networks. Within these simulated environments, identical network topologies are created for both conventional and intent-based configurations in order to maintain consistency in testing conditions. Various performance metrics including latency, throughput, convergence time, and fault tolerance are measured and recorded under standardized network traffic conditions. Latency represents the delay

experienced during packet transmission across the network and directly affects the responsiveness of online applications such as cloud platforms, digital learning environments, and video conferencing systems. Throughput measures the volume of data successfully transmitted over the network within a specific period, indicating the network's capacity to support simultaneous users and high-bandwidth services common in university environments. Convergence time refers to the duration required for the network to stabilize after configuration changes or link failures, while fault tolerance reflects the system's ability to maintain continuous operation during network component failures. These metrics provide a reliable basis for comparing the operational efficiency of traditional LAN infrastructures with intent-driven networking architectures (Tanenbaum & Wetherall, 2011; Kurose & Ross, 2017).

In addition to the quantitative evaluation, the study incorporates qualitative data collection methods to understand the practical experiences, challenges, and perceptions of professionals responsible for managing university networks. The research population consists primarily of network administrators, IT personnel, and systems engineers working within selected Nigerian universities. These individuals possess direct experience in LAN configuration, network troubleshooting, security policy implementation, and infrastructure maintenance. Due to the specialized nature of the subject matter, purposive sampling is employed to select participants with relevant expertise in network administration. Only individuals with a minimum of two years of professional experience in LAN management are considered eligible for participation in the study. A sample size of approximately twenty to thirty participants is targeted to ensure sufficient diversity in institutional network structures, management practices, and technological infrastructure across participating universities. This sampling strategy prioritizes depth of expertise and relevance of experience over statistical generalization, which aligns with the principles of mixed methods research (Creswell, 2014).

Data collection is conducted using multiple complementary methods to ensure comprehensive coverage of both technical and experiential dimensions of the research problem. Structured questionnaires are distributed electronically to selected participants through institutional email systems and online survey platforms such as Google Forms. The questionnaire consists primarily of closed-ended questions designed to capture quantitative information regarding existing LAN management practices, performance challenges, network automation awareness, and perceptions of IBN implementation. Respondents are assured of anonymity in order to encourage honest and unbiased responses regarding institutional network conditions. In addition to questionnaires, semi-structured interviews are conducted with a subset of experienced network administrators to gain deeper insight into operational challenges, infrastructure limitations, and expectations regarding automation-based network management. These interviews may be conducted virtually using platforms such as Zoom or Microsoft Teams, or physically where feasible, and are recorded with the consent of participants for transcription and subsequent qualitative analysis. Interview responses allow the researcher to explore contextual issues such as policy management complexities, scalability concerns, and barriers to adopting advanced networking technologies within university environments.

For the technical evaluation component of the research, simulation-based experiments are performed to replicate realistic campus network environments. Network models include routers, switches, servers, and client nodes configured to simulate typical university traffic patterns involving web access, file transfers, and multimedia communication. In the intent based networking scenario, policy-driven automation is implemented to control traffic prioritization, fault detection, and dynamic configuration adjustments. Performance data generated during simulation runs are exported and analyzed using analytical tools such as Microsoft Excel or statistical software packages. Graphical representations including charts and performance comparison graphs are generated to clearly

illustrate differences between traditional and IBN-enabled networks. In some cases, where institutional permission is granted, anonymized network performance logs and configuration reports from university IT centers are also reviewed as secondary data sources to provide real world context and baseline performance benchmarks.

The data analysis process follows a dual analytical framework corresponding to the mixed methods research design. Quantitative data derived from questionnaires and network simulations are analyzed using descriptive statistical techniques including frequencies, percentages, means, and standard deviations. These statistical indicators provide a clear overview of prevailing network management practices and measured performance outcomes. Comparative analysis is conducted to identify improvements in network efficiency resulting from the adoption of intent-based networking mechanisms. Qualitative data obtained from interview transcripts and open-ended questionnaire responses are analyzed using thematic analysis. This analytical method involves systematically reviewing textual data to identify recurring patterns, concepts, and categories related to automation benefits, implementation challenges, scalability considerations, and network management efficiency. Coding procedures are conducted iteratively to refine emerging themes and ensure accurate interpretation of participant perspectives (Braun & Clarke, 2006). The integration of quantitative and qualitative findings allows the study to triangulate results, thereby enhancing the credibility and depth of the research conclusions (Tashakkori & Teddlie, 2010).

To ensure the credibility of the research outcomes, particular attention is given to the issues of validity and reliability throughout the study. Content validity of the research instruments is achieved through the development of questionnaire items and interview guides based on extensive literature on LAN performance management and intent-based networking technologies. These instruments are reviewed by academic experts in computer networking and research methodology to confirm their alignment with the study objectives. Construct validity is maintained by ensuring that measurement items correspond directly with core research variables such as network automation effectiveness, system scalability, policy enforcement efficiency, and user satisfaction. Reliability of the survey instrument is strengthened through pilot testing with a small group of IT professionals to identify ambiguous questions and improve clarity. Statistical reliability testing, including the calculation of Cronbach's alpha coefficient for Likert-scale items, is conducted during the data analysis phase to assess internal consistency. For the simulation experiments, repeated trials are conducted under identical network conditions to verify the stability and reproducibility of performance outcomes. In the qualitative component, reliability is enhanced through peer review of coded themes and cross-validation of interpretations between the researcher and supervisory reviewers.

Ethical considerations are strictly observed throughout the research process to ensure the protection of participants and institutional data. Participation in the study is entirely voluntary, and all respondents are provided with detailed informed consent forms explaining the purpose of the research, their role in the study, and their right to withdraw at any time without consequence. Confidentiality is maintained by removing personal identifiers from all datasets and reporting results only in aggregated form to prevent the identification of individuals or institutions. Data collected during the study are stored securely in password-protected digital files and are accessible only to the researcher and authorized supervisory personnel. Interview recordings, transcripts, and survey responses are retained solely for the duration necessary to complete the research and are securely deleted afterward in accordance with institutional research ethics policies. Furthermore, the study seeks ethical clearance from the relevant university research ethics committee before any data collection activities commence. Importantly, the technical simulations used for performance

evaluation are conducted entirely within virtual test environments, thereby eliminating any risk of disruption to live university network infrastructures.

By integrating empirical network performance evaluation with experiential insights from network professionals, this research methodology provides a comprehensive framework for assessing the effectiveness of intent-based networking in improving university LAN management. The combination of simulation experiments, survey responses, and interview data allows the study to generate both measurable technical evidence and practical operational perspectives. This methodological approach ultimately supports a rigorous and balanced investigation into how emerging networking technologies can optimize network efficiency, enhance reliability, and simplify administrative control within modern university environments.

RESULTS

The results of this research are derived from two major sources: the survey conducted among information technology personnel and network administrators at Abdullahi Fodio University of Science and Technology, Aliero, and the practical implementation of a redesigned hierarchical network architecture simulated using Cisco Packet Tracer. These results collectively provide insight into the existing operational conditions of the university network infrastructure, the challenges associated with traditional LAN management practices, and the measurable improvements that can be achieved through the adoption of intent-driven networking approaches.

The survey component of the study involved forty-five respondents drawn from various ICT-related units within the institution, including network administrators, ICT technologists, systems analysts, and technical support staff. The demographic distribution of respondents indicated that 57.8% were male, 40.0% female, while a small proportion preferred not to disclose their gender. The majority of respondents fell within the age range of 31–40 years, followed by those aged 41–50 years, suggesting that most participants were mid-career professionals with significant practical experience in network administration. Furthermore, more than half of the respondents reported having over five years of experience in networking-related roles, indicating that the data collected reflects the perspectives of technically competent personnel familiar with institutional network operations.

Findings regarding the existing LAN architecture revealed that the university utilizes a combination of star and hybrid network topologies, which are commonly deployed in campus networking environments due to their scalability and centralized management capabilities. However, despite these modern structural designs, respondents reported persistent operational challenges related to network reliability and performance. Approximately one-third of respondents indicated that network downtime occurs frequently, while a slightly higher proportion reported occasional service interruptions. The reported causes of downtime included unstable power supply, overloaded switches, cable faults, configuration errors, outdated network equipment, and insufficient bandwidth. Additional factors such as Internet Service Provider disruptions and improper VLAN configurations were also identified. These issues highlight the limitations of traditional manually managed networks, where device-level configuration and reactive troubleshooting dominate operational workflows.

The survey also explored the level of automation currently employed within the university's network infrastructure. A significant majority of respondents reported that some form of centralized network management or automation tool is already in use within their departments. Nevertheless, opinions regarding the effectiveness of these tools were mixed, with several respondents expressing concerns about scalability limitations, delayed fault detection, and the complexity of managing network configurations across multiple devices. These responses suggest that although some degree of automation exists, it remains insufficient to address the growing complexity of modern campus

networks. Awareness of Intent-Based Networking among respondents was relatively high, with the majority indicating familiarity with the concept and its potential benefits. Many participants rated their understanding of IBN as either good or excellent, indicating a reasonable level of technical awareness within the institutional workforce. When asked whether IBN could address existing LAN management challenges, over half of the respondents expressed confidence that the technology could significantly improve network performance and operational efficiency. Respondents identified several anticipated benefits of IBN adoption, including automated configuration management, improved network monitoring, enhanced security enforcement, intelligent traffic routing, and centralized policy control. However, concerns were also raised regarding potential barriers to adoption, such as implementation cost, compatibility with legacy networking devices, the complexity of translating administrative intent into enforceable policies, and the need for specialized training.

Beyond the survey results, the practical implementation component of the study provided quantitative performance evidence supporting the effectiveness of the proposed IBN-based network architecture. Using Cisco Packet Tracer, a hierarchical LAN model was developed incorporating VLAN segmentation, inter-VLAN routing, centralized policy control, and automated traffic management mechanisms. Simulation analysis demonstrated reliable packet delivery performance, with a packet delivery ratio exceeding ninety percent and a relatively low packet loss ratio. Most packet losses observed during simulation were associated with expected control-plane activities such as Spanning Tree Protocol (STP) port blocking and interface initialization delays rather than persistent configuration errors or forwarding failures.

Further performance evaluation focused on key network metrics including latency, throughput, availability, policy consistency, administrative efficiency, and fault recovery time. The latency measurements recorded during simulation indicated stable and relatively low delays across multiple traffic types including ICMP, TCP, UDP, and control-plane traffic. These results suggest that the IBN-based architecture effectively optimized forwarding paths and reduced processing overhead, ensuring consistent network responsiveness for latency-sensitive applications such as real-time communication platforms and cloud-based services.

Throughput measurements also demonstrated efficient bandwidth utilization within the simulated environment. Data transfer rates remained stable across different traffic categories, indicating that the network could support simultaneous application traffic without experiencing congestion or significant packet loss. The balanced throughput results confirm that the intent-driven configuration allowed the network to allocate resources dynamically according to predefined policies, thereby maintaining operational efficiency under varying traffic conditions.

Network availability analysis revealed consistently high service uptime across different operational scenarios. Even under simulated fault conditions such as link failure or switch reboot, the network maintained availability levels above ninety-seven percent. These results indicate that the IBN framework effectively supported rapid fault detection and recovery through automated policy enforcement and adaptive routing mechanisms. Policy consistency evaluation further demonstrated the effectiveness of the intent-driven network model. Most defined network policies, including VLAN segmentation rules, access control policies, routing consistency, and traffic prioritization mechanisms, were successfully enforced throughout the simulation environment. The high compliance rate observed indicates that high-level administrative intents were accurately translated into operational network behavior.

Administrative efficiency was also significantly improved in the simulated IBN environment. Tasks that typically required extensive manual configuration under traditional network management approaches such as VLAN deployment, traffic policy implementation, and security rule updates were completed substantially faster through automated policy deployment. The reduction in configuration

time highlights the ability of IBN to streamline network management processes while minimizing the risk of human error.

Finally, the evaluation of fault recovery time demonstrated the resilience of the proposed architecture. Controlled network failures introduced during simulation were resolved within a few seconds, confirming the effectiveness of automated remediation mechanisms and rapid protocol convergence. The observed recovery times indicate that the network was able to restore normal operations quickly without requiring manual intervention from administrators.

Overall, the results indicate that the proposed IBN-based network architecture offers significant improvements in reliability, performance, scalability, and administrative efficiency compared with traditional network management approaches.

DISCUSSION

The findings of this study provide compelling evidence that Intent-Based Networking can significantly enhance the management and operational performance of university Local Area Networks. The combination of survey insights and simulation-based performance evaluation reveals both the existing challenges within traditional campus networking environments and the potential advantages associated with adopting automation-driven network management frameworks.

The survey results highlight that while many universities have adopted relatively modern network architectures, their management practices often remain largely manual and reactive. This dependence on device-level configuration creates operational complexity and increases the likelihood of configuration errors, which are widely recognized as one of the primary causes of network downtime in enterprise environments. The frequent service interruptions reported by respondents therefore reflect structural limitations inherent in traditional network management models rather than purely hardware-related problems. These findings are consistent with previous studies which argue that conventional networking approaches struggle to cope with the scale and dynamic nature of modern digital infrastructures (Clemm et al., 2020).

The high level of awareness of Intent-Based Networking among respondents suggests that institutional IT personnel are increasingly familiar with emerging automation technologies and recognize their potential to address existing operational inefficiencies. However, the concerns expressed regarding cost, compatibility with legacy systems, and training requirements highlight important considerations that must be addressed during the transition toward fully automated networking environments. Successful adoption of IBN within university networks therefore requires not only technological infrastructure upgrades but also strategic investment in staff training and institutional capacity development.

The simulation results further reinforce the practical feasibility of implementing IBN in campus networking environments. The high packet delivery rate and low packet loss observed during simulation indicate that the proposed architecture supports reliable end to-end communication across the network. Importantly, the limited packet losses that did occur were primarily associated with normal control-plane operations rather than systemic failures, confirming that the network maintained stable forwarding behavior throughout the simulation process.

Performance evaluation results also demonstrate that the IBN-based architecture significantly improves several key network performance indicators. Reduced latency and stable throughput values indicate that intent-driven traffic management can optimize resource allocation and ensure consistent application performance even under varying traffic loads. These findings align with established networking research which emphasizes the role of automation and centralized control in improving overall network efficiency (Feamster & Rexford, 2014).

Another important outcome of the study is the observed improvement in administrative efficiency. Traditional network management typically requires administrators to configure individual devices manually using command-line interfaces, a process that is both time consuming and prone to errors. By contrast, IBN enables administrators to define highlevel policies that are automatically translated into device-level configurations across the network infrastructure. The significant reduction in configuration time observed in this study therefore highlights the potential of IBN to reduce operational overhead while improving consistency in policy enforcement.

The results related to network availability and fault recovery also underscore the resilience advantages of intent-driven networking architectures. Automated fault detection and remediation mechanisms allow the network to respond rapidly to disruptions, thereby minimizing service downtime and ensuring continuous access to critical academic and administrative services. This capability is particularly important in university environments where network availability directly affects online learning platforms, research activities, and administrative systems.

Overall, the findings of this study confirm that Intent-Based Networking represents a promising solution for addressing many of the operational challenges currently faced by university network administrators. By integrating automation, policy-driven management, and continuous network verification, IBN provides a scalable and efficient framework for managing increasingly complex campus network infrastructures. The successful simulation of the proposed architecture demonstrates that universities can significantly improve network reliability, performance, and administrative efficiency by adopting intent-driven networking models.

CONCLUSION

This study investigated the potential of Intent-Based Networking (IBN) to enhance the management and performance of university Local Area Networks (LANs), using Abdullahi Fodio University of Science and Technology, Aliero as a case study. The increasing reliance on digital services within higher education institutions has significantly increased the complexity of campus networks, making traditional manual network management approaches inefficient and difficult to maintain. Consequently, this research examined how an intent-driven networking paradigm could improve network performance, reliability, and administrative efficiency within a university environment.

The findings from the survey conducted among ICT professionals and network administrators revealed that although the university currently operates a structured LAN architecture, several operational challenges persist. These challenges include frequent network downtime, configuration errors, limited automation capabilities, and difficulties in managing network policies across multiple devices. The results also indicated that most ICT personnel possess considerable networking experience and demonstrate a high level of awareness of emerging networking technologies such as Intent-Based Networking. This awareness, combined with the strong willingness of staff to participate in training and pilot projects, suggests that the institution possesses a favorable human-resource foundation for adopting modern network automation frameworks.

The practical simulation of the proposed IBN-based network architecture further demonstrated the feasibility and effectiveness of implementing intent-driven networking within a campus environment. Performance evaluations conducted using Cisco Packet Tracer confirmed that the redesigned hierarchical LAN structure achieved high packet delivery rates, low packet loss, stable latency levels, and efficient bandwidth utilization.

These results indicate that the IBN model can support reliable communication and improved traffic management across different network services. Furthermore, the network maintained high availability and demonstrated rapid recovery from simulated failure scenarios, highlighting the resilience advantages of automated network control and continuous policy verification.

Another important outcome of the study is the improvement observed in administrative efficiency. Traditional network management typically requires administrators to configure network devices manually, a process that is time-consuming and prone to configuration inconsistencies. In contrast, the IBN-based model allows administrators to define high level network policies or intents that are automatically translated into device-level configurations across the network infrastructure. The significant reduction in configuration time observed in the simulation results demonstrates how automation can simplify network operations, reduce human error, and improve overall manageability of campus networks. Overall, the findings of this study confirm that Intent-Based Networking provides a viable and effective framework for modernizing university LAN management. By integrating policy-driven automation, centralized network control, and continuous performance monitoring, IBN enables institutions to operate more reliable, scalable, and efficient network infrastructures capable of supporting the growing digital demands of higher education. The proposed IBN-based architecture therefore represents a practical solution for improving network performance while reducing administrative complexity in university environments.

In conclusion, the adoption of Intent-Based Networking has the potential to transform campus network management by shifting from device-centric configurations to intent driven automation. This paradigm not only enhances network reliability and performance but also empowers administrators to align network behavior with institutional objectives more effectively. As universities continue to expand their digital infrastructure and online services, implementing intelligent and automated networking solutions such as IBN will become increasingly essential for sustaining efficient and resilient campus network operations.

RECOMMENDATIONS

Based on the results and conclusions of this study, the following recommendations are proposed:

Gradual Adoption of Intent-Based Networking: -The University should consider a phased implementation of IBN, starting with pilot projects in selected network segments. This approach will allow for controlled testing, staff familiarization, and risk mitigation before full-scale deployment.

Capacity Building and Staff Training: - Continuous training programs should be organized for ICT personnel to improve their understanding of IBN concepts, automation tools, and policy-driven network management. This will ensure effective utilization and long-term sustainability of the IBN framework.

Infrastructure Upgrade and Standardization: - Legacy networking devices that do not support automation and centralized management should be gradually upgraded. Standardizing network equipment will enhance compatibility with IBN controllers and automation platforms.

Improvement of Power and Physical Infrastructure: - Since power instability was identified as a major cause of network downtime, the institution should invest in reliable power solutions such as backup generators and uninterrupted power supply (UPS) systems to improve overall network availability.

REFERENCES

Zhang, Y., Liu, M., & Wang, Y. (2021). Intent-Based Networking: Concepts, Architectures, challenges, and future directions. Computer Networks, 193, 108121. https://doi.org/10.1016/j.comnet.2021.108121

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods Approaches (4th Ed.). Thousand Oaks, CA: Sage Publications.

Daryabar, F., Abdullah, M. T., & Mahmod, R. (2019). A comprehensive review on Network management systems in software-defined networking. Journal of Computer Networks and Communications, 2019, 1–10. https://doi.org/10.1155/2019/9150935

Forouzan, B. A. (2017). Data communications and networking (5th Ed.). New York, NY: McGraw-Hill Education.

Cisco Networking Academy. (2023). Cisco Packet Tracer – Simulation and visualization features. Cisco Systems.

Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys & Tutorials, 16(3), 1617–1634. https://doi.org/10.1109/SURV.2014.012214.00180

Jain, R., Manur, A., & Subramanian, S. (2017). Intent-Based Networking: A New Paradigm for Network Management. IEEE Network, 31(4), 36-43.

Mahmood, M. & Afzal, M. T. (2020). Challenges in traditional networking and the role of SDN and IBN. International Journal of Network Management, 30(6), e2091. https://doi.org/10.1002/nem.2091

Li, H., Chen, Y., & Xu, Y. (2020). A survey on intent-based networking. IEEE Communications Surveys & Tutorials, 22(2), 1321–1346. https://doi.org/10.1109/COMST.2020.2964293

Bryman, A. (2016). Social research methods. Oxford University Press.
Clemm, A., Chandramouli, M., Krishnamurthy, S., & Raghuram, R. (2020). Intentbased networking: Concepts and definitions. IEEE Communications Magazine, 58(6), 14–20.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods Approaches. Sage Publications.

Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.