World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Autonomous Enterprise Networks: The Convergence of AI-Driven Infrastructure and Smart Building Technologies

Jithendra Babu Punugubati *

JNTU Hyderabad, India.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(03), 2305-2311

Publication history: Received on 12 May 2025; revised on 21 June 2025; accepted on 23 June 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.3.1072

Abstract

The rapid evolution of enterprise networking infrastructure presents unprecedented opportunities for integration with smart building technologies. Recent advancements in intent-based networking have enabled autonomous configuration based on high-level business objectives, significantly reducing manual intervention while enhancing operational efficiency. AI-enhanced switches now serve as intelligent nodes capable of anomaly detection, traffic optimization, and self-healing during network disruptions. Concurrently, green Ethernet standards facilitate dynamic power management, addressing critical sustainability concerns in large-scale deployments. Digital twin modeling has emerged as a powerful simulation tool for network behavior within building automation systems, allowing for performance optimization without physical infrastructure modifications. The incorporation of wireless mesh networks with traditional enterprise switching creates seamless connectivity for IoT devices throughout smart buildings. Enhanced security protocols now dynamically adjust access policies based on contextual factors, safeguarding against both cyber and physical threats. These technological convergences collectively point toward fully autonomous, self-regulating network ecosystems that balance agility, security, and energy efficiency—fundamental components for next-generation smart building infrastructure.

Keywords: Enterprise Networking; Intent-Based Networking; AI-Driven Switches; Digital Twins; Cyber-Physical Security; Green Ethernet

1. Introduction to Next-Generation Enterprise Network Management

Enterprise networking infrastructure faces unprecedented challenges in today's digital landscape. The exponential growth in connected devices, increasing bandwidth demands, and complex security requirements have pushed traditional network management approaches beyond their practical limits. Manual configuration and troubleshooting processes struggle to keep pace with rapidly evolving business needs, resulting in operational inefficiencies and performance bottlenecks across organizational ecosystems.

1.1. Current Landscape of Enterprise Networking Challenges

A significant paradigm shift toward AI-driven management solutions has emerged in response to these challenges. As noted in the comprehensive work "Artificial Intelligence for Future Networks," intelligent systems now enable predictive maintenance, automated optimization, and advanced anomaly detection capabilities that were previously unattainable [1]. These technologies fundamentally transform how enterprise networks operate, moving from reactive management toward proactive, autonomous infrastructure that anticipates and resolves issues before they impact business operations.

* Corresponding author: Jithendra Babu Punugubati

1.2. Shift Toward AI-Driven Management Solutions

The integration of AI with network management systems represents a convergence of multiple technological domains, including machine learning, data analytics, and software-defined networking. This convergence aims to create self-regulating network ecosystems capable of adapting to changing conditions without human intervention. According to "Research of Modern Enterprise Intelligent System Based on Rule Engine and Workflow," rule engines and workflow automation serve as foundational elements for implementing this intelligent infrastructure [2].

1.3. Research Objectives and Methodology

The significance of intelligent infrastructure for modern enterprises extends beyond operational efficiency. Next-generation network management systems enable organizations to implement dynamic resource allocation, enhance security postures through behavioral analysis, and achieve sustainability goals through optimized energy consumption. These capabilities provide competitive advantages in increasingly digitized markets where network performance directly impacts customer experience and business outcomes.

1.4. Significance of Intelligent Infrastructure for Modern Enterprises

As enterprise environments continue to evolve toward smart building integration, AI-driven network management will play a pivotal role in orchestrating the complex interactions between physical infrastructure, digital systems, and human occupants. This orchestration requires sophisticated intent translation mechanisms that can convert high-level business objectives into granular network configurations while maintaining performance, security, and compliance requirements as highlighted in the research on enterprise intelligent systems [2].

2. Intent-Based Networking: Automating Enterprise Infrastructure

Intent-Based Networking (IBN) represents a revolutionary approach to network management, fundamentally altering how enterprise infrastructure is designed, deployed, and maintained. This paradigm shift moves networking from device-centric configuration to a business-outcome orientation, where high-level objectives automatically translate into detailed network policies and configurations.

2.1. Theoretical Foundations of Intent-Based Networking (IBN)

The conceptual framework of IBN centers on abstraction layers that separate business requirements from technical implementation details. This architecture enables non-technical stakeholders to express desired outcomes while the system handles the complexity of configuration. As outlined by A. Campanella in "Intent-Based Network Operations," the IBN model consists of four essential components: intent ingestion, translation, validation, and assurance [3]. These components work in concert to create a closed-loop system that continuously monitors network state against declared intent, automatically adjusting configurations when discrepancies emerge.

2.2. Translation Mechanisms from Business Intent to Network Configuration

The translation layer serves as the critical bridge between human-expressed intentions and machine-executable configurations. This process involves sophisticated semantic analysis to interpret business requirements and convert them into precise network policies. The translation engine must account for existing topology, available resources, and policy constraints while generating optimal configuration instructions. Similar to enterprise system implementation strategies discussed by D.M. Strong and O. Volkoff, the translation mechanisms must address both technical and organizational dimensions to ensure successful deployment [4].

2.3. Comparative Analysis of Manual vs. Intent-Driven Network Management

Traditional manual network management relies heavily on human expertise and direct device configuration, creating significant operational challenges at scale. Intent-driven approaches offer substantial advantages through automation, consistency, and error reduction. Where manual processes struggle with documentation gaps and configuration drift, IBN systems maintain a continuous alignment between intent and implementation. The automatic validation capabilities prevent misconfigurations that frequently occur in manual processes, significantly reducing potential downtime and security vulnerabilities.

Table 1 Comparison of Traditional vs. Intent-Based Network Management Approaches [3, 4]

Characteristic	Traditional Network Management	Intent-Based Network Management
Configuration Method	Device-by-device manual	Business intent translation
Abstraction Level	Low-level technical commands	High-level business outcomes
Validation	Manual post-deployment	Automated pre-deployment
Documentation	Manual, often outdated	Automated intent repository
Troubleshooting	Reactive, human-driven	Proactive, automated
Scalability	Limited by human expertise	Highly scalable
Change Implementation	Days to weeks	Minutes to hours

2.4. Case Studies of IBN Implementation in Enterprise Environments

Implementation experiences across various enterprise settings demonstrate both the transformative potential and practical challenges of adopting IBN frameworks. Organizations transitioning to intent-based models typically experience initial resistance related to skills adaptation and process changes, mirroring the implementation roadmap challenges identified by Strong and Volkoff [4]. However, successful deployments show marked improvements in operational efficiency, with network changes that previously required days now completed in minutes. The operational benefits extend beyond time savings to include enhanced security posture, improved compliance management, and greater business agility.

Campanella notes that organizations implementing IBN realize substantial benefits in optical network operations through automated path computation and dynamic resource allocation [3]. These capabilities enable networks to adapt to changing conditions without human intervention, maintaining service levels even during unexpected events. The continuous feedback loop between intent verification and network state ensures that the infrastructure remains aligned with business objectives regardless of environmental changes or evolving requirements.

3. AI-Enhanced Smart Switches: Core Building Blocks for Intelligent Networks

The evolution of enterprise network infrastructure has reached an inflection point with the integration of artificial intelligence capabilities directly into switching hardware. These AI-enhanced switches represent a fundamental advancement beyond traditional networking equipment, enabling autonomous operation and intelligent decision-making at the network edge.

3.1. Embedded AI Capabilities in Modern Switching Hardware

Modern switching platforms increasingly incorporate specialized hardware accelerators designed specifically for AI workloads. These purpose-built components enable complex computational tasks to be performed directly within the network fabric rather than requiring external processing. As highlighted in "Artificial Intelligence Hardware Design: Challenges and Solutions," the integration of AI processing units within network switches presents unique engineering challenges related to power consumption, thermal management, and computational density [5]. Despite these challenges, embedded AI capabilities enable switches to process and analyze network traffic in real-time, facilitating immediate responses to changing conditions without central coordination.

Table 2 AI Capabilities in Modern Enterprise Switches [5, 6]

Capability	Function	Network Benefit
Traffic Analysis	Real-time pattern recognition	Improved Quality of Service
Anomaly Detection	Identification of abnormal patterns	Enhanced security
Predictive Maintenance	Forecasting component failures	Reduced downtime
Dynamic Routing	Adaptive path selection	Optimized throughput
Self-Healing	Automatic recovery from failures	Increased resilience

3.2. Anomaly Detection and Traffic Optimization Algorithms

The ability to identify abnormal patterns within network traffic flows represents one of the most valuable applications of AI-enhanced switches. Advanced anomaly detection algorithms continuously monitor traffic characteristics across multiple time scales, establishing baseline behavior profiles and flagging deviations that may indicate security threats or performance issues. Research on multi-scale network traffic anomaly detection demonstrates how genetic algorithm approaches can significantly improve detection accuracy while reducing false positives [6]. These techniques enable switches to distinguish between benign traffic variations and genuine anomalies, providing security teams with actionable intelligence while minimizing alert fatigue.

3.3. Self-Healing Mechanisms During Network Failures

AI-enhanced switches exhibit remarkable resilience through self-healing capabilities that activate during network disruptions. When failures occur, these intelligent devices can automatically reroute traffic, reconfigure redundant paths, and isolate problematic segments to maintain service continuity. The self-healing process involves sophisticated decision-making algorithms that consider current network state, traffic priorities, and available resources to implement optimal recovery strategies. This autonomous response capability dramatically reduces mean time to recovery compared to traditional approaches that require manual intervention, as noted in research on AI hardware design implementations [5].

3.4. Performance Metrics and Benchmarking Methodologies

Evaluating the effectiveness of AI-enhanced switches requires specialized performance metrics that extend beyond traditional networking benchmarks. These metrics must capture not only basic forwarding performance but also learning efficiency, inference accuracy, and adaptation capabilities. Benchmarking methodologies for these devices typically incorporate synthetic traffic generation with programmed anomalies to assess detection sensitivity and false positive rates. Additionally, recovery time measurements under various failure scenarios provide insights into self-healing effectiveness. The multi-scale approach to performance evaluation outlined in traffic anomaly detection research offers a valuable framework for comprehensive assessment of these intelligent networking components [6].

The integration of AI capabilities into switching hardware represents a transformative development for enterprise networks, enabling levels of autonomy and intelligence previously unattainable. As these technologies mature, they will increasingly serve as the foundation for self-organizing, self-optimizing network infrastructures capable of adapting to changing business requirements without human intervention.

4. Energy Efficiency and Green Ethernet Standards

As enterprise networks expand in scale and complexity, their energy consumption has emerged as a critical concern from both economic and environmental perspectives. The power requirements of networking infrastructure represent a significant component of organizational energy footprints, driving interest in more efficient technologies and operational practices.

4.1. Power Consumption Challenges in Enterprise Networks

Enterprise network infrastructure presents unique energy efficiency challenges due to its distributed nature, continuous operation requirements, and varied utilization patterns. Traditional network equipment was designed with performance and reliability as primary considerations, often at the expense of power efficiency. As Priya Mahadevan, et al. observe in "On Energy Efficiency for Enterprise and Data Center Networks," networking devices typically consume nearly constant power regardless of traffic load, creating substantial energy waste during periods of low utilization [7]. This inefficiency is compounded by overprovisioning practices common in enterprise environments, where networks are dimensioned for peak demands that occur infrequently.

4.2. Dynamic Power Adjustment Technologies in Switching Infrastructure

Modern enterprise switches incorporate several dynamic power adjustment technologies that enable energy consumption to scale with actual network utilization. These capabilities include adaptive link rate switching, intelligent port hibernation, and dynamic packet buffering. The IEEE 802.3az Energy Efficient Ethernet (EEE) standard, as detailed by Ken Christensen, et al., introduced the Low Power Idle (LPI) technique that allows physical layer devices to enter sleep states during inactive periods while maintaining link status [8]. This innovation represents a fundamental departure from previous approaches where links remained fully powered regardless of activity levels.

4.3. Implementation Strategies for Green Ethernet Standards

Successful implementation of green Ethernet standards requires holistic strategies that address technology deployment, operational practices, and organizational policies. At the technical level, enterprises must carefully evaluate equipment compatibility and feature support across their infrastructure to ensure seamless operation of energy-saving functions. Operational considerations include traffic engineering to consolidate flows during off-peak periods, enabling more equipment to enter low-power states. As highlighted in research on energy efficiency for enterprise networks, policy frameworks should establish clear power management governance, including monitoring requirements and escalation procedures for performance issues [7].

4.4. Quantitative Analysis of Energy Savings in Smart Building Deployments

The integration of energy-efficient networking technologies within smart building environments yields compound benefits through interaction with other building systems. When networking infrastructure incorporates green Ethernet standards, it not only reduces direct energy consumption but also enables more sophisticated building automation capabilities. These capabilities include occupancy-based network provisioning, where network resources dynamically adjust to building usage patterns. The Energy Efficient Ethernet approach described by Christensen, et al. provides a foundation for these advanced integration scenarios by ensuring that network interfaces can transition between power states without disrupting critical building management communications [8].

Energy efficiency considerations have evolved from peripheral concerns to central design principles in enterprise networking. As organizations increasingly prioritize sustainability objectives and operational cost reduction, green Ethernet standards and related technologies will continue to advance, further reducing the environmental impact of network infrastructure while maintaining the performance and reliability expected in enterprise environments.

5. Digital Twin Modeling and Cyber-Physical Security

The convergence of physical infrastructure with digital systems has created new paradigms for network management and security in enterprise environments. Digital twin modeling and cyber-physical security approaches address the unique challenges that emerge when networking infrastructure becomes deeply integrated with building automation systems and Internet of Things (IoT) devices.

5.1. Digital Twin Applications for Network Simulation in Building Automation

Digital twin technology provides virtualized representations of physical network infrastructure, enabling sophisticated simulation and predictive analytics capabilities. In building automation contexts, these virtual models capture the complex interactions between networking equipment, sensors, actuators, and control systems. As described by Gary Hildebrandt, et al. in "Data Integration for Digital Twins in Industrial Automation," successful implementation requires comprehensive data integration strategies that harmonize information from disparate sources [9]. These digital replicas allow network administrators to simulate configuration changes, predict performance impacts, and identify potential issues before deployment in production environments. For building automation systems, digital twins support scenario planning for varied occupancy patterns, environmental conditions, and usage requirements without disrupting operational networks.

Table 3 Digital Twin Applications in Enterprise Network Management [9]

Application	Purpose	Operational Benefit
Configuration Testing	Validate changes before deployment	Reduced implementation risks
Capacity Planning	Model future network requirements	Optimized investments
Failure Simulation	Test recovery mechanisms	Enhanced disaster preparedness
Performance Optimization	Identify bottlenecks virtually	Improved user experience
Security Analysis	Evaluate defensive measures	Strengthened protection

5.2. Wireless Mesh Integration with Enterprise Switching for IoT Coverage

The proliferation of IoT devices in smart buildings has created connectivity challenges that traditional wired network architectures struggle to address efficiently. Wireless mesh networking offers complementary capabilities that extend

coverage to areas where wired infrastructure is impractical while providing the redundancy essential for mission-critical applications. The integration of mesh networks with enterprise switching infrastructure requires sophisticated orchestration mechanisms to maintain consistent security policies, quality of service parameters, and management visibility across heterogeneous network segments. This hybrid approach creates comprehensive coverage for IoT devices throughout building environments while leveraging the performance and security advantages of traditional switching infrastructure for core network functions.

5.3. Emerging Threats to Enterprise Switch Infrastructure

As enterprise switching infrastructure becomes more intelligent and interconnected, its attack surface expands correspondingly. GEORGIOS MICHAIL MAKRAKIS, et al. document in "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents" how sophisticated threat actors increasingly target network infrastructure as both an attack vector and primary objective [10]. Modern switches face threats ranging from firmware compromise and configuration manipulation to side-channel attacks that exploit hardware vulnerabilities. The integration of switches with building automation systems introduces additional risks related to physical access and operational technology protocols that were not designed with robust security features. These emerging threat vectors require comprehensive defense strategies that address both conventional cybersecurity concerns and the unique vulnerabilities introduced by cyber-physical system integration.

5.4. Dynamic Security Protocols Based on Contextual Factors

Traditional static security models have proven inadequate for protecting modern enterprise switching infrastructure, particularly in smart building environments where operating conditions and threat landscapes constantly evolve. Dynamic security protocols that adapt protection mechanisms based on contextual factors offer more effective defense capabilities. These adaptive approaches consider variables including physical location, behavioral patterns, and temporal context when making access control decisions and applying security policies. As highlighted in research on industrial and critical infrastructure security, context-aware security models can detect anomalous patterns that might indicate compromise even when individual actions appear legitimate in isolation [10]. Implementation of these dynamic protocols requires integration between physical access systems, network monitoring platforms, and identity management infrastructure to create comprehensive security contexts for decision-making.

The integration of digital twin modeling with adaptive security approaches represents a promising direction for addressing the complex challenges of enterprise network management in smart building environments. By creating virtual replicas of physical infrastructure and implementing context-aware security protocols, organizations can enhance both operational efficiency and security posture while supporting the advanced automation capabilities essential for next-generation smart buildings.

6. Conclusion

The evolution of enterprise networking infrastructure has reached a pivotal transformation point through the convergence of artificial intelligence, intent-based systems, and cyber-physical integration. These technological advancements collectively establish the foundation for autonomous, self-regulating network ecosystems essential for next-generation smart buildings. Intent-based networking fundamentally shifts management paradigms from technical configuration to business outcome orientation, enabling non-technical stakeholders to drive network behavior through high-level objectives. AI-enhanced switches serve as intelligent nodes capable of anomaly detection, traffic optimization, and self-healing during disruptions, dramatically reducing the need for human intervention while improving operational resilience. The integration of green Ethernet standards addresses critical sustainability concerns through dynamic power management capabilities that adapt energy consumption to actual utilization patterns. Digital twin modeling provides powerful simulation environments for predicting network behavior under varied conditions, supporting proactive optimization without risking production environments. These innovations must be secured through adaptive protection mechanisms that consider contextual factors when implementing security policies, safeguarding the increasingly critical infrastructure from emerging threats. Looking forward, the continued evolution toward fully autonomous network ecosystems promises unprecedented levels of agility, efficiency, and resilience—fundamental requirements for sustainable, intelligent infrastructure in the interconnected enterprise environments of tomorrow.

References

[1] Mohammad A. Matin, et al., "Artificial Intelligence for Future Networks," Wiley-IEEE Press, 2025. https://ieeexplore.ieee.org/book/10811668

[2] Liu Chen, et al., "Research of Modern Enterprise Intelligent System Based on Rule Engine and Workflow," IEEE International Conference on Intelligent Computing and Intelligent Systems, December 6, 2010. https://ieeexplore.ieee.org/abstract/document/5658451

[3] A. Campanella, "Intent-Based Network Operations," Optical Fiber Communications Conference and Exhibition (OFC), April 25, 2019. https://ieeexplore.ieee.org/abstract/document/8696962/authors#authors

[4] D.M. Strong and O. Volkoff, "A Roadmap for Enterprise System Implementation," Computer (Volume 37, Issue 6), 30 June 2004. https://ieeexplore.ieee.org/abstract/document/1306380

[5] Albert Chun-Chen Liu and Oscar Ming Kin Law, "Artificial Intelligence Hardware Design: Challenges and Solutions," Wiley-IEEE Press, 2021. https://ieeexplore.ieee.org/book/9536220

[6] Yiping Chen and Fengshan Yuan, "Multi-Scale Network Traffic Anomaly Detection Based on Improved Genetic Algorithm," IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), 06 April 2022. https://ieeexplore.ieee.org/document/9744988

[7] Priya Mahadevan, et al., "On Energy Efficiency for Enterprise and Data Center Networks," IEEE Communications Magazine (Volume 49, Issue 8), August 11, 2011. https://ieeexplore.ieee.org/document/5978421/references#references

[8] Ken Christensen, et al., "IEEE 802.3az: The Road to Energy Efficient Ethernet," IEEE Communications Magazine, September 30, 2010. https://cse.usf.edu/~kchriste/energy/commMag10b.pdf

[9] Gary Hildebrandt, et al., "Data Integration for Digital Twins in Industrial Automation," IEEE Access, September 24, 2024. https://ieeeaccess.ieee.org/featured-articles/dataintegration_digitaltwins/

[10] GEORGIOS MICHAIL MAKRAKIS, et al., "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," IEEE Access, 2021. https://ieeexplore.ieee.org/ielaam/6287639/9312710/9638617-aam.pdf