Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

The impact of intent-based networking on network configuration management and security

Adeola Adewa [1,*], Vincent Anyah [2], Omoniyi David Olufemi [1], Adedeji Ojo Oladejo [1] and Toluwanimi Olaifa [3]

[1] *J. Warren McClure School of Emerging Communication Technologies, Ohio University, Athens, Ohio, USA.*
[2] *Department of Computer Science, New Mexico Highlands University Las Vegas, New Mexico, USA.*
[3] *Information Technology Department, Softbrooks, Sheridan, Wyoming, USA.*

Global Journal of Engineering and Technology Advances, 2025, 22(01), 063-068

Publication history: Received on 03 December 2024; revised on 12 January 2025; accepted on 14 January 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.22.1.0012

Abstract

Intent-based networking (IBN) has emerged as a transformative paradigm in network management, revolutionizing how networks are configured, monitored, and secured. By leveraging artificial intelligence (AI) and machine learning (ML), IBN translates high-level business objectives into automated network configurations, ensuring that operational intents are consistently achieved. This paper explores the profound impact of IBN on network configuration management and security.

Firstly, we examine how IBN streamlines network configuration through automation, reducing manual intervention and mitigating configuration errors, which are among the leading causes of network outages. IBN's ability to validate intents against real-time network states ensures that configurations align with business policies, enabling agile and reliable network operations.

Secondly, the role of IBN in enhancing network security is analyzed. By continuously monitoring network behavior against predefined intents, IBN systems can detect and respond to anomalies or potential threats in real time. This proactive approach minimizes the window of vulnerability and ensures compliance with security policies. Furthermore, the use of AI-driven insights facilitates predictive threat management and adaptive security measures.

Finally, we discuss the challenges and future prospects of adopting IBN, including the integration with legacy systems, the reliance on accurate intent definitions, and the need for robust AI models. The findings underscore that IBN not only simplifies network management but also fortifies network defenses, making it a cornerstone of modern, resilient network architectures.

Keywords: Intent-Based Networking (IBN); Network Configuration Management (NCM); Artificial Intelligence (AI); Machine Learning (ML)

1. Introduction

In today's rapidly evolving digital landscape, businesses face increasing demands for agility, scalability, and security within their network infrastructures. Traditional network management methods, heavily reliant on manual configurations and complex command-line interfaces, struggle to keep pace. These methods are often time-consuming, error-prone, and ill-equipped to handle the dynamic needs of modern applications and cloud environments.

* Corresponding author: Adeola Adewa

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

Intent-Based Networking (IBN) emerges as a transformative paradigm that shifts the focus from low-level device configurations to high-level business intents. Instead of meticulously configuring individual devices and their interconnections, network engineers can express their desired network behavior using simple, declarative statements. For example, an IBN system can understand intents such as "ensure application X has low-latency access to service Y" or "prioritize critical traffic during peak hours."[1] Unlike traditional approaches, which rely heavily on manual configurations and rule-based systems, IBN integrates AI and ML to ensure that network behavior dynamically adapts to changing demands[2]. This integration enhances network agility, reduces operational complexity, and improves overall performance.

Network configuration management (NCM) and security are essential for ensuring stable and secure communication in modern networks. Traditionally, these processes have relied on manual configurations and rule-based security measures. However, with the growing complexity of network environments—driven by factors like cloud computing, IoT, and 5G—manual methods have become insufficient [3,4].

2. Network Configuration Management

2.1. Definition and Importance

Network configuration management ensures that devices in a network, such as routers and switches, are correctly configured to support efficient operation. The goal is to avoid inconsistencies, misconfigurations, and ensure that network resources are optimized for performance and security [5].

2.2. Challenges in Traditional Network Configuration

Traditional network configuration, characterized by manual and static methods, has long been the standard approach for managing network infrastructure. However, this method faces numerous challenges that limit its efficiency, scalability, and adaptability in the rapidly evolving technological landscape. Modern dynamic networks require more agile and scalable solutions to keep pace with changing conditions.

2.2.1. Manual Configuration Errors

Manual configuration is prone to human error, which is a significant cause of network downtime, security vulnerabilities, and performance issues. Even experienced network engineers can make mistakes while entering or modifying configurations. These errors often require extensive troubleshooting, consuming valuable time and resources. [6]

2.2.2. Time-Consuming Processes

Manually configuring individual devices in a network is labor-intensive and time-consuming. The deployment of new devices or updates across a network, especially in large-scale setups, can result in significant delays. This inefficiency hampers an organization’s ability to adapt quickly to changing requirements.

2.2.3. Lack of Scalability

Traditional configuration methods struggle to scale efficiently as networks grow in size and complexity. Adding or modifying devices and services becomes increasingly challenging, requiring more effort and expertise to maintain consistent operations.

2.2.4. Static Configurations

Static configurations in traditional networks lack the flexibility to adapt to dynamic workloads or evolving requirements. This rigidity makes it difficult to respond to real-time demands, scale resources up or down, or optimize performance in response to shifting needs.

2.2.5. Limited Visibility and Monitoring

Traditional tools for monitoring and managing network performance often provide limited visibility. This lack of comprehensive, real-time insights can delay the detection and resolution of issues, resulting in suboptimal resource utilization and prolonged downtimes.

2.2.6. Security Vulnerabilities

Manual processes make it challenging to enforce consistent security policies across the network. Inconsistent configurations can create vulnerabilities, exposing the network to potential threats and attacks. Moreover, traditional networks often lack the advanced tools needed to monitor and mitigate security risks effectively.

2.2.7. High Operational Costs

The significant time and resources required for manual configuration and maintenance lead to higher operational costs. Frequent errors and prolonged downtimes further exacerbate financial losses, making traditional methods less economically viable in the long term.

2.2.8. Vendor-Specific Dependencies

Traditional networking approaches often rely on proprietary hardware and software, resulting in vendor lock-in. This dependency limits flexibility increases costs and makes it challenging to integrate solutions from multiple vendors.

2.2.9. Incompatibility with Modern Applications

Many traditional networks are not optimized to support the demands of modern applications such as cloud computing, virtualization, and containerized services. These applications require a dynamic and scalable network infrastructure, which static traditional methods cannot provide efficiently. [9]

2.2.10. Difficulty in Implementing Automation

Legacy systems are often incompatible with modern automation tools and frameworks, making it difficult to implement automation in traditional network setups. Integrating automation requires significant effort and investment, further delaying modernization efforts.

3. Impact of Intent-Based Networking on Network Configuration Management

3.1. Intent-Based Networking

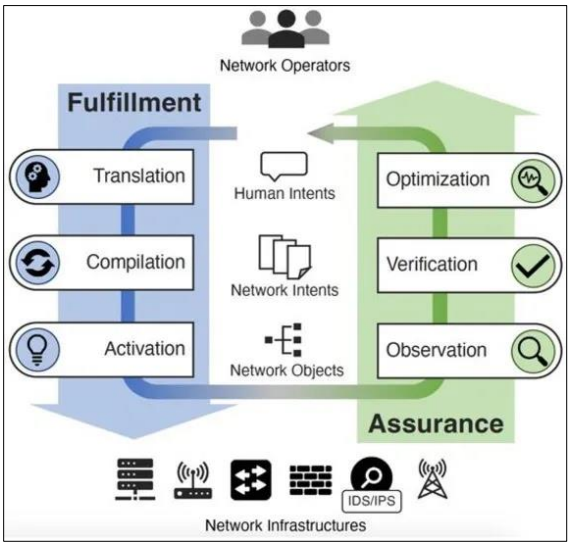

Figure 1 Intent lifecycle within IBN. The lifecycle includes two main stages, *fulfillment*, and *assurance*, that ultimately form a feedback loop toward automated, semantically rich network functionality

Intent-based networking is a software-driven approach to automation that relies on advanced intelligence, analytics, and orchestration to optimize network performance and reliability. Instead of manually configuring individual tasks, operators define the desired business outcomes, and the network autonomously generates and applies the necessary configurations to achieve those goals.

For example, consider the need for secure communications between two networks. An *intent* would broadly state that a secure tunnel is needed between Network A and Network B. An operator would identify which traffic should use the

tunnel and describe any other desired general properties of the tunnel(*what*). However, the operator wouldn't specify *how* the tunnel is to be implemented, such as the number of devices to be used, how BGP advertisements should be made, or which specific features and parameters to turn on[7]. The intent follows a lifecycle at a high level as shown in figure 1.

3.2. Intent Translation and Automation

IBN systems translate high-level business intents (e.g., "ensure seamless video conferencing") into actionable network policies. These policies are then automatically implemented and validated across the network, reducing manual input and improving efficiency. The ultimate goal is for the network to continuously monitor and adjust network performance to ensure the desired business outcome[8]

3.3. Predictive Configuration Management

IBN enhances predictive analytics by ensuring configurations align with defined intents. This capability allows for proactive adjustments to prevent potential network failures or congestion before they arise.

3.4. Self-Optimizing Networks

Intent-Based Networking (IBN) enables self-optimizing networks by leveraging automation, machine learning (ML), and artificial intelligence (AI) to dynamically adjust network configurations in real-time. These capabilities ensure that all optimizations are precisely aligned with organizational intents, creating a seamless, adaptive, and resilient network environment.

Through its intelligent framework, IBN translates high-level business goals into actionable policies that the network continuously enforces and monitors. By integrating advanced telemetry and predictive analytics, IBN-powered networks proactively identify performance bottlenecks, potential failures, or security vulnerabilities, taking corrective actions before they impact operations[9]

4. Network Security Challenges

4.1. Current Threat Landscape

Modern network environments are vulnerable to increasingly sophisticated cyber threats, such as DDoS attacks, malware, and insider threats. These threats are difficult to manage with traditional rule-based security systems, which can struggle to detect emerging attack patterns [10].

4.2. Challenges in Traditional Network Security

Traditional security approaches rely heavily on predefined rules and known threat signatures. This makes them effective against known threats but less so against new, evolving attack vectors. Additionally, the sheer volume of network traffic makes it challenging for human analysts to monitor and respond to threats in real time.

5. Impact of Intent-Based Networking on Network Security

5.1. Intent-Centric Threat Mitigation

Intent-Based Networking (IBN) enhances security by ensuring that threat detection mechanisms are closely aligned with overarching security intents, such as "protect sensitive customer data." By translating high-level intents into dynamic, automated security policies, IBN creates a more adaptive and context-aware defense system. This approach enables organizations to proactively identify and mitigate threats, ensuring that security measures are consistently aligned with business objectives and compliance requirements. As a result, IBN facilitates a more resilient and responsive security posture.

5.2. Real-Time Compliance and Adaptation

Intent-Based Networking (IBN) enables dynamic enforcement of security policies, ensuring continuous compliance with defined security intents, such as data protection and regulatory adherence. By translating high-level security objectives into network policies, IBN can automatically adjust network configurations to maintain these objectives. Furthermore, IBN systems are capable of detecting deviations from these intents in real-time, rapidly identifying and rectifying misconfigurations or breaches. This proactive, automated approach allows organizations to swiftly adapt to emerging

threats, enhancing their overall security posture while ensuring compliance with evolving security standards and regulation.

5.3. Enhanced Incident Response

Intent-Based Networking (IBN) integrates seamlessly with AI-driven incident response systems to enhance real-time threat mitigation. By aligning network behavior with predefined security intents, IBN ensures that responses to threats are not only automated but also contextually appropriate. For instance, when a part of the network is compromised, IBN can dynamically isolate that segment, preventing the spread of malicious activity. Similarly, IBN can leverage AI to identify and block malicious traffic in real-time, dramatically reducing response times and minimizing the impact of an attack. This combination of IBN and AI allows organizations to maintain a proactive security posture, swiftly adapting to new threats while preserving the integrity of the network.

6. Benefits of Intent-Based Networking in Network Configuration and Security

6.1. Improved Efficiency and Accuracy

Intent-Based Networking (IBN) leverages automation to significantly improve the efficiency and accuracy of both network configuration and security management. By eliminating the need for manual intervention in routine tasks, IBN reduces the likelihood of human error, ensuring that network configurations and security policies are consistently applied and up to date. This automation allows for the rapid adaptation of networks to changing conditions, such as shifting security threats or evolving business requirements, while maintaining compliance with predefined security intents. As a result, organizations benefit from more reliable and secure network environments, with reduced administrative overhead and faster response time.

6.2. Scalability

IBN simplifies scaling across large, complex networks by translating high-level business intents into network-wide policies while ensuring operational complexities are managed seamlessly.

6.3. Adaptive Security

IBN enables proactive, adaptive security measures by continuously enforcing security intents and dynamically adjusting to evolving threats, helping prevent cyberattacks before they can cause damage.

7. Future Trends and Developments

7.1. Autonomous Networks

As Intent-Based Networking (IBN) advances, it paves the way for fully autonomous networks. These networks can self-configure, self-optimize, and self-heal in real-time, adapting to changing conditions without requiring manual intervention. This evolution leads to more reliable and efficient networks by minimizing human error, speeding up response times, and improving overall network performance and resilience. Integrating IBN into these networks will result in further automation, reducing operational overhead and enhancing network agility[11,14]

7.2. IBN in 5G and Beyond

Intent-Based Networking (IBN) will be essential in managing the complexity of 5G networks by optimizing performance, handling the influx of connected devices, and securing the network infrastructure. With 5G introducing higher data speeds, lower latencies, and massive device connectivity, IBN can automate network configurations and ensure seamless operations. As the industry moves toward 6G and quantum networks, IBN's role will only grow in importance [12]. It will be crucial in managing the increasing complexity and scale of these networks, ensuring they remain secure, efficient, and capable of meeting evolving demands for speed, connectivity, and performance

7.3. Zero Trust Architectures

It enhances Zero Trust security models by dynamically verifying and enforcing trustworthiness throughout the network. It ensures that access is granted only to verified users and devices, continuously monitoring and validating their identity, behavior, and security posture. This approach minimizes the risk of unauthorized access by applying strict security policies that are consistently enforced across the network, ensuring that no entity, inside or outside the

network, is automatically trusted[13]. With IBN, the Zero Trust model becomes more effective by automating the enforcement of access policies and providing real-time insights into network activity and security threats.

8. Conclusion

Intent-based networking is reshaping both network configuration management and network security. IBN significantly enhances network performance and security by automating routine tasks, enabling predictive maintenance, and improving real-time threat detection. As networks become more complex with the rise of 5G and beyond, IBN will be indispensable in ensuring that networks remain efficient, scalable, and secure. The future promises even more advancements, with autonomous networks and IBN-driven security systems paving the way for a new era in network management.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] A. Leivadeas and M. Falkner, "A Survey on Intent-Based Networking," in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 625-655, First quarter 2023, doi: 10.1109/COMST.2022.3215919.

[2] Falkner, Matthias & Apostolopoulos, John. (2022). Intent-based networking for the enterprise: a modern network architecture. Communications of the ACM. 65. 108-117. 10.1145/3538513.

[3] Clemm, A. (2021). Intent-Based Network Management. In: Toy, M. (eds) Future Networks, Services and Management. Springer, Cham. https://doi.org/10.1007/978-3-030-81961-3_14

[4] S. Minhas, R. Jaswal, A. Sharma and S. Singla, "Revolutionizing Networking: A Comprehensive Overview of Intent-Based Networking," 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP), Sonipat, India, 2024, pp. 463-468, doi: 10.1109/INNOCOMP63224.2024.00081.

[5] Steven M. Bellovin and Randy Bush. Configuration management and security. IEEE Journal on Selected Areas in Communications, 27(3):268--274, April 2009

[6] Liu, Fanglin & Kibalya, Godfrey & Kumar Svn, Santhosh & Zhang, Peiying. (2022). Challenges of Traditional Networks and Development of Programmable Networks. 10.1007/978-3-030-89328-6_3.

[7] Juniper Networks, "What Is Intent-Based Networking" (2025), online: Juniper Networks https://www.juniper.net/us/en/research-topics/what-is-intent-based-networking.html.

[8] Yiming Wei, Mugen Peng, Yaqiong Liu, "Intent-based networks for 6G: Insights and challenges" Digital Communications and Networks, Volume 6, Issue 3,2020,

[9] Zeydan, Engin & Turk, Yekta. (2020). "Recent Advances in Intent-Based Networking: A Survey". 1-5. 10.1109/VTC2020-Spring48590.2020.9128422.

[10] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010, pp. 305-316

[11] Mahdi MF, Mahmoud MS. A Structured Literature Review of Intent Based Network for Future Networks. Journal of Optoelectronics Laser. 2022 Apr 30;41(4):677-84.

[12] Rychlik A. The IBN Networks for 6G Technology to Optimize Investments in Telecommunications Infrastructure. In Proceedings of the International Scientific and Practical Conference, Intellectual Systems and Information Technologies, Odessa, Ukraine 2021 Sep 13.

[13] Rivera JJ, Afaq M, Song WC. Blockchain and intent-based networking: A novel approach to secure and accurate network policy implementation. In2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS) 2023 Sep 6 (pp. 77-82). IEEE

[14] Jacobs AS, Pfitscher RJ, Ferreira RA, Granville LZ. Refining network intents for self-driving networks. InProceedings of the Afternoon Workshop on Self-Driving Networks 2018 Aug 7 (pp. 15-21).