Enterprise Networking Trends and Evaluation of AI Assistants

Pavel Segeč
Department of Information Networks
Faculty of Management Science and Informatics
University of Žilina
Žilina, Slovakia
pavel.segec@fri.uniza.sk

Jana Uramová
Department of Information Networks
Faculty of Management Science and Informatics
University of Žilina
Žilina, Slovakia
Jana.Uramová@fri.uniza.sk

Patrik Grexa
Department of Information Networks
Faculty of Management Science and Informatics
University of Žilina
Žilina, Slovakia
grexa@stud.uniza.sk

Marek Moravčík
Department of Information Networks
Faculty of Management Science and Informatics
University of Žilina
Žilina, Slovakia
Marek.Moravcik@fri.uniza.sk

Jozef Papán
Department of Information Networks
Faculty of Management Science and Informatics
University of Žilina
Žilina, Slovakia
Jozef.Papan@fri.uniza.sk

2025 International Conference on Emerging eLearning Technologies and Applications (ICETA) | 979-8-3315-7426-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICETA67772.2025.11280233

***Abstract*— Enterprise networking is rapidly evolving under the influence of cloud adoption, software-defined infrastructures (SDx), and artificial intelligence (AI). Although solutions addressing network automation and security frameworks, such as SD-WAN and SASE, have received attention, the practical role of AI assistants in network engineering tasks seems interesting too, despite their potential to augment configuration, monitoring, and troubleshooting processes. This paper investigates the intersection of enterprise network design trends and AI-driven support tools. First, we review actual architectural principles of wired and wireless LAN, cloud integration, and emerging models such as SASE/SSE. Then, we propose an evaluation framework to test five AI assistants (ChatGPT, Copilot, Gemini, Grok, and DeepSeek) in two key tasks: generating Cisco access switch configurations and interpreting CLI show outputs. Our results demonstrate varying levels of correctness and usability, with some models producing near-flawless configurations and reliable analysis, while others remain inconsistent. The findings highlight both the opportunities and limitations of current AI assistants, offering insight into their potential integration into enterprise network operations. Finally, we discuss implications for future research in AI-powered automation, anomaly detection, and digital twin approaches in enterprise networks.**

Keywords—Network Operative, Trends, Design, AI Assistants, Enterprise Network

I. INTRODUCTION

Modern organizations are built on enterprise networks, which provide them with safe, effective data exchange and communication abilities. Traditional hierarchical design, typically structured into access, distribution, and core layers, is evolving with the onset of modern software-defined paradigms, like Software-Defined Access, WAN Networks (SDN-Access, SD-WAN), and Secure Access Service Edge (SASE). These frameworks combine centralized policy enforcement with distributed connectivity and improve scalability, performance, and network security. However, the wide adoption of modern digital technologies, such as cloud and edge computing, has introduced new challenges that require enterprises to evolve classical design principles and operational practices.

At the same time, new trends such as Artificial Intelligence (AI) and machine learning (ML) are increasingly recognized as important enablers of network automation and resilience. Their adoption has the potential to reduce downtime and improve network operational maintenance and efficiency. AI-driven orchestration with emerging concepts such as intent-based networking and digital twins indicates a shift that has the potential to significantly transform long-held design principles and open doors for fresh concepts.

Although solutions addressing network automation and security frameworks, such as SD-WAN and SASE, have received considerable attention [1], the practical role of AI assistants in network engineering tasks seems overlooked, despite their potential. This gap is particularly relevant given the rapid progress of general-purpose AI assistants that claim applicability across technical domains. A systematic evaluation of their capabilities in networking tasks is therefore timely and necessary.

The paper aims to contribute to the field of enterprise network design trends with emphasis on LAN/WLAN architecture, cloud integration, and emerging frameworks such as SD-WAN and SASE/SSE. We highlight current trends in enterprise networking and the growing role of AI in automation and monitoring. We then propose a lightweight evaluation framework for assessing AI assistants in practical tasks, empirically evaluating five AI assistants, ChatGPT, Copilot, Gemini, Grok, and DeepSeek, on their ability to generate access-switch configurations and interpret show CLI outputs. Finally, we discuss observed strengths, limitations, and implications for integrating AI assistants into enterprise network operations.

Respecting this intention, the test of the article is organized as follows. Section II introduces enterprise network design trends. Section III reviews current trends and AI-driven operations in enterprise networking. Section IV presents the evaluation framework and results, discussing findings and implications. In Section V, we conclude the paper with directions for future research.

Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:33:37 UTC from IEEE Xplore. Restrictions apply.

II. ENTERPRISE NETWORKING: TRENDS

Enterprise networks are the basis of critical infrastructures that support the transport and control of information across organizational boundaries. Their design is not limited to providing connectivity, but also to ensuring confidentiality, integrity, and availability of transmitted data. The design phase directly reflects the operational demands placed on such networks: high reliability, predictable performance, and strong security enforcement. These requirements make network design a structured engineering discipline rather than an ad-hoc deployment activity.

In practical terms, enterprise network design represents the process of planning and implementing IP-based infrastructures to achieve performance objectives while allowing the network to scale and remain manageable over time [1]. Centralized models, common in earlier enterprise deployments, simplified administration but introduced architectural weaknesses. They created single points of failure and constrained flexibility, which limited the ability of enterprises to adopt new services or expand geographically. Current and widely used practice has moved to layered architectures composed of access, distribution, and core [3]. Each layer fulfills a distinct role. The access layer terminates end devices and enforces local access policies. The distribution layer aggregates multiple access blocks, provides routing, and redundancy. The core is optimized for speed and resiliency, ensuring low-latency transport and minimizing the impact of failures. This segmentation improves operational clarity, facilitates troubleshooting, and increases fault tolerance, since redundant elements in one layer can replace failing devices without affecting the entire network.

The layered model also enables integration with modern paradigms such as virtualization, Software-Defined Networking (SDN) applied to local (SDN-LAN/Access), wide (SD-WAN), or WiFi networks (SDN-WiFi). By separating functional roles, the architecture allows incremental adoption of new technologies without redesigning the entire network. Cloud services, dynamic traffic management, and identity-driven security policies can be integrated consistently. As a result, the layered design not only addresses availability but also provides the structural basis for incorporating cloud and software-defined solutions.

These principles define the baseline of enterprise networking. In the following sections, we discuss how wired and wireless LAN, SD-WAN, and SASE/SSE frameworks are applied in practice. They represent the foundation upon which further automation and AI-assisted operations may be introduced in enterprise environments [1] [2].

A. Wired and Wireless LAN design considerations

Wired and wireless local area networks represent the essential access infrastructure in enterprises. Their design influences not only local performance, but also the scalability and manageability of the whole enterprise system. Wired and wireless LANs form a combined access platform that must support redundancy, security, and integration with cloud services. Modern designs prefer Layer 3 to the access layer, stacking or fabric for resilience, and unified management for wired and wireless devices. These principles prepare the ground for higher-level technologies such as SD-WAN and SASE, which extend control and security to remote and cloud environments [3].

1) Wired LAN

The wired part of the enterprise network is still the primary medium for stable and predictable transmission. In traditional deployments, access switches were connected at Layer 2, aggregated by a distribution layer, and then forwarded into the core. Such designs required a spanning tree and introduced complexity when multiple closets or redundant uplinks were present. Current practice moves Layer 3 boundaries closer to the access layer. This reduces dependence on spanning tree reconvergence, improves convergence time after failure, and enables the use of equal-cost multipath routing for better bandwidth utilization.

Stacking technologies are commonly applied at both access and distribution. Multiple switches operate as one logical unit, providing simplified configuration and faster recovery in case of hardware failure. For large campus networks, fabric-based architecture automates the creation of overlays, provides built-in segmentation, and optimizes traffic flows. These designs allow enterprises to meet higher demands on availability and consistency across many access domains.

2) Wireless LAN

Wireless LAN becomes the default access method for a growing portion of users and devices. Enterprise WLAN depends on the stability of the wired backhaul and uses controllers or cloud-based platforms to coordinate access points. The controller manages channel selection, roaming, authentication, and policy enforcement. In larger deployments, redundant controllers are required to avoid single points of failure. In smaller sites, simplified architecture may be sufficient, but integration with wired security controls remains necessary. Power over Ethernet (PoE/PoE+) and redundant uplinks are standard requirements to ensure the reliability of access points.

3) Cloud integration – cloud-managed LANs

Many enterprises adopt cloud-based management for both wired and wireless LAN [10]. This approach centralizes configuration and monitoring, eliminates the need for complex on-premises controllers, and enables consistent policy across distributed sites. Encrypted tunnels and certificate-based authentication ensure secure connectivity to the management plane. Cloud platforms simplify provisioning of switches and access points, and integrate with enterprise identity systems such as RADIUS, Active Directory (AD), or cloud identity providers (IAM). This allows unified enforcement of authentication and authorization policies [10].

4) Security considerations

Identity-based access control is mandatory at the LAN edge. Wired networks typically deploy IEEE 802.1X for per-port authentication, with dynamic VLAN assignment based on user or device identity. Wireless networks use WPA3-Enterprise with centralized authentication servers. Segmentation is achieved with VLANs, VRFs, or fabric overlays, and in larger deployments, microsegmentation is applied to isolate sensitive traffic. Continuous monitoring of the access layer, combined with strong authentication and segmentation, forms the basis for a secure enterprise campus.

5) LAN/WLAN: Software-defined trends

979-8-3315-7426-0/25/$31.00 ©2025 IEEE

Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:33:37 UTC from IEEE Xplore. Restrictions apply.

Software-defined concepts are increasingly applied in enterprise LAN and WLAN. Traditional designs depend on device-by-device configuration, which increases complexity and limits flexibility. SD-LAN and software-defined wireless networking (SD-WiFi) shift control to a centralized platform, separating control and data planes and enabling consistent policy enforcement [12].

In a wired LAN, software-defined concepts are applied to unify configuration and policy across access switches. Central controllers, such as Cisco DNA Center or Aruba Central, automate VLAN and routing configuration, enforce segmentation, and provide visibility of connected devices. Functions like automated provisioning, dynamic role assignment, and policy-based traffic steering reduce manual effort and minimize configuration errors. These capabilities allow consistent operation across large campus deployments and simplify integration with higher-layer services such as SD-WAN or SASE.

In WLAN, SDN principles allow centralized orchestration of access points. Controllers or cloud-based systems manage radio resources, roaming, and security enforcement. Advanced features include traffic engineering, load balancing, and network slicing for different applications. Features such as identity-driven access and microsegmentation improve security in dense environments such as campuses or healthcare facilities.

B. Software Defined WAN (SD-WAN)

SD-WAN is a modern way to manage and operate wide-area networks. Instead of configuring each branch router separately, the system is controlled from a central platform. This platform enables administrators to centrally define routing intent, security policies, and quality parameters, and then distribute them to devices located at multiple branches. One important function of SD-WAN is application-aware routing. The system monitors transport parameters such as delay, jitter, and packet loss and selects the best available path for each traffic flow. Real-time traffic-like voice or video is usually placed on a stable, low-latency link, while non-critical data can use cheaper broadband connections. Security is directly included in SD-WAN design principles. Tunnels between sites are encrypted, and segmentation separates business-critical services from guest or different types of traffic. Firewall functions and intrusion detection are often part of advanced SD-WAN platforms. Another important point is support for local internet breakout. When branch traffic goes directly to the internet, latency to cloud services is reduced compared to traditional backhauling through a central data center.

To integrate SD-WAN into enterprise infrastructure, the central controller and management nodes need to be deployed in a highly available way. Vendors provide this in the cloud or in redundant on-premises sites. Edge devices located in branch offices or data centers connect to multiple WAN transports such as MPLS, broadband, or LTE/5G.

Large-scale use of SD-WAN depends on automation. Zero-touch provisioning is often applied so that new devices can be shipped to remote sites and configured automatically after connecting to the controller. Many enterprises also extend the SD-WAN fabric into the public cloud. Virtual edges apply the same routing and security policies to workloads hosted in cloud environments [1][4].

C. Secure Access Service Edge (SASE) / Security Service Edge (SSE)

Secure Access Service Edge (SASE) is a model that combines wide-area connectivity with security functions delivered from the cloud. It typically leverages SD-WAN for networking, but other WAN technologies may also be used, together with a set of cloud-based security services known as Security Service Edge (SSE). The idea is that users and devices, regardless of location, connect to applications through a cloud point of presence where policy is enforced. SSE includes several components. A Secure Web Gateway (SWG) filters traffic at the application level. Firewall-as-a-Service (FWaaS) replaces or complements on-premises firewalls. Cloud Access Security Broker (CASB) inspects traffic to SaaS platforms and enforces data policies. Zero Trust Network Access (ZTNA) provides identity and context-based access instead of a traditional VPN (Virtual Private Network). These services together create a unified enforcement layer close to the user or device.

The design principle of SASE is cloud-first. Instead of sending all traffic back to a central site, enterprise branches and mobile users connect directly to the nearest cloud enforcement point. This reduces latency and allows a consistent policy regardless of user location. Identity is central: each connection is checked, and access is limited by role, device type, or context. For monitoring and user experience, many solutions integrate Digital Experience Monitoring (DEM). This function measures end-to-end performance and helps to detect problems before users notice them. SSE can be deployed independently of SD-WAN, but in SASE, they are integrated to provide both connectivity and security. Deploying SASE and SSE requires careful transition. Enterprises should align existing policies with cloud-delivered services and ensure redundancy of enforcement nodes. The result is a distributed architecture where networking and security are delivered together, supporting cloud adoption and hybrid work in a secure way [5][1].

D. Discussion of Architectural Principles

Based on the analyzed papers, we may note that enterprise networks are today designed by combining several approaches. The layered model with access, distribution, and core is still used. It gives structure and allows redundancy. SD-WAN adds centralized control of the WAN and application-aware routing. SASE and SSE integrate cloud-delivered security functions. These technologies together form the base design that many enterprises use.

However, other approaches are starting to influence this approach. One example is intent-based networking (IBN) that builds upon SDN principles by adding a layer of abstraction. This allows administrators to define high-level business intents of the network. The controller translates this intent into a configuration for the devices. Advanced IBN platforms leverage AI/ML to optimize policy enforcement and predict network anomalies. Today, IBN is increasingly applied in hybrid cloud environments, where dynamic policy enforcement is critical.

Another recognizable trend is the use of digital twins. A digital twin is a virtual copy of the network. Operators can test failures, new routing policies, or security rules on the twin before they are applied in production. Vendors already

Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:33:37 UTC from IEEE Xplore. Restrictions apply.

include such functions, and there is also active research in this area.

III. AI OPERATIONS IN ENTERPRISE NETWORKS: TRENDS

Today, enterprise networks must constantly adapt to new demands, such as cloud adoption, mobility, and increased security demands. Traditional architecture still forms the basis of many deployments, but operating models are changing. Centralized management remains dominant, but there is a visible shift towards distributed and software-defined approaches. Security functions are no longer deployed as separate and isolated, but are integrated directly into the network. Monitoring has moved from passive observation to proactive anomaly detection. Artificial intelligence-enabled solutions in these areas are becoming a practical reality, already part of several vendor platforms.

This chapter presents selected trends that directly affect enterprise networks. First, the role of centralized and decentralized management is discussed. Next, the convergence of security functions is introduced, where identity, policy, and traffic control are applied in a single and unified model. The third subsection examines network monitoring and how AI methods enhance the detection of anomalies and performance issues. Finally, AI operations are described with examples of automation, self-healing, and digital twin concepts in enterprise environments.

1) Network management: centralized vs. decentralized

Traditionally, enterprise network management has been centralized, where a single platform is used to manage many devices. This model simplifies operations on one side, but it also introduces risks. If a central system becomes unavailable, management functions are disrupted. Scalability is another issue, as the management must be able to process data from thousands of devices and users.

Decentralized approaches are now gaining more attention. One example is the concept of decentralized physical infrastructure networks (DePIN). In this model, management tasks are distributed among several nodes. Each node contributes resources and shares responsibility for monitoring and enforcing policies.

Trends in decentralizing artificial intelligence deployment are also being explored, where AI models run closer to the data source rather than in one central location. This can reduce latency and improve resiliency.

Finally, cloud computing plays a significant role, too. Many vendors provide their management platforms as a cloud service to achieve global reachability and redundancy. Enterprises can then use cloud controllers to manage their branch offices and remote locations without running on-premises servers.

Trends indicate that enterprises must carefully balance between centralization and a decentralized approach. Centralized management remains dominant due to the support of mature vendors. However, the shift towards distributed and cloud-native management will continue, especially as networks grow in scale and demand greater resilience [2].

2) Security Convergence

The rise of cyber-physical systems (CPS) and the widespread adoption of IoT devices have increased the demand for a unified security platform that can monitor and protect both the digital and physical domains in real time. As a result, Enterprises therefore adopt integrated security platforms that provide a single view of risks. Instead of handling events in isolation, incidents are correlated, and responses are coordinated across the infrastructure.

Cloud-based solutions play a key role in this convergence. Cloud platforms provide an easy way to update detection mechanisms in real time. Through a central cloud service, we can distribute new signatures, policies, and analytics to all connected devices more easily. This reduces the response time needed to solve emerging threats.

Artificial intelligence is also a further security convergence driver. ML models are applied to both network traffic and system protocols. They are also used in automated incident response (SOAR), where predefined actions are taken immediately after an attack is detected. Integrating AI with security information and event management (SIEM) systems. Altogether, it improves event correlation and increases the complex security overview. The principle of zero trust also supports a paradigm shift. Combined with AI-based analytics and cloud-based enforcement, it creates a more robust security posture.

As a final note, the network security convergence is therefore not just a technical improvement, but a new operating model. By integrating digital and physical domains, leveraging AI for detection and response, and applying zero trust principles, enterprises can create security frameworks that are comprehensive and resilient in a rapidly changing threat landscape [7].

3) Monitoring

Monitoring is a basic function in network operations, but the character of monitoring has changed over time. In the past, monitoring was passive. Systems collected SNMP counters, interface statistics, or syslog events, and operators checked dashboards. Such monitoring was reactive, and problems were often detected only after users reported issues. Modern enterprise networks require more proactive methods. With the growth of cloud, mobility, and IoT, the number of devices and applications has become large, which makes manual checking impossible. Monitoring must provide early warning and automatic analysis. Granularity is also important; network operators expect visibility not only at the device level but also at the level of flows, sessions, and even user experience.

AI/ML learning is now applied in this area, as monitoring provides a large volume of data that models process and may detect anomalies that indicate faults or attacks. For example, sudden changes in traffic patterns, unusual latency, or new device behavior can be flagged automatically. AI-based monitoring tools can also predict the degradation of a link or all devices (hardware) before they fail.

Integration with zero trust is another development, as monitoring should work across all internal segments. In such a case, each flow can be verified and inspected. IoT monitoring is also a separate challenge, because many IoT devices have limited built-in security. Specialized AI applications may profile their behavior and generate alerts when deviations occur.

Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:33:37 UTC from IEEE Xplore. Restrictions apply.

Cloud-based monitoring platforms are common, since they provide scalability and real-time updates. They also allow correlation between events in different sites. Vendors integrate these functions with SD-WAN and SASE so that monitoring, policy, and security are managed in one framework.

4) AI in network operations

AI is moving from theory into practice in enterprise networks and is becoming a core component of enterprise networking platforms, moving beyond experimental use into mainstream operations. Vendors already include AI in their platforms, where AI is integrated not as a separate function but as part of daily operations. The goal is to reduce manual work, improve fault detection, and shorten the time to recover. However, we need to point out that most applications of AI in this area of networking rely on machine learning models trained on telemetry and historical data.

One important application domain is the automation of configuration and policy changes. AI actually can recommend changes or verify if the configuration is consistent with intent. This reduces human errors, which are still one of the main causes of outages. Some systems already allow operators to interact in natural language and receive commands translated into device configuration.

Self-healing functions are another area. AI models analyze telemetry, detect abnormal behavior, and can restart services or reconfigure paths automatically. For example, if an SD-WAN link shows degradation, the controller can redirect traffic before users notice the problem. This principle is now deployed in Cisco Catalyst Center and Juniper Marvis.

Predictive operations are also possible. Machine learning models process historical data and predict failures such as hardware degradation or wireless interference. Operators receive alerts in advance and can schedule maintenance.

Another active domain of AI is the concept of a digital twin. A digital twin is a virtual model of the enterprise infrastructure where new policies or changes can be tested. AI plays an important role in creating and maintaining network digital twins. Machine learning models process telemetry and configuration data to build accurate virtual representations of the network. These AI-driven twins allow simulation of failures and policy changes with higher precision than manual modeling.

AI also relates to 5G and edge computing, where distributed intelligence close to the data source enables faster reaction. In practice, AI operations are not replacing network engineers but assist them with visibility, troubleshooting, and faster decision-making [6][8][9].

5) Discussion

The analysis of current trends shows that enterprise networking is in transition. Centralized management is still common but distributed and cloud-based models are becoming important for scale and resilience. Security functions are no longer separated. They converge into unified platforms. Monitoring has moved from passive observation to proactive anomaly detection. Telemetry, AI models, and zero trust principles together create visibility at higher granularity.

AI operations mark the next step. Automation, self-healing, predictive analytics, and digital twins are no longer theoretical but integrated in vendor platforms.

The main direction is clear: enterprise networks evolve from device-level management to policy-driven and intelligent infrastructures. However, migration is gradual. Many enterprises will keep hybrid environments, where classical layered design coexists with AI-enhanced functions. This mix reflects the need to balance innovation with operational stability.

IV. Evaluation of AI LLM Assistants in Enterprise Network Tasks

The use of AI language assistants in enterprise networks is a promising direction for partially deployed automation of IT processes. These tools are designed for general language interaction, but their potential in technical areas still must be verified. Our main interest is whether such assistants can perform practical network tasks that require both an understanding of human language and the application of technical rules. Large Language Models (LLM) are trained on large volumes of text and learn to predict words based on context. From this process, they build internal representations of syntax and meaning. This general capability may allow them to parse configuration requirements or interpret device command outputs. However, the quality of results in a specialized domain like enterprise networking is not guaranteed.

In this chapter, we analyze two cases that were chosen because they represent typical operations in enterprise network management. Five AI assistants were selected for evaluation in versions from April of 2025: ChatGPT (gpt-4o mini), Copilot (GPT-4 arch), Gemini (2.0 Flash), Grok, and DeepSeek. The results show how these systems perform in configuration accuracy and in the analysis of device outputs.

A. Research Questions and Goals

The objective of the study is to understand how general-purpose AI assistants can be applied to some enterprise network tasks, the generation of switch configurations, and the interpretation of CLI outputs. Both are frequent daily work activities of network engineers and can serve as indicators of practical usefulness.

Two research questions were formulated:

- Q1: Can AI assistants generate usable Cisco switch configurations when given textual requirements?
- Q2: Can AI assistants correctly interpret CLI outputs from Cisco switches and explain the state of the device?

The goals are:

- To compare the performance of several AI assistants (ChatGPT, Copilot, Gemini, Grok, DeepSeek) on the same set of tasks.
- To measure the correctness and completeness of their answers using predefined scoring scales.
- To observe differences between sequential prompting and single combined prompts in configuration generation.

Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:33:37 UTC from IEEE Xplore. Restrictions apply.

- To identify strengths and weaknesses of each assistant in relation to enterprise operations.

The results are expected to show whether AI assistants can support network engineers by reducing manual effort, or whether their current limitations make human validation always necessary.

B. Methodology

The evaluation was designed as a comparative experiment with five selected AI assistants. The aim was to test their ability to complete practical networking tasks that require both language understanding and technical accuracy. We prepared two types of tasks:

- **Configuration generation** – assistants were asked to generate the access layer switch configuration for Cisco IOS OS. Requirements included VLAN definition, trunk configuration, and access control settings. Prompts were given in two ways: sequential prompts with step-by-step questions and a single combined prompt containing all requirements. This allowed comparison of models in multi-turn versus single-turn scenarios.
- **CLI output interpretation** – assistants were asked to analyze ten real outputs collected from a production Cisco Catalyst switch. Ten commands were selected, covering device and protocol status: interface counters, spanning tree, routing table, DHCP, and port security. Each assistant was asked to interpret the output and explain the device condition. These outputs were originally obtained in laboratory testing and validated during diploma work on high-availability campus design

Each prompt was issued in a new session to avoid the influence of previous attempts, except in the sequential scenario for configuration, where context was intentionally preserved.

A scoring system was applied to measure results. Configuration task scales from 1 to 5:

- 1 = flawless configuration,
- 2 = minor errors,
- 3 = major errors or missing blocks,
- 4 = required further prompting,
- 5 = unusable output.

For the CLI task, a scale from 1 to 3 was used:

- 1 = no errors in interpretation,
- 2 = minor mistakes,
- 3 = major mistakes.

All outputs were stored, checked against reference configurations, and validated against CLI outputs. Correctness was verified manually by comparing with working switch configurations and expected command behavior. Scores for CLI were averaged across all ten outputs for each assistant. Evaluation criteria focused on technical correctness, completeness of answer, and practical usability for enterprise operations.

C. Results

Here, results are presented for both configuration generation and CLI interpretation tasks. Evaluation was performed according to the scoring system defined in the methodology for all five assistants.

1) Configuration Task

To preserve integrity, all assistants received the same questions. As a separate task, they were also asked all previous questions combined in one prompt within a new chat. The assumption was that assistants with a strong ability to use chat history perform better in the sequential scenario, while others without such ability might produce better results in the single combined prompt.

The outcomes showed that **Copilot and Gemini** were able to generate complex Cisco access switch configurations with only minor mistakes that did not cause major issues. Both assistants demonstrated results that are considered usable in enterprise networks.

ChatGPT provided a flawless configuration in terms of syntax and completeness, but did not fully follow the instructions given in the prompts. This required additional queries from the evaluator. A similar conclusion was observed for **DeepSeek**, which also produced flawless configuration that failed to meet all criteria requested in the assignment. **Grok** did not provide any usable configuration. Its responses consisted of partial commands or descriptions of technologies, and therefore, it could not be compared with the other assistants. Compared with earlier tests conducted three months before (January 2025), **Copilot** showed major improvement. In the earlier evaluation, it produced unusable outputs, while in this study its configuration was significantly better. This indicates continuous improvement and updates of AI models.

When comparing the two prompting modes, **Copilot and Gemini** produced poorer results in the single combined prompt scenario than in the sequential questioning. **ChatGPT** showed slight improvement with the combined prompt, while **DeepSeek** achieved major improvement under this condition. **Grok** again failed to generate a configuration and only briefly described the technologies used.

TABLE 1 CLI OUTPUT EVALUATION

Q.	Show output validation				
	ChGPT	Gemini	Copilot	Grok	DeepS.
1	1	2	1	1	2
2	2	1	1	1	2
3	1	1	2	1	1
4	1	1	1	1	2
5	1	1	2	1	2
6	1	3	3	3	3
7	2	1	2	1	1
8	1	1	2	1	1
9	1	2	1	2	2
10	1	1	2	1	1
Score	**1.2**	**1.4**	**1.7**	**1.3**	**1.7**

2) CLI Interpretation

979-8-3315-7426-0/25/$31.00 ©2025 IEEE
Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:33:37 UTC from IEEE Xplore. Restrictions apply.

The second task evaluated the ability of AI assistants to interpret real show command outputs. Ten outputs were provided, covering common operational commands.

The results are summarized in Table 1. Average scores were **ChatGPT** 1.2, **Grok**: 1.3, **Gemini**: 1.4, **Copilot**: 1.7, and **DeepSeek** for 1.7. The evaluation confirmed that **ChatGPT** was the most reliable in analyzing *show* outputs, consistently describing the prompts without mistakes. **Grok**, despite being unusable in configuration tasks, performed well in CLI interpretation and provided correct analysis. **Gemini** ranked closely behind. **Copilot** and **DeepSeek** achieved lower accuracy, with more frequent small errors and incomplete descriptions.

D. Discussion of Findings

The results show clear differences between configuration generation and CLI interpretation. Configuration for AI assistants remains a complicated task. Although ChatGPT and DeepSeek produced flawless outputs in terms of syntax, they failed to meet all the requested requirements, limiting their usability without further human validation. Copilot and Gemini generated configurations with minor errors, demonstrating progress compared to earlier tests. Grok, however, could not provide usable results.

In CLI interpretation, the performance was much better. ChatGPT achieved the best accuracy, while Grok and Gemini also performed well. Copilot and DeepSeek were less consistent. The average scores confirm that the interpretation of outputs is a more suitable task for current AI assistants than configuration generation.

The comparison of sequential versus combined prompts provided further insight. Copilot and Gemini performed better with step-by-step questions, while DeepSeek improved in the single combined scenario. This suggests that the internal memory and context-handling of models strongly affect their performance.

V. Conclusion

In the article, we reviewed current trends in enterprise networking and evaluated the use of AI language assistants in selected operational tasks on enterprise network administration tasks. The first part addressed LAN and WLAN architectures, the role of SD-WAN for connectivity, and the integration of SASE and SSE as cloud-based security frameworks. Emerging approaches such as intent-based networking, AI-driven monitoring, and digital twins were also discussed as future directions in network design.

The second part presented an evaluation of five AI assistants. Two tasks were analyzed. In the configuration task, Copilot and Gemini produced usable configurations with minor errors. ChatGPT and DeepSeek generated flawless syntax but failed to follow the requested requirements, which required additional prompting. Grok did not provide usable configurations. In the CLI interpretation task, performance was better. ChatGPT achieved the best accuracy, followed by Grok and Gemini, while Copilot and DeepSeek showed less consistent results.

Our findings suggest that AI assistants already provide valuable support for troubleshooting and interpreting CLI outputs, but configuration generation remains problematic. Their role is therefore supportive and requires human validation. The study is limited by the small dataset, focus on a single vendor, and rapid evolution of AI models. Future work should expand to multi-vendor environments, larger datasets, and further study of AI-driven automation and digital twins for enterprise networks.

Acknowledgement

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

References

[1] O. Afolalu and M. S. Tsoeu, "Enterprise Networking Optimization: A Review of Challenges, Solutions, and Technological Interventions," Future internet, no. 17, p. 133, 2025, DOI: 10.3390/fi17040133

[2] J. Dobie and R. Holder, "Network System of Systems Manager," 2024 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 2024, pp. 1-14, doi: 10.1109/ICNS60906.2024.10550591.

[3] "Campus LAN and Wireless LAN Solution Design Guide," 04 05 2020. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html.

[4] "Secure Guest Access for Cisco IOS-XE SD-WAN Devices Deployment Guide," 19 05 2020. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-secure-guest-access-deploy-guide.html.

[5] „Cisco Secure Access Service Edge (SASE) and Security Service Edge (SSE) Architecture Guide," 23 01 2025. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/sase-sse-ag.html

[6] A. León, D. Perdices, J. L. García-Dorado, J. Ramos a J. Aracil, „An expert-aware Markovian system for end-user proactive troubleshooting in the Network and Security Operations Center," Expert Systems With Applications, Expert Systems with Applications, Volume 276, 2025, 127072, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2025.127072.

[7] L. Yuexi, "Construction of network access Layer security protection System based on zero trust architecture," in The 4th International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy, Procedia Computer Science, Volume 243, 2024, Pages 1013-1022, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.09.121.

[8] S. Ahmad, A. Haque, H. A. M. Abdeljaber, A. E. Eljialy, J. Nazeer a B. K. Mishra, „Machine Learning Approaches in Cybersecurity to Enhance Security in Future Network Technologies," SN Computer Science, Procedia Computer Science, Volume 251, 2024, Pages 727-733, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.11.176.

[9] F. Wilhelmi, D. Salami, G. Fontanesi, L. Galati-Giordano and M. Kasslin, "AI/ML-based Load Prediction in IEEE 802.11 Enterprise Networks," in International Conference on Machine Learning for Communication and Networking, 2024.

[10] "Cisco Cloud Campus LAN Design Guide (CVD)," 27 08 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-campus/cloud-campus-lan-design-guide.html.

[11] D. Drost, "A brief history of language models," 12 3 2023. [Online]. Available: https://medium.com/data-science/a-brief-history-of-language-models-d9e4620e025b .

[12] I. T. Haque and N. Abu-Ghazaleh, "Wireless Software Defined Networking: A Survey and Taxonomy," in IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2713-2737, Fourthquarter 2016, doi: 10.1109/COMST.2016.2571118.

979-8-3315-7426-0/25/$31.00 ©2025 IEEE Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:33:37 UTC from IEEE Xplore. Restrictions apply.