Beyond automation

Building smarter, self-driven networks

White Paper
Beyond Automation: Building Smarter, Self-Driven Networks

Alcatel·Lucent
Enterprise

Introduction

In today's digital era, enterprise networks are growing increasingly complex due to the rapid adoption of cloud computing, the proliferation of IoT devices and evolving cybersecurity threats. Managing these dynamic environments manually has become unsustainable, as traditional methods struggle to meet the pace and demands of modern business operations.

This paper explores the **evolution from traditional network automation to autonomous networks, highlighting the pivotal role of Artificial Intelligence (AI) and Machine Learning (ML)**. Autonomous networks offer a robust solution by continuously monitoring, analyzing and optimizing performance in real time, minimizing the need for human intervention.

The paper presents validated AI-based use cases that address critical network management challenges not resolved by conventional automation. These use cases demonstrate the shift from reactive AI, which responds after issues occur, to proactive and preventive AI, which anticipates and mitigates problems before they impact operations. The journey culminates in prescriptive AI, where intelligent systems deliver data-driven recommendations that support informed, strategic decision-making.

By combining automation with AI initiatives, enterprises can ensure the reliability and efficiency of their network operations, achieving sustained stability, resilience and a competitive edge in today's complex IT landscape.

Understanding the autonomous network

An autonomous network is a self-operating system. It functions in alignment with business objectives without requiring human intervention beyond the initial input (in the form of intents, goals, policies or specific configuration data). It is designed to manage itself through various self-governing operations, including self-configuration, self-diagnosis, self-repair, self-healing, self-optimization and self-protection. These capabilities are supported by the autonomous network's ability to automatically discover operational information and act upon it.

An autonomous network has the following key attributes:

- **Awareness** – It continuously monitors its operational environment, performance and internal states to determine whether it is meeting predefined and agreed-upon objectives.
- **Adaptiveness** – It dynamically adjusts its operations to accommodate changes in its environment over both the short and long term. This includes modifying its decisions and behaviors to ensure sustained operational performance.
- **Automation** – It can independently control internal resources and operations and function without manual intervention.

The level of "capability" of a network can vary, ranging from basic automation to full autonomy.

The difference between automation and autonomy

Network automation and network autonomy are two concepts that are often confused but have distinct differences in their approach, functionality and level of human intervention.

Network automation involves using software tools and processes to manage network infrastructure and services programmatically. It automates repetitive tasks, such as configuration, deployment and maintenance, to improve efficiency and reduce human error. Automation typically requires **human intervention** for decision-making and setting rules. It operates within predefined parameters and conditions. Generative AI can help streamline communication between administrators and the network.

Network autonomy, on the other hand, refers to a **self-managing network architecture** that leverages AI/ML to minimize or eliminate human intervention. It can configure, monitor, maintain and secure itself. Decisions are system-led, and humans are outside the loop unless needed for oversight. Achieving an autonomous network is a gradual process. Before administrators can fully relinquish control, the system must progressively increase its level of autonomy to build their trust.

Each concept addresses a different network management scenario. Automation is used for well-known repetitive problems; administrators invest their time and efforts to develop technical ways to resolve these problems. Autonomy is responsible for rare, often unknown problems, that can be identified using AI/ML methods. **Together, the two methods provide a robust foundation for well-functioning networks**.

Network management with automation

At its core, automation enables tasks to be executed without human intervention. This is achieved by introducing automatic functions or enhancing, replacing or modifying manual processes with automation tools, such as scripts that execute a sequence of commands.

Automation operates at various levels of granularity, from individual tasks and processes to the complete management and operation of the infrastructure (encompassing the entire life cycle of networks and services including installation, configuration, provisioning and termination). This automation can be further enhanced by innovations such as the decoupling of control and data planes and virtualization techniques, introducing greater flexibility. However, a key challenge is integrating these composable components into cohesive, high-performance, robust, extensible and reconfigurable automation systems. This underscores the need for standardized interfaces, models and mechanisms.

Developing a fully integrated automation solution remains a complex and open challenge. Such a solution requires the seamless orchestration of automated functions with the following characteristics:

- **Vertical end-to-end automation**, spanning the entire protocol stack from the service layer to the physical layer
- **Horizontal end-to-end automation**, covering multiple technologies and administrative domains
- **Repeatability and reusability,** leveraging standardized interfaces and best practices for broad applicability
- **Dynamic provisioning** of customizable control points, allowing human oversight within the automation loop

It is important to determine to what extent the automation is driven by technical policies or business intents.A single technology backbone will manage everything

With this integrated infrastructure, Smart Building 5.0 will manage temperature, lighting and window shades room-by-room using multiple sensors. It will leverage its truly intelligent architecture to collect data, analyze it, report it and independently act on all the information available to support ongoing operation. In addition, the building will be able to predict changes in operating parameters that are needed based on data about in-building and exterior environmental conditions and act on those predictions as needed to maintain regenerative building objectives.

Policy-driven automation

Automated actions can often be governed by policies. Many network deployments already incorporate dynamic policy management, enabling automated adjustments in life cycle management and other network configurations.

At the core of policy-based automation lies **the concept of pre-defined rules that trigger specific actions** when certain conditions are met. These conditions can include:

- Time-based triggers (time of day, day of week, etc.)
- Network load thresholds
- System failures
- Combinations of the above

When a trigger condition occurs, the local management entity executes the corresponding pre-defined actions, such as:

- Deploying or terminating services/components
- Scaling resources
- Migrating workloads
- Replacing instances
- Adjusting configurations
- Managing software updates

Once policies are in place, policy-driven automation enables fully autonomous, **zero-touch management**. However, creating policies and dynamically adapting them to evolving conditions remains a complex challenge. Applying high level business-oriented intents can improve the situation.

Intent-based automation

Intent-based automation is based on Intent-Based Networking (IBN), which leverages intelligent software to understand user goals and automatically translate them into concrete service or network configurations. IBN is a relatively new mechanism, so its definition varies, and no standardized framework currently exists.

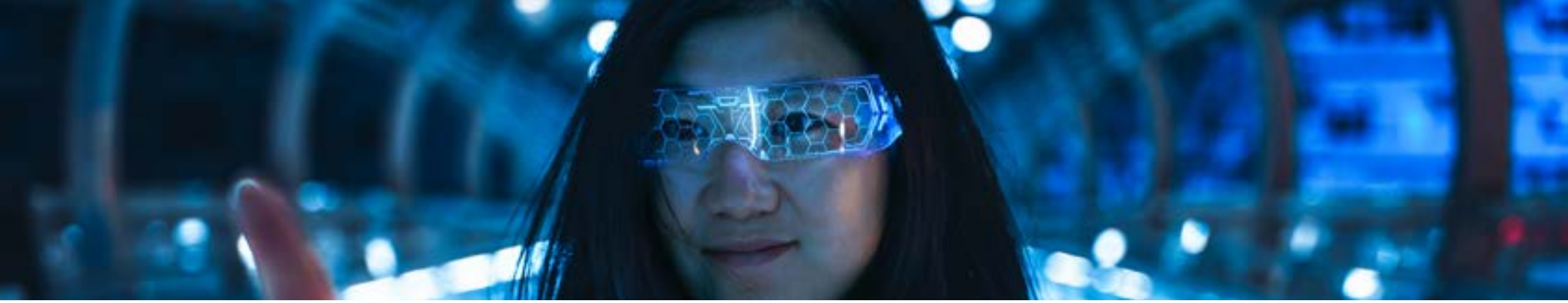
IBN is the next step of network management after policy-based automation. While policies define specific decision-making rules, intent represents a higher-level declarative goal. An intent-based API allows users to specify desired outcomes, while the underlying system dynamically determines the optimal network setup.

Traditional management systems require configuration modifications when the requirements for a service change. A truly intent-driven approach relies on semantic modeling that enables behavior-driven automation without manual configuration manipulations. Unlike policies, intents remain unchanged by infrastructure changes or faults. This frees management applications from network-specific details, simplifying service development, testing and deployment.

An extensible intent API allows **independently developed services** to express their requirements in a unified language. This is critical for modern environments that integrate SDN, SD-WAN, MPLS, private/public cloud and edge computing.

Generative AI can bridge the gap between high-level business intents and low-level network configurations. It does this by interpreting natural language input from users and translating it into actionable technical policies. For example, if a user specifies a goal like «prioritize video conferencing traffic,» GenAI can identify the necessary quality of service (QoS) settings to implement that intent. It leverages models trained on networking data and policy rules to ensure accurate and relevant translations. This allows non-technical stakeholders to express goals without needing to understand complex configuration syntax.

GenAI also takes into account the context of the network environment, such as existing policies, performance metrics and compliance requirements. This helps prevent conflicts and ensures the new configurations align with the overall network strategy. Over time, GenAI can learn from user feedback and network behavior to improve its policy generation capabilities. **This makes network management more intuitive, agile and aligned with business objectives**.



AI in networking

Three key types of AI are particularly relevant to network management: Predictive AI, Generative AI and Agentic AI.

Predictive AI

Predictive AI uses historical data, statistical models and machine learning algorithms to forecast future outcomes or behaviors. It identifies patterns and trends to make informed predictions, such as anticipating system failures or degraded performance.

Key applications for Predictive AI include:

- **Dynamic thresholds for anomaly detection:** Unlike static, preconfigured thresholds, ML-driven ones are adjusted in real time based on evolving patterns and trends, ensuring more adaptive and responsive monitoring which leads to efficient anomaly detection.
- **Automated event correlation:** AI identifies hidden relationships between events, providing the means for efficient root cause analysis which significantly enhances incident response times and reduces manual effort.
- **Intelligent log analysis:** AI can leverage historical data to classify and interpret new and rare syslog messages, identifying critical events without the need for predefined parsing rules.

Generative AI

Generative AI creates new content by learning patterns from data by applying Large Language Models (LLMs).

Key applications for Generative AI include:

- **Adaptive reporting:** AI generates real-time, context-aware reports tailored to current network conditions, ensuring that relevant insights are always available.
- **Natural language interface for admins:** AI translates natural language commands into network configurations or queries. It can also enable intuitive interaction with network data through conversational prompts.

Agentic AI

Agentic AI leverages advanced logic to make decisions and take actions on behalf of the user, using predictive and generative models. It demonstrates goal-oriented behavior through multi-step reasoning and adaptive learning, constantly improving via a real-time feedback loop that evaluates outcomes and adjusts accordingly.

The key application of agentic AI is intelligent workflows. A network engineer delegates a wide range of network management tasks to an AI agent, the agent autonomously determines how to fulfill the request—often involving interactions with multiple systems that are gathering data, executing follow-up queries and interpreting results. Once the process is complete, the AI agent delivers a comprehensive response back to the engineer.

Network management with autonomy

Traditionally, network automation has concentrated on streamlining high-frequency or mission-critical tasks, such as:

- **Applying parsing rules** to commonly encountered syslog messages
- **Generating alerts** when key metrics exceed predefined thresholds
- **Correlating events** based on typical patterns or recurring combinations

However, this approach overlooks a wide range of less defined, yet potentially crucial tasks. Addressing these tasks requires a fundamentally different strategy—one that leverages the capabilities of AI and ML. These technologies allow for automation and optimization even in the absence of explicitly defined rules for every scenario.

The three types of AI mentioned above, along with automation methods and other technologies, are integrated to enable the core driver of network autonomy: closed-loop automation.

Closed-loop automation is an approach in which a system continuously gathers data, analyzes it, makes and applies configuration decisions and iterates this cycle to improve outcomes based on feedback from previous actions.

As networks progress from manual operation to full autonomy, they go through multiple levels such as assisted, partial, conditional, high and full automation. At higher levels, closed-loop automation becomes more sophisticated, enabling self-healing, self-optimization and proactive issue resolution.

The main stages of a closed-loop automation are Monitoring, Analysis, Decision and Execution.

Monitoring stage: Data collection and ingestion

The Monitoring stage is responsible for gathering and pre-processing data from network devices—a process known as data ingestion. This involves transferring data from one or multiple sources to a central repository for storage and analysis. The collected data can take various forms including events, logs, telemetry and traffic captures.

Analysis stage: Extracting insights

In the Analysis stage, insights are derived from real-time data gathered in the Monitoring stage, historical records, network configuration and knowledge base information describing the network. Insights provide answers to key questions, such as:

- «What happened?»: Detecting anomalies or unusual network behavior
- «Why did it happen?»: Applying root cause analysis to identify the underlying issue

This insight generation is an ongoing process, continuously refined with new incoming data from the Monitoring stage.

Decision stage: Determining actions

The Decision stage translates insights into workflows that guide the system's response. This stage dictates the appropriate course of action based on detected issues, which can be:

- **Reactive:** Addressing problems as they occur
- **Proactive:** Preventing potential issues based on detection of data patterns normally observed before these issues occur
- **Predictive:** Anticipating future network problems based on data trends

By leveraging AI/ML, rules and policies, the Decision stage transforms found insights into list of actions, steering the network toward an optimal state.

Execution stage: Implementing actions

The Execution stage carries out the workflows determined in the Decision stage, applying corrective or adaptive actions to the network. These workflows consist of one or more operations that must be carefully orchestrated to ensure seamless implementation. Modern model-based approaches like YANG and associated protocols like NETCONF and RESTCONF are an important part of that.

After the workflows are executed, the closed-loop automation logic starts the new cycle of Monitoring, Analysis, Decision and Execution to take into account consequences of the actions of the previous cycle as well as new external network conditions.

Conclusion

Transitioning to autonomous networks is a crucial step for enterprises seeking to boost operational efficiency, agility and user satisfaction. Traditional network automation already brings significant benefits, such as **reducing manual workloads, minimizing human error and accelerating routine operations**. Building on this foundation, closed-loop automation enables real-time monitoring and automated response to network conditions, ensuring faster issue resolution and improved reliability. It also supports continuous optimization by learning from network behavior and adapting without manual intervention. As the result, autonomous networks empower enterprises with self-managing, self-healing and self-optimizing capabilities. **This reduces operational costs while enhancing scalability and resilience**. Embracing this evolution will be key for enterprises to stay agile and competitive in an increasingly complex networking environment.

DID25080802EN (August 2025)

Alcatel·Lucent Enterprise