Workgroup:	RTG
Internet-Draft:	draft-king-rokui-ainetops-usecases-00
Published:	10 February 2025
Intended Status:	Informational
Expires:	14 August 2025

Authors: R. Rokui *Ciena* D. King *Lancaster University*

Artificial Intelligence (AI) for Network Operations

Abstract

This document explores the role of the IETF and IRTF in advancing Artificial Intelligence for network operations (AINetOps), focusing on requirements for IETF protocols and architectures. AINetOps applies AI/ML techniques to automate and optimize network operations, enabling use cases such as reactive troubleshooting, proactive assurance, closed-loop optimization, misconfiguration detection, and virtual operator assistance.

The document addresses AINetOps for both single-layer IP or Optical networks and multi-layer IP/Optical networks. It defines the concept of AINetOps for networking and provides its operational benefits such as network assurance, predictive analytics, network optimization, multi-layer planning, and more. It aims to guide the evolution of IETF protocols to support AINetOps-driven network management.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The increasing complexity of modern networks has driven the need for innovative approaches to network operations and management. Artificial Intelligence for Network Operations (AINetOps) has emerged as a transformative concept, leveraging artificial intelligence (AI) and machine learning (ML) to automate, enhance, and optimize network management tasks. AINetOps offers the potential to reduce operational costs, improve service reliability, and enhance user experiences by enabling intelligent automation, predictive insights, and efficient decision-making.

The IETF and IRTF play a critical role in defining the protocols, architectures, and standards that underpin global networking. As AINetOps becomes integral to network operations, there is a growing need to evaluate how existing IETF technologies can support AINetOps use cases and to identify gaps that may require new or extended solutions. This document aims to outline key AINetOps use cases, highlight associated technical challenges, and propose requirements for protocols and architectures to address these challenges effectively.

The use cases considered in this document span multiple aspects of network operations, including reactive troubleshooting, proactive assurance (e.g., anomaly detection, predictive maintenance), closed-loop optimization, and misconfiguration detection. Emerging capabilities, such as generative AI for operational insights and virtual operator assistants, further emphasize the need for a robust framework to support AI-driven network management. Additionally, the multi-layered nature of these use cases, encompassing IP, optical, and cross-layer optimization, underscores the complexity of integrating AINetOps into existing networks.

This document provides a foundation for advancing IETF protocols and architectures to enable AINetOps-driven network operations by exploring these use cases, the requirements, and their implications.

1.1. Background

Efficient and coordinated use of resources is paramount for maintaining optimal performance and reliability of many network environments. The applicability of Artificial Intelligence is well-established, and the use cases are outlined in this document.

Editors note: Future versions of this document will include will include prior IRTF and IETF work.

2. Conventions and Definitions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are used in this document:

- AI: Artificial Intelligence aims to create systems capable of performing tasks that typically require human intelligence, such as understanding natural language, recognizing patterns, and making decisions.
- ML: Machine Learning is a subset of AI that involves training algorithms on large datasets to enable them to learn patterns and make predictions or decisions without being explicitly programmed.
- Gen-AI: Generative-AI is a subset of ML techniques that creates new content, such as text, images, or audio, by learning from existing data.
- NLP: Natural Language Processing is a field of AI that focuses on the interaction between computers and humans through natural language.
- AINetOps: Artificial Intelligence for Network Operations refers to the application of AI, ML, and generative-AI techniques to enhance and automate network operations.
- Closed-Loop Optimization: Automated feedback-driven processes for continuously improving network performance and reliability.
- Multi-Layer Optimization: Addressing cross-layer dependencies and optimizing resources across different network layers, such as IP and optical layers.

3. AI, ML, Deep Learning and Gen-AI

Artificial Intelligence (AI) is the broad field dedicated to creating systems that can perform tasks typically requiring human intelligence, such as reasoning, problem-solving, and understanding language. Within AI, Machine Learning (ML) is a subset that focuses on developing algorithms that enable computers to learn from and make decisions based on data, improving their performance over time without explicit programming. Deep Learning is a further subset of ML that utilizes neural networks with many layers (hence "deep") to analyze various factors of data. This approach is particularly powerful in handling large and complex datasets, making significant advancements in areas such as image and speech recognition, natural language processing, and autonomous systems.

Generative AI (Gen-AI) is a specialized branch of ML that involves training models to generate new content, such as text, images, or music, by learning patterns from existing data, thereby enhancing the creative and adaptive capabilities of AI systems. Deep Learning techniques are often employed in Gen-AI to create more sophisticated and realistic outputs, pushing the boundaries of what AI can achieve in terms of creativity and innovation.

Figure 1 shows the relationship between AI, ML, Deep Learning, and Gen-AI.

```
|-------------------------------------|
|                  AI                 |
|   |-----------------------------|   |
|   |              ML             |   |
|   |   |---------------------|   |   |
|   |   |    Deep Learning    |   |   |
|   |   |   |-------------|   |   |   |
|   |   |   |   Gen-AI    |   |   |   |
|   |   |   |             |   |   |   |
|   |   |   |             |   |   |   |
|   |   |   |-------------|   |   |   |
|   |   |---------------------|   |   |
|   |-----------------------------|   |
|-------------------------------------|
```

Figure 1: Figure 1: Relationship between AI, ML, Deep Learning, and Gen-AI

4. Definition of AINetOps

Figure 2 illustrates the concept of AI for Network Operations (AINetOps), which leverages AI, ML, Gen-AI techniques and rule-based systems to enhance and automate network operations. By integrating both historical and real-time streaming data, AINetOps employs advanced data analytics to uncover hidden patterns, establish data correlations, and provide trend forecasts and anomaly detection. These insights lead to significant operational benefits, including improved network performance, reduced downtime, and more efficient management of IP optical networks. Additionally, AINetOps enables proactive and predictive analytics, allowing network operators to address potential issues before they impact users, thereby ensuring more resilient and reliable network operations.

This draft introduces the term “Operational Benefit”, which encompasses the comprehensive suite of tools, and methodologies that facilitate the efficient management, debugging, troubleshooting, monitoring, configuration, and optimization of IP Optical networks. These operational benefits might include network management systems, automated diagnostic tools, performance monitoring and telemetry systems, configuration management platforms, and optimization algorithms. By leveraging these resources, operators can ensure the robust performance, reliability, and scalability of the network, ultimately enhancing service delivery and reducing operational costs. The integration of these operational benefits is crucial for maintaining seamless network operations and achieving strategic business objectives

Section 5 expands the Operational benefits shown in Figure 2 and provides a detailed explanation of the various operational benefits offered by AINetOp.

Figure 2 shows the relationship between AI, ML, Deep Learning, and Gen-AI.

```
|------------|    |--------------|      |-----------------------|
|            |    |  AI /        |      |                       |
|    Big     |    |  ML /        |      |                       |
|    Data    |  + |  Gen-AI/     |   =  |        AINetOps       |
|            |    |  Rule-based  |      |                       |
|            |    |              |      |                       |
|------------|    |--------------|      |-----------------------|
                                         AINetOPS provides
                                         Operational Benefits
Big Data: Historical or Real-time data
         (e.g., time series PM, Alarm, Topology, Log,
          OAM data, product content/documentation etc.)
```

Figure 2: Figure 2: Definition of AINetOp

5. Operational Benefits Provided by AINetOps

AINetOps has the potential to revolutionize network operations by addressing the inherent complexity, scale, and dynamic nature of modern networks. By applying various AI/ML/Gen-AI techniques, network operators can transition from traditional manual or rule- based operations to intelligent, automated systems capable of real- time adaptation, predictive insights, and optimized decision-making.

This section outlines the following key areas where AINetOps can be applied effectively in network operations, leveraging both data- driven models and domain-specific knowledge.

- Section 5.1 "Operator Network Assistance"
- Section 5.2 "Network active and reactive assurance". This area is also related to "Root Cause Analysis" Section 5.2.1
- Section 5.3 "Predictive Analytics" which includes "Proactive Network Assurance and Monitoring" Section 5.3.1, "Anomaly Detection" Section 5.3.2, "Trending and Forecasting" Section 5.3.3, "Predictive Maintenance" Section 5.3.4 and "Network Capacity Planning" Section 5.3.5
- Section 5.4 "Network Operational Insight". This area can be grouped into "Operational Insights Requiring No Further Analysis " Section 5.4.1 and "Operational Insights Requiring Further Analysis " Section 5.4.2
- Section 5.5 "Network Configuration Management"
- Section 5.6 "IP/Optical multi-layer Planning"
- Section 5.7 "Cross-Layer and Multi-Layer Optimization"
- Section 5.8 "Traffic Optimization"
- Section 5.9 "Closed-Loop Automation"
- Section 5.10 "Network Maintenance and Cleanup"
- Section 5.11 "Network API Construction"
- Section 5.12 "AI-Driven Security Monitoring"

5.1. Operator Network Assistance

Powered by Gen-AI, the operator network assistant functions as a virtual network engineer, providing a real-time recommendations, insights, and automated solutions. These systems use NLP for interface interaction, deep learning for anomaly classification, and contextual understanding to enhance operator decision-making.

AI-powered operator assistants function as virtual network engineers, providing real-time recommendations, insights, and automated solutions. These advanced systems leverage the power of natural language processing (NLP) to facilitate seamless and intuitive interactions between operators and the network management interface. By understanding and interpreting human language, these AI assistants can effectively communicate with operators, making it easier for them to manage complex network environments without needing extensive technical expertise.

In addition to NLP, Operator Assistance can integrate other AINetOps functions to solve operators scenarios and use-cases. This capability allows the system to provide timely alerts and recommendations, helping operators to address issues before they escalate into major disruptions. The deep learning models continuously improve over time, becoming more adept at recognizing new types of anomalies and adapting to evolving network conditions.

Furthermore, the contextual understanding capabilities of AI-powered operator network assistant significantly enhance operator decision- making. By considering the broader context of network operations, including historical data, current network state, and external factors, the AI can offer more relevant and actionable insights. This holistic approach ensures that operators receive comprehensive guidance tailored to the specific circumstances of their network. As a result, operators can make more informed decisions, optimize network performance, and maintain high levels of service reliability and efficiency. In essence, AI-powered operator network assistants are transforming network management by augmenting human capabilities with advanced technology, leading to smarter and more proactive network operations.

5.2. Network active and reactive assurance

Network active and reactive assurance and troubleshooting, both at the single- layer (IP or Optical) and multi-layer (IP over Optical), are critical components in maintaining the health and stability of modern IP, Optical, and IPoDWDM networks. This process involves the identification and resolution of network issues as they arise, ensuring that any disruptions or degradations are promptly addressed. By employing AINetOps techniques, network engineers can quickly pinpoint the root cause of problems, whether they originate in the IP layer, the optical layer, or across both. This reactive approach is essential for minimizing downtime and maintaining the quality of service expected by network users.

In single-layer troubleshooting, the focus is on isolating and resolving issues within a specific layer of the network. For example, in an IP network, this might involve diagnosing routing problems, addressing IP address conflicts, IP layer misconfiguration, hardware failure or resolving issues with network protocols. In an optical network, single-layer troubleshooting could involve identifying fiber cuts, optical signal degradation, or equipment failures

Multi-layer troubleshooting, on the other hand, requires a more integrated approach, as it involves identifying and resolving issues that span across multiple layers of the network. This could include problems where an issue in the optical layer affects the IP layer, such as signal impairments that impact data transmission quality. By effectively managing both single-layer and multi-layer troubleshooting, network engineers can ensure a more robust and resilient network infrastructure.

The importance of assurance and troubleshooting cannot be overstated in today's high-demand network environments. Rapid response to network issues is crucial to maintaining service continuity and meeting the expectations of end-users. Advanced diagnostic tools and techniques, such as real-time monitoring, automated alerts, and detailed analytics, play a vital role in this process. These tools enable engineers to quickly detect anomalies, assess their impact, and implement corrective actions. Through continuous improvement of assurance and troubleshooting practices, network operators can enhance their ability to maintain network performance, reduce operational risks, and deliver a reliable and high-quality service to their customers.

5.2.1. Root Cause Analysis

In the context of "Network active and reactive assurance," Root Cause Analysis (RCA) is a critical aspect that extends the reactive troubleshooting process to uncover the underlying reasons behind network issues. When an issue is detected in the network, RCA leverages advanced AINetOps techniques to correlate events across different layers of the network, whether it be IP, Optical, or a combination of both. This comprehensive approach ensures that the root cause of an issue is accurately identified, rather than just addressing the symptoms. Techniques such as graph-based analysis enable network engineers to visualize and trace the sequence of events leading to a problem, providing a clear pathway to the source of the issue.

Moreover, natural language processing (NLP) for log analysis plays a significant role in RCA by automating the examination of vast amounts of log data generated by network devices. NLP can sift through logs to identify patterns and anomalies that might be missed by manual inspection. This capability is particularly useful in multi-layer networks where issues in one layer can propagate and manifest in another. By efficiently parsing through logs and correlating data, NLP helps pinpoint the exact cause of disruptions, thereby reducing the mean time to resolution (MTTR). Additionally, knowledge graph representations provide a structured and interconnected view of network components and their relationships, aiding in the rapid identification of fault points and their impact on the network.

By accurately diagnosing the root cause of network issues, network operators can implement targeted corrective actions that address the core problem, preventing recurrence and ensuring long-term stability. This precision in troubleshooting not only minimizes downtime but also enhances the overall reliability and performance of the network. Furthermore, insights gained from RCA can inform proactive measures and optimization strategies, contributing to a more resilient network infrastructure. In essence, RCA empowers network engineers with the tools and knowledge needed to maintain high service quality and meet the demands of modern, high-performance networks.

5.3. Predictive Analytics

Predictive analytics or advanced analytics uses historical and real- time network data, statistical algorithms, and ML techniques to identify the likelihood of future outcomes based on past data. In the context of network operations, predictive analytics involves the use of these methodologies in following areas to anticipate network issues, optimize performance, and improve operational efficiency. By examining patterns and trends in historical network data, predictive analytics can potentially forecast network problems before they occur, allowing for proactive management and maintenance.

The core idea behind predictive analytics is to transform data into actionable insights. For network operations, this means analyzing various metrics such as traffic patterns, latency, performance management (PM) data, and equipment performance to predict future states of the network. For instance, by identifying trends that have historically led to network failures, predictive analytics can alert operators to potential future failures, enabling them to take preventive measures. This proactive approach helps in minimizing downtime, enhancing service reliability, and optimizing resource allocation.

In summary, predictive analytics in network operations is about leveraging historical data and advanced analytical techniques to foresee and address potential issues before they impact the network. This approach leads to more efficient, reliable, and secure network operations, ultimately enhancing the overall performance and user experience. The AINetOps can address the following operator's scenarios.

5.3.1. Proactive Network Assurance and Monitoring (Health Check)

Proactive Network Assurance and Monitoring represents a paradigm shift from the Network active and reactive assurance discussed in Section 5.2. Instead of waiting for issues to arise and then addressing them, proactive network assurance involves anticipating potential problems and implementing measures to prevent them from occurring. This forward-thinking strategy leverages AINetOps to predict and mitigate network issues before they impact service quality.

In single-layer proactive assurance, the focus is on continuously monitoring and analyzing the health of a specific layer IP or Optical layer of the network to identify early warning signs of potential issues. For instance, in an IP network, this might involve analyzing traffic patterns to detect anomalies that could indicate an impending routing problem or hardware failure. ML algorithms can be employed to predict IP address conflicts or protocol misconfigurations before they cause disruptions. Similarly, in an optical network, proactive assurance could involve monitoring signal quality and fiber integrity to detect and address degradations before they lead to significant impairments or outages.

Multi-layer proactive assurance takes this approach a step further by integrating monitoring and analysis across both the IP and optical layers. This holistic view allows for the detection of complex issues that span multiple layers, such as optical signal impairments that could degrade IP data transmission quality. By correlating data from both layers, AINetOps solution can provide insights into how changes in the optical layer might affect IP performance and vice versa. This enables operators to take preemptive actions, such as optimizing signal paths or adjusting routing protocols, to maintain optimal network performance.

The benefits of proactive network assurance and monitoring are substantial. By identifying and addressing potential issues before they escalate, network operators can significantly reduce downtime and improve service reliability. This proactive stance not only enhances the user experience by ensuring consistent network performance but also reduces operational costs associated with emergency troubleshooting and repairs. Furthermore, the use of advanced analytics and machine learning in AIOps allows for continuous learning and improvement, enabling networks to become more resilient and adaptive over time.

In today's dynamic and high-demand network environments, proactive network assurance and monitoring is one of the operational benefits provided by AINetOps and are essential for staying ahead of potential issues and maintaining a competitive edge. By leveraging the power of AINetOp, network operators can transform their approach from reactive to proactive, ensuring that their networks are not only robust and resilient but also capable of delivering the high-quality service that users expect. This shift towards proactive assurance represents a significant advancement in network management, paving the way for more intelligent, efficient, and reliable network operations.

5.3.2. Anomaly Detection

A critical component of AINetOps in the context of predictive analytics is "Anomaly Detection", which leverages advanced ML algorithms to enhance network reliability and performance. By employing ML techniques such as supervised, unsupervised or reinforcement learning, AINetOps can predict anomalies in real-time by analyzing vast amounts of network telemetry data. Supervised learning models, trained on historical data, recognize known issues, while unsupervised models identify new anomalies by spotting outliers. This comprehensive detection mechanism ensures both familiar and novel network issues are identified promptly. Predictive models, utilizing techniques like time-series forecasting, enable the identification of potential network problems, such as link failures or traffic congestion, before they occur. By forecasting future network states based on historical and current data, these models provide early warnings, allowing for timely interventions to prevent unexpected downtime and maintain optimal performance.

Clustering techniques further enhance anomaly detection by grouping similar data points to identify patterns and trends that signal imminent failures or suboptimal behavior. This method allows ML models to discern subtle changes in network behavior that might otherwise go unnoticed. For example, clustering can reveal traffic congestion patterns under specific conditions, enabling preemptive measures to alleviate potential issues. Additionally, clustering helps identify the root causes of anomalies by correlating various network events and metrics, facilitating a more effective troubleshooting process. By integrating these advanced ML techniques, AINetOps not only improves anomaly detection but also empowers network operators with the insights needed to maintain a high-performing and reliable network infrastructure.

5.3.3. Trending and Forecasting

"Trending and Forecasting" operational benefit is distinct but is related to "Anomaly Detection" Section 5.3.2. Trending and forecasting in the context of single-layer or multi-layer IP optical networks are pivotal components of predictive analytics, providing significant operational benefits through AINetOps. In single-layer networks, such as purely IP or optical networks, trending involves analyzing historical data to identify patterns and behaviors over time. For instance, in an IP network, trends in traffic volume, latency, and packet loss can be monitored to predict future network performance and capacity needs. Similarly, in an optical network, trends in signal quality, attenuation, and equipment performance can be tracked. By leveraging these trends, predictive models can forecast potential issues such as bandwidth bottlenecks or equipment degradation, allowing network operators to proactively optimize resources, plan for upgrades, and prevent service disruptions.

In multi-layer IP optical networks, where both IP and optical layers interact, trending and forecasting become even more powerful. This approach involves correlating data from both layers to gain a comprehensive understanding of network behavior. For example, trends in optical signal impairments can be analyzed alongside IP traffic patterns to predict how physical layer issues might impact data transmission and overall network performance. Forecasting in this multi-layer context can identify potential cross-layer issues, such as how an increase in optical signal noise might lead to higher IP packet error rates. By anticipating these issues, network operators can implement preemptive measures, such as rerouting traffic or adjusting signal parameters, to maintain seamless service. The integration of trending and forecasting through AIOps thus enhances the resilience and efficiency of IP optical networks, ensuring superior performance and reliability.

5.3.4. Predictive Maintenance

Predictive maintenance in the context of single-layer or multi-layer IP optical networks is other aspect of predictive analytics, offering substantial operational benefits through AINeetOps. In single-layer networks, such as purely IP or optical networks, predictive maintenance involves using historical and real-time data to forecast when network components might fail or degrade. For instance, in an IP network, data from routers and switches, such as CPU usage, temperature, and error rates, can be analyzed to predict hardware failures. Similarly, in an optical network, monitoring parameters like signal strength, attenuation, and equipment performance helps predict when optical amplifiers or transceivers might need maintenance. By accurately forecasting these maintenance needs, network operators can schedule interventions before failures occur, reducing unplanned downtime and extending the lifespan of network components.

In multi-layer IP optical networks, predictive maintenance becomes even more effective by considering the interactions between the IP and optical layers. This approach involves analyzing data from both layers to predict maintenance needs that could impact the entire network. For example, if optical layer data indicates a gradual degradation in fiber quality, predictive models can assess how this might affect IP layer performance, such as increased packet loss or latency. By understanding these cross-layer dependencies, network operators can prioritize maintenance activities that have the most significant impact on overall network health. This proactive approach ensures that both layers of the network are maintained optimally, preventing cascading failures and maintaining high service quality. Through the integration of predictive maintenance with AIOps, IP optical networks can achieve greater reliability, efficiency, and cost-effectiveness, ensuring uninterrupted service delivery to end-users.

5.3.5. Network Capacity Planning

Predictive analytics also plays a crucial role in capacity planning and performance management. By forecasting future traffic demands, network operators can ensure that the infrastructure is adequately scaled to meet those demands without over-provisioning. This not only optimizes the use of resources but also ensures that the network can handle peak loads efficiently. Additionally, predictive analytics can help in identifying and mitigating potential security threats by analyzing traffic patterns and detecting anomalies that may indicate malicious activities.

5.3.6. Traffic Optimization

Referring to Section 5.8 for details of AINetOps "Traffic Optimization".

If "Traffic Optimization" is based on prediction of the traffic flows, it can be categorized as one of the areas of "Predictive Analytics".

5.4. Network Operational Insights

"Network Operational Insights" refers to the comprehensive visibility and understanding of an IP optical network's performance and behavior. This concept involves collecting and analyzing detailed data about the network's operations. By providing this valuable insight to network operators, they can gain a holistic view of the network's health and performance. This enables operators to understand their network better and ensure a robust and resilient infrastructure.

By having a detailed understanding of network usage patterns, traffic flows, and performance metrics, operators can make data-driven decisions to optimize resource allocation and improve overall efficiency. This insight is particularly valuable in multi-layer IP/ Optical networks, where the interplay between different network layers can be complex. By leveraging these insights, operators can ensure that both the IP and optical layers are operating harmoniously, leading to optimal performance and cost efficiency. In essence, Network Operational Insights empower operators with the knowledge needed to maintain a high-performing, resilient, and future-proof network infrastructure.

The network operational insight can be grouped into two categories. By categorizing network operational insights into these two categories, operators can better prioritize their efforts and resources, ensuring both immediate and long-term network health and performance.

5.4.1. Operational Insights Requiring No Further Analysis

Network Operational Insights that fall under this category are those that can be obtained directly from existing data and real-time monitoring without the need for further analysis or simulation. These insights provide immediate, actionable information that can help network operators quickly identify and address issues.

These insights are typically derived from real-time monitoring systems that continuously track network performance and health metrics. For example, showing the Network Element (NE) with the highest alarms or displaying the current alarm table for a specific NE (e.g., NE 1.1.1.1) can provide immediate visibility into potential issues. Similarly, identifying the NEs with the highest problems during the last hour or plotting the Bit Error Rate (BER) for the 10 worst modems in a specific region (e.g., Northeast) allows operators to quickly pinpoint areas that require attention. These insights are crucial for maintaining network stability and ensuring prompt resolution of emerging issues.

These insights also include detailed information about network components and their performance. For instance, identifying which photonic services cross a specific fiber (e.g., OTS1) or determining which modems are in use for a particular optical service (e.g., SVC- 1) can help operators understand the current network configuration and its operational status. Additionally, insights such as the average time to failure for similar equipment in the network or identifying geographic regions with higher rates of network issues provide valuable context for proactive maintenance and resource planning. By leveraging these direct insights, operators can maintain a well-functioning network with minimal downtime and optimal performance.

5.4.2. Operational Insights Requiring Further Analysis

Network Operational Insights in this category require deeper analysis and possibly simulation to derive meaningful conclusions. These insights often involve complex scenarios where simple monitoring data is insufficient, and further investigation is needed to understand the underlying causes or to predict future behavior.

Insights that require investigation and simulation often involve predictive analytics and scenario planning. For example, determining whether an L0 optical service can be created between two cities (e.g., city A and Y) involves analyzing the current network topology, available resources, and potential constraints. Similarly, understanding why an IP TE-tunnel cannot be established between two points (e.g., point A and B) may require simulation of different routing scenarios and examination of network policies. These investigations help operators to not only troubleshoot current issues but also to plan and optimize future network expansions and configurations.

These insights are crucial for long-term network health and performance optimization. Identifying the most common failure points in the network or detecting signs of degradation in wireless network performance requires a combination of historical data analysis and predictive modeling. By simulating different maintenance activities based on current network health, operators can prioritize tasks that will have the most significant impact. For instance, understanding what maintenance activities are needed based on the current network health can help in scheduling proactive maintenance that prevents future outages. These insights enable operators to take a strategic approach to network management, ensuring sustained performance and reliability over time.

5.5. Network Configuration Management

AI can assist in automating the generation and enforcement of network configurations, significantly enhancing network reliability and performance. By leveraging AI/Gen-AI algorithms, network operators can automate the creation of configuration templates that are precisely tailored to specific network requirements. These templates can encompass a wide range of settings, such as Quality of Service (QoS) parameters, Access Control Lists (ACLs), tunnel configurations, and service configuration ensuring that each network segment is optimized for its intended purpose. This automation not only speeds up the deployment process but also reduces the likelihood of human errors that can occur during manual configuration, leading to a more robust and efficient network infrastructure.

Furthermore, AINetOps can play a role on validation of network configuration, i.e., "network configuration audit". AINetOps plays a crucial role in validating configurations against predefined network configuration, ensuring that all network setups comply with intent configuration. By continuously monitoring network configurations, AINetOps can detect and flag any deviations or misconfigurations that could pose security risks or operational inefficiencies. For example, an AI system can identify inconsistencies in ACLs that might allow unauthorized access or detect suboptimal QoS settings that could degrade service quality. By proactively addressing these issues, AINetOps helps maintain the integrity and performance of the network, enabling operators to focus on strategic initiatives rather than troubleshooting configuration errors. This proactive approach to configuration management not only enhances network security and efficiency but also supports the dynamic and scalable nature of modern network environments.

5.6. IP/Optical Multi-layer Planning

Multi-layer planning is an approach that integrates the planning of IP and optical networks based on traffic patterns, network simulations, and capacity planning. By analyzing these factors, IP optical network can be designed to optimize resource allocation, enhance network efficiency, and ensure the network can handle current and future demands, resulting in a more resilient and scalable infrastructure.

5.7. Cross-Layer and Multi-Layer Optimization

AI can address the dependencies between different network layers, such as IP and optical layers, by integrating data and decision- making across these layers. Multi-layer optimization algorithms ensure resource efficiency and performance by aligning the goals of individual layers, such as minimizing power consumption at the physical layer while maintaining SLA guarantees at the application layer.

Moreover, Network Operational Insights facilitate informed decision- making for network optimization and capacity planning. By having a detailed understanding of network usage patterns, traffic flows, and performance metrics, operators can make data-driven decisions to optimize resource allocation and improve overall efficiency. This insight is particularly valuable in multi-layer IP/Optical networks, where the interplay between different network layers can be complex. By leveraging these insights, operators can ensure that both the IP and optical layers are operating harmoniously, leading to optimal performance and cost efficiency. In essence, Network Operational Insights empower operators with the knowledge needed to maintain a high-performing, resilient, and future-proof network infrastructure

5.8. Traffic Optimization

Another AINetOps operational benefits is "Traffic Optimization" where IP/Optical network traffic flows can be monitored and appropriate adjustments to network protocols, network topology, network configuration, load balancing, bandwidth allocation and so on can be dynamically initiated. AINetOps traffic optimization considers multiple factors such as latency, packet loss, and link utilization, enabling networks to adapt to changing conditions in real time.

Expanding on this, AINetOps traffic optimization leverages advanced algorithms to continuously monitor network conditions and predict potential congestion points before they impact service quality. By analyzing historical data and real-time metrics, machine learning models can forecast traffic patterns and proactively adjust routing decisions to ensure optimal performance. For instance, AINetOps can reroute traffic through less congested paths when high utilization is detected, balancing the load and enhancing overall network efficiency. This intelligent management reduces latency and packet loss while maximizing bandwidth utilization.

Furthermore, traffic optimization enhances the network's ability to respond to sudden changes in demand, such as peak usage times or unexpected traffic spikes. Traditional static configurations may struggle with such fluctuations, leading to bottlenecks and degraded performance. With AI, the network can dynamically reconfigure itself in real-time, redistributing traffic loads and reallocating bandwidth as needed. This adaptability reduces the need for manual interventions and allows network operators to focus on strategic initiatives. In essence, AI-driven traffic optimization enables networks to be more resilient, responsive, and capable of delivering consistent high-quality service.

Note that "Traffic Optimization" AINetOps operational benefits is closely related to "Predictive Analytics" covered in Section 5.3.

5.9. Closed-Loop Automation

Closed-loop automation systems use AI to adjust network configurations based on real-time data dynamically. Reinforcement learning (RL) algorithms and policy-based decision frameworks can automate traffic engineering, resource allocation, and fault remediation tasks. AI-driven systems ensure optimal network performance without human intervention by continually monitoring network state and applying corrective actions.

5.10. Network Maintenance and Cleanup

AI can automate cleanup operations by identifying and resolving transient issues, removing redundant configurations, and optimizing resource utilization. These tasks may involve the identification of "stale" network states or unused resources, enabling networks to operate more efficiently.

5.11. Network API Construction

Another significant operational benefit of implementing AINetOps in single-layer or multi-layer IP/Optical networks is the generation of various Network Controller APIs. These APIs are essential for the seamless integration of network controllers (whether IP, Optical, or multi-layer) with Operational Support Systems (OSS) or other network controllers. A key advantage of this operational benefit is that operators do not need to possess in-depth knowledge of the APIs. Typically, network operators spend considerable time creating and verifying APIs to integrate IP or Optical network elements with the broader management layer, including OSS/BSS. By developing robust and versatile APIs, network operators can ensure smooth communication and coordination between different network management systems, thereby enhancing overall network efficiency and performance

The APIs developed for network controllers serve as a bridge, enabling the OSS to interact with the underlying network infrastructure in a more dynamic and automated manner. This integration allows for real-time data exchange, automated provisioning, and efficient fault management, which are essential for maintaining optimal network performance. Moreover, these APIs facilitate the orchestration of network resources across different layers, whether it be IP or Optical, ensuring that the network can adapt to varying demands and conditions with minimal manual intervention.

AINetOps leverages the power of Generative AI (Gen-AI) to further enhance this integration process. By translating the operator's intent into precise network controller APIs, Gen-AI enables a more intuitive and user-friendly approach to network management. This translation capability ensures that even complex operational requirements can be seamlessly converted into actionable commands for the network controllers. This not only reduces the operational burden on network engineers but also significantly enhances the agility and responsiveness of the network to changing conditions and user demands.

5.12. AI-Driven Security Monitoring

AI is becoming a cornerstone of modern network security, enabling proactive, adaptive, and intelligent measures to safeguard network operations against a rapidly evolving threats. By leveraging AI, network operators can enhance their ability to detect, prevent, and respond to threats in real-time while automating complex security processes. This section details the key areas where AI drives security enhancements in network operations.

5.12.1. Threat Detection and Mitigation

AI significantly enhances threat detection and mitigation through ML and deep learning. By analyzing vast amounts of network traffic data, AI models identify unusual patterns and behaviors indicative of malicious activity. This includes detecting anomalies that signal threats like zero-day attacks or insider threats, generating real-time alerts, and incorporating external threat intelligence to recognize known attack signatures. Together, these capabilities enable faster response times and improved threat recognition.

5.12.2. Intrusion Detection and Prevention

AI improves intrusion detection systems (IDS) and intrusion prevention systems (IPS) by enhancing accuracy and reducing false positives. It achieves this through behavioral analysis, which identifies unauthorized access or suspicious activities, and automated responses that isolate compromised devices or block malicious IP addresses. Additionally, AI’s adaptive learning capabilities ensure continuous updates to address new threats in dynamic environments.

5.12.3. Security Policy Automation

Using AI would simplify the creation and enforcement of security policies by automating configurations and adjustments, reducing the potential for human error. It dynamically updates firewall rules and access controls based on real-time threat intelligence, assigns risk scores to network devices and applications to prioritize enforcement, and ensures compliance with regulatory standards by monitoring for deviations and recommending corrective actions.

6. AINetOps Scenarios and Use-cases

This section further expands Section 5 by exploring scenarios and use cases for applying AINetOps in network operations, focusing on their architectural, procedural, and protocol-level requirements. Each use case highlights how AINetOps can be leveraged to address challenges in network management and optimization, while identifying the relevant IETF protocols, interfaces, and data models that are involved or need enhancement.

For every use case described, the following dimensions are examined to provide a comprehensive understanding of its implications and requirements.

- Architecture: The high-level architecture necessary to support the use case, including control-plane and data-plane interactions, as well as integration points for AI-driven systems
- Interfaces and APIs: The key interfaces between AI systems and network elements, including management APIs (e.g., NETCONF, RESTCONF, gNMI) and telemetry interfaces
- Protocols: IETF protocols involved in enabling the use case, and potential extensions to existing protocols to accommodate AI- driven operations.
- Data Models: The data models required to represent network state, telemetry, policies, and configurations
- Processes and Procedures: Workflow considerations for integrating AI systems into existing operational practices, including training, validation, and deployment.

- Alignment with IETF Standards: Analysis of how existing IETF standards can be leveraged or extended to support the use case.

6.1. Network Active and Reactive Assurance

Network active and reactive assurance, both at the single- layer (IP or Optical) and multi-layer (IP over Optical), are critical components in maintaining the health and stability of modern IP, Optical, and IPoDWDM networks. This process involves the identification and resolution of network issues as they arise, ensuring that any disruptions or degradations are promptly addressed. By employing AINetOps techniques, network engineers can quickly pinpoint the root cause of problems, whether they originate in the IP layer, the optical layer, or across both. This reactive approach is essential for minimizing downtime and maintaining the quality of service expected by network users.

In single-layer troubleshooting, the focus is on isolating and resolving issues within a specific layer of the network. Multi-layer troubleshooting, on the other hand, requires a more integrated approach, as it involves identifying and resolving issues that span across multiple layers of the network. This could include problems where an issue in the optical layer affects the IP layer.

In both reactive and active assurance, network faults have already occurred. These faults may include impairments such as optical fiber cuts, IP packet drops, IP link latency issues, or Threshold Crossing Alarms (TCA), among others.

As illustrated in Figure 3, reactive assurance assumes that a fault occurs in the IP/Optical network (Step A) and is subsequently detected by the operator through various means (Step B). Detection methods may include alarm monitoring, performance telemetry data analysis, or customer reports indicating service disruptions. To initiate troubleshooting, the operator can launch the AIOps-Assistant, which acts as the front-end interface for AINetOps (Step C). The assistant then utilizes the backend assurance and troubleshooting mechanisms, leveraging a Gen-AI multi-agent framework. In Step D, a dynamic workflow is executed to diagnose the issue and identify potential root causes. Optionally, at Step E, the Gen-AI dynamic workflow can recommend remedial actions to resolve the issue and implement these actions in a closed-loop fashion, ensuring automated network recovery.

```
                                       |-------------------|
                                       |  Gen-AI based     |
                    (E) |--------------|  Multi-Agent      |
                        |              |  Dynamic workflow |
                        |              |-------------------|
                        |                      ^
                        |                      | (D)
                        v                      |
                |---------------|              |
                |   P-PNC(s),   |        |-----------|
                |   O-PNC(s),   |        |   AIOps   |
                |   MDSC        |        | Assistant |
                |---------------|        |-----------|
                        ^                      ^
                        | (A)                  | (C)
             +----------|----------+           |
             |                     |          (B)
             |  IP/Optical Network |
             |                     |
             +---------------------+

Legend:
(A) A fault happened in the network
    (e.g., Fiber cut, IP packet drop, TCA crossing etc.)
(B) Operator is aware of the network issue
(C) To start troubleshooting, Operator starts AIOps-Assistant
(D) Start troubleshooting using Gen-AI multi-agent dynamic workflow
(E) Optional remedial actions
```

Figure 3: Multi-layer Reactive Assurance Using Gen-AI

In both reactive and active assurance, network faults have already occurred. These faults may include impairments such as optical fiber cuts, IP packet drops, IP link latency issues, or Threshold Crossing Alarms (TCA), among others.

The active assurance and troubleshooting process is illustrated in Figure 4. In contrast to Figure 3, active assurance assumes that a fault occurs in the IP/Optical network (Step A) and is subsequently detected automatically by higher-layer controllers (Step B). These controllers may employ detection methods that include monitoring alarms, analyzing performance telemetry data, or processing customer reports indicating service disruptions. To initiate troubleshooting, the detection logic launches the AIOps-Assistant, which serves as the front-end interface for AINetOps (Step C). Steps D and E are identical to those depicted in Figure 3.

```
                                       |-------------------|
                                       |  Gen-AI based     |
                    (E) |--------------|  Multi-Agent      |
                        |              |  Dynamic workflow |
                        |              |-------------------|
                        |                      ^
                        v                      | (D)
                |---------------|              |
                |   P-PNC(s),   |  (C)   |-----------|
            (B) |   O-PNC(s),   | -----> |   AIOps   |
                |   MDSC        |        | Assistant |
                |---------------|        |-----------|
                        ^
                        | (A)
             +----------|----------+
             |                     |
             |  IP/Optical Network |
             |                     |
             +---------------------+

Legend:
(A) A fault happened in the network
    (e.g., Fiber cut, IP packet drop, TCA crossing etc.)
(B) The higher layer Controller notifies Operator
(C) To start troubleshooting, AIOps-Assistant starts automatically
(D) Start troubleshooting using Gen-AI multi-agent dynamic workflow
(E) Optional remedial actions
```

Figure 4: Multi-layer Active Assurance Using Gen-AI

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.2. Network Pro-active Assurance

Unlike reactive and active assurance, proactive assurance does not wait for a fault to occur in the IP/Optical network. Instead, the network is continuously monitored through a series of trending and forecasting processes designed to detect early signs of deterioration that may eventually lead to faults.

As illustrated in Figure 5, achieving proactive assurance involves running multiple processes that continuously monitor network performance. These processes collect and analyze a wide array of network telemetry data—including performance monitoring (PM) data, alarms, logs, network topology, and inventory details (Step A). By employing various techniques including advanced AI/ML algorithms, these processes provide real-time trending and forecasting insights, identifying patterns and anomalies that could indicate potential degradation (Step B).

When these background processes detect any signs of deterioration or anomalous behavior, they trigger the AIOps-Assistant for further investigation (Step C). The AIOps-Assistant then leverages a Gen-AI multi-agent framework to initiate the assurance and troubleshooting procedures. In Step D, a dynamic workflow is executed to thoroughly diagnose the emerging issue and identify potential root causes. Optionally, at Step E, the Gen-AI dynamic workflow can recommend remedial actions to resolve the identified issues. These recommendations can be implemented in a closed-loop fashion, ensuring automated network recovery and continuous improvement of network performance. This proactive approach not only mitigates the risk of unexpected network faults but also optimizes operational efficiency by addressing issues before they escalate into service-impacting events.

Furthermore, by integrating advanced analytics with automated corrective measures, proactive assurance enhances overall network resilience. It enables network operators to maintain a high quality of service and reliability, even in complex and dynamic network environments.

```
                                          |-------------------|
                                          |  Gen-AI based     |
       (E) |------------------------------|  Multi-Agent      |
           |                              |  Dynamic workflow |
           |                              |-------------------|
           |                                        ^
           v                                        | (D)
    |---------------|                               |
    |   P-PNC(s),   |  (B)   |-----------| (C)  |------------|
(A) |   O-PNC(s),   | <----> | Monitoring| ---->| AIOps       |
    |   MDSC        |        | Processes |      | Assistant  |
    |---------------|        |-----------|      |------------|
            ^
            |
  +---------|-----------+
  |                     |
  |  IP/Optical Network |
  |                     |
  +---------------------+

Legend:
(A) Collect the IP/Optical telemetry data, inventory, logs etc.
(B) Processes which monitor the network
(C) Upon detection of potential issue, start AIOps-Assistant
(D) Start troubleshooting using Gen-AI multi-agent dynamic workflow
(E) Optional remedial actions
```

Figure 5: Multi-layer Pro-active Assurance Using Gen-AI

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.3. Network Anomaly Detection

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.4. Network Predictive Maintenance

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.5. Detection of Network Misconfiguration

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.6. Generate Node Configuration

Generate node config with certain customer requirement (e.g., certain QOS, policy, ACL, tunnels, ...)

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.7. Cognitive Search On Internal Operator Data

Cognitive Search on internal Enterprise MOP, documentation, content etc.

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.8. Network Operator Assistant

Operator-Assistant as a virtual-expert-network-engineer.

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.9. Gen-AI based Network Operational Insights

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.10. Network Traffic Prediction

Telefonica use-case: Traffic-prediction using AI

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.11. Multi-layer Use-case

Multi-layer aspect of above use-cases, e.g.,

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.12. Multi-layer Network Planning

IP/Optical Planning, multi-layer optimization

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.13. Causality Discovery

Causality discovery: you want to know to be updated by Vincenzo.

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.14. Network Clean Up

Clean-up procedure in the network

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

6.15. Other Use Cases

To be discussed and agreed.

- Architecture

To be added.

- Interfaces and APIs

To be added.

- Protocols

To be added.

- Data Models

To be added.

- Alignment with IETF

To be added.

7. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Appendix A. IANA Considerations

This document has no IANA actions.

Acknowledgments

This work has benefited from several discussions at the IETF and the AI4NETWORK Side Meetings.

This work is supported by the UK Department for Science, Innovation and Technology under the Future Open Networks Research challenge project TUDOR (Towards Ubiquitous 3D Open Resilient Network).

Contributors

Cheng Li
Huawei
Email: c.l@huawei.com

Daniele Ceccarelli
Cisco
Email: dceccare@cisco.com

Arashmid Aakhavain
Huawei
Email: arashmid.akhavain@huawei.com

Oscar González de Dios
Telefonica
Email: oscar.gonzalezdedios@telefonica.com

Ignacio Dominguez Martinez-Casanueva
Telefonica
Email: ignacio.dominguezmartinez@telefonica.com

Vincenzo Riccobene
Huawei
Email: vincenzo.riccobene@huawei-partners.com

Nathalie Romo-moreno
Telekom
Email: nathalie.romo-moreno@telekom.de

C. L.
Huawei
Email: c.l@huawei.com

Authors' Addresses

Reza Rokui
Ciena
Email: rrokui@ciena.com

Daniel King
Lancaster University
Email: d.king@lancaster.ac.uk