Evolving Challenges and Solutions in Network Management

Jaime Jiménez
jaime.jimenez@ericsson.com
Ericsson, ER
Jorvas, Finland

Scott Mansfield
scott.mansfield@ericsson.com
Ericsson, BNEW TS ST
Jorvas, Finland

Raquel Rodriguez A
raquel.a.rodriguez@ericsson.com
Ericsson, ETAC
Jorvas, Finland

Mikko Pesonen
mikko.pesonen@ericsson.com
Ericsson, ETAC
Jorvas, Finland

Vesa Torvinen
Vesa.Torvinen@ericsson.com
Ericsson, ETAC
Jorvas, Finland

ABSTRACT

This paper explores network management challenges and solutions, emphasizing scalability, telemetry, and security. It underscores the impact of AI and machine learning in enhancing operations via platforms like the Ericsson Transport Automation Controller (ETAC). The discussion includes legacy system complexities and diverse data sources, advocating for standardized schemas and efficient data streaming. It also covers the transition to zero-trust architectures and generative AI, highlighting the need for collaboration to create scalable, secure, and interoperable solutions. These insights aim to guide the industry in meeting modern telecommunications demands.

This paper is submitted in full conformance with the provisions of BCP 78 and BCP 79.

IAB NEMOPS WS, December 2024,
.

KEYWORDS

network management, scalability, telemetry, security, AI, zero-trust, interoperability

Reference:

Jaime Jiménez, Scott Mansfield, Raquel Rodriguez A, Mikko Pesonen, and Vesa Torvinen. 2024. Evolving Challenges and Solutions in Network Management. In *submissions to the IAB Next Era of Network Management Workshop*, 6 pages.

1 INTRODUCTION

The IAB workshop on the Next Era of Network Management Operations (NEMOPS) serves as a pivotal platform for fostering dialogue between network operators and protocol developers. This initiative is instrumental in guiding the Internet Engineering Task Force (IETF) as it evolves network management protocols. The workshop's primary objectives are to assess past achievements and delineate future requirements for network management operations.

In this paper, we introduce a comprehensive analysis of the current challenges and emerging solutions in network management. The subsequent sections delve into various facets of network management and operations. The **Overall Architecture** section 1.1 provides a detailed overview of the standard components within a network management controller, focusing on the Ericsson Transport Automation Controller (ETAC) and

its integration with other network elements. The **Scalability** section 2 examines the challenges of scaling network models and protocols, highlighting the need for standardized models. The **Telemetry** section 3 discusses the complexities of data transmission and the importance of efficient data streaming. The **Security** section 5 addresses the diverse security protocols and the shift towards zero-trust architectures. Finally, the **Network Management Evolution** section 6 explores future trends, including the role of generative AI and new standard interfaces.

1.1 ETAC overal Architecture

Ericsson Transport Automation Controller (ETAC) [12] is a cloud-native Transport Automation and SDN Controller that leverages artificial intelligence and machine learning to deliver advanced analytics and automation functionalities across microwave, IP, and optical fronthaul networks.

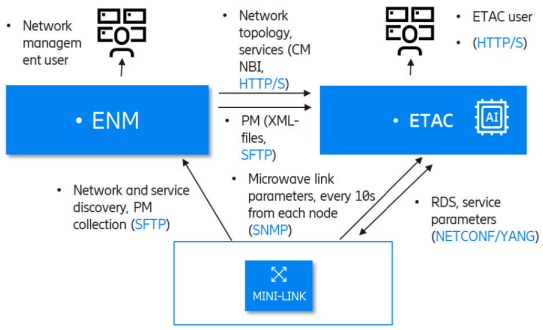

Figure 1: General Architecture

The **Ericsson Network Manager (ENM)** is a centralized platform responsible for managing network and service discovery, as well as collecting performance metrics. ENM interfaces with network elements like microwave nodes, known as **MINI-LINK**, to gather critical performance management (PM) data using **SFTP** [15].

ENM also exposes network topology and service information to external systems through its Configuration Management Northbound Interface (CM NBI) over **HTTP/S** [13], enabling seamless integration with other platforms. This allows **Network Management Users** to monitor and control the network environment via a secure web-based interface.

On the other side of the ecosystem lies the **ETAC** platform [12], an AI-enhanced tool designed to provide deeper insights and advanced analytics. ETAC communicates with ENM to retrieve PM data via **SFTP** [15], ensuring it has the necessary information to optimize network performance. ETAC also interfaces with MINI-LINK directly, using **SNMP** [10] to receive real-time microwave link parameters. These parameters help ETAC maintain a granular view of the network's operational status.

Furthermore, ETAC leverages **NETCONF/YANG** [3, 11] to configure and manage RDS (Radio Data System) and service parameters within MINI-LINK. This protocol enables precise, programmatic control over network devices, aligning with the industry's shift towards more automated and dynamic network configurations.

Finally, both platforms provide secure **HTTP/S** [13] interfaces for their respective user bases—ENM for Network Management Users and ETAC for ETAC-specific users.

2 SCALABILITY

YANG Schema Mount

Scalability in YANG presents significant challenges, as highlighted by Boyd [9]. The concern is about the viability of the current implementation of YANG Schema Mount [4] and the need to support a mechanism that is better suited for partitioning the data in the hierarchical data tree.

Even an enhanced solution for this issue will really only be solved by a better underlying modeling implementation including ACID/transactional, time-series, object-relational views with a query-language and the ability to add triggers or embedded code that becomes part of the solution. The complexity of YANG is intensifying, largely driven by its hierarchical architecture.

Efficient Data Streaming for Analytics

The efficient and scalable transfer of analytics data from its source to post-processing systems remains a significant challenge. Legacy network elements predominantly rely on periodic data harvesting, which imposes unnecessary load on the network elements and delays data accessibility. To address this, data sources should implement active streaming of data to post-processing systems immediately upon production. This approach

ensures that post-processing systems and closed-loop automation have access to data in near real-time.

3 TELEMETRY

Quality of data

Legacy network elements generate data that is not optimized for modern IT-style post-processing analytics systems. This data requires embedded metadata within its schema to support long-term storage and external post-processing, detailing the "what, where, when, and by whom," and identifying the precise source, such as a container, pod, application, node, or CaaS-cluster.

Currently, the lack of alignment in analytics data schemas and metadata complicates and increases the cost of post-processing and analytics. Simple discrepancies, like varying timestamp formats, can cause significant issues. Ideally, standardized, extendable schemas and encodings for different analytics data types would simplify data processing across diverse vendor systems.

Reliability of telemetry data may be less critical when used for visualization purposes and manual check-ups, however, it becomes crucial once telemetry is used as input for AI training and assisted network configuration

Diversity of data

Currently, analytic data is accessed through various APIs and follows diverse patterns (e.g., file harvesting, SNMP for FM data streaming, state notifications via NETCONF/RESTCONF, etc). This diversity complicates data collection and ingestion processes. There is a pressing need for an efficient, scalable, and universal transfer system to stream analytics data from its source to post-processing systems. This system must be optimized for bandwidth and CPU efficiency, ensure security, and be applicable to all types of analytics data streams, including metrics, events (e.g., alarms and notifications), logs, and state data.

Lineage of data

It is essential to establish the lineage and integrity of any record used for purposes beyond visualization. Utilizing data with uncertain integrity can introduce new attack vectors, such as enabling adversaries to exploit closed-loop automation by manipulating the input data. It is important to note that analytics data may flow directly from the source to the post-processing system; however, there are instances where data may traverse cloud provider PaaS functions. Therefore, a mechanism to ensure data integrity across multiple domains is necessary.

State-Data Handling

In passive data sources where analytics data is just exposed (as opposite to streamed) the data has to be actively harvested by external entities, thus there must be APIs or interfaces for collection of such data. In systems where data is streamed, the data sources (often involved in critical functions such as traffic handling) do not need to expose interfaces for harvesting analytics data, which makes the attack surface smaller and system more secure in general.

Modern network elements have a lot of state-data which can not be efficiently leveraged through config model notifications. There are components and elements in the applications/data sources, which one does not to expose in a model, but still the analytics data about the state of such components should be available for post-processing systems. For example, one ideally would like to keep the model of cloud service realization agnostic, and use the same model for the cloud service, whether the application-instances of those services run in virtual machines or in container. Having to model compute resources in order to convey the state data would make it very tricky to separate realization and model from each other, and keep the model backwards compatible as the application realizations evolve and technologies change.

4 QUERY RANGE

TBD!

5 SECURITY

Security challenges

Security configuration in network management is complex due to the absence of a unified infrastructure. This complexity arises from the need to support multiple security protocols across diverse devices and vendors. Key points include:

- **Diverse Protocols:** Network management applications must accommodate various security protocols, such as TLS, SSH, and username/password mechanisms.

- **TLS Potential:** TLS, especially with client-server certificates, is a strong candidate for unified security but lacks universal support across all network management protocols and devices.
- **SSH Limitations:** there is no security infrastructure available that would distribute and help verifying the SSH public keys and facilitate flexible re-keying.The security configuration of SSH itself remains to be manual.
- **Username/Password Usage:** Widely used for basic access and protocols like SNMPv3. Mechanisms for centralized authentication exists but cannot completely replace the need for local authentication because centralized mechanisms may not be always available. Manual security configuration leads easily to poor security practises as key renewals, password upgrades are easily neglected simply because it is error prone and expensive.

Standardization process

The transition from standards to widespread network deployment is often very slow, particularly when new standards are to replace existing components. While implementing a new mechanism on a single device can be swift, updating all network devices is time-consuming. Management applications typically require market adoption or commitment to the new mechanism before implementation is deemed worthwhile. For this reason, phasing out legacy security mechanisms is challenging.

Zero-Trust Architecture

Ericsson develops products that are configured to use secure protocols and configurations by default. But we still see in legacy networks that sometimes the transport network is assumed to be secured, trusted, so that a lower degree of security is sometimes accepted. This may work in some networks but the trend is definitely towards zero-trust.

Regulators and local legislation is also setting new requirements for critical infrastructure, such as telecom networks. The interest is not only on the security capabilities required from the network devices but also development processes, documentation, FOSS usage, security assurance and various aspects of the way how networks are deployed and managed.

One unfortunate reality is that some network devices in life networks are actually very old. If the network operates correctly, any upgrade or change to it may start looking like a risk. This may lead to neglection of software and security upgrades. This could work in the walled-garden paradigm but definitely not anymore in zero-trust. Continuous deployments and upgrades are the only path to truly secure networks. And all this would need to be automated in secure way, covering the software upgrades, re-configurations and testing.

6 NETWORK MANAGEMENT EVOLUTION

Generative AI

Generative AI (GenAI) is set to transform network management by incorporating AI systems that follow the autonomic networking principles outlined RFC7575.

> "The fundamental goal is self-management, including self-configuration, self-optimization, self-healing, and self-protection." [1]

Agentic architectures, characterized by AI agents that autonomously discover and utilize tools provide dynamic interactions with complex systems, effectively adapting to changes that static codebases cannot. AI agents are capable of decomposing user intents into executable individual steps and can interact autonomously with other systems through well-known interfaces (e.g., Network and Management APIs). Agents can further federate and specialize in multi-agent systems, which improve on challenges such as hallucinations, specialization, and scalability. The interest in multi-agent systems was reflected during the past IETF 121 side meeting, as detailed in the ai4network agenda [14].

Agents are particularly useful in the telecommunications sector, where the complexity of specifications and codebases demands innovative solutions. Moreover, the current trend in 5G Networks is marked by a shift towards exposing network functionalities through APIs. This trend facilitates the integration of agentic systems that can dynamically interact with these APIs.

CoRECONF

The -CONF ecosystem comprises the following components:

- **NETCONF** [11]: Serializing YANG over a stateful TCP connection.

- **RESTCONF** [2]: Serializing YANG over stateless HTTP.
- **CoRECONF** [6]: Serializing YANG modules in a CBOR [5] map over stateless CoAP.

CoRECONF, in particular,is utilized by constrained devices in Low-Power and Lossy Networks, which are typically composed of numerous embedded devices with limited power and memory. Although primarily used for IoT, CoAP has also been specified for the signaling of DDoS-related telemetry [8] and [7], as outlined in the now-concluded DOTS Working Group.

This suggests potential applications for retrofitting CoAP on telemetry or management-type signaling within the network management domain. Specially in UDP-oriented evinronments as CoAP comes with an additional reliability mechanism and in environments where compression and smaller payloads are welcomed.

7 CONCLUSIONS

This paper has explored the evolving landscape of network management, highlighting the challenges and solutions in scalability, telemetry, and security. The integration of advanced technologies such as AI and machine learning within platforms like the Ericsson Transport Automation Controller (ETAC) demonstrates the potential for enhanced analytics and automation in network operations. However, the complexity of legacy systems and the diversity of data sources present significant hurdles that require innovative approaches, such as standardized schemas and efficient data streaming mechanisms.

The transition towards zero-trust architectures and the adoption of generative AI indicate a shift towards more secure and autonomous network management systems. These advancements necessitate a collaborative effort between industry stakeholders and standardization bodies to ensure seamless integration and widespread adoption. As the network management domain continues to evolve, the focus must remain on developing scalable, secure, and interoperable solutions that can adapt to the dynamic demands of modern telecommunications networks.

8 ACKNOWLEDGMENTS

We would like to thank Ericsson for their support of this work. Special thanks to ...

REFERENCES

[1] M. Behringer, M. Pritikin, S. Bjarnason, A. Clemm, B. Carpenter, S. Jiang, and L. Ciavaglia. 2015. *Autonomic Networking: Definitions and Design Goals.* Request for Comments RFC 7575. RFC Editor. https://www.rfc-editor.org/rfc/rfc7575 Informational.

[2] A. Bierman, M. Bjorklund, and K. Watsen. 2017. RESTCONF Protocol. RFC 8040. https://www.rfc-editor.org/info/rfc8040 RESTCONF Protocol.

[3] M. Bjorklund. 2010. *YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF).* Request for Comments RFC 6020. RFC Editor. https://www.rfc-editor.org/rfc/rfc6020 Accessed: 2024-11-07.

[4] M. Bjorklund and L. Lhotka. 2019. YANG Schema Mount. RFC 8528. https://www.rfc-editor.org/info/rfc8528 Standards Track.

[5] C. Bormann and P. Hoffman. 2022. Encoding of Data Modeled with YANG in the Concise Binary Object Representation (CBOR). RFC 9254. https://www.rfc-editor.org/info/rfc9254 Encoding of Data Modeled with YANG in the Concise Binary Object Representation (CBOR).

[6] C. Bormann, P. van der Stok, and A. Sehgal. 2023. CoAP Management Interface (CoMI). Internet-Draft draft-ietf-core-comi. https://datatracker.ietf.org/doc/draft-ietf-core-comi/ Work in Progress.

[7] M. Boucadair and J. Shallow. 2023. Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Configuration Attributes for Robust Block Transmission. RFC 9362. https://www.rfc-editor.org/info/rfc9362 Proposed Standard.

[8] M. Boucadair, J. Shallow, and T. Reddy.K. 2021. Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification. RFC 9132. https://www.rfc-editor.org/info/rfc9132 Proposed Standard, Obsoletes RFC 8782.

[9] A. Boyd. 2023. Scalable YANG. IEEE 802.1 YANGsters. https://www.ieee802.org/1/files/public/docs2023/yangsters-boyd-scalable-yang-1123-v01.pdf Presentation on scalable YANG models.

[10] J. Case, M. Fedor, M. Schoffstall, and J. Davin. 1990. *Simple Network Management Protocol (SNMP).* Request for Comments RFC 1157. RFC Editor. https://www.rfc-editor.org/rfc/rfc1157 Accessed: 2024-11-07.

[11] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman. 2011. *Network Configuration Protocol (NETCONF).* Request for Comments RFC 6241. RFC Editor. https://www.rfc-editor.org/rfc/rfc6241 Accessed: 2024-11-07.

[12] Ericsson. 2024. Ericsson Transport Automation Controller (ETAC). https://www.ericsson.com/en/portfolio/networks/ericsson-radio-system/mobile-transport/ericsson-transport-automation-controller. Accessed: 2024-11-07.

[13] R. Fielding and J. Reschke. 2014. *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing.* Request for Comments RFC 7230. RFC Editor. https://www.rfc-editor.org/rfc/rfc7230 Accessed: 2024-11-07.

[14] Daniel King and Weiqiang Cheng. 2023. ai4network: An IETF Side Meeting for the Discussion of AI and its Applicability to the Network. IETF 121 Side Meeting. https://github.com/

danielkinguk/ai4network/blob/main/ietf121/agenda-121.md

[15] T. Ylonen and C. Lonvick. 2006. *The Secure Shell (SSH) Transport Layer Protocol*. Request for Comments RFC 4253. RFC Editor. https://www.rfc-editor.org/rfc/rfc4253 Accessed: 2024-11-07.