Linnæus University
Sweden

Bachelor Degree Project

Network Management System Selection Process Based on Modern Challenges and Industry Needs

Authors:
Haraldur Blöndal Kristjansson
Lasse-Pekka Kylmäaho
Supervisor: Ola Flygt
Examiner: Mattias Davidsson
Semester: VT 2023
Subject: Computer Science

Abstract

Network management systems (NMS) monitor, configure and maintain computer networks. Network operators providing networking services are responding to the evolving bandwidth, availability, and latency requirements by upgrading from legacy management systems to alternatives utilizing modern technologies. This paper addresses the trends and challenges of transitioning from legacy NMS to modern management systems. The academic research on network management systems is limited, and we aim to provide a knowledge base on the subject matter by conducting a literature review. The literature review consisted of 43 primary studies from which eight themes were identified by conducting thematic analysis. An NMS's typical upgrade and selection process is largely unsystematic and based on anecdotal requirements. We utilize the discovered trends and challenges as the basis for the network management system selection process. The selection process was developed via the design science research methodology. The proposed selection process combines the business problems perceived by network service providers with state-of-the-art network research. The results of the review and the process development outline practical implications in the subject area of NMS and introduce potential future research areas in the field of network management.

Keywords

network management systems, selection process, service providers, network infrastructure

Preface

We would like to take this opportunity to thank our degree project supervisor Ola Flygt from Linnaeus University, who helped us in the right direction and gave valuable feedback throughout the whole research process. We would also like to thank Wexnet and Joakim Grundström for the opportunity to work with them as a part of their project to upgrade from legacy network management to a network management system capable of addressing modern challenges and industry requirements. Additionally, we want to thank our families and close friends for providing us with motivational support and words of encouragement at times of stress. Lastly, we would like to thank the course supervisor Daniel Toll of Linnaeus University, for organizing the thesis workshops and providing us with resources, feedback, and guidance.

Contents

1 Introduction

On January 2022, the European Commission outlined as their target for 2030 to provide secure and digital infrastructures for the residents of the European Union [1]. One of the key action points of the aforementioned agenda is Gigabit connectivity to everyone. The ambitious goals pertaining to the connection speeds coupled with the aims to digitalize 100% of European e-Health and key public services put the network infrastructure providers under more pressure in the ever-growing digital landscape.

1.1 Background

The 2022 Axon study commissioned by European Telecommunications Network (ETNO) highlighted some perceived disparity in the majority of the usage of the network infrastructure being utilized by over-the-top service providers such as streaming platforms who benefit from the network infrastructure greatly but have done little to support its development [2].

The pressure of both the ambitious digital growth agendas of the public sector and the growing private sector of auxiliary service providers puts the telecommunication providers under increased pressure to manage their networks better with more and more automated tools capable of notifying the operators of potential service-level deviations.

The research area of the research project is computer networking and, more specifically, the area of network management systems. The main application area is network infrastructure and network services. The benefits of advancements in the application area have large-scale effects both on the public sector, such as the availability and level of service in e-Health services, as well as the private sector pertaining to OTT services such as media streaming platforms, social media, and voice services [1, 2].

The main target group of the thesis is professionals and researchers involved in the selection, development, or implementation of network management systems. This project proposes a process for selecting network management systems that would answer the current and upcoming challenges of the digital era of the 2030s.

The research project was initiated by the Swedish network service provider company Wexnet[1]. Wexnet is a subsidiary of the municipal energy company Växjö Energi, and they act as the metropolitan network service provider of the Växjö municipality and the neighboring municipalities of Alvesta, Lessebo, and Tingsryd. The motivation for the company-initiated research project stems from Wexnet's plan to upgrade its network management infrastructure to answer modern trends and challenges. In this research project, we aim to cover the current network infrastructure trends and the challenges relating to these trends and propose a selection model for Wexnet's future network management infrastructure.

The results of this research project aim to aid Wexnet's network architects and network engineers in forming motivated choices of network management tools and to aid them in understanding the underlying trends and challenges that cause the

[1] https://wexnet.se/

feature requirements for a network management system (NMS).

1.2 Related Work

The paper ”Network Management Challenges and Trends in Multi-Layer and Multi-Vendor Settings for Carrier-Grade Networks” by A. Martinez et al. [3] presents an in-depth analysis of the interoperability challenges in managing multi-layer and multi-vendor carrier-grade networks. Although published in 2014, this paper provides valuable insights into the management issues faced by Internet service providers (ISPs) in the context of multi-layer infrastructures. The authors discuss various approaches to overcoming the isolation between management ecosystems and enabling inter-layer interoperability, which can significantly reduce operational and capital expenses while facilitating complex management operations.

However, since 2014, numerous advancements have been made in the field of network technologies, including the emergence of network function virtualization (NFV) and the increasing use of AI/ML for network automation and scalability. While the paper by A. Martinez et al. [3] focuses on the challenges and trends of multi-layer network management at the time, our work aims to investigate the broader trends in network technologies and their implications on NMS in the current landscape. Additionally, we provide a practical NMS feature matrix in the form of a tool that summarizes the essential features an NMS needs to fulfill for managing novel network technologies, which can be utilized by network managers when engaging with NMS providers.

As for more recent papers, a paper by Angelopoulos et Al. [4] presents a monitoring framework for 5G service deployments. The paper identifies the key requirements for monitoring in software-defined networking (SDN) and NFV landscapes, highlighting important features that differentiate a monitoring system from the currently available solutions. The proposed solution has been designed to perform real-time monitoring data acquisition and collect event information occurring in the physical and virtual infrastructure resources. Although the focus of their study is on 5G networks, the paper provides valuable insights into the challenges and requirements for monitoring in modern networking technologies, making it relevant to our research. However, our work differs from it as we aim to gather direct requirements imposed by novel networking technologies on the Network Management System (NMS) in the area of fixed-access network management, while the author’s paper is focused on developing a monitoring framework for 5G services.

In the paper ”Defining future SDN based network management systems characterization and approach” [5], Sasidharan et Al. discuss the challenges and approaches for achieving SDN-based NMS by mitigating the limitations of traditional NMS. The paper also explores the potential benefits of SDN in terms of flexibility and programmability and defines the characteristics of a futuristic NMS over SDN. The authors categorize the expectations of an SDN-based NMS and research the key functionalities that can meet these expectations.

The paper provides insights into the characteristics of a futuristic NMS over SDN and highlights the need for a structured approach to designing a well-suited

NMS for SDN. The paper is relevant to our study as it focuses on defining the characteristics of NMS that can manage SDN and identifies the core and augmenting functionalities required for a futuristic NMS over SDN.

L. Bondan et al. [6] present a performance analysis of three prominent virtualization solutions, ClickOS, CoreOS, and OSv, for running Virtualized Network Functions (VNFs). The paper analyzes the NFV management requirements from a network operator's perspective and shows how the right choice of virtualization solution is crucial for the network operator, as it directly affects the network performance and management support.

This paper is relevant to our study as it evaluates the effectiveness of virtualization solutions regarding management requirements, which directly affect network performance and support.

The research by Angelopoulos et al. [4] and Bondan et Al. [6] discuss the management requirements of novel networking technologies, such as SDN and NFV, Sasidharan et al. [5] specifically focuses on SDN-based network management systems' characterization and approach. All three papers provide valuable insights into managing novel networking technologies from different perspectives but do not present a general overview or analysis of requirements. Our work aims to expand on specific management requirements by discovering relevant trends and describing the overall challenges.

Finally, the paper by M. Waseem et al. [7] presents a Systematic Mapping Study (SMS) that aims to identify, analyze, and classify the publication trends, research themes, approaches, tools, and challenges in the context of testing Microservices Architecture (MSA)-based applications.

The paper identifies five research themes characterizing testing approaches in MSA-based applications, and the study found that integration and unit testing are the most popular testing approaches and automated testing and inter-communication testing are frequently reported challenges.

The paper uses thematic analysis (TA) to find the main research themes and open coding and constant comparison techniques from Grounded Theory to analyze the qualitative data extracted from the selected studies to identify testing approaches and challenges. The paper is not directly related to the topic of our study, which is network management systems (NMS). However, the paper's method is relevant to our research project as it provides insights into how to structure a literature review and thematic analysis to identify requirements posed on NMS by the big trends in network technology. The paper's approach to qualitative analysis can serve as a model for the current study.

1.3 Problem formulation

In our review of related literature, we discovered that much of the research in this field has centered on quantitative analysis of specific challenges pertaining to a particular network technology. However, qualitative analysis of the requirements imposed on NMS by upcoming trends in network technologies is hard to come by.

As such, we aim to bridge this gap in the field by conducting a comprehensive thematic analysis of the state-of-the-art technologies in networking and extracting

the possible requirements that these technologies pose on NMS. By combining these requirements with the needs of our target audience, we can design a feature matrix to compare and evaluate enterprise-leading NMS tools.

The knowledge contribution and proposed action of this research project are to analyze current research in the field of Network Management Systems and how current research findings can be used in support of the selection of tools or combination of tools to implement network management. The resulting NMS feature matrix could also provide value to the network engineers aiming to develop network management systems.

The proposed network management selection process will utilize previous research to investigate how well the currently available products answer the challenges researchers and professionals face in the network monitoring field face. Network managers can use the resulting feature matrix to base their NMS tool selection on academic research and expert insight. The potentially improved network monitoring tool selection will have a beneficial effect on the users of the network.

The improvement on the proposed NMS selection process will benefit the customers or users of the network where the network managers have selected the tools to correspond to the novel and current requirements of modern networks. The research project aims to answer the following research questions:

RQ1: What state-of-the-art network technology trends and challenges are most relevant to fixed-access networks?

RQ2: What are the requirements for network management tools to manage and monitor fixed-access networks in light of these trends and challenges?

RQ3: How can current research of network technologies support network service providers in selecting network management systems capable of addressing these trends and challenges?

1.4 Motivation

Networks are becoming more complex and larger, making it difficult to meet customers' needs and increasing operational costs [8]. The increasing networking demands from over-the-top media service streaming and ambitious policy goals further stress the network service providers. Automation is important to address these challenges but can be difficult to implement on traditional network infrastructure [9]. While previous design studies have examined the platforms necessary for this transition and the associated challenges, to the best of our knowledge, there has not been a comprehensive examination of the challenges and potential requirements that network management systems must address [4]. Our research aims to address this gap by designing an NMS selection process consisting of a feature matrix that lists these requirements, a description of selection steps, and an analysis of the ability of current enterprise NMS to address the challenges and requirements. We believe that this research will be valuable not only to network administrators navigating the transition from conventional networking to SDN and NFV networks but also to developers of these systems to understand the requirements necessary to compete in the near-term future of network management.

1.5 Results

In this paper, we present a knowledge base of the technological trends and challenges relating to NMS and a systematic and evidence-based process for network management system selection. We present a design science project consisting of a limited literature review (LLR), thematic analysis (TA), and NMS feature matrix development. Out of 155 studies included in the LLR, we obtained 43 primary studies, of which we identified eight themes relevant to modern network management. The contributions aim to provide an objective foundation for NMS selection and to allow future researchers to use the findings to guide further research.

1.6 Scope/Limitation

The primary limitation of this research project is that it does not involve any experimental laboratory work. The evaluation of existing network monitoring tools will be based on literature review and analysis rather than practical experimentation. The evaluation is limited to the context of fixed access optical networks (FAON) and not 5G/6G wireless services providers. Furthermore, the scope of the research project is focused on the selection process of NMS tools rather than discovering the objectively optimal tool, as this is subjective to the network service provider's needs. Lastly, the research project is initiated by a single NSP, so the scope of the business requirements received is limited. The limitations of this research project could later be expanded on by following future research. Expanding the analysis to wireless networks, including multiple network service providers, and conducting controlled experiments on the tool testing would expand the scope of this thesis project.

1.7 Target group

The main target group of our thesis project is professionals working in the maintenance, design, and development of network infrastructures, namely network service-, internet service- and telecommunication service providers. Professionals could use the theoretical knowledge base of the study to gain a further understanding of the state-of-the-art research themes, and the selection process can allow for more deliberate and informed decisions. Researchers in the field can utilize the reviewed primary studies to gain an overview of recent research, and the open problems can direct future research to address practical societal problems. The proposed selection process could be researched further, and its use in similar problems could be potentially investigated.

1.8 Outline

The research project is outlined as follows. In Section 2, the knowledge gap of the study is described, and the theoretical foundation relating to the subject matter of network management and network management systems is presented. Section 3 describes the multi-paradigm design science research methodology, the research methods, the motivation for the method selection, possible alternatives for the method choices, the reliability and validity of the methods, and the potential ethical considerations. In Section 4, the results of the conducted literature review

and thematic analysis are presented. In Section 5, we present the results of our research in the form of trends and challenges received from the thematic analysis, along with a comprehensive list of features that these trends pose for Network Management Systems (NMS). Additionally, in this section, we introduce the final product of this research project, the NMS feature matrix. In Section 6, analysis of the produced results of the limited literature review, thematic analysis, and the NMS feature matrix are analyzed. Section 7 discusses the validity of the results, the implications of the results for the target group, and the relationship of the findings to prior research. Section 8 concludes the research project, its findings regarding the research questions and generalizability, and proposes future work in light of these findings. The obtained trends and challenges of modern network infrastructure management are included in the Appendix A in further detail.

2 Theoretical Background

In this section, the knowledge gap of the study is described, and the theoretical foundation relating to the subject matter of fixed-access networks, network management, and network management systems is presented.

2.1 Fixed-Access Networks

Wexnet and Fixed Access Networks

Fixed access networks refer to wired networks that deliver connectivity services to end-users through a physical infrastructure, such as copper wires or optical fibers. Unlike mobile networks that accommodate user mobility and rely on wireless communication, fixed access networks are stationary, meaning the user device needs to be physically connected to the network.

Wexnet, our partner company, has its main infrastructure based on fiber-optic fixed access networks. It is essential to clarify that while wireless technologies, such as 5G and the upcoming 6G, are emerging as significant trends and have more various service functions than fixed ones, they were not the subject of our investigation. Our primary focus remained on fixed access networks in alignment with Wexnet's needs. [10].

2.2 Network Management

In essence, network management involves the processes undertaken to ensure a network operates satisfactorily. A satisfactorily operational network successfully transports traffic while adhering to predetermined performance parameters, such as maximum delay or minimum throughput [11].

In this context, we delve into FCAPS, a model for network management introduced by the International Organization for Standardization (ISO) in the early 1980s. FCAPS outlines five key aspects of network management: Fault, Configuration, Accounting, Performance, and Security [11]:

- **Fault Management:** Network faults are inevitable despite proactive preventative measures. Fault management in FCAPS aims to detect these faults, mitigate their impact, and restore the network system. FCAPS proposes a five-step cyclical workflow to handle faults: detection, diagnosis and isolation, correlation and aggregation, restoration, and resolution.

- **Configuration Management:** Ensures that network systems function as expected throughout their lifecycle, including during updates, upgrades, and scaling processes. This area involves both hardware and software management, such as inventory management, allocation management, and software versioning.

- **Accounting Management:** Seeks to optimize resource distribution among network clients. It includes administrative tasks like updating the inventory of network resources, billing management, and determining appropriate permissions and access rights for each network client.

- **Performance Management:** Involves monitoring and enhancing overall network performance. Performance improvements can manifest in several ways, such as maximizing throughput, minimizing latency, and preventing bottlenecks. Performance management's primary goal is to improve service quality and client experience.

- **Security management:** Involves controlling access to network resources and equipment, especially sensitive ones. It prevents improper access and modifications in the network, thereby ensuring network functionality and client security. Security management includes deploying network functions designed to identify and mitigate attacks.

2.3 Network Management Systems

Network Management Systems (NMS) are software applications or platforms that enable network administrators to monitor, control, and optimize network resources' performance and availability. NMS is responsible for detecting, diagnosing, and resolving network issues and providing insights into the overall health of a network infrastructure. By leveraging NMS, network managers can collect performance data, configure network devices, ensure network security, and perform capacity planning and fault management tasks. The ultimate goal of an NMS is to simplify network administration and ensure optimal network performance and end-user Quality of Service (QoS) while minimizing downtime.

Choosing a Network Management System is a task that requires careful consideration and due diligence. NMS plays a crucial role in the overall performance and stability of the network, and any change could significantly impact the organization. Additionally, a change in NMS may require substantial time and resources, as it involves migrating configurations, retraining personnel, and possibly even modifying the network infrastructure.

Before contemplating a change in their Network Management System, network managers must thoroughly assess the current system to pinpoint any weaknesses or limitations that might warrant a change. Additionally, they should examine the compatibility of the new NMS with existing network devices, protocols, and standards. Furthermore, it is essential to consider emerging trends in network technology and the foreseeable future because the time and cost of selecting a new system should not merely cater to the present infrastructure but also consider upcoming challenges and developments in the ever-evolving networking landscape [12].

2.4 Current State and Evolution of Network Technologies

The modern network landscape is evolving rapidly due to increasing demand for high-bandwidth and quasi-instantaneous communication, primarily fueled by over-the-top (OTT) service providers like video-on-demand (VoD) platforms. Consequently, customers expect a higher quality of service (QoS) and quality of experience (QoE) from network service providers (NSPs), placing significant strain on their infrastructure. To meet these demands, NSPs must adopt new technologies

and approaches to optimize network performance, manage traffic effectively, and deliver content efficiently [13].

According to ”The Road to SDN: An Intellectual History of Programmable Networks” by Feamster et al. [14], the traditional network infrastructure is challenging to manage since it often relies on equipment from multiple vendors. These devices run heterogeneous, closed, and proprietary distributed control software. In these scenarios, network administrators typically configure individual network devices using configuration interfaces that vary across vendors—and even between different products from the same vendor. However, this mode of operation is not well-suited to handle modern networks' complex and dynamic nature.

To address these challenges, modern network infrastructures are adopting new technologies such as software-defined networking (SDN), network function virtualization (NFV), Segmented Routing, and artificial intelligence for network automation. These technologies allow for greater flexibility, scalability, and automation in managing complex network environments.

In addition to the new technologies, the changed landscape requires new ways of cooperation among service providers, such as interconnection and peering agreements, as well as the use of network caching and content delivery networks (CDNs) to ensure fast and reliable delivery of content. By leveraging these new approaches, modern network infrastructures can better meet the demands of today's dynamic and complex networks [13].

From our study of past research in our Related Work section 1.2, we found that much of the work done so far has focused on managing individual new technologies or unique ways to handle their network management. But, there hasn't been a lot of focus on how these broader trends impact NMS in the current network environment, especially for fixed-access networks.

In response to this identified knowledge gap, our study enriches existing literature by meticulously examining the impact of these trends on NMS; see appendix A. We aim to supply comprehensive, up-to-date insights into the changing demands of NMS through state-of-the-art network technologies.

Beyond understanding these implications, we construct a practical tool, a NMS feature matrix, distilling the essential characteristics an NMS must possess to handle these dynamic requirements adeptly. This feature matrix, we believe, will serve as a valuable guide for network managers in their interactions with vendors, ultimately aiding them in choosing an NMS that aligns with the complexities of the current and future network technology landscape.

3 Method

This section describes the use and motivation behind the selected methods. The section begins with an overview of the multi-paradigm research methodology followed by a more detailed description of each of the methods used. At the end of the section, we briefly discuss the potential alternatives for our selected methods.

3.1 Research Methods

As the research problem and practical challenge from Wexnet introduce a combination of both a practical business problem and a large body of secondary academic research, we intend to utilize the design science research methodology (DSRM) proposed by Peffers et Al. in 2007 as our methodology [15]. The design science (DS) methodology outlined by the authors aims to provide relevant solutions for important information systems (IS) business problems based on prior research [15].

As outlined in Section 1.4 above, the challenges posed by the shift from traditional hardware-based networking to modern, software-defined, virtualized, and programmable networks is not only recognized by Wexnet but a general challenge that is emphasized with the increased requirements of modern multimedia platforms and the ever-increasing interconnectivity of the world [1, 2, 16].

Integral steps in the DSRM are identifying and motivating the problem and defining the objectives of the improved solution, known as a design artifact. In the context of this research project, we refer to the design science artifact as the NMS feature matrix, as that is the solution for the business problem. The later introduced network management selection process refers to the process of how to utilize the NMS feature matrix. We identify the problem to be solved by combining prior research on the topic of computer networking trends with the requirements outlined by the professionals of Wexnet. The resulting design science artifact will be an NMS feature matrix describing the feature requirements and considerations of a network monitoring system suitable for transitioning from legacy network management infrastructure to an infrastructure capable of answering the requirements of modern-day network service providers.

As design science is a multimethod research method, we use the methods of limited literature review (LLR) [17] and thematic analysis [18, 19] to aid in the gathering of the requirements and the formulation of the NMS feature matrix.

The use of the three methodologies was conducted as follows:

1. **Limited Literature Review:**

   The primary studies discussing computer networking trends and the challenges relating to these requirements are gathered by conducting a limited literature review (LLR) [17]. The term LLR is used to distinguish from implementing a complete systematic literature review with vast iteration steps and iterative quality assessment, data extraction, and data synthesis [17]. We follow the methodology proposed by

Kitchenham et Al., but implement the steps of iteration, quality assessment of primary studies, data synthesis and extraction to lesser degree. All of the steps of the LLR are discussed in Section 3.3 in further detail.

2. **Thematic Analysis:**

   The themes of primary studies resulting from the LLR will be identified by conducting thematic analysis (TA) on the primary studies [18]. The themes identified in the TA phase of the research project will then be used to categorize the feature requirements identified in the primary studies.

3. **Design Science Artifact:**

   Finally, the feature requirements identified from the academic research are combined with the requirement specification received from the NSP, Wexnet. From the combination of the requirements, we devise a list of features a desired NMS would fulfill, compare it to the currently available NMS product solutions to demonstrate the NMS selection process along with a NMS feature matrix to aid in the future selection of NMS products [15].

The resulting feature matrix will aid Wexnet in the selection process of suitable network management tools to replace their legacy management infrastructure. In the following sections, we describe the methodologies in further detail and the relationship between the methods and the research questions can be seen below in Figure 1.

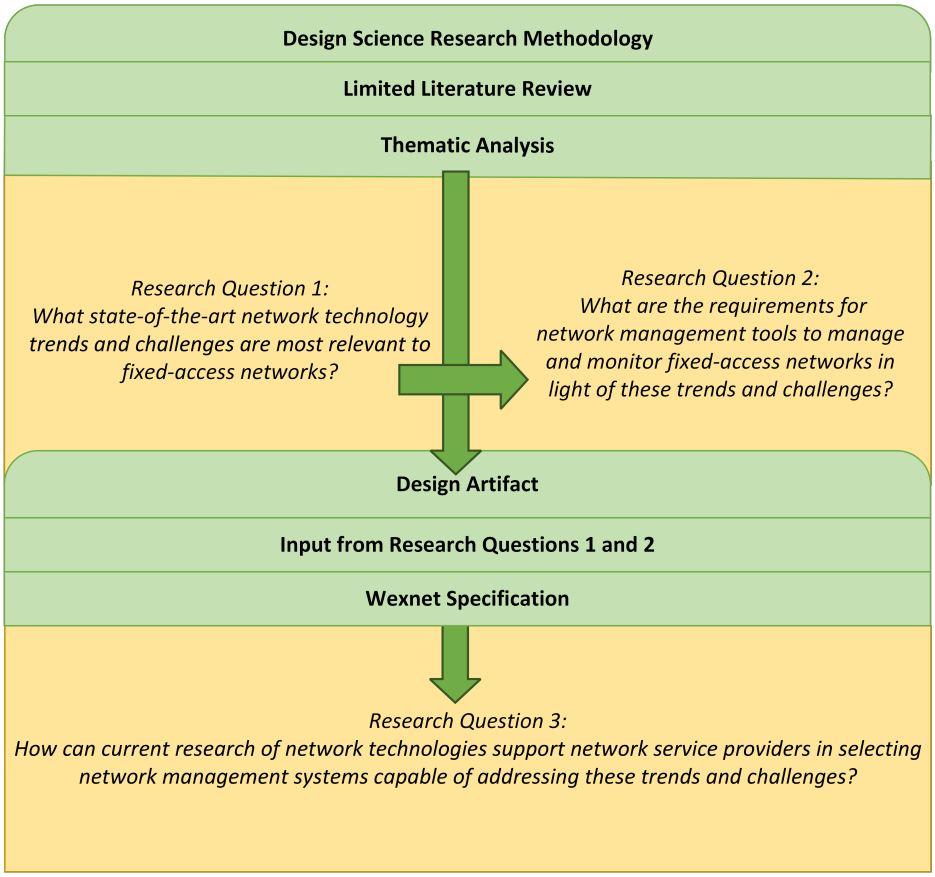

Figure 1: Flow diagram of the usage of the methodologies in relation to the research questions.

The limited literature review is used as the basis for the academic background to answer research questions 1 and 2. The themes to answer research question 1 are discovered utilizing thematic analysis. In addition to the primary studies, the themes discovered from research question 1 are further investigated to discover the requirements. The third research question is answered in the form of the design artifact of the design science research methodology process. The findings of RQ1, RQ2 and the network management specification of Wexnet are used as input for the design of the feature matrix.

3.2 Design Science Research Method

In this section, we start off by firstly giving a brief introduction to the DSRM process, followed by a description of the different research entry points for a DSRM project, and finally, describing the steps of the DSRM process and how the DSRM process is conducted in this research project.

3.2.1 Introduction

Design science is considered the primary methodology of the research project. DSRM process is a problem-solving process, and as such, the motivation for a project utilizing the DSRM stems from knowledge and understanding of a problem

[15, 20].

In ”Guidelines for Design Science in Information Systems”, Hevner et al. describe the goal of DS artifact as both understanding the business problem and solving an unsolved problem or solving a known problem more efficiently or effectively [20]. The company-initiated project forms the basis for the knowledge and understanding of the business problem for the design science process. The Wexnet-specific business problem is further motivated by including further academic research and European publications that highlight the evolving network infrastructure landscape [2].

From the two solution goals outlined by Hevner et al., the selection process proposed by this research project aims to **solve a known problem in a more efficient and effective manner** [20]. The DSRM process can be utilized for various types of business problems, and the entry point for research can vary based on the business problem and the type of problem solution the researchers aim to produce [15].

3.2.2 Research Entry Points

Peffers et al. describe four possible research entry points for initiating a DSRM project in IS: The context or client-centered, design and development-centered, objective-centered, and problem-centered entry points. The research entry points define the activity wherein the research project is started.

Client- or Context-Centered Initiation

The research entry-point for this research project is client-initiated as the need for a more effective solution to select a network management system comes from the NSP Wexnet. We observe the previous practical approach of basing the NMS selection process on professional knowledge and non-academic or unsystematic research and aim to improve on the process by introducing current academic understanding and systematic methodology to the selection process [15]. The research entry point of a DSRM process does not majorly affect the nominal process sequence, as the process is iterative. The nominal sequence of the DSRM process respects the iterative nature of design science and allows for iteration between the activities [15]. The first step of the nominal process sequence is identifying and motivating the problem, and it will be a logical starting point no matter what the initial research entry point was [15].

Problem-Centered Initiation

If the business problem of selecting a network management tool was initially identified from prior research or direct observation of the problem, the research entry point for this research project could have been motivated as problem-centered initiation [15].

Objective-Centered Initiation

Objective-centered initiation is described as a research entry point in which the need for further research is caused by research or industry needs that could be

addressed by developing an artifact. Insufficient measures to abstract or communicate the problem could trigger this research entry. In the context of this research paper, it could have meant developing a high-level grading system for different network management systems [15].

Design and Development-Centered Initiation

An example of design and development-centered research entry point would be a DSRM project wherein the researchers have identified a pre-existing artifact that answers a closely related problem and aim to utilize the DSRM process to investigate the use of the prior artifact for an unrelated problem [15]. In the context of this research project, this could have been a feasible entry point if a solution to a similar problem was identified. The related solution could have then solved the problem or provided a more effective solution.

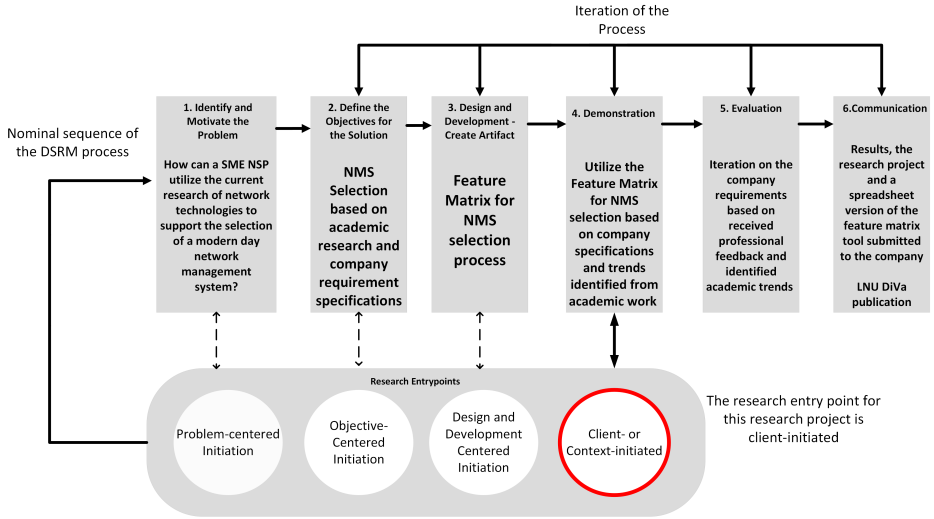

Figure 2: DSRM Process for the feature matrix-based NMS selection. The bidirectional connection between the research points and the activity is visualized by a bidirectional arrow [15].

The four research entry points correspond with the starting activity, as can be seen from Figure 2 above. Regardless of the starting activity or research entry point, the DSRM process remains nominal, and all activities are relevant for all DS research. Figure 2 also visualizes the nominal DSRM process sequence and the activities of DSRM. The process activities will be described in further detail in the sections below.

3.2.3 Activity 1. Problem Identification and Motivation

In the problem identification and motivation activity, the specific research problem is defined, and the value of an improved solution is justified [15]. The resulting problem definition is used to design an NMS feature matrix that can effectively answer the business problem. Thus we divide the problem to allow for the solution to capture the complexity of the problem.

We derive the problem from Wexnet's client-initiated business problem. We base the justification of the value for an improved solution on acknowledging their business problem and providing support for the generalizability of the problem by discovering societal publications and academic research relating to the causes of the problem [1, 2, 21]. The problem is atomized to form the research questions of the research project. In the process of dissecting the problem, we discover the prerequisites of identifying the current trends in network infrastructures and the challenges these trends pose. The prerequisites formed the basis for our research questions 1 and 2 and motivated the selection of the additional methods discussed in the upcoming Sections 3.3 and 3.4.

3.2.4 Activity 2. Define the Objectives for a Solution

In the second step of the DSRM process, we define the objectives for the solution. Research questions 1 and 2, required to define the objectives fully, are obtained by conducting the LLR and TA. The basis for the solution that the NMS feature matrix aims to improve is Research Question 3: "How can current research of network technologies support network service providers in selecting network management systems capable of addressing these trends and challenges?"

The following objectives for the NMS feature matrix are inferred from research question 3:

Artifact Objectives

O1 Provide a more efficient and structured process for selecting a network management system

O2 Combine the requirements for network management tools based on RQ1, RQ2 and Wexnet specification

O3 Compare how well the reviewed NMS solutions answer these requirements

O4 Present the level on which the NMS solution supports a feature

O5 Provide the steps for network management solution selection

The objectives of a DS artifact aim to describe the desirable solution and can describe how the improved solution is expected to solve the problem [15]. The description of the objectives can be either qualitative or quantitative in nature.

3.2.5 Activity 3. Design and Development of the Artifact

The artifact was created by designing and developing an NMS feature matrix that fulfills the objectives outlined in the previous activity. The DSRM process states that the problem dictates the type of the artifact and that the artifact can, for example, be a social resource, an informational resource, a method, or a model [15]. Conceptually the artifact is described as a designed object that includes the research contribution in its design [15].

For the design and development of our NMS feature matrix, we determine that the solution to Wexnets business problem of selecting a new network management system to replace their legacy infrastructure is a feature requirement matrix constructed by combining the company requirement specification with the feature requirements identified by conducting the LLR and TA.

3.2.6 Activity 4. Demonstration

We demonstrate the solution by showcasing the use of the NMS selection process toward available network management system solutions. The demonstration is done to identify how well different NMS fulfill the required specifications. This will showcase how to use the NMS feature matrix to solve the problem [15]. Peffers et Al. state the artifact should be demonstrated with an instance of the problem [15].

3.2.7 Activity 5. Evaluation

In evaluating the artifact, the solution is compared to the objectives defined for the solution in Activity 2. Again the evaluation requires a deep understanding of the problem, which can include quantitative, qualitative, interviews, or satisfaction survey results [15]. In the evaluation phase, the iterative process of DSRM can be utilized, and the researcher can return to artifact development of Activity 4. The iteration is not mandatory, and the DSRM states that the research venue can dictate if such iteration is feasible [15]. For the scope and limited time frame of thesis work, the time available for iteration is limited. However, the future improvements made by Wexnet on the NMS selection process can be seen as part of the iteration process, even if they do not fall under the DSRM itself.

We evaluate the NMS feature matrix by comparing the solution to the objectives stated above and client feedback received from Wexnet. The NMS feature matrix is evaluated by including the company professionals in the iteration and development of the artifact. Wexnet, as the client, has an influence on both the artifact objectives of Activity 2 and the evaluation of these steps. The iteration between activities 2, 4, and 5 is performed and recorded throughout the research project.

3.2.8 Activity 6. Communication

The last activity of the DSRM is the communication of the problem, its importance, the solution artifact to the justified problem, and its effectiveness to researchers and members of relevant target groups [15]. Practicing professionals and researchers of the subject area can be considered as the audience that the communication should reach [15].

We aim to communicate the research project results to the client by submitting Wexnet the spreadsheet version of the NMS feature matrix alongside this research project document. For the academic audience and target group, we will publish this work on the LNU DiVa-publication platform of Linnaeus University. Further publications are not decided, but the potential of an ArXiv release was discussed to provide the work to a broader audience.

3.3 Limited Literature Review

Limited literature review (LLR), was conducted to discover the computer networking trends and challenges investigated in research questions 1 and 2. The DS paradigm requires a deep understanding of the problem to be solved and the problem domain. The aforementioned requirement acts as the motivation behind implementing a partial SLR process to effectively combine the prior research relating to the identification and motivation behind Wexnet's business problem.

3.3.1 LLR Process

Kitchenham et Al. divide the literature review process into three major stages [17]. The three stages of conducting a review are:

1. **Planning the Review**
   (a) Identifying the Need for a Review
   (b) Specifying the Research Questions
   (c) Developing a Review
2. **Conducting the Review**
   (a) Identification of Research
   (b) Selection of the Primary Studies
   (c) Quality Assessment of Studies
   (d) Data Extraction
   (e) Data Synthesis
3. **Reporting the Review**
   (a) Specifying the Dissemination Strategy
   (b) Formatting the Main Review Report
   (c) Communicating the Results (Dissemination)

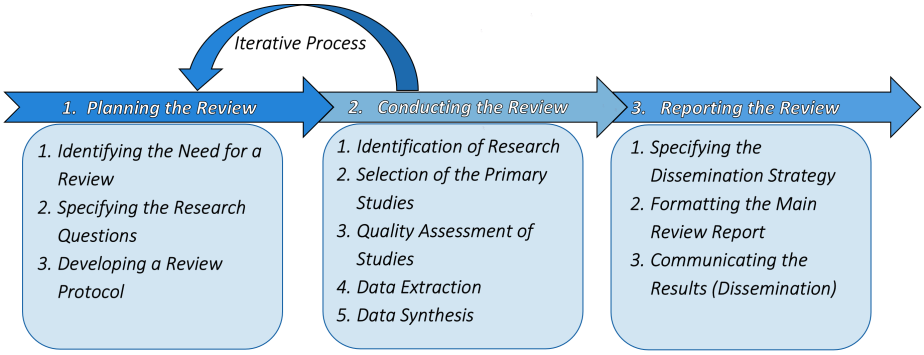

Figure 3: Literature Review iterative methodology process [17]

The sequential literature review process proposed by Kitchenham et Al. [17] can be seen in Figure 3. The iterative nature of SLR shares the iterative nature with the nominal DS process discussed and visualized in Figure 2.

3.3.2 Limited Literature Review Process

In this section, we define how the literature review process is implemented for the conducted LLR and describe how each of the stages of the LLR was implemented. Parts of the literature review process that were not implemented or implemented in a limited capacity are also discussed. Namely, the steps of data extraction, in-depth quality assessment, and data synthesis steps of the methodology were implemented in a limited capacity.

Planning the Review

Identifying the Need for a Review

The need for a review is identified by defining the objectives for the review. We identify the need for the review based on the DS requirement of a deep understanding of the problem topic. The research is directed at current and novel research of network infrastructure, and as such, the review is directed at topical works.

Specifying the Research Questions

The specification of research questions drives and directs the review [17]. Thus, the research questions are an important part of any systematic review. The search process and data extraction of the review must address the research questions.

The usage of DSRM initiates the research project, but the following research questions 1 and 2 are answered by the LLR and the following thematic analysis.

- RQ1: What state-of-the-art network technology trends and challenges are most relevant to fixed-access networks?
- RQ2: What are the requirements for network management tools to manage and monitor fixed-access networks in light of these trends and challenges?

[17]. The research questions are constructed to be suitable with both the DS artifact and to conform to the usage of LLR through iteration of the wording and phrasing of the research questions.

Developing a Review Protocol

The development and specification of a pre-defined review protocol are carried out to reduce the risk of researcher bias based on expectations [17].

Research questions 1 and 2, the timetable of the research project, and the usage of thematical analysis to support the LLR act as the basis of the review protocol. The data extracted from the primary studies are based on the later thematic analysis, and the following DSRM artifact, NMS feature matrix acts as the synthesis of the primary studies. The dissemination of the review is carried out as described in the DSRM activity 6. The review is communicated as part of the research project publication on LNU DiVa and potentially on ArXiv as part of the broader publication.

Conducting the Review

Identification of Research
The aim of a review is described to be to find as many primary studies relevant to the research questions as possible [17]. This is achieved by conducting preliminary searches to identify the digital libraries and sources to include.

For our search strategy, we selected the digital libraries of IEEE, ScienceDirect, ACM, and ArXiv to conduct two searches on each. Iterations and improvements are important in this stage to identify the most relevant digital libraries for the subject area [17]. We initially planned to use ResearchGate and GoogleScholar, but these digital libraries introduced large amounts of secondary publications and duplicate results. ArXiv was included in achieving state-of-the-art and bleeding-edge studies.

The first query is constructed to give current networking trends, and the second one is to provide results for research classified as state-of-the-art. In addition to the query words, the publication date was used to develop the queries matching current and state-of-the-art trends.

The search protocol for the research project is :

1. Initial Search Queries
2. Filter by Title (Include if Uncertain, escalate further)
3. Filter by Abstract (Include if Uncertain, escalate further)
4. Filter by full-text read
5. And finally conduct thematic analysis to provide input for the design artifact (NMS feature matrix)

The search queries and digital libraries can be seen below:

3.3.3 Search Strategy

Search Queries		
Database	**Search No.**	**Search Query String**
IEEE	1	(”networking” OR ”network technology” OR ”network infrastructure”) AND (”state of the art” OR ”cutting-edge” OR ”latest”) AND (”network service providers” OR ”telecom operators” OR ”internet service providers”)
IEEE	2	((”networking” OR ”network infrastructure”) AND (”trends” OR ”future” OR ”novel”) AND (”network service providers” OR ”telecom operators” OR ”internet service providers”) NOT (”5G”))

ScienceDirect	1	((”networking” OR ”network technology” OR ”network infrastructure”) AND (”state of the art” OR ”cutting-edge” OR ”latest”)) AND ((”network service providers” OR ”telecom operators” OR ”internet service providers”))
ScienceDirect	2	((”networking” OR ”network technology” OR ”network infrastructure”) AND (”trends” OR ”future” OR ”novel”) AND (”network service providers” OR ”telecom operators” OR ”internet service providers”))
ArXiv	1	In Abstract: ”networking” OR ”network technology” OR ”network infrastructure” AND ”state of the art” OR ”cutting-edge” OR ”latest” AND ”network service providers” OR ”telecom operators” OR ”internet service providers”
ArXiv	2	”networking” OR ”network technology” OR ”network infrastructure” AND ”trends” OR ”future” OR ”novel” AND ”network service providers” OR ”telecom operators” OR ”internet service providers”
ACM	1	[[Publication Title: ”networking”] OR [Publication Title: ”network technology”] OR [[Publication Title: ”network infrastructure”] AND [Publication Title: ”state of the art”]] OR [Publication Title: ”cutting-edge”] OR [[Publication Title: ”latest”] AND [Publication Title: ”network service providers”]] OR [Publication Title: ”telecom operators”] OR [Publication Title: ”internet service providers”]] AND [[Keywords: ”networking”] OR [Keywords: ”network technology”] OR [[Keywords: ”network infrastructure”] AND [Keywords: ”state of the art”]] OR [Keywords: ”cutting-edge”] OR [[Keywords: ”latest”] AND [Keywords: ”network service providers”]] OR [Keywords: ”telecom operators”] OR [Keywords: ”internet service providers”]] AND NOT [Abstract: ”5g”] AND [E-Publication Date: (01/01/2013 TO 03/31/2023)]

ACM	2	[[Abstract: ”networking”] OR [Abstract: ”network technology”] OR [Abstract: ”network infrastructure”]] AND [[Abstract: ”trends”] OR [Abstract: ”future”] OR [Abstract: ”novel”]] AND [[Abstract: ”network service providers”] OR [Abstract: ”telecom operators”] OR [Abstract: ”internet service providers”]] AND [E-Publication Date: (01/01/2018 TO 02/28/2023)]

Selection of the Primary Studies

The search protocol was utilized to identify potential primary studies on network technology trends. The inclusion-exclusion criteria are then applied to each of the primary study candidates. The criteria are applied throughout the primary study selection process for some of the requirements as the requirements for the language, peer-review, and publication date requirements are apparent at the early stages of the search protocol. Exclusion criteria are implemented to eliminate redundant, ungeneralizable, outdated, or non-peer-reviewed studies.

Inclusion Criteria

Selection criteria:

- Studies that have their main research topic in technologies related to network infrastructure
- Studies that evaluate network infrastructure management solutions or technologies

- -

Exclusion criteria:

- The study, or another version of the study, is already included.
- Studies only investigate a specialized implementation of a network management technology and not a general technology.
- Studies published before 2013.
- Studies that have not been peer-reviewed.
- Studies that are not written in English

Quality Assessment of Studies

The quality assessment of the primary studies was conducted to a limited degree as the primary studies were mainly utilized as the basis for the following thematic analysis. The digital libraries and the peer-reviewed nature of most of the primary studies were a sufficient quality assessment for the purpose of utilizing the LLR

process coupled with the thematic analysis. The motivation for the limited implementation of the quality assessment was due to the nature of the following usage of the data and to comply with the time constraints.

Data Extraction and Data Synthesis

The data extraction and data synthesis steps of the methodology were substituted with utilizing the thematic analysis as a supplemental method. The themes extracted from the data were synthesized as the feature requirements of the proposed NMS selection process. The main objective of the LLR was to provide an adequate knowledge base for the design of the network management selection process and to allow for the identification of relevant trends.

Reporting the Review

Reporting the review is conducted by publishing the research project on the LNU DiVa publication platform. The dissemination and submission of the end product are also provided to Wexnet. The reporting of the review is largely dictated by the DSRM methodology's Activity 6 Communication covered in Section 3.2.8.

3.4 Thematic Analysis

The thematic analysis (TA) is a widely used qualitative analysis method [22]. We utilize TA to identify themes of the primary studies produced by the LLR to discover network infrastructure trends and challenges [18, 19, 22]. In the LLR phase of the research project, we highlighted a lack of qualitative descriptions of both primary NMS studies and current studies describing technological trends relating to the selection of NMS. This motivated the introduction of thematic analysis as a form of qualitative analysis to the research project.

As per Braun et Al., TA is seen as one of the foundational methods for qualitative analysis (QA). We utilize TA to identify and categorize the obtained primary studies in primary research themes and potential sub-themes [22].

Extensive qualitative analysis, qualitative comparative analysis, grounded theory, and coding are all complex research methodologies capable of extracting qualitative traits and themes of large bodies of data sets [22, 18]. Qualitative analysis and thematic analysis aid in the data extraction of research results in varied data, interviews, and research that does not directly address the research question required. For this research project, we aim to utilize TA in a limited capacity by identifying network technology themes from **research which does not directly address the research question requires**.

After obtaining the primary studies from the LLR process, the TA process is conducted in 6 steps outlined by Braun et Al. [22].

1. Familiarising yourself with your data
2. Generating initial code
3. Searching for themes
4. Reviewing the Themes

5. Defining and naming themes

6. Producing the report

The initial step of familiarizing ourselves with the data was already partially conducted as part of the LLR process' full read phase, wherein we selected and obtained the final primary studies. After the final selection, the studies were re-read, and initial ideas for themes and subjects were noted down.

The initial code generation of the studies was conducted from the notes produced in the first step. Themes and keywords relating to the studies were noted down to be later generalized to identify any reoccurring themes in the primary studies. The amount of primary and latent themes was not restricted at this step.

From the initial codes noted down in the second step, we then derived a main theme and potential subthemes if the research had a clearly defined primary and secondary research area.

In the fourth step, the themes were further refined to a more concise and general form. Preliminary primary themes with extremely specified research topics on a certain general research area were generalized. For example, software-defined-optical networking was generalized to the higher-level theme of software-defined networking. The coherent themes identified in this step were moved to the following steps. Both of the researchers conducted the steps outlined, and theme analysis and generalization of high-level themes were made in cooperation to minimize researcher bias.

In the fifth step of the TA process, the coherent naming of the themes was conducted. The name of the high-level themes identified in step four was standardized to define the final name for the network technology themes.

The final step of the described thematic analysis process is the production and analysis of reporting the themes. This step is conducted as part of the results of this research project, and ultimately the thematic analysis forms the outline for the trends and challenges in network management systems. The thematic analysis itself is also reported as part of this thesis project.

3.5 Alternative Methods

Systematic Literature Review

As we conduct a limited literature review as our main supporting methodology of the multimethod DSRM, we could have also opted for a research project strictly conducting an SLR on the topic of network management systems. A systematic review combining novel research on the subject matter could have produced a greater understanding of the proposed future work on network management systems and their selections. Still, it would not have directly given a solution to the business problem of Wexnet. From the LLR process of our thesis, we also recognize the scarcity of academic research discussing network management systems. From the primary studies identified by our LLR, none of the studies cover network management systems as their main topic. SLR as a research methodology is most feasible to utilize when there is a large body of research on a subject matter and there is

a recognized need to draw more general conclusions and trends on the existing research [17].

Controlled Experiment

Another possible methodology we could have used is a controlled experiment. Conducting a controlled experiment would have allowed us to test a limited number of network management solutions for Wexnet. Experimenting is quite similar to the practical approach of a company testing a software solution to compare it to other available or already implemented solutions. When conducting a controlled experiment, scrutinizing the measurements and simulations of the different solutions would likely be much more in-depth than what companies would generally conduct. As such, it would take much more time. A controlled experiment would have produced Wexnet with a better understanding of a limited set of solutions. Still, it would not help them in the future, and the benefit of the project would be limited to only the solutions in the scope of the experiment. We perceive the practical testing following our research project as the just alternative to a controlled experiment. The practical testing of different NMS solutions conducted by Wexnet can be seen as the continuation of the selection process aided by our network management selection process. If time constraints were not an issue, a controlled experiment on the NMS solutions we use to demonstrate the selection process would be an excellent addition to our multimethod approach.

3.6 Reliability and Validity

One of the primary challenges of this thesis project is that it does not involve any experimental laboratory work. The evaluation of existing network monitoring solutions will be based on literature review and analysis rather than practical experimentation.

To effectively leverage the cooperation with Wexnet, access to relevant internal documents to describe their business problem will be requested.

In addition to the expert information received from Wexnet, we will combine the current academic understanding of the matter with the requirements received from the company.

We must consider the potential limitations of generalizability in our research. By comparing various software solutions, we run the risk of only addressing the specific needs of the company in question.

We mitigate this by separating the NMS solutions by their features and do not take into consideration the specific deployment requirements of Wexnet. Considerations such as hardware vendors or software compatibility are not taken into consideration when including solutions that we inspect. To fulfill the nature of the cooperation with Wexnet, we will propose a feature matrix and NMS selection process steps. Still, their possible preferences or limitations will not impact the generalizability of this research project.

We aim to reduce/minimize the bias by scoping the requirements to be vendor agnostic and by generalizing the requirements of the NSP.

Selection of NMS for Demonstrating the NMS Feature Matrix Choosing Network Management Systems (NMS) to demonstrate our NMS feature matrix's application was meticulously carried out to ensure a robust validation of its functionality and relevance. The 2019 Gartner Magic Quadrant for Network Performance Monitoring and Diagnostics [23] (see Figure 4) served as the foundation for our NMS solution selection.

We consulted with our partner company, Wexnet, seeking their input on prioritizing the choice of NMS solutions for review. It is important to clarify that our primary intent was to effectively demonstrate the utility of the NMS feature matrix rather than to ascertain the superiority of any specific NMS solution. Gartner's Network Performance Monitoring and Diagnostics magic quadrant consists of four categories separated into quadrants. The categories of Gartner's diagram are market leaders, visionaries, niche players, and challengers. Because of time constraints, it was not feasible to choose all of Gartner's NMS to demonstrate the NMS feature matrix. Wexnet proposed to prioritize market leaders, followed by visionaries, niche players, and finally, challengers. Additionally, to cater to the specific interests of our partner, we added three vendors to the top priority group: ScienceLogic, Micro Focus, and ITRS.

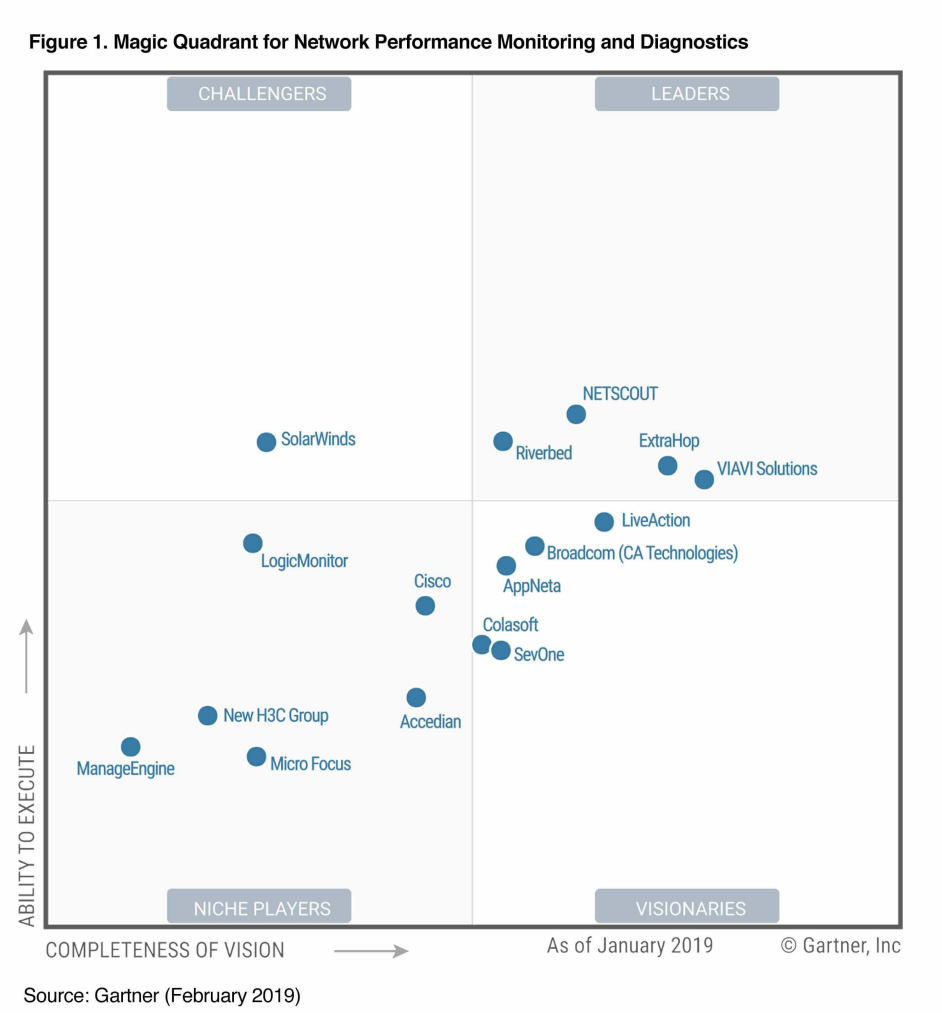

Figure 4: Gartner's Magic Quadrant from the year 2019 [23]

3.7 Ethical Considerations

Potential risk associated with the research project is the confidentiality and handling of sensitive information the cooperating company provides. This could include information related to security vulnerabilities in their systems, which could have serious consequences if exposed to the general public.

To mitigate this risk, it is essential to have strict protocols in place for handling and protecting sensitive information. This could have included non-disclosure agreements (NDA) and establishing clear communication with the cooperating company to ensure that any sensitive information is handled according to their guidelines and regulations. The requirement for an NDA was deemed unnecessary, and the guidelines for company co-operation were deemed sufficient. The findings of this research will be presented in a way that does not reveal information about the infrastructure of the partner company. All the data and information used in the research will be handled with confidentiality and will not be shared with any third party without explicit permission from the cooperating company. The company

representatives review the work and approve that no sensitive infrastructure information is included. The ethical consideration was also mitigated by the limitation of the research project. The research did not conduct practical laboratory testing at the Wexnet environment, and as such, the exposure to sensitive information was minimal.

4 Results of the Literature Review and the Thematic Analysis

The results and distribution of the primary studies discovered by the LLR and the themes identified by the thematic analysis are discussed below. This section focuses on the results of the supporting methodologies of LLR and TA and the following Section 5 focuses on the results of the design science project.

4.1 Limited Literature Review

The limited literature included 155 studies from which we obtained 43 primary studies. The 43 final primary studies were the result of utilizing a search protocol and predetermined inclusion and exclusion criteria. Each of the four digital libraries was searched using two search queries. The majority of the studies were excluded at the title review stage. The most common reason for excluding a study was the need for more relevance to the fixed-access networking research area. Many of the excluded studies focused on low-level design choices of network technologies. They did not introduce high-level trends or challenges relating to the research area of this paper.

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) is the standard of preferred means of reporting reviews [24]. The PRISMA flow diagram is PRISMA's standardized method of visualizing the process of conducting a review. The flow diagram visualizes the different exclusion steps and sources of studies. The flow diagram for the LLR process of this research project can be seen below in Figure 5.

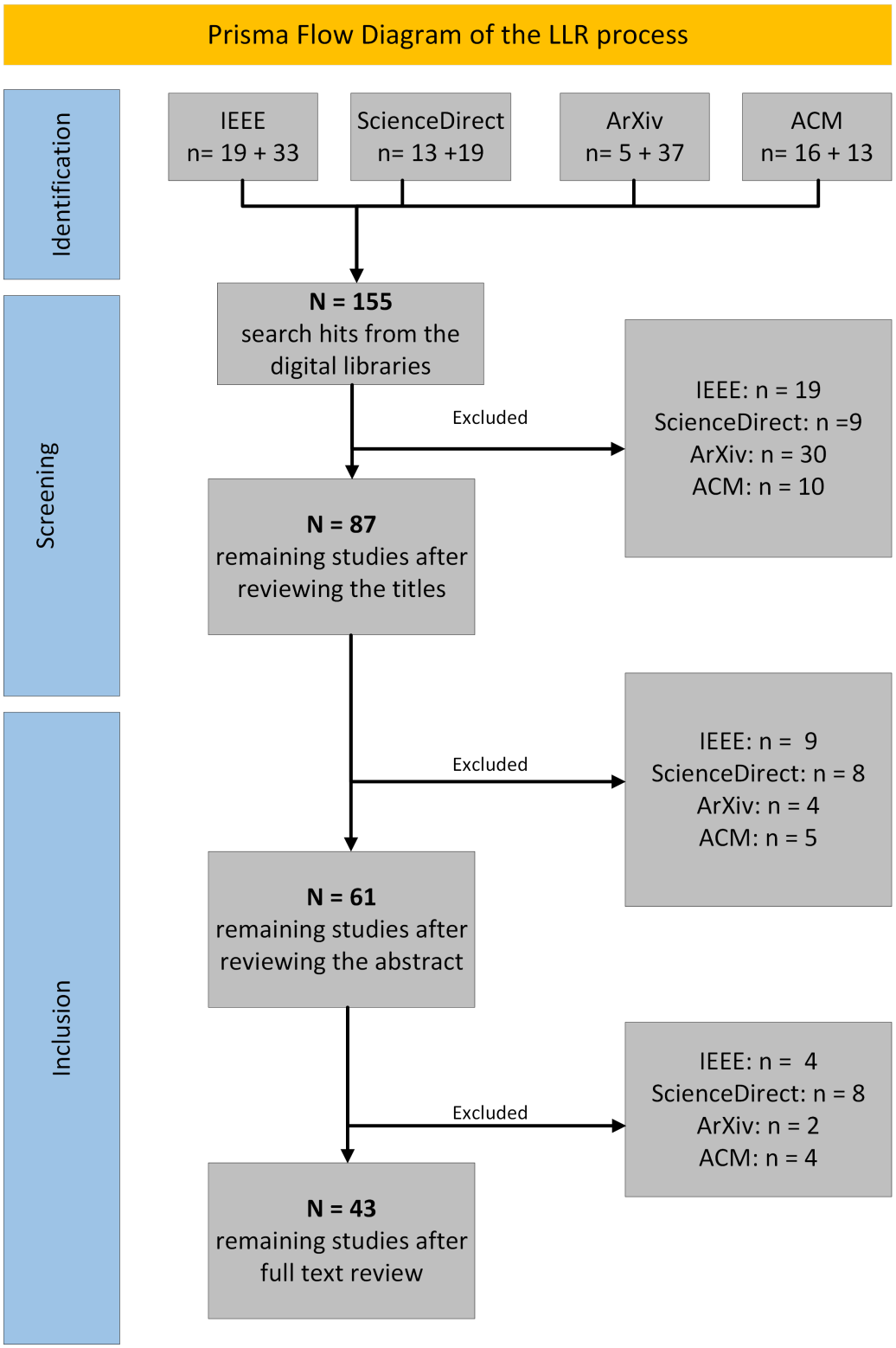

Figure 5: PRISMA flow diagram of the inclusion process visualizes the study selection at each stage of the LLR process. From the 155 initial studies, the review generated 43 primary studies to be analyzed by thematic analysis. [24]

4.1.1 Review Results

IEEE was the digital library with the highest number of initial studies and resulted in the highest number of selected primary studies after the final selection step of the LLR. All of the digital libraries resulted in primary studies, and nearly 27,7% of the initial studies resulted in a primary study.

Database	Search No.	Date	Hits
IEEE	1	19.2.2023	9
IEEE	2	19.2.2023	11
ScienceDirect	1	19.2.2023	3
ScienceDirect	2	19.2.2023	4
ArXiv	1	19.2.2023	1
ArXiv	2	19.2.2023	5
ACM	1	19.2.2023	4
ACM	2	19.2.2023	6

Table 1: The final search results of the 8 search queries as part of the LLR

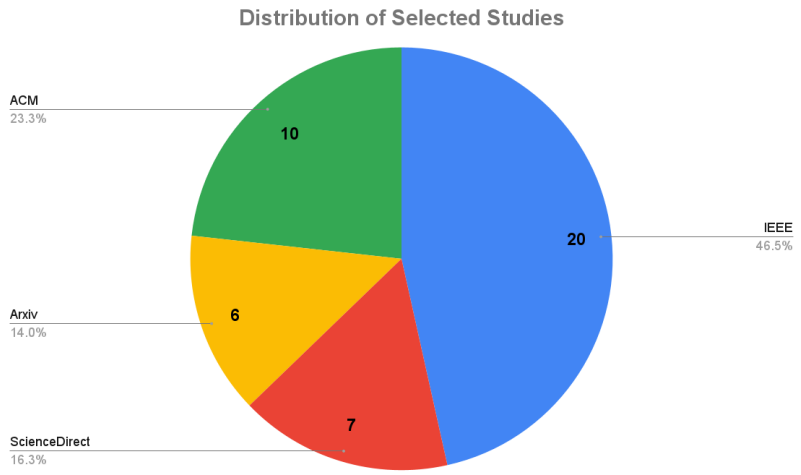

Figure 6: The distribution of selected studies by the four publishers. IEEE published the most studies, followed by ACM. The difference between ScienceDirect and ArXiv was not major.

The 43 papers identified as the product of the LLR are further analyzed utilizing the TA methodology covered in the section below. The theme analysis and identification are conducted as the data extraction phase of the LLR. The identified themes will outline the challenges and trends for the NMS selection features.

4.2 Thematic Analysis

The primary studies identified in the limited literature review above were then analyzed to identify the technological trends relating to computer networking and

requirements for network management systems. The prior research was analyzed for the main theme and possible sub-theme if the research was carried out research in an identifiable second theme. The LLR primary studies, their names, themes, and applicable sub-themes are recorded in Table 2 below.

Theme	Subtheme	Name	Study
AI/ML		Applying Machine Learning Technology to Optimize the Operational Cost of the Egyptian Optical Network	[S1]
		Coordination between control layer AI and on-board AI in optical transport networks	[S2]
Energy GreenIT ESG	NFV	Energy efficiency with service availability guarantee for Network Function Virtualization	[S3]
	SLA	GreenDataFlow: Minimizing the Energy Footprint of Global Data Movement	[S4]
Network Caching	Information-centric networking (ICN)	The Road Ahead for Networking: A Survey on ICN-IP Coexistence Solutions	[S5]
	AI/ML, future networks	Deep Reinforcement Learning for Adaptive Caching in Hierarchical Content Delivery Networks	[S6]
	Peer-to-peer content delivery	Controlling P2P-CDN Live Streaming Services at SDN-Enabled Multi-Access Edge Datacenters	[S7]
	Information-centric networking (ICN)	Optimal False-Positive-Free Bloom Filter Design for Scalable Multicast Forwarding	[S8]
	Content centric networks (CCN)	Assisted DASH-aware networking over SDN–CCN architecture	[S9]
Network Function Virtualization (NFV)	VNF, Service function chaining	Availability Evaluation of Multi-tenant Service Function Chaining Infrastructures by Multidimensional Universal Generating Function	[S10]
		Efficiently Embedding Service Function Chains with Dynamic Virtual Network Function Placement in Geo-Distributed Cloud System	[S11]
		How physical network topologies affect virtual network embedding quality: A characterization study based on ISP and datacenter networks	[S12]
		Joint Placement and Allocation of VNF Nodes With Budget and Capacity Constraints	[S13]
		Network Function Virtualization-Aware Orchestrator for Service Function Chaining Placement in the Cloud	[S14]
NFV	Service function chaining	Profit Maximization of Online Service Function Chain Orchestration in an Inter-Datacenter Elastic Optical Network	[S15]
		Virtual Network Functions Placement and Routing Optimization	[S16]
		VLAN-based Traffic Steering for Hierarchical Service Function Chaining	[S17]
OTT	Multi-Path TCP (MPTCP)	Multi-Path TCP in Real-World Setups – An Evaluation in the NORNET CORE Testbed	[S18]
		On the Tussle Between Over-the-Top and Internet Service Providers: Analysis of the Netflix- Comcast Type of Deals	[S19]
QoS	Microservices	Exploring microservices for enhancing internet QoS	[S20]
	QoE and QoE management	QoE Management of Multimedia Streaming Services in Future Networks: A Tutorial and Survey	[S21]
	Edge Computing	Frend for Edge Servers: Reduce Server Number! Keeping Service Quality!	[S22]
SDN	QoS routing	Dynamic Resource Allocation by Batch Optimization for Value-Added Video Services Over SDN	[S23]
	Network-Aware Applications (NAA) Application-Aware Networking (AAN)	Towards Deep Network Application Integration: Possibilities, Challenges, and Research Directions	[S24]
		An SDN-Based CDN/ISP Collaboration Architecture for Managing High-Volume Flows	[S25]
		A new GSO based method for SDN controller placement	[S26]
		A Real-time Simulation Framework for Complex and Large-scale Optical Transport Networks based on the SDN Paradigm	[S27]
	Software Defined Optical Networking (SDON)	Blockchain-enhanced cross-ISP spectrum assignment framework in SDONs: SpectrumChain	[S28]
		One Step at a Time: Optimizing SDN Upgrades in ISP Networks	[S29]

Theme	Subtheme	Name	Study
SDN		Optimizing Gradual SDN Upgrades in ISP Networks	[S30]
		Performance Modelling and Analysis of Software-Defined Networking under Bursty Multimedia Traffic	[S31]
	Multipath routing	Scalable and Efficient Multipath Routing via Redundant Trees	[S32]
		SDN-enabled distributed open exchange: Dynamic QoS-path optimization in multi-operator services	[S33]
		Simultaneously Reducing Latency and Power Consumption in OpenFlow Switches	[S34]
	High Flow SDN	TeraFlow: Secured Autonomic Traffic Management for a Tera of SDN flows	[S35]
		Towards Adaptive State Consistency in Distributed SDN Control Plane	[S36]
	NFV	A moving target defense and network forensics framework for ISP networks using SDN and NFV	[S37]
		Future Direction of Traffic Classification in SDN from Current Patents Point-of-view	[S38]
	Inter-domain SDN	ICONA: a peer-to-peer approach for Software Defined Wide Area Networks using ONOS	[S39]
		Novel SDN architecture for smart MPLS Traffic Engineering-DiffServ Aware management	[S40]
Segment Routing Traffic Engineering		Segment Routing: A Comprehensive Survey of Research Activities, Standardization Efforts, and Implementation Results	[S41]
		Deploying near-optimal delay-constrained paths with Segment Routing in massive-scale networks	[S42]
		Failure Resiliency With Only a Few Tunnels – Enabling Segment Routing for Traffic Engineering	[S43]

Table 2: Classification of computer networking research themes based on the thematic analysis conducted on the primary studies identified by the limited literature review.

- The largest theme identified by the conducted thematic analysis is software-defined networking with 18 primary studies - 41,9% of the studies
- Followed by network function virtualization with eight papers - 18,6% of primary studies
- Network caching five studies, 11,6%
- Segment Routing/Traffic Engineering and Quality of Service 3 studies - 7%
- Followed by 2 studies for AI/ML , Energy-GreenIT-ESG and OTT studies - 4,7%

The above division is visualized in Figure 7 below.

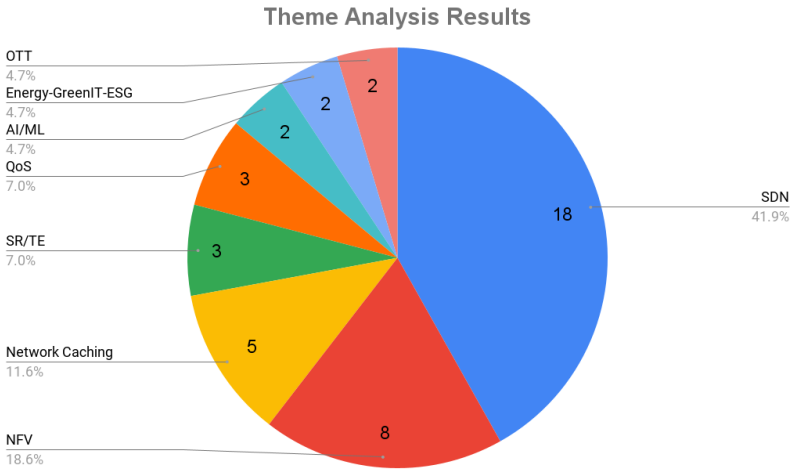

Figure 7: The theme distribution of the themes identified in the thematic analysis

5 Results of the Design Science Project

In this section, we present the results of our research:

- Brief overview of the eight novel networking trends found by our LLR and TA.
- The NMS features identified after the literature review of the eight identified network themes and Wexnet's specific requirements.
- Demonstrate the use of the NMS feature matrix by reviewing three network management solutions.

5.1 RQ1 and RQ2: The novel network trends and their implications on NMS

This section addresses the results of the first and second research questions, as stated in the problem formulation:

- RQ1: What state-of-the-art network technology trends and challenges are most relevant to fixed-access networks?
- RQ2: What are the requirements for network management tools to manage and monitor fixed-access networks in light of these trends and challenges?

Thematic analysis of the primary studies led to the identification of eight distinct themes encapsulating the state-of-the-art and emergent trends in network technologies presented in Table 2:

- Over-The-Top Providers (OTTP) and Service Providers Cooperation
- High Demands for Quality of Service (QoS) and Quality of Experience (QoE)
- Network Caching, Content Delivery Networks (CDNs), and Information-Centric Networking (ICN)
- Network Function Virtualization (NFV)
- Segment Routing and Traffic Engineering
- Software Defined Networks (SDN)
- Network Automation and Scalability (AI/ML)
- Energy Management and Environmental, Social, and Governance (ESG) Factors

The selection of features listed in the next sub-section (see Figures 8 -17) was derived through a review of existing literature on each respective technology. For each thematic area, an extensive assortment of research papers and industry publications was consulted to glean a comprehensive understanding of the technology in question, with particular emphasis on its general characteristics, fundamental components, and widely-adopted protocols. This compilation of information was then rigorously synthesized, leading to the articulation of a set of concise yet comprehensive, features. These criteria are reflective of the core aspects and prevailing practices associated with the technology and serve as a benchmark against which Network Management Systems (NMS) can be evaluated to ascertain the extent of their support and alignment with the established norms and conventions of the domain. A more comprehensive analysis of these eight themes is available in the appendix A.

5.2 RQ3: The NMS feature matrix and the NMS Review

In the following sections, we will present and demonstrate the NMS feature matrix. To demonstrate the practical application and usability of our feature matrices, we selected three NMS solutions according to the NMS selection process described in Section 3.6:

- ITRS OP5 Monitor
- Microfocus Network Operations Management (NOM)
- Netscout nGeniusOne

Figures 8 and 9 provide insights into the features required of Wexnet. The remaining eight Figures (10, 11, 12, 13, 14, 15, 16, 17) each correspond to one of the trends discussed earlier, showcasing the specific features these trends necessitate in a network management system.

Description of the NMS Feature Matrix
The NMS feature matrix was constructed as a spreadsheet, wherein each tab is dedicated to a unique theme. A snapshot of a portion of the tab designated for Wexnet is displayed in Figure 8. Every tab is comprehensively structured with sub-themes and features to enhance usability and readability.

The initial column lists the sub-themes and features, with a detailed explanation of each feature embedded as a note, accessible upon hovering the mouse over it. These explanatory notes mirror the descriptions in the second column of the required tables in this paper's appendices.

Columns two through n are reserved for evaluating the Network Management System (NMS) solutions. Each feature is accompanied by a drop-down menu offering five selectable options:

- **Choose Option**: The initial default selection in the drop-down menu.

- **Supported**: Indicates that the NMS solution under review supports the feature in question.
- **Not Supported**: Indicates that the NMS solution under review does not support the feature in question.
- **Partially Supported**: Suggests the feature is only partially supported by the solution, for example when the solution supports 5 out of 6 listed routing protocols, for instance.
- **Not Found**: Chosen in instances where the review process does not yield clear information as to whether the solution supports the feature.

5.3 Wexnet's Specific NMS Features

Figures 8 and 9, displayed below, offer a snapshot of Wexnet's requirements. These figures outline the sub-themes and features that apply to Wexnet. This particular list comprises seven sub-themes and a total of 65 distinct features. Wexnet compiled these features to represent their specific requirements from a Network Management System (NMS). For a deeper understanding of the foundation of this feature matrix, please refer to Appendix A."

Feature	ITRS OP5	Micro Focus NOM	Netscout nGeniusOne
SLA Measurement and Report Features			
SLA report generation [1]	Supported	Supported	Not Found
Customer-specific SLA information, uptime, logs, and comments [2]	Supported	Supported	Not Found
Customizable reporting time periods [3]	Supported	Not Found	Not Found
SLA weighting for prioritization of hosts [4]	Not Found	Supported	Not Found
Automatic SLA calculation based on group membership [5]	Not Found	Not Found	Not Found
Customizable SLA levels according to client's terms [6]	Supported	Supported	Not Found
Other Reporting Features			
Scheduled report generation [7]	Not Found	Supported	Not Found
Reporting of custom time periods [8]	Supported	Supported	Not Found
Reporting active switch ports [9]	Supported	Supported	Not Found
Reporting monitored elements per group or customer [10]	Supported	Supported	Not Found
Reporting monitored elements per model type	Supported	Supported	Not Found
Reporting unrnanaged elements [11]	Not Found	Supported	Not Found
Ranking of the nodes based on errors or load [12]	Supported	Supported	Not Found
Bandwidth utilization reports [13]	Supported	Supported	Not Found
Exporting of hosts and services as CSV files	Supported	Supported	Not Found
Graphical trend reports (min 1-year timespan) [14]	Supported	Not Found	Not Found
Mapping and Visualization Features			
Support for topologies with different views and layers [15]	Supported	Supported	Supported
Network asset placement on a geographical map based on GPS coordinates [16]	Supported	Not Found	Not Found
Customizable user view [17]	Supported	Supported	Not Found
Graphing of all monitored network elements [18]	Supported	Supported	Supported
Large-scale graphing capacity of minimum 100.000 ports and 6000 switches [19]	Not Found	Supported	Not Found
Graphing of all monitored services [20]	Supported	Supported	Supported
Easy-to-use management system for both logical and geographical topologies [21]	Supported	Partially Supported	Not Found
Capability to revert changes to the map management system using an undo function [22]	Not Found	Not Found	Not Found
Automatic discovery function with support for CDP, LLDP, OSPF,BGP [23]	Partially Supported	Supported	Not Found
Scalable, real-time concurrent monitoring capacity (minimum 6000 switches and 8000 APs) [25]	Not Found	Supported	Not Found
Server hardware monitoring for Windows and Linux OS [26]	Supported	Supported	Not Found
Server services monitoring for Windows and Linux OS [27]	Supported	Supported	Not Found
Server processes monitoring for Windows and Linux [28]	Supported	Supported	Not Found
Server Memory monitoring for Windows and Linux OS [29]	Supported	Supported	Not Found
Server CPU monitoring for Windows and Linux OS [30]	Supported	Supported	Not Found
Monitoring common server protocols such as: HTTP/HTTPS, SSH, FTP, SNMP, DNS, DHCP, SMTP	Not Found	Supported	Supported
Distributable remote polling agent to report routing conflicts [33]	Not Found	Not Found	Not Found
Optional SNMP OIDs monitoring [32]	Supported	Not Found	Not Found
Automatic scanning of hosts with IP range and black-list support [34]	Supported	Supported	Not Found
Search feature for hosts and services [35]	Supported	Supported	Not Found
Network element identification by address [36]	Not Found	Supported	Not Found
Monitoring Cisco QoS quality [37]	Supported	Supported	Not Found
Monitoring Cisco Multicast quality [38]	Supported	Supported	Not Found
Monitoring Cisco VOIP quality [39]	Supported	Supported	Not Found
Monitoring state on BGP/OSPF/IS-IS links [40]	Supported	Supported	Not Found
Monitoring access points via Wireless Controller [41]	Supported	Supported	Not Found
Monitoring end-to-end services (client experience) [42]	Not Found	Supported	Supported
Support for network element groups	Supported	Not Found	Not Found

Figure 8: The Wexnet's specific features 1 of 2

Feature	ITRS OP5	Micro Focus NOM [43]	Netscout nGeniusOne
Alerting and Notifications Features			
SMS and email alerting capability [44]	Supported	Supported	Supported
Error event correlation [45]	Supported	Not Found	Not Found
Event commenting functionality [46]	Supported	Not Found	Not Found
Temporary interruption scheduling [47]	Not Found	Supported	Not Found
SNMP trap processing with customizable rules [48]	Supported	Not Found	Not Found
Event processing with customizable rules [49]	Supported	Supported	Not Found
Color-coding and labeling of alarms [50]	Supported	Supported	Supported
Filtering of alarms based on label [51]	Supported	Supported	Not Found
Configurable notification settings based on time of day and type of event [52]	Not Found	Supported	Not Found
Support for different alarm delay based on network element group [53]	Supported	Not Found	Not Found
Customizable SNMP rules with MIB import support [54]	Supported	Supported	Not Found
Scalability and Redundancy Features			
Support for backup servers [55]	Not Found	Not Found	Not Found
API and integration support [56]	Supported	Supported	Supported
Built-in backup and restore functionality	Partially Supported	Supported	Not Found
Security Features			
Customer-specific access control for their respective topology and alarms [57]	Supported	Supported	Not Found
Encrypted management traffic for all protocols [58]	Not Found	Not Found	Not Found
Customer Support and Localization Features			
Built-in chat support	Not Found	Not Found	Not Found
Enterprise customer service	Supported	Supported	Supported
Has web API	Supported	Supported	Supported
On-site hosting	Supported	Supported	Supported
Cloud-based with servers located only in Sweden	Not Found	Not Found	Not Found

Figure 9: The Wexnet's specific features 2 of 2

5.4 OTTPs and Service Providers Cooperation Specific NMS Features

Figure 10, illustrated below, provides a screenshot captured from our NMS feature matrix. It showcases features associated with the 'OTTPs and Service Providers Cooperation' theme. This feature list encompasses no sub-themes and has in total six distinct features, all of which have been derived from the results of the previous section, 'OTTPs and Service Providers Cooperation'. For a more detailed insight into the basis of the feature matrix, please refer to Appendix B.

Feature	ITRS OP5	Micro Focus NOM	Netscout nGeniusOne
OTT coop Network Management Features			
Peering Point Management [1]	Not Found	Not Found	Supported
Routing Policy Configuration [2]	Not Found	Not Found	Supported
Traffic Monitoring [3]	Not Found	Not Found	Supported
Data Sharing [4]	Not Found	Not Found	Supported
Secure Communications [5]	Not Found	Not Found	Not Found
Reporting of Peering Agreement [6]	Not Found	Not Found	Supported

Figure 10: OTTP cooperation specific NMS features

5.5 Quality of Service Specific NMS Features

Figure 11, illustrated below, provides a screenshot captured from our NMS feature matrix. It showcases the sub-themes and features of the 'Quality of Service' theme. This feature list encompasses two sub-themes and has in total six distinct features,

all of which have been derived from the results of the previous section, 'Quality of Service'. More details about the requirements behind the feature matrix can be found in Appendix C.

Feature	ITRS OP5	Micro Focus NOM [1]	Netscout nGeniusOne
Protocol Support for Additional Value:			
DiffServ [2]	Not Found	Not Found	Not Found
RSVP [3]	Not Found	Not Found	Not Found
MPLS [4]	Supported	Supported	Supported
QoS related features for Additional Value:			
Quality of Experience-aware mechanisms [5]	Not Found	Supported	Supported
Support for SDN [6]	Not Found	Supported	Supported
Northbound API [7]	Not Found	Supported	Supported

Figure 11: QoS specific NMS features

5.6 Network Caching and Content Delivery Networks Specific NMS Features

Figure 12, illustrated below, provides a screenshot captured from our NMS feature matrix. It showcases the sub-themes and features of the 'Network Caching and Content Delivery Networks' theme. This feature list encompasses three sub-themes and has in total 13 distinct features, all of which have been derived from the results of the previous section, 'Network Caching and Content Delivery Networks'. More details about the requirements behind the feature matrix can be found in Appendix D.

Feature	ITRS OP5	Micro Focus NOM [1]	Netscout nGeniusOne
Network Caching			
Cache Content Management [2]	Not Found	Not Found	Not Found
Cache Server Configuration and Optimization [3]	Not Found	Not Found	Not Found
Load Balancing and Fault Tolerance [4]	Not Found	Supported	Not Found
Cache Server Health Monitoring [5]	Not Found	Supported	Not Found
Cache Traffic Analysis [6]	Not Found	Supported	Supported
Content Delivery Networks (CDN)			
CDN Distribution Optimization [7]	Not Found	Supported	Choose Option
CDN DNS Resolution Monitoring [8]	Not Found	Supported	Supported
CDN Mapping & Monitor [9]	Not Found	Supported	Supported
CDN Latency Monitoring [10]	Not Found	Supported	Not Found
CDN Image Optimization Monitoring [11]	Not Found	Not Found	Not Found
Information-Centric Networks (ICN) and Content-Centric Networks (CCN)			
Content Name-based Communication [12]	Supported	Supported	Not Found
ICN and CCN Traffic Analysis [13]	Not Found	Supported	Not Found
CCN Content Chunk Management [14]	Not Found	Supported	Not Found

Figure 12: Network Caching, CDN, and ICN/CCN Specific NMS Features

5.7 Network Function Virtualization Specific NMS Features

Figure 13, illustrated below, provides a screenshot captured from our NMS feature matrix. It showcases the sub-themes and features of the 'Network Function Virtualization' theme. This feature list encompasses six sub-themes and has, in total, 22 distinct features, all of which have been derived from the results of the previous

section, 'Network Function Virtualization'. More details about the requirements behind the feature matrix can be found in Appendix E.

Feature	ITRS OP5	Micro Focus NOM [1]	Netscout nGeniusOne
VNF Deployment			
Instantiation [2]	Not Found	Supported	Not Found
Configuration [3]	Not Found	Supported	Not Found
Integration with existing network services [4]	Not Found	Not Found	Not Found
Automation and orchestration [5]	Not Found	Not Found	Not Found
VNF Discovery			
Automatic discovery of deployed VNFs [6]	Not Found	Supported	Supported
VNFs reporting [7]	Not Found	Supported	Supported
Discovering relationships with the underlying physical infrastructure	Not Found	Supported	Supported
Tracking VNF dependencies [9]	Not Found	Supported	Not Found
Visualization and monitoring [10]	Not Found	Supported	Supported
VNF Scaling			
Monitor the performance and resource utilization of VNFs [11]	Not Found	Supported	Supported
Analyze and predict performance requirements [12]	Not Found	Supported	Supported
Automatically scale VNFs based on requirements and constraints [1	Not Found	Not Found	Not Found
Implement scaling policies and rules [14]	Not Found	Not Found	Not Found
VNF Decommissioning:			
Data migration [15]	Not Found	Not Found	Not Found
Resource release [16]	Not Found	Supported	Not Found
Automatic update of network configuration [17]	Not Found	Supported	Supported
Network Slicing Support:			
Support for network slicing [18]	Not Found	Not Found	Not Found
Service Function Chaining Requirements			
Dynamic Service Chaining [19]	Not Found	Not Found	Not Found
SFC monitoring [20]	Not Found	Not Found	Supported
SFC Analytics [21]	Not Found	Not Found	Supported
SFC Traffic Steering [22]	Not Found	Not Found	Not Found
SFC Security Enforcement [23]	Not Found	Not Found	Not Found

Figure 13: Network Function Virtualization Specific NMS Features

5.8 Software Defined Networks Specific NMS Features

Figure 14, illustrated below, provides a screenshot captured from our NMS feature matrix. It showcases the sub-themes and features of the 'Software Defined Networks' theme. This feature list encompasses five sub-themes and has, in total, 24 distinct features, all of which have been derived from the results of the previous section, 'Software Defined Networks'. More details about the requirements behind the feature matrix can be found in Appendix F.

Feature	ITRS OP5	Micro Focus NOM [1]	Netscout nGeniusOne
Essential Protocol Support			
OpenFlow [2]	Not Found	Supported	Supported
BGP-LS [3]	Not Found	Supported	Not Found
PCEP [4]	Not Found	Not Found	Not Found
NETCONF/YANG [5]	Not Found	Supported	Supported
RESTCONF [6]	Not Found	Not Found	Supported
REST [7]	Not Found	Supported	Supported
gRPC [8]	Not Found	Supported	Not Found
HyperFlow [9]	Not Found	Not Found	Not Found
Protocol Support for Additional Value			
ForCES [10]	Not Found	Not Found	Not Found
I2RS [11]	Not Found	Not Found	Not Found
ALTO [12]	Not Found	Not Found	Not Found
P4 [13]	Not Found	Not Found	Not Found
Flow Management and Monitoring			
Flow monitoring [14]	Partially Supported	Supported	Supported
Flow rule management [15]	Partially Supported	Supported	Supported
Flow rule conflict detection [16]	Partially Supported	Supported	Supported
Telemetry and Analytics			
gNMI [17]	Not Found	Not Found	Not Found
NetFlow [18]	Supported	Supported	Supported
sFlow [19]	Supported	Supported	Supported
IPFIX [20]	Supported	Supported	Supported
Essential Controller Support			
ONOS (Open Network Operating System) [21	Not Found	Not Found	Not Found
OpenDaylight [22]	Not Found	Not Found	Supported
Cisco ACI (Application Centric Infrastructure)	Not Found	Supported	Supported
Juniper Contrail [24]	Not Found	Not Found	Not Found
HP VAN SDN Controller [25]	Not Found	Supported	Not Found

Figure 14: Software Defined Networks Specific NMS Features

5.9 Segment Routing and Traffic Engineering Specific NMS Features

Figure 15, illustrated below, provides a screenshot captured from our NMS feature matrix. It showcases the sub-themes and features of the 'Segment Routing and Traffic Engineering' theme. This feature list encompasses five sub-themes and has, in total, 20 distinct features, all of which have been derived from the results of the previous section, 'Segment Routing and Traffic Engineering'. More details about the requirements behind the feature matrix can be found in Appendix G.

Feature	ITRS OP5	Micro Focus NOM [1]	Netscout nGeniusOne
Network Discovery and Representation:			
Discover and represent all SR-enabled network elements [2]	Not Found	Not Found	Not Found
Discover and represent the links between all SR network elements [3]	Not Found	Not Found	Not Found
Discover and represent segment identifiers (SIDs) [4]	Not Found	Not Found	Not Found
Traffic Engineering and Management:			
Create and modify traffic engineering policies [5]	Not Found	Not Found	Not Found
Traffic steering through specific paths and links using segment routing features [6]	Not Found	Not Found	Not Found
Path computation [7]	Not Found	Not Found	Not Found
Path optimization [8]	Not Found	Not Found	Not Found
Performance Monitoring and Analysis:			
Real-time monitoring [9]	Supported	Supported	Supported
Monitor segment routing-based network performance - Throughput [10]	Not Found	Not Found	Not Found
Monitor segment routing-based network performance - Latency [11]	Not Found	Not Found	Not Found
Monitor segment routing-based network performance - Packet loss [12]	Not Found	Not Found	Not Found
Monitor segment routing-based network performance - Resource utilization [13]	Not Found	Not Found	Not Found
Routing Flexibility and Control:			
Ad-hoc routes support [14]	Not Found	Not Found	Not Found
Dynamic traffic management [15]	Not Found	Supported	Supported
Integration and Compatibility:			
Segment Routing over MPLS (SR-MPLS) [16]	Not Found	Not Found	Not Found
Segment Routing over IPv6 (SRv6) [17]	Not Found	Not Found	Not Found
Programmability with IPv6 in SRv6 [18]	Not Found	Not Found	Not Found
Open Shortest Path First (OSPF) with Segment Routing Extensions [19]	Not Found	Not Found	Not Found
Intermediate System to Intermediate System (IS-IS) with Segment Routing Extensions [20]	Not Found	Not Found	Not Found
Border Gateway Protocol (BGP) with Segment Routing Extensions [21]	Not Found	Not Found	Not Found

Figure 15: Segmented Routing and Traffic Engineering Specific NMS Features

5.10 Artificial Intelligence and Machine Learning Specific NMS Features

Figure 16, illustrated below, provides a screenshot captured from our NMS feature matrix. It showcases features associated with the 'Artificial Intelligence and Machine Learning' theme. This feature list encompasses no sub-themes and has in total seven distinct features, all of which have been derived from the results of the previous section 'Artificial Intelligence and Machine Learning'. More details about the requirements behind the feature matrix can be found in Appendix H.

Feature	ITRS OP5	Micro Focus NOM [1]	Netscout nGeniusOne
AI/ML-driven Network Management Features			
Big data capabilities from diverse sources [2]	Not Found	Supported	Supported
Advanced data analytics [3]	Not Found	Supported	Supported
AI/ML-driven anomaly detection [4]	Not Found	Supported	Supported
Adaptive learning capabilities [5]	Not Found	Not Found	Supported
Automated root cause analysis [6]	Not Found	Supported	Not Found
Proactive problem resolution [7]	Not Found	Not Found	Not Found
Capacity planning and optimization [8]	Not Found	Not Found	Supported

Figure 16: AI/ML Specific NMS Features

5.11 Energy Management, GreenIT, and ESG Monitoring specific NMS Features

Figure 17, illustrated below, provides a screenshot captured from our NMS feature matrix. It showcases features associated with the theme of 'Energy Management, GreenIT, and ESG Monitoring' theme. This feature list encompasses no

sub-themes and has in total ten distinct features, all of which have been derived from the results of the previous section, 'Energy Management, GreenIT, and ESG Monitoring' More details about the requirements behind the feature matrix can be found in Appendix I.

Feature	ITRS OP5	Micro Focus NOM [1]	Netscout nGeniusOne
Energy usage monitoring [2]	Not Found	Supported	Supported
Carbon footprint estimation [3]	Not Found	Partially Supported	Not Found
Hardware lifecycle tracking [4]	Not Found	Not Found	Not Found
Cooling and power efficiency monitoring [5]	Not Found	Partially Supported	Not Found
Integration with energy management systems [6]	Not Found	Supported	Not Found
Customizable ESG metric dashboards [7]	Not Found	Not Found	Not Found
Automated ESG reporting [8]	Not Found	Not Found	Not Found
ESG Alerting and notifications [9]	Not Found	Not Found	Not Found
Integration with ESG data sources [10]	Not Found	Not Found	Not Found
Benchmarking and analytics [11]	Not Found	Partially Supported	Not Found

Figure 17: Energy, GreenIT and ESG Monitoring specific NMS Features

6 Analysis

The proceeding sections bridge the foundation laid in the previous sections to the eventual conclusions and insights drawn from this research. The contents of this section can be supplemented with the synthesis of the more comprehensive discussion provided in Appendix A. We will first address the state-of-the-art network technology trends and challenges that are most pertinent to fixed-access networks (RQ1), summarizing the eight distinct themes identified in the results section 5. Subsequently, we will analyze the requirements that network management tools must possess to effectively manage and monitor these networks in the backdrop of the identified trends (RQ2). Lastly, we will analyze how the current research in network technologies can bolster network service providers in selecting network management systems adept at addressing these trends and challenges (RQ3).

6.1 Research Question 1 - Current Trends

Research Question 1: What state-of-the-art network technology trends and challenges are most relevant to fixed-access networks?

The rapid expansion of Over-The-Top (OTT) services is significantly reshaping the network management landscape. These services' escalating demand necessitates elevated innovation and cooperation from network service providers. This necessity not only accelerates the adoption of the other trends covered in this thesis but also emphasizes their relevance and importance in the current landscape.

The rise of major tech players like Meta, Alphabet, Apple, Microsoft, Amazon, and Netflix has led to a substantial increase in internet traffic. Consequently, this exerts significant pressure on network infrastructure. Furthermore, the nature of traffic generated by these OTT services is particularly demanding. As OTT services often involve quasi-instantaneous applications such as Video on Demand (VoD) and Voice over IP (VoIP), they require high bandwidth and low latency for optimal user experience. Consequently, this increasingly emphasizes the need for Quality of Service (QoS) and Quality of Experience (QoE). As the prevalence of OTT traffic continues to surge, the challenge to maintain high QoS and QoE concurrently escalates.

The surge in OTT services has prompted Telecommunication Service Providers (TSPs) to diversify their business models, unveiling varied-cost contracts that cater to the evolving demands of OTTs. However, a challenge arises in this context as OTTs generate substantial traffic and derive profit from it but largely leave the burden of the infrastructure load to TSPs.

In response to these challenges, network service providers have adopted key strategies. One such strategy includes the implementation of interconnection and peering agreements. These agreements facilitate mutual data exchange, easing the load on individual networks. As OTT services persist in their expansion, the importance of such agreements becomes increasingly apparent. They prove instrumental in managing the burgeoning network pressure. Moreover, innovative solutions are deployed to ensure efficient content delivery and maintain service quality amidst the OTT surge. These include technologies such as Content De-

livery Networks (CDN) and caching servers, which are crucial in this evolving landscape.

This new landscape signifies a shift in the network management paradigm, compelling service providers to adapt and innovate continually. Technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), Segment Routing and Traffic Engineering, and AI/ML-based network automation are instrumental in this transformation. They enable a more dynamic, flexible, and efficient approach to network management, particularly suited to the challenges posed by the proliferation of OTT services.

SDN, in particular, facilitates the management of increasingly complex, multi-vendor networks, as it decouples the network's control plane from the data plane, allowing for centralized control. Similarly, NFV allows for the virtualization of network services traditionally run on proprietary, dedicated hardware. With NFV, these services can be run on standard servers, storage, and Ethernet switches, simplifying the management of multi-vendor environments.

Moreover, Segment Routing and Traffic Engineering techniques are critical for optimizing network resources and ensuring high QoS/QoE. They enable intelligent traffic routing based on network conditions, ensuring optimal use of network infrastructure and maintaining service quality in the face of high, fluctuating OTT traffic demands.

On another note, this paradigm shift is about more than just managing traffic and infrastructure; it's also about aligning with the rising importance of Green-IT/ESG considerations. Network technologies need to be efficient not just in terms of traffic handling but also in terms of energy consumption and environmental impact. This aspect increasingly shapes service providers' strategies and network technologies' development.

The rapid growth of OTT services and the resulting challenges drive accelerated adoption and development of advanced network technologies. These technologies are crucial for service providers to manage the burgeoning network pressure, optimize their operations, and align with the evolving efficiency, quality, and sustainability expectations.

As we delve deeper into the complexity of the current network management landscape, it becomes increasingly clear that the NMS solutions employed to manage and monitor these networks must rise to the occasion. These advanced network technologies necessitate equally advanced network management tools to harness their full potential and address the challenges posed by OTT traffic and other emerging trends. The following section will focus on the essential requirements for these network management tools. We will discuss these requirements in the context of the trends identified in this thesis, exploring how each trend imposes specific demands on Network Management Systems (NMS).

6.2 Research Question 2 - NMS Requirements

Research Question 2: What are the essential requirements for network management tools to effectively manage and monitor these networks in light of these trends?

OTTPs and Service Providers cooperation
The interplay between OTT providers (OTTPs) and Telecommunication Service Providers (TSPs) necessitates an advanced Network Management System (NMS). Efficient Peering Point Management is essential for maintaining optimal network performance. Routing Policy Configuration allows for effective network traffic management, which is vital given the fluctuating demands of OTT services. Traffic Monitoring is a requisite feature, enabling real-time assessment of interconnected network performance.

Furthermore, secure and efficient Data Sharing bridges understanding between TSPs and OTTPs, fostering a cooperative relationship. Secure Communications prevent unauthorized access or data breaches, ensuring trust in OTT-TSP cooperation. Lastly, Reporting of Peering Agreement provides a clear view of the performance and adherence of the peering agreement. These features underscore the importance of a capable NMS in managing OTTP-TSP cooperation effectively in the context of growing OTT services.

Quality of Service
The requirement for Quality of Service (QoS) protocols like Differentiated Services (DiffServ), Resource Reservation Protocol (RSVP), and Multiprotocol Label Switching (MPLS) reflect the evolving complexity of network traffic management. These protocols ensure efficient data packet delivery, which is especially critical in handling OTT services that demand high bandwidth and low latency.

Additional requirements, such as Quality of Experience (QoE)-aware mechanisms, enable the NMS to assess and optimize the user-perceived quality, an essential aspect in OTT-dominated environments. Software-Defined Networking (SDN) support is vital for adaptive QoS measures, allowing for flexible network traffic management. The Northbound API support enables automation and implementation of comprehensive network policies, contributing to a dynamic and efficient network environment. These features ensure the optimization of network resources, thereby improving QoS and QoE amidst the burgeoning OTT traffic.

Network Caching and CDN
The requirements for Network Caching and Content Delivery Chains revolve around improving content delivery efficiency and reducing latency, which is vital for OTT services. For Network Caching, the emphasis lies on effective content management, cache server configuration, health monitoring, and traffic analysis. These requirements underscore the significance of maximizing cache hit ratios and ensuring fault tolerance.

On the other hand, Content Delivery Networks (CDN) requirements focus on optimizing content distribution, monitoring DNS resolutions, mapping, latency, and image optimization. This implies that CDN performance is crucial in delivering OTT services, especially in handling high-resolution content.

Lastly, the emerging Information-Centric Networks (ICN) and Content-Centric Networks (CCN) paradigm, focusing on content name-based communication, traffic analysis, and content chunk management, represent a shift toward more efficient

content delivery, a significant trend given the rise in content-based services like OTT.

Network Function Virtualization
In terms of Network Function Virtualization (NFV), several areas are key requirements that NMS needs to support for robust network management.

The first is VNF Deployment, encompassing the entire process of integrating new VNF instances into the network. This process is mainly about automation and orchestration, the key to ensuring efficient and seamless deployment.

Next up is VNF Discovery. With automatic detection, comprehensive reporting, and visualization, we can keep tabs on all deployed VNFs, their dependencies, and their relationship with the physical infrastructure.

Another critical aspect is VNF Scaling, which is all about adaptability. We can ensure our network can handle any demand by monitoring VNF performance and resource utilization, predicting future requirements, and implementing autoscaling. Plus, having the flexibility to define scaling rules and policies ensures we're always in control.

Regarding VNF Decommissioning, the focus shifts to data security and resource management. Safely migrating data and releasing resources back to the pool is critical, along with updating the network configuration automatically to reflect changes.

Network Slicing is all about customization. By creating multiple virtual networks on a shared physical infrastructure, we can cater to specific needs, offering a tailored service.

Finally, the requirements around Service Function Chaining (SFC) emphasize dynamism and security. The ability to create, modify, and delete SFCs dynamically, monitor performance, steer traffic, and enforce security policies within SFCs ensures a secure, efficient, and agile network.

Software Defined Networks
The Software Defined Networks (SDN) requirement list is the longest among the themes. However, this reflects its critical nature in the modern-day network landscape. SDN is gaining more and more traction as network complexity and demands continue to increase, and as such, the requirements for managing these networks are expanding. Regarding Software Defined Networks (SDN), several areas are key requirements that a Network Management System (NMS) needs to support for robust network management.

Firstly, we have Essential Protocol Support. These protocols serve as the backbone of SDN operations. They include OpenFlow, the foundational protocol for SDN, and BGP-LS, which is necessary for exchanging link-state information between SDN controllers and traditional routing protocols. PCEP, NETCONF/YANG, RESTCONF, REST, gRPC, and HyperFlow also fall under this category, each playing unique roles in path computation, remote device management, and synchronization between distributed SDN controllers.

Next on the list is Protocol Support for Additional Value. While not as essential as the aforementioned protocols, the ones listed here—ForCES, I2RS, ALTO, and P4—can add substantial value in specific scenarios or network architectures. For instance, P4 allows for defining custom forwarding plane behavior, offering added flexibility.

Telemetry and Analytics is another significant area. NMS solutions like gNMI, NetFlow, sFlow, and IPFIX are required here. These tools enable the collection of traffic flow data for analysis and reporting. Each tool offers a unique approach, such as gNMI's efficient data collection and low latency or sFlow's sampling-based monitoring suitable for high-speed networks.

Flow Management and Monitoring is another critical area. This covers everything from real-time monitoring of flow entries to managing flow rules directly from the Network Management System (NMS). Conflict detection and resolution for flow rules are also crucial requirements here.

Lastly, we have Controller Support, both essential and additional. The Essential list includes widely used open-source SDN controllers like ONOS and OpenDaylight and proprietary options from Cisco, Juniper, HP, and Huawei. Each controller has unique features, whether ONOS's low hardware requirements or Cisco ACI's full native Layer 2-7 integration.

Additional Controller Support includes platforms like Beacon, Ryu, POX, NOX, and Floodlight. While these platforms may not be as essential, they offer unique features like Beacon's modularity and extensibility or Ryu's lightweight, component-based architecture that enables the rapid development of custom network applications.

Segment Routing and Traffic Engineering

Segmented Routing and Traffic Engineering, though not as widely discussed as Software Defined Networks (SDN), is equally critical in a Network Management System (NMS) context. It addresses the need for more flexible, efficient, and scalable routing and traffic management techniques, especially in large and complex network environments.

Under Network Discovery and Representation, the NMS must discover and represent all Segment Routing (SR)-enabled network elements, their connections, and Segment Identifiers (SIDs).

In Traffic Engineering and Management, the NMS should define or modify traffic engineering policies using SR features. It should also calculate and optimize the most efficient paths for data packets based on real-time network conditions.

Performance Monitoring and Analysis is key. The NMS should provide real-time network performance data and monitor SR-path performance regarding throughput, latency, packet loss, and resource utilization.

Routing Flexibility and Control requirements include supporting the creation and management of ad-hoc routes and enabling dynamic traffic management.

Finally, the NMS should integrate with SR-MPLS and SRv6, support programmability with IPv6 in SRv6, and work with OSPF, IS-IS, and BGP along with their segment routing extensions for Integration and Compatibility.

Artificial Intelligence and Machine Learning

Artificial Intelligence and Machine Learning (AI/ML) has increasingly become a fundamental component of modern Network Management Systems (NMS). It provides the ability to analyze, predict, and respond to network conditions in real-time, enhancing network performance and stability.

The NMS should include AI/ML-driven network management features. It needs big data capabilities to gather and consolidate data from diverse sources like logs, metrics, real-time events, network devices, and service ticketing systems. Additionally, advanced data analytics capabilities are required to analyze this data, including traffic patterns, resource utilization, network performance metrics, and incidents.

Key features include AI/ML-driven anomaly detection, leveraging AI/ML algorithms to identify and flag unusual events, patterns, or trends. The system should also have adaptive learning capabilities to continuously learn from data, improving the accuracy and efficiency of anomaly detection and network management processes over time.

Automated root cause analysis is another vital feature, using AI/ML algorithms to correlate abnormal events across different data sources, pinpointing the root cause of performance problems or incidents. Proactive problem resolution is also needed, implementing AI/ML-driven automation to address detected anomalies or issues promptly, minimizing network performance's impact.

Lastly, AI/ML should be leveraged for capacity planning and optimization. Predicting future capacity requirements and optimizing resources based on historical and real-time data can improve network performance and reduce costs by ensuring that resources are efficiently allocated.

Energy Management, GreenIT and ESG

Energy usage monitoring is crucial as network devices and servers consume significant energy. Real-time and historical data can identify patterns and inefficiencies, informing energy-saving measures. Estimating the carbon footprint of network infrastructure is another essential feature. The system can calculate GHG emissions using energy consumption data and emission factors.

Lifecycle tracking of network devices and servers, including procurement, usage, and end-of-life management, helps assess the environmental impact of equipment disposal and recycling. Monitoring the efficiency of cooling systems and power distribution units in data centers can highlight potential areas for improvement.

The NMS should integrate with other energy management systems, like BMS or DCIM solutions, for a holistic view of energy consumption and efficiency. Visualization of ESG metrics through customizable dashboards and automated report generation is critical. Alerts for deviations from ESG thresholds can facilitate timely interventions.

Finally, benchmarking and predictive analytics capabilities are essential for comparing and forecasting ESG performance.

The exhaustive investigation into the essential requirements for network management tools has highlighted the expansive landscape of modern network environments. While the identified trends and requirements provide a comprehensive overview of the current and future landscape, it's crucial to recognize that these may not necessarily present a one-size-fits-all solution. The unique characteristics of individual network environments, such as network size, customer base, and underlying infrastructure, can significantly shape the relevance and priority of these requirements.

Different networks might require different levels of focus on these themes, dictated by their unique characteristics and operational requirements. For instance, a network primarily serving OTT services might need a higher emphasis on Quality of Service and Network Caching. In contrast, a network with significant green energy commitments might prioritize Energy Management, Green IT, and ESG requirements. Similarly, the scale of the network could influence the necessity for advanced AI/ML capabilities or the extent of Software-Defined Networking requirements.

In recognition of this variability, our NMS feature matrix is designed with a high degree of flexibility. It is structured with nine different tabs, each representing a distinct theme, allowing network managers to include or exclude themes or sub-themes based on their needs and interests. This flexible design empowers network managers to tailor the tool to their unique circumstances, ensuring it remains relevant and valuable across various network environments.

Therefore, the value of this research extends beyond simply identifying the essential requirements for network management tools. It also offers a flexible, customizable framework for applying these requirements in diverse real-world network environments. As the network landscape evolves, this flexibility will be a key strength, enabling network managers to continuously adapt and optimize their network management strategies in line with emerging trends and changing needs.

6.3 Research Question 3 - NMS Feature Matrix Analysis

Research Question 3: How can telecommunication service providers utilize the current research of network technologies to support the selection of a modern-day network management system?

In this section, our primary focus is to examine the effectiveness of our NMS feature matrix in the selection process of Network Management System (NMS) tools. By undertaking a comprehensive analysis of three distinct NMS tools, we aim to demonstrate how this feature matrix aids in making informed decisions for our partner company Wexnet.

Our NMS feature matrix encompasses Wexnet's specific requirements and additional features derived from our eight themes in the theoretical background. The primary goal of our analysis is to showcase the usefulness of the NMS feature matrix in making informed decisions about NMS solutions rather than determining the absolute best fit for our partner company. This approach emphasizes the value of the feature matrix as a tool for guiding the decision-making process while also

providing valuable insights into the suitability of different NMS solutions based on their features and capabilities. In addition to demonstrating the feature matrix, we propose a three-level approach to the selection process of NMS solutions.

NMS Review Process

- **Level 1 - Online Research:** At this stage, we will gather information from publicly available resources, such as vendor white papers, case studies, data sheets, and FAQs. We understand that the absence of a specific feature in these materials does not necessarily indicate that the solution lacks that feature. It could mean the information is not disclosed in the materials, or we might have missed it during our review.
- **Level 2 - Vendor Cooperation:** If additional information is required after our Level 1 review, we will contact the respective companies to inquire about the features not supported or disclosed in the available materials. This stage can help us identify additional features not found during the Level 1 review.
- **Level 3 - NMS Testing:** In this final stage, we would request a trial of the NMS and test it in a lab environment. This hands-on approach allows us to verify the support for specific features and potentially discover additional features not identified in the previous levels of review.

Given our thesis's time and size constraints, we will primarily focus on the Level 1 review. This ensures we can efficiently gather and analyze substantial information within our limited resources. However, if necessary, we may delve into Level 2 to obtain crucial information that might be missing from the available materials.

The NMS Feature Matrix's Evaluation Process
We conducted a trial run to evaluate our NMS feature matrix by applying it to an NMS review. We also sought feedback from our Wexnet. After adjusting based on this feedback, we ran another test and asked the company for more input. This process was repeated until the feature matrix was determined to be finished. Each modification we made after every evaluation was kept track of in a change log. The entire process and the sequence of changes are shown in Figure 18 below.

Date	Version	Changes	Author	Note/Improvement
20.4.2023	0.8	Created the Google Sheets version	Haraldur Kristjansson, Lasse-Pekka Kylmäaho	Add requirement as Note instead of separate document
24.4.2023	0.85	Added notes with descriptions from the requirement tables Added new column for each NMS with drop-down menu with options 'Partial' and 'Ambiguous'	Haraldur Kristjansson, Lasse-Pekka Kylmäaho	Remove tick box, and add all options under the drop-down menu
25.4.2023	0.9	Removed the column with tick box, and all options are now under the drop-down menu: 'Supported', 'Not Supported' 'Partially Supported' 'Ambiguous'	Haraldur Kristjansson, Lasse-Pekka Kylmäaho	Feedback on the NMS features on to investigate the AI/ML, OTTP and Caching further.
3.5.2023	0.95	Changed the Ambiguous to "No infromation available" This is now the default of a cell. Added requirements for the requested AI/ML, OTTP, Caching Features we discovered	Haraldur Kristjansson, Lasse-Pekka Kylmäaho	Final company review of the feature matrix with before release. Received positive feedback of the carried out changes and the version 1.0 of the feature matrix was deemed ready.
8.5.2023	1.0	Version 1.0 of the Feature Matrix complete and ready for demonstration		

Figure 18: Change log of the feature matrix

The designed NMS feature matrix successfully meets the objectives set out in the design science method section:

O1 Provide a more efficient and structured process for selecting a network management system

O2 Combine the requirements for network management solutions based on RQ1, RQ2 and Wexnet specification

O3 Compare how well the reviewed NMS solutions answer these requirements

O4 Present the level on which the solution supports a feature

O5 Provide the steps for network management solution selection

1. Objective one was met by delivering a streamlined and well-structured spreadsheet for NMS selection. By structuring the feature sets and visualizing them in the feature matrix, we have provided a more efficient means of NMS review.

2. For objective two, the requirements based on research questions one and two and Wexnet's specifications were successfully integrated into the feature matrix's criteria. This combination ensures a comprehensive and relevant approach to evaluating potential NMS tools.

3. Objective three was addressed by comparing different NMS tools in relation to the defined requirements. This comparative analysis can be seen in the feature matrix snapshots presented in the results.

4. Objective four was accomplished by providing three levels of feature support: full support, partial support, and no support. This level of detail offers a clear understanding of how each NMS solution matches the requirements.

5. Finally, objective five was met by outlining a clear step-by-step process for selecting a network management tool, using the three levels of feature support as a guide.

ITRS - OP5

ITRS OP5 is a Network Management System (NMS) tool that offers comprehensive monitoring and management solutions built on Nagios, an open-source NMS. The company provides extensive Level 1 information through whitepapers, case studies, learning guides, and FAQs. Most of the readily available information primarily focuses on general monitoring and traditional networks, fulfilling most of the requirements of Wexnet. Still, we did not find much support for the themes covered in the theoretical background.

When we contacted the company to inquire about the more specific features related to novel technologies (such as SDN, NFV, SR-TE, Green IT, and QoS), we learned that the ITRS OP5 product is built on Nagios. Nagios is a well-known and widely used monitoring platform that supports a wide range of novel technologies. OP5 leverages this compatibility by offering support for Nagios plugins and allowing customers to develop customized plugins that can be integrated with the Nagios platform.

As a result, ITRS OP5 has the potential to accommodate the requirements of Wexnet and address the additional features identified in our theoretical background research. However, given the close relationship between ITRS OP5 and Nagios, conducting a Level 1 review of Nagios is recommended as well. This will provide a more comprehensive understanding of the features and capabilities that ITRS OP5 can support through its integration with Nagios. With this information in hand, a more informed and effective Level 2 and Level 3 review of ITRS OP5 can be carried out, ensuring a thorough evaluation of the NMS tool's suitability to meet our NMS feature matrix's requirements.

Micro Focus - Network Operations Management (NOM)

Micro Focus Network Operations Management (NOM) is a versatile solution that addresses organizations' network management and monitoring needs with diverse network infrastructures. Micro Focus NOM supports traditional and cutting-edge network technologies, such as software-defined networks and virtualization network functions.

Just like ITRS OP5, Micro Focus NOM provides comprehensive Level 1 information through various online resources, including whitepapers, case studies, learning guides, and FAQs. These resources encompass a wide array of technologies and features. According to our Level 1 review, Micro Focus NOM fulfills most of the traditional network management requirements specified by Wexnet. Additionally, the product offers support for numerous novel technology features, such as SDN, NFV, caching server management and monitoring, and the application of AI/ML. However, we did not find information about the NMS solution's support for segmented routing and specific service provider peering features. Furthermore, Micro Focus NOM supports Green IT monitoring, specifically energy

monitoring, but we could not find information on specific ESG features.

Netscout - nGeniusOne
Netscout's nGeniusOne is a network performance management solution aimed at delivering comprehensive network visibility, troubleshooting, and proactive service assurance. nGeniusOne is designed to support complex and modern network infrastructures, providing necessary insights to maintain optimal network performance.

Our Level 1 review of nGeniusOne revealed a scarcity of detailed information from the vendor's whitepapers, case studies, and other material provided. This makes it challenging to evaluate the extent of its capabilities, particularly its proficiency in traditional network management tasks as specified by Wexnet's feature list. However, the high-level information available suggests strong provision for these standard requirements.

The information presented by nGeniusOne's vendor was somewhat more detailed regarding cutting-edge network technologies, although it primarily concentrated on the NMS tool's high-level capabilities. A notable distinction from the other NMS solutions was the absence of in-depth user manuals and learning guides, which, based on our observations, typically offer the most comprehensive information on the features the tool supports.

7 Discussion

In this section, we aim to delve deeper into the analysis conducted in the previous section and to assess their relevance and implications in the broader context of network technology trends. The discussion is structured to address the following key aspects: comparison of the analyzed results with related works, evaluation of the validity of the analyzed results, and discuss the implications of these results for the target group.

7.1 Comparison with related works

The comparison between our findings and existing literature is instrumental in establishing the validity and significance of the research. We did not find any other work that was focused on the same combination of objectives as our study. Our study undertook a limited literature review and thematic analysis to identify the current trends in network technology, with a particular focus on fixed-access networks. Additionally, the study explored the requirements these trends imposed on Network Management Systems (NMS) and created a feature matrix tool for network managers. In contrast, the existing literature that we discovered is extensive but tends to focus on investigating specific technologies in detail, with much emphasis placed on novel network communications such as 5G and Internet Of Things (IoT) wireless communications.

In comparison, A. Martinez et al. [3] addressed the challenges faced by Internet service providers in managing multi-layer and multi-vendor carrier-grade networks in 2014. Since then, advancements such as SDN, NFV, and AI/ML have reshaped the landscape, and this is well-reflected in our research. Notably, while Martinez et al.'s work focused on challenges specific to multi-layer networks, our research provides a more encompassing analysis of the trends and their implications on NMS, including some themes that have emerged post-2014, such as AI/ML in network automation and ESG factors.

The paper by Angelopoulos et al. [4] aligns more closely with our research, as it also examines modern networking technologies. However, it predominantly focuses on monitoring in 5G networks, whereas our work explores a broader spectrum of themes and specifically addresses the features required in NMS for fixed-access network management.

Sasidharan et al. [5] provide insights into SDN-based NMS and the expected features for the future. Our work complements this by identifying features and requirements not only for SDN but also for other emerging trends, providing a more comprehensive set of criteria for NMS.

In essence, our research extends the scope beyond what has been addressed in the related work by incorporating a broader range of themes and pinpointing the direct requirements imposed by these evolving networking technologies on NMS. Moreover, creating a feature matrix tool is a distinct contribution, as it offers a practical means for network managers to evaluate NMSs in light of these trends.

The subsequent sections will further discuss the validity of the analyzed results and explore the implications of these findings for the target audience.

7.2 Validity and implications for the target group

After reviewing the three NMS solutions and exploring numerous others, we have concluded that obtaining information on Level 1 is often a difficult task due to several factors:

- Vendors not providing comprehensive lists of features their NMS tools support.
- Having to gather information from various scattered documents to confirm feature support.
- Restricted access to user manuals and configuration guides for non-customers.
- Available information often being a high-level overview without specific technical details, such as protocol support.

As a result, it becomes challenging to determine the extent to which these NMS solutions fulfill our NMS feature matrix's requirements. Furthermore, vendors typically offer a suite of tools that individually cover management, visualization, artificial intelligence features, and more.

Through our interaction with our partner company, we discovered that in real-world scenarios, organizations often bypass the Level 1 review and proceed directly to Level 2. In this process, the feature matrix is forwarded to vendors, who are then asked to indicate or specify which features their respective tools incorporate or support. This allows the vendor to choose the most suitable tools for different themes and offers the company a tailored suite of NMS tools and their specific capabilities. Consequently, this approach facilitates a more accurate comparison of tools. It helps organizations make informed decisions regarding which tools to select for a Level 3 review, such as on-site testing, based on their unique requirements.

It is important to recognize the breadth and complexity of the topic studied in this thesis. While our approach through LLR and Thematic Analysis was methodical, the scope of the research was constrained by the nature of a bachelor's thesis. Consequently, while our feature list provides an important starting point, it should be acknowledged that it may not be exhaustive. A more detailed literature review focusing on the themes identified could be beneficial for gaining a deeper understanding and for creating a more comprehensive feature list. In this regard, we posit that the feature list generated in this research represents an important foundation but not an exhaustive set of criteria.

Concerning the validity of the features chosen, we have an extensive annex, A, which includes detailed discussions on each theme. This appendix was developed based on a review of numerous papers and other materials, which we believe offers readers insights into why the features selected are significant for NMS. For readers seeking an even deeper understanding of a specific topic, we provide a list of high-quality references that can be used as a basis for further exploration.

With respect to the target group, our collaboration with Wexnet, a company operating within the domain of interest, was invaluable. The positive feedback

from Wexnet reaffirms the practical relevance and usability of the feature matrix developed. Particularly, the modular structure based on themes was appreciated, enabling network managers to focus on specific aspects of interest or bypass those irrelevant to their infrastructure. This customization potential indicates the feature matrix's versatility in catering to diverse organizational needs.

In conclusion, this research has made meaningful contributions to understanding the current trends in network technology and the requirements these trends impose on Network Management Systems. While there are limitations to consider, especially given the scale of the subject matter, this work can serve as a valuable resource in making informed decisions about network management tools that are aligned with the evolving technological landscape.

8 Conclusion and Future Work

In this thesis, we address the problem of selecting appropriate network management system (NMS) tools for network service providers (NSPs) in the context of rapidly evolving network technologies. We pose research questions related to identifying key trends and requirements for modern network management and developing an NMS feature matrix as a design artifact to aid NSPs in their decision-making process. Our main objective is to provide guidance for our partner company, Wexnet, in selecting the most suitable NMS tool based on their requirements and the latest trends in network management.

We identify the main trends and novel technologies in networking, such as software-defined networking (SDN), network function virtualization (NFV), segment routing and traffic engineering (SR-TE), energy management (Green IT and ESG), and quality of service (QoS), through a limited literature review and thematic analysis. Based on these findings, we create a feature matrix encompassing the requirements for NMS tools derived from our theoretical background research and Wexnet's specific needs. We then apply a three-level approach to evaluate four NMS tools, focusing primarily on Level 1 review due to time and size constraints. The three-level NMS review process and the developed feature matrix form the proposed NMS selection process based on modern challenges and industry needs.

Our research findings and the developed feature matrix can assist Wexnet's network architects and engineers in making informed decisions about their network management infrastructure. By considering the latest trends and challenges in network management, Wexnet can potentially improve its service offerings and address the needs of its customers more effectively.

This research contributes to the current understanding of network management systems by identifying the challenges researchers and professionals face. Our feature matrix is a valuable tool for guiding the decision-making process for network management tool selection, incorporating academic research and expert insights. This approach can help NSPs to select NMS tools that are well-suited to address the challenges and requirements of modern network infrastructures. The societal effect of supporting NSPs in their decision-making can help network infrastructure managers meet the ambitious goals outlined by policies such as the European Union's digital decade 2030. In addition to guiding the NMS selection process, the developers and researchers of networking and NMS can utilize the feature requirements presented to understand the modern challenges and industry needs further.

In conclusion, this thesis addresses the problem of selecting suitable NMS tools for NSPs in the context of rapidly evolving network technologies. By developing an NMS feature matrix as a design artifact and employing a three-level approach for evaluating NMS tools, we offer valuable insights to NSPs like Wexnet, enabling them to make motivated and informed decisions in their network management infrastructure. Our research advances the understanding of network management systems and provides a practical solution that addresses the challenges and requirements of modern network infrastructures.

8.1 Future work

The proposed selection process introduces three levels for selecting an NMS: online research, vendor cooperation, and NMS tool testing. The scope of this research project focuses on the demonstration of Level 1, which may provide an incomplete understanding of NMS tools' capabilities as the NMS vendors might not address all the supported features. Future work could involve further cooperation with the NMS vendors by further carrying out the proposed review and selection process. Practical testing of the NMS solutions and expanding the number of evaluated NMS tools would provide more in-depth analysis and potentially result in a more accurate feature listing for the NSPs. Including more industry professionals or network service providers would allow for a further understanding of the business problems and perceived challenges.

Further research could also focus on comparing the findings between the vendor-supplied white papers and data sheets to the fulfillment of the feature requirements discovered in the controlled testing of the NMS tools. Controlled experiments could uncover potential discrepancies between what the vendors communicate in their publications and what the NMS tools support or do not support. The majority of the publications relating to the research area are commercial, and as such general future research direction could address the lack of academic research on the research area of network management systems.

References

[1] European Commission., "Europe's digital decade: digital targets for 2030s," 2022, [Accessed: 29.1.2023]. [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[2] Europe's telecommunication network operator (ETNO) and Axon Partners Group, "Europe's internet ecosystem," 2022, [Accessed: 29.1.2023]. [Online]. Available: https://etno.eu/component/attachments/attachments.html?task=download&id=8193

[3] A. Martinez, M. Yannuzzi, V. Lopez, D. Lopez, W. Ramirez, R. Serral-Gracia, X. Masip-Bruin, M. Maciejewski, and J. Altmann, "Network management challenges and trends in multi-layer and multi-vendor settings for carrier-grade networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2207–2230, 2014, [Accessed: 14.3.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6826469

[4] I. Angelopoulos, E. Trouva, and G. Xilouris, "A monitoring framework for 5g service deployments," in *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2017, pp. 1–6, [Accessed: 29.1.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/document/8031617/

[5] S. Sasidharan and S. K. Chandra, "Defining future sdn based network management systems characterization and approach," in *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*. IEEE, 2014, pp. 1–5, [Accessed: 22.2.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/abstract/document/6963137

[6] L. Bondan, C. R. P. dos Santos, and L. Z. Granville, "Comparing virtualization solutions for nfv deployment: A network management perspective," in *2016 IEEE Symposium on Computers and Communication (ISCC)*. IEEE, 2016, pp. 669–674, [Accessed: 14.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/stamp/stamp.jsp?tp=&arnumber=7543814

[7] M. Waseem, P. Liang, G. Márquez, and A. Di Salle, "Testing microservices architecture-based applications: A systematic mapping study," in *2020 27th Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, 2020, pp. 119–128, [Accessed: 14.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/stamp/stamp.jsp?tp=&arnumber=7543814

[8] J. Networks, "Four reasons to automate your network right now," 2016, [Accessed: 29.1.2023]. [Online]. Available: https://www.juniper.net/content/dam/www/assets/white-papers/us/en/four-reasons-to-automate-your-network-right-now.pdf

[9] E. Coronado, R. Behravesh, T. Subramanya, A. Fernàndez-Fernàndez, M. S. Siddiqui, X. Costa-Pérez, and R. Riggio, "Zero touch management: A survey of network automation solutions for 5g and 6g networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2535–2578, 2022, [Accessed: 29.1.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/document/9913206

[10] G. Mirjalily and Z. Luo, "Optimal network function virtualization and service function chaining: A survey," *Chinese Journal of Electronics*, vol. 27, no. 4, pp. 704–717, 2018, [Accessed: 08.04.2023]. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/epdf/10.1049/cje.2018.05.008

[11] V. Fulber-Garcia, "Network management: The fcaps model," 2022, accessed: yyyy-mm-dd. [Online]. Available: https://www.baeldung.com/cs/network-management-fcaps-model

[12] R. Dhole. (2023) Exploring the booming network management system market: Trends, key players, and future growth prospects. LinkedIn. Accessed: 2023-05-11. [Online]. Available: https://www.linkedin.com/pulse/exploring-booming-network-management-system-market-trends-dhole/

[13] M. Wichtlhuber, R. Reinecke, and D. Hausheer, "An sdn-based cdn/isp collaboration architecture for managing high-volume flows," *IEEE Transactions on Network and Service Management*, vol. 12, no. 1, pp. 48–60, 2015, [Accessed: 27.3.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7044567

[14] N. Feamster, J. Rexford, and E. Zegura, "The road to sdn: An intellectual history of programmable networks," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 2, p. 87–98, apr 2014, [Accessed: 27.3.2023]. [Online]. Available: https://doi.org/10.1145/2602204.2602219

[15] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, pp. 45–77, 01 2007, [Accessed: 29.1.2023]. [Online]. Available: https://www.researchgate.net/publication/284503626_A_design_science_research_methodology_for_information_systems_research

[16] M. Karakus and A. Durresi, "Quality of service (qos) in software defined networking (sdn): A survey," *Journal of Network and Computer Applications*, vol. 80, pp. 200–218, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804516303186

[17] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[18] W. S. R. Carla Willig, Wendy Stainton Rogers / Carla Willig, *The SAGE handbook of qualitative research in psychology*, second edition ed. London: SAGE Publications Ltd, 2017.

[19] J. Attride-Stirling, "Thematic networks: an analytic tool for qualitative research," *Qualitative Research*, vol. 1, no. 3, pp. 385–405, 2001. [Online]. Available: https://doi.org/10.1177/146879410100100307

[20] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004. [Online]. Available: http://www.jstor.org/stable/25148625

[21] M. G. Alabarce and P. P. Mariño, "Optical network design and analysis tools: A test of time," *Optical Switching and Networking*, vol. 44, p. 100651, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1573427721000485

[22] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, Jan. 2006. [Online]. Available: https://doi.org/10.1191/1478088706qp063oa

[23] M. Stevens, "Appneta named a "visionary" in 2019 gartner npmd magic quadrant," Feb 2019, [Accessed: 27.3.2023]. [Online]. Available: https://www.appneta.com/blog/appneta-named-a-visionary-in-2019-gartner-npmd-magic-quadrant/

[24] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, and D. Moher, "The prisma 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, 2021. [Online]. Available: https://www.bmj.com/content/372/bmj.n71

[25] M. Peitz and T. Valletti, "Reassessing competition concerns in electronic communications markets," *Telecommunications Policy*, vol. 39, no. 10, pp. 896–912, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0308596115001159

[26] E. T. Bilbil, "Methodology for the regulation of over-the-top (ott) services: The need of a multi-dimensional perspective," *International Journal of Economics and Financial Issues*, vol. 8, pp. 101–110, 2018.

[27] Sandvine, "Global internet phenomena report 2023," [Accessed: 10.4.2023]. [Online]. Available: https://www.sandvine.com/phenomena

[28] K. T. Bagci and A. M. Tekalp, "Dynamic resource allocation by batch optimization for value-added video services over sdn," *IEEE Transactions on Multimedia*, vol. 20, no. 11, pp. 3084–3096, 2018.

[29] Cisco, "Vni complete forecast highlights," [Accessed: 13.4.2023]. [Online]. Available: https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf

[30] European Parliament, "Regulation (eu) 2015/2120 of the european parliament," [Accessed: 13.4.2023]. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2015/2120/2018-12-20

[31] Traficom , "Open internet and net neutrality," [Accessed: 13.4.2023]. [Online]. Available: https://www.traficom.fi/en/communications/communications-networks/open-internet-or-net-neutrality

[32] Cisco ThousandEyes, "Isp peering," [Accessed: 10.4.2023]. [Online]. Available: https://www.thousandeyes.com/learning/techtorials/isp-peering

[33] A. Ahmad, A. Floris, and L. Atzori, "Ott-isp joint service management: A customer lifetime value based approach," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2017, pp. 1017–1022.

[34] A. A. Barakabitze, N. Barman, A. Ahmad, S. Zadtootaghaj, L. Sun, M. G. Martini, and L. Atzori, "Qoe management of multimedia streaming services in future networks: A tutorial and survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 526–565, 2020.

[35] A. Nikkhah and S. Jordan, "Analysis of the requirements of settlement-free interconnection policies," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2023, [Accessed: 03.5.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10064193

[36] T. Orme, "Essential guide: Ott monitoring uncovered," June 2019, [Accessed: 03.5.2023]. [Online]. Available: https://www.thebroadcastbridge.com/content/entry/13603/ott-monitoring-uncovered

[37] National Institute of Standards and Technology, "Quality of service," [Accessed: 13.4.2023]. [Online]. Available: https://csrc.nist.gov/glossary/term/Quality_of_Service

[38] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path-quality monitoring in the presence of adversaries: The secure sketch protocols," *IEEE/ACM Transactions on Networking*, vol. 23, no. 6, pp. 1729–1741, 2015.

[39] Fortninet, "Fortinet cyberglossary : Qos," [Accessed: 13.4.2023]. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service

[40] ——, "Traffic shaping," [Accessed: 13.4.2023]. [Online]. Available: https://docs.fortinet.com/document/fortigate/6.4.5/administration-guide/297431/traffic-shaping

[41] ——, "Fortinet cyberglossary mpls," [Accessed: 13.4.2023]. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/mpls

[42] S. Nacakli and A. M. Tekalp, "Controlling p2p-cdn live streaming services at sdn-enabled multi-access edge datacenters," *IEEE Transactions on Multimedia*, vol. 23, pp. 3805–3816, 2021.

[43] A. Vakali and G. Pallis, "Content delivery networks: status and trends," *IEEE Internet Computing*, vol. 7, no. 6, pp. 68–74, 2003.

[44] D. Bhamare, M. Samaka, A. Erbad, R. Jain, and L. Gupta, "Exploring microservices for enhancing internet qos," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 11, p. e3445, 2018, e3445 ETT-17-0393.R1. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3445

[45] B. Zolfaghari, G. Srivastava, S. Roy, H. R. Nemati, F. Afghah, T. Koshiba, A. Razi, K. Bibak, P. Mitra, and B. K. Rai, "Content delivery networks: State of the art, trends, and future roadmap," *ACM Comput. Surv.*, vol. 53, no. 2, apr 2020. [Online]. Available: https://doi.org/10.1145/3380613

[46] A. Sadeghi, G. Wang, and G. B. Giannakis, "Deep reinforcement learning for adaptive caching in hierarchical content delivery networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 4, pp. 1024–1033, 2019.

[47] M. Conti, A. Gangwal, M. Hassan, C. Lal, and E. Losiouk, "The road ahead for networking: A survey on icn-ip coexistence solutions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2104–2129, 2020.

[48] J. Gu, W. Wang, A. Huang, H. Shan, and Z. Zhang, "Distributed cache replacement for caching-enable base stations in cellular networks," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 2648–2653.

[49] M. A. Salahuddin, J. Sahoo, R. Glitho, H. Elbiaze, and W. Ajib, "A survey on content placement algorithms for cloud-based content delivery networks," *IEEE Access*, vol. 6, pp. 91–114, 2018.

[50] Catchpoint, "Cdn monitoring," in *The Guide to Synthetic Monitoring*. Catchpoint, 2021, ch. 5, [Accessed: 03.5.2023]. [Online]. Available: https://www.catchpoint.com/guide-to-synthetic-monitoring/cdn-monitoring

[51] R. Jmal and L. Chaari Fourati, "Assisted dash-aware networking over sdn—ccn architecture," *Photonic Netw. Commun.*, vol. 38, no. 1, p. 37–50, aug 2019. [Online]. Available: https://doi-org.proxy.lnu.se/10.1007/s11107-019-00835-1

[52] P. v. Anvith, N. Gunavathi, B. Malarkodi, and B. Rebekka, "A survey on network functions virtualization for telecom paradigm," in *2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW)*, 2019, pp. 302–306, [Accessed: 07.04.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/document/8933271?reason=concurrency

[53] K. Kaur, V. Mangat, and K. Kumar, "A review on virtualized infrastructure managers with management and orchestration features in nfv architecture," *Computer Networks*, p. 109281, 2022, [Accessed: 07.04.2023]. [Online]. Available: https://www-sciencedirect-com.proxy.lnu.se/science/article/pii/S1389128622003395

[54] A. Leonhardt, "Networking for nerds: Defining the elements of nfv architectures," 2019, [Accessed: 29.3.2023]. [Online]. Available: https://blog.equinix.com/blog/2019/10/17/networking-for-nerds-defining-the-elements-of-nfv-architectures/

[55] J. G. Herrera and J. F. Botero, "Resource allocation in nfv: A comprehensive survey," *IEEE Transactions on Network and Service Management*, vol. 13, no. 3, pp. 518–532, 2016, [Accessed: 08.04.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/stamp/stamp.jsp?tp=&arnumber=7534741

[56] K. Kaur, V. Mangat, and K. Kumar, "A comprehensive survey of service function chain provisioning approaches in sdn and nfv architecture," *Computer Science Review*, vol. 38, p. 100298, 2020, [Accessed: 07.04.2023]. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013720303981

[57] S. Park, H.-G. Kim, J. Hong, S. Lange, J.-H. Yoo, and J. W.-K. Hong, "Machine learning-based optimal vnf deployment," in *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2020, pp. 67–72, [Accessed: 08.04.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/document/9236970

[58] R. Chayapathi, S. F. Hassan, and P. Shah, *Network Functions Virtualization (NFV) with a Touch of SDN: Netw Fun Vir (NFV EPub_1)*. Addison-Wesley Professional, 2016, [Accessed: 08.04.2023]. [Online]. Available: https://ptgmedia.pearsoncmg.com/images/9780134463056/samplepages/9780134463056.pdf

[59] European Telecommunications Standards Institute (ETSI), "Network functions virtualisation (nfv); use cases," ETSI, Group Report GR NFV 001 V1.2.1, 5 2017, [Accessed: 08.04.2023]. [Online]. Available: https://www.etsi.org/deliver/etsi_gr/NFV/001_099/001/01.02.01_60/gr_NFV001v010201p.pdf

[60] A. Diana. (2018, 5) Network slicing: It ain't just for 5g. [Accessed: 08.04.2023]. [Online]. Available: https://www.broadbandworldnews.com/author.asp?section_id=548&doc_id=742774

[61] S. K. N. Rao, "Sdn and its use-cases- nv and nfv: A state-of-the-art survey," NEC Technologies India Limited, White Paper, n.d., [Accessed: 08.04.2023]. [Online]. Available: https://in.nec.com/en_IN/pdf/NTI_whitepaper_SDN_NFV.pdf

[62] E. Nikolouzou, G. Milenkovic, G. Bafoutsou, and S. Bryska, "Nfv security in 5g: Challenges and best practices," European Union Agency for Cybersecurity, Tech. Rep., February 2022, [Accessed: 08.04.2023]. [Online]. Available: https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

[63] A. J. Gonzalez, G. Nencioni, A. Kamisiński, B. E. Helvik, and P. E. Heegaard, "Dependability of the nfv orchestrator: State of the art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3307–3329, 2018, [Accessed: 08.04.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/stamp/stamp.jsp?tp=&arnumber=8350296

[64] F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and openflow: From concept to implementation," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014, [Accessed: 28.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/document/6819788

[65] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2014, [Accessed: 29.3.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6994333

[66] M. Paliwal, D. Shrimankar, and O. Tembhurne, "Controllers in sdn: A review report," *IEEE Access*, vol. 6, pp. 36 256–36 270, 2018, [Accessed: 28.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/abstract/document/8379403

[67] F. J. B. V. Neto, C. J. Miguel, A. C. d. S. de Jesus, and P. N. Sampaio, "Sdn controllers-a comparative approach to market trends," in *9th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2021)*, 2021, pp. 48–51, [Accessed: 16.4.2023]. [Online]. Available: https://hal.science/hal-03133692/

[68] J. Medved, R. Varga, A. Tkacik, and K. Gray, "Opendaylight: Towards a model-driven sdn controller architecture," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, 2014, pp. 1–6, [Accessed: 31.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/abstract/document/6918985

[69] S. Hadla, G. Saba, and M. Alchaita, "" interconnection between sdn adhoc controllers," *Arab Journal for Scientific Publishing (AJSP) ISSN*, vol. 2663, p. 5798, [Accessed: 28.3.2023]. [Online]. Available: https://www.ajsp.net/research/Interconnection%20between%20SDN%20Adhoc%20Controllers.pdf

[70] I. Šeremet and S. Čaušević, "An analysis of reconvergence delay when using bgp-ls/pcep as southbound protocols," in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2019, pp. 415–420, [Accessed: 31.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/document/8757057

[71] O. Santos. (2023, 03) Security comparison between netconf, restconf, and snmp. [Accessed: 16.4.2023]. [Online]. Available: https://community.cisco.com/t5/security-knowledge-base/security-comparison-between-netconf-restconf-and-snmp/ta-p/4805483

[72] A. Atlas, J. Halpern, S. Hares, D. Ward, and T. Nadeau, "An Architecture for the Interface to the Routing System," RFC 7921, June 2016, [Accessed: 31.3.2023]. [Online]. Available: https://www.hjp.at/doc/rfc/rfc7921.html#sec_6.4.2

[73] W. Zhou, L. Li, M. Luo, and W. Chou, "Rest api design patterns for sdn northbound api," in *2014 28th International Conference on Advanced Information Networking and Applications Workshops*, 2014, pp. 358–365, [Accessed: 31.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/document/6844664

[74] S. G. Du, J. W. Lee, and K. Kim, "Proposal of grpc as a new northbound api for application layer communication efficiency in sdn," in *Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication*, 2018, pp. 1–6, [Accessed: 31.3.2023]. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3164541.3164563

[75] V. K. Gurbani, M. Scharf, T. V. Lakshman, V. Hilt, and E. Marocco, "Abstracting network state in software defined networks (sdn) for rendezvous services," in *2012 IEEE International Conference on Communications (ICC)*, 2012, pp. 6627–6632, [Accessed: 04.4.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/abstract/document/6364858

[76] R. Vilalta, C. Manso, N. Yoshikane, R. Muñoz, R. Casellas, R. Martínez, T. Tsuritani, and I. Morita, "Telemetry-enabled cloud-native transport sdn controller for real-time monitoring of optical transponders using gnmi," in *2020 European Conference on Optical Communications (ECOC)*. IEEE, 2020, pp. 1–4, [Accessed: 31.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/stamp/stamp.jsp?tp=&arnumber=9333143

[77] R. Vilalta, N. Yoshikane, R. Casellas, R. Martínez, T. Tsuritani, I. Morita, and R. Muñoz, "Controlling and monitoring optical network equipment in optical sdn networks," in *2020 European Conference on Optical Communications (ECOC)*. IEEE, 2020, pp. 1–4, [Accessed: 31.3.2023]. [Online]. Available: https://ieeexplore-ieee-org.proxy.lnu.se/stamp/stamp.jsp?tp=&arnumber=9333345

[78] I. Cisco Systems, "Data center telemetry and network automation using gnmi and openconfig," 2020, [Accessed: 31.3.2023]. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-744191.pdf

[79] R. Grimmick. (2021) Network flow monitoring explained: Netflow vs sflow vs ipfix. [Accessed: 10.4.2023]. [Online]. Available: https://www.varonis.com/blog/flow-monitoring

[80] M. Afaq, S. Rehman, and W.-C. Song, "Large flows detection, marking, and mitigation based on sflow standard in sdn," *Journal of Korea Multimedia Society*, vol. 18, no. 2, pp. 189–198, 2015, [Accessed: 10.4.2023]. [Online]. Available: https://koreascience.kr/article/JAKO201509139907021.pdf

[81] S. Kumarsamy. (2019, Sep.) Ip flow information export (ipfix) vs. netflow. [Accessed: 10.4.2023]. [Online]. Available: https://blog.gigamon.com/2019/09/17/ipfix-vs-netflow/

[82] A. Liatifis, P. Sarigiannidis, V. Argyriou, and T. Lagkas, "Advancing sdn from openflow to p4: A survey," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–37, 2023, [Accessed: 10.4.2023]. [Online]. Available: https://dl.acm.org/doi/full/10.1145/3556973

[83] M. Karakus and A. Durresi, "Quality of service (qos) in software defined networking (sdn): A survey," *Journal of Network and Computer Applications*, vol. 80, pp. 200–218, 2017, [Accessed: 16.4.2023]. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804516303186

[84] L. L. Peterson, C. Cascone, B. O'Connor, M. Vachuska, and B. S. Davie, *Software-Defined Networks: A Systems Approach*, 2nd ed. Systems Approach LLC, 2022, accessed: yyyy-mm-dd. [Online]. Available: https://sdn.systemsapproach.org/index.html

[85] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for sdn? implementation challenges for software-defined networks," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 36–43, 2013, [Accessed: 10.4.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6553676

[86] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn security: A survey," in *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*,

2013, pp. 1–7, [Accessed: 10.4.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6702553

[87] T. Schüller, N. Aschenbruck, M. Chimani, M. Horneffer, and S. Schnitter, "Traffic engineering using segment routing and considering requirements of a carrier ip network," *IEEE/ACM Transactions on Networking*, vol. 26, no. 4, pp. 1851–1864, 2018, [Accessed: 12.04.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8418309

[88] T. D. Nadeau, *MPLS Network Management: MIBs, Tools, and Techniques*. San Francisco, CA: Elsevier, 2003, [Accessed: 12.04.2023]. [Online]. Available: https://www-sciencedirect-com.proxy.lnu.se/science/article/pii/B9781558607514500097

[89] B. Fortz, J. Rexford, and M. Thorup, "Traffic engineering with traditional ip routing protocols," *IEEE communications Magazine*, vol. 40, no. 10, pp. 118–124, 2002, [Accessed: 12.04.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1039866

[90] P. L. Ventre, S. Salsano, M. Polverini, A. Cianfrani, A. Abdelsalam, C. Filsfils, P. Camarillo, and F. Clad, "Segment routing: a comprehensive survey of research activities, standardization efforts, and implementation results," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 182–221, 2020, [Accessed: 14.04.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9253580

[91] A. Mendiola, J. Astorga, E. Jacob, and M. Higuero, "A survey on the contributions of software-defined networking to traffic engineering," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 918–953, 2016, [Accessed: 12.04.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7762818

[92] B. Fortz, J. Rexford, and M. Thorup, "Traffic engineering with traditional ip routing protocols," *IEEE communications Magazine*, vol. 40, no. 10, pp. 118–124, 2002, [Accessed: 10.04.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1039866

[93] P. L. Ventre, S. Salsano, M. Polverini, A. Cianfrani, A. Abdelsalam, C. Filsfils, P. Camarillo, and F. Clad, "Segment routing: a comprehensive survey of research activities, standardization efforts, and implementation results," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 182–221, 2020, [Accessed: 10.04.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9253580

[94] L. Davoli, L. Veltri, P. L. Ventre, G. Siracusano, and S. Salsano, "Traffic engineering with segment routing: Sdn-based architectural design and open source implementation," in *2015 Fourth European Workshop on Software*

Defined Networks. IEEE, 2015, pp. 111–112, [Accessed: 10.04.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7313628

[95] R. Mota. (2018, Aug) Segment routing. [Accessed: 10.04.2023]. [Online]. Available: https://www.linkedin.com/pulse/segment-routing-ray-mota-phd

[96] H. Vasconcelos, M. Jörke, M. Grunde-McLaughlin, T. Gerstenberg, M. Bernstein, and R. Krishna, "Explanations can reduce overreliance on ai systems during decision-making," 2023.

[97] Y. Wang, R. Forbes, C. Cavigioli, H. Wang, A. Gamelas, A. Wade, J. Strassner, S. Cai, and S. Liu, "Network management and orchestration using artificial intelligence: Overview of etsi eni," *IEEE communications standards magazine*, vol. 2, no. 4, pp. 58–65, 2018, [Accessed: 02.5.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8636837

[98] S. McGillicuddy, "Ema research report: Network performance management for today's digital enterprise," Enterprise Management Associates (EMA), Tech. Rep., May 2019, [Accessed: 02.5.2023]. [Online]. Available: https://download.manageengine.com/network-monitoring/EMA-Digital-Network-Performance-Monitoring-Survey-Report.pdf

[99] "What is aiops?" https://www.ibm.com/topics/aiops, IBM, n.d.

[100] R. Akkiraju, https://www.ibm.com/cloud/blog/art-of-automation-chapter-5, IBM, May 2021, [Accessed: 02.5.2023]. [Online]. Available: TheArtofAutomation:Chapter5-AIOps

[101] B. Lutkevich and E. McLaughlin. (no-date) Green it (green information technology). TechTarget. [Accessed: 13.04.2023]. [Online]. Available: https://www.techtarget.com/searchcio/definition/green-IT-green-information-technology

[102] D. Farmer. (2023, 3) Esg metrics: Tips and examples for measuring esg performance. TechTarget. [Accessed: 13.04.2023]. [Online]. Available: https://www.techtarget.com/sustainability/feature/ESG-metrics-Tips-and-examples-for-measuring-ESG-performance

[103] J. Lorincz, Z. Klarin, and D. Begusic, "Advances in improving energy efficiency of fiber–wireless access networks: A comprehensive overview," *Sensors*, vol. 23, no. 4, p. 2239, 2023, [Accessed: 13.04.2023]. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/2239

[104] J. Borgini. (2023, Mar) 8 green computing best practices. Spacebarpress Media. [Accessed: 13.04.2023]. [Online]. Available: https://www.techtarget.com/sustainability/article/8-green-computing-best-practices

[105] J. von Perner, V. Friderikos, J. Erfanian, J. Liu, S. Ansari, D. Dianat, D. L'opez-P'erez, M. Dohler, L. Jorguseski, E. B. Gedik, K. Yaman, G. Kalem, A. G. Serrano, M. Oikonomakou, G. Li, W. Redmond, and M.-P. Odini, "Network energy efficiency," *NGMN Alliance*, vol. 1.1, 12 2021, [Accessed: 14.04.2023]. [Online]. Available: https://www.ngmn.org/wp-content/uploads/211009-GFN-Network-Energy-Efficiency-1.0.pdf

[106] Y. Tan, W. Liu, and Q. Qiu, "Adaptive power management using reinforcement learning," in *Proceedings of the 2009 International Conference on Computer-Aided Design*, 2009, pp. 461–467, [Accessed: 13.04.2023]. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1687399.1687486

[107] S. Zavrak and M. Iskefiyeli, "A research on green networking in sdn," *ResearchGate*, 2018, [Accessed: 10.04.2023]. [Online]. Available: https://www.researchgate.net/publication/322473731_A_Research_on_Green_Networking_In_SDN#fullTextFileContent

[108] C. Stedman, "Esg strategy and management: Complete guide for businesses," April 2023, [Accessed: 14.04.2023]. [Online]. Available: https://www.techtarget.com/sustainability/feature/ESG-strategy-and-management-Complete-guide-for-businesses

[109] The IFRS Foundation's International Sustainability Standards Board (ISSB), "The sustainability reporting ecosystem," [Accessed: 20.04.2023]. [Online]. Available: https://www.sasb.org/about/sasb-and-other-esg-frameworks/

Primary Studies

[S1] K. H. Rahouma and A. Ali, "Applying machine learning technology to optimize the operational cost of the egyptian optical network," *Procedia Computer Science*, vol. 163, pp. 502–517, 2019, 16th Learning and Technology Conference 2019Artificial Intelligence and Machine Learning: Embedding the Intelligence. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919321726

[S2] Y. Zhao, B. Yan, Z. Li, W. Wang, Y. Wang, and J. Zhang, "Coordination between control layer ai and on-board ai in optical transport networks [invited]," *Journal of Optical Communications and Networking*, vol. 12, no. 1, pp. A49–A57, January 2020.

[S3] L. Mai, Y. Ding, X. Zhang, L. Fan, S. Yu, and Z. Xu, "Energy efficiency with service availability guarantee for network function virtualization," *Future Generation Computer Systems*, vol. 119, pp. 140–153, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21000479

[S4] M. S. Q. Z. Nine, L. D. Tacchio, A. Imran, T. Kosar, M. F. Bulut, and J. Hwang, "Greendataflow: Minimizing the energy footprint of global data movement," *CoRR*, vol. abs/1810.05892, 2018. [Online]. Available: http://arxiv.org/abs/1810.05892

[S5] M. Conti, A. Gangwal, M. Hassan, C. Lal, and E. Losiouk, "The road ahead for networking: A survey on icn-ip coexistence solutions," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 2104–2129, 2020.

[S6] A. Sadeghi, G. Wang, and G. B. Giannakis, "Deep reinforcement learning for adaptive caching in hierarchical content delivery networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 4, pp. 1024–1033, 2019.

[S7] S. Nacakli and A. M. Tekalp, "Controlling p2p-cdn live streaming services at sdn-enabled multi-access edge datacenters," *IEEE Transactions on Multimedia*, vol. 23, pp. 3805–3816, 2021.

[S8] J. Tapolcai, J. Bíró, P. Babarczi, A. Gulyás, Z. Heszberger, and D. Trossen, "Optimal false-positive-free bloom filter design for scalable multicast forwarding," *IEEE/ACM Transactions on Networking*, vol. 23, no. 6, pp. 1832–1845, 2015.

[S9] R. Jmal and L. Chaari Fourati, "Assisted dash-aware networking over sdn—ccn architecture," *Photonic Netw. Commun.*, vol. 38, no. 1, p. 37–50, aug 2019. [Online]. Available: https://doi-org.proxy.lnu.se/10.1007/s11107-019-00835-1

[S10] M. Di Mauro, M. Longo, and F. Postiglione, "Availability evaluation of multi-tenant service function chaining infrastructures by multidimensional universal generating function," *IEEE Transactions on Services Computing*, vol. 14, no. 5, pp. 1320–1332, Sep. 2021.

[S11] J. Pei, P. Hong, K. Xue, and D. Li, "Efficiently embedding service function chains with dynamic virtual network function placement in geo-distributed cloud system," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 10, pp. 2179–2192, Oct 2019.

[S12] M. Caggiani Luizelli, L. Richter Bays, L. Salete Buriol, M. Pilla Barcellos, and L. Paschoal Gaspary, "How physical network topologies affect virtual network embedding quality: A characterization study based on isp and datacenter networks," *Journal of Network and Computer Applications*, vol. 70, pp. 1–16, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804516300959

[S13] G. Sallam and B. Ji, "Joint placement and allocation of vnf nodes with budget and capacity constraints," *IEEE/ACM Transactions on Networking*, vol. 29, no. 3, pp. 1238–1251, June 2021.

[S14] H. Hawilo, M. Jammal, and A. Shami, "Network function virtualization-aware orchestrator for service function chaining placement in the cloud," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 643–655, March 2019.

[S15] H. Yu, Z. Chen, G. Sun, X. Du, and M. Guizani, "Profit maximization of online service function chain orchestration in an inter-datacenter elastic optical network," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 973–985, 2021.

[S16] B. Addis, D. Belabed, M. Bouet, and S. Secci, "Virtual network functions placement and routing optimization," in *2015 IEEE 4th International Conference on Cloud Networking (CloudNet)*, 2015, pp. 171–177.

[S17] H. Hantouti, N. Benamar, and T. Taleb, "Vlan-based traffic steering for hierarchical service function chaining," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 1–6.

[S18] T. Dreibholz, X. Zhou, and F. Fa, "Multi-path tcp in real-world setups – an evaluation in the nornet core testbed," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, March 2015, pp. 617–622.

[S19] X. Wang and R. T. B. Ma, "On the tussle between over-the-top and internet service providers: Analysis of the netflix- comcast type of deals," *IEEE/ACM Transactions on Networking*, vol. 28, no. 6, pp. 2823–2835, 2020.

[S20] D. Bhamare, M. Samaka, A. Erbad, R. Jain, and L. Gupta, "Exploring microservices for enhancing internet qos," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 11, p. e3445, 2018, e3445 ETT-17-0393.R1. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3445

[S21] A. A. Barakabitze, N. Barman, A. Ahmad, S. Zadtootaghaj, L. Sun, M. G. Martini, and L. Atzori, "Qoe management of multimedia streaming services in future networks: A tutorial and survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 526–565, 2020.

[S22] P. Li, Y. Zhang, W. Wang, K. Zhao, B. Lian, K. Xu, and Z. Zhang, "Frend for edge servers: Reduce server number! keeping service quality!" in *2021 IEEE 23rd Int Conf on High Performance Computing &amp Communications 7th Int Conf on Data Science &amp Systems 19th Int Conf on Smart City 7th Int Conf on Dependability in Sensor, Cloud &amp Big Data Systems &amp Application (HPCC/DSS/SmartCity/DependSys)*. IEEE, Dec. 2021. [Online]. Available: https://doi.org/10.1109/hpcc-dss-smartcity-dependsys53884.2021.00041

[S23] K. T. Bagci and A. M. Tekalp, "Dynamic resource allocation by batch optimization for value-added video services over sdn," *IEEE Transactions on Multimedia*, vol. 20, no. 11, pp. 3084–3096, 2018.

[S24] D. Lachos, Q. Xiang, C. Rothenberg, S. Randriamasy, L. M. Contreras, and B. Ohlman, "Towards deep network amp; application integration: Possibilities, challenges, and research directions," in *Proceedings of the Workshop on Network Application Integration/CoDesign*, ser. NAI '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1–7. [Online]. Available: https://doi-org.proxy.lnu.se/10.1145/3405672.3405804

[S25] M. Wichtlhuber, R. Reinecke, and D. Hausheer, "An sdn-based cdn/isp collaboration architecture for managing high-volume flows," *IEEE Transactions on Network and Service Management*, vol. 12, no. 1, pp. 48–60, 2015, [Accessed: 27.3.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7044567

[S26] S. Torkamani-Azar and M. Jahanshahi, "A new gso based method for sdn controller placement," *Computer Communications*, vol. 163, pp. 91–108, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366420319186

[S27] A. Shah, M. Mussini, F. Nicassio, G. Parladori, F. Triggiani, G. Grieco, G. Iaffaldano, and G. Piro, "A real-time simulation framework for complex and large-scale optical transport networks based on the sdn paradigm," in *2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, Sep. 2020, pp. 1–4.

[S28] E. Guler, M. Karakus, and S. Uludag, "Blockchain-enhanced cross-isp spectrum assignment framework in sdons: Spectrumchain," *Computer Networks*, vol. 223, p. 109579, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128623000245

[S29] K. Poularakis, G. Iosifidis, G. Smaragdakis, and L. Tassiulas, "One step at a time: Optimizing sdn upgrades in isp networks," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, 2017, pp. 1–9.

[S30] ——, "Optimizing gradual sdn upgrades in isp networks," *IEEE/ACM Transactions on Networking*, vol. 27, no. 1, pp. 288–301, 2019.

[S31] W. Miao, G. Min, Y. Wu, H. Wang, and J. Hu, "Performance modelling and analysis of software-defined networking under bursty multimedia traffic," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 12, no. 5s, sep 2016. [Online]. Available: https://doi-org.proxy.lnu.se/10.1145/2983637

[S32] J. Tapolcai, G. Rétvári, P. Babarczi, and E. R. Bérczi-Kovács, "Scalable and efficient multipath routing via redundant trees," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 5, pp. 982–996, 2019.

[S33] K. Tolga Bagci and A. Murat Tekalp, "Sdn-enabled distributed open exchange: Dynamic qos-path optimization in multi-operator services," *Computer Networks*, vol. 162, p. 106845, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128618308387

[S34] P. T. Congdon, P. Mohapatra, M. Farrens, and V. Akella, "Simultaneously reducing latency and power consumption in openflow switches," *IEEE/ACM Transactions on Networking*, vol. 22, no. 3, pp. 1007–1020, 2014.

[S35] R. Vilalta, R. Muñoz, R. Casellas, R. Martínez, V. López, O. G. de Dios, A. Pastor, G. P. Katsikas, F. Klaedtke, P. Monti, A. Mozo, T. Zinner, H. Øverby, S. Gonzalez-Diaz, H. Lønsethagen, J.-M. Pulido, and D. King, "Teraflow: Secured autonomic traffic management for a tera of sdn flows," in *2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, 2021, pp. 377–382.

[S36] E. Sakic, F. Sardis, J. W. Guck, and W. Kellerer, "Towards adaptive state consistency in distributed sdn control plane," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–7.

[S37] A. Aydeger, N. Saputro, and K. Akkaya, "A moving target defense and network forensics framework for isp networks using sdn and nfv," *Future Generation Computer Systems*, vol. 94, pp. 496–509, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18307817

[S38] F. Audah, T. S. Chin, R. Kapsin, N. Omar, and A. Tajuddin, "Future direction of traffic classification in sdn from current patents point-of-view," in *2019 15th International Computer Engineering Conference (ICENCO)*, Dec 2019, pp. 121–125.

[S39] M. Gerola, F. Lucrezia, M. Santuari, E. Salvadori, P. L. Ventre, S. Salsano, and M. Campanella, "Icona: A peer-to-peer approach for software defined wide area networks using onos," in *2016 Fifth European Workshop on Software-Defined Networks (EWSDN)*, Oct 2016, pp. 37–42.

[S40] A. Bahnasse, F. E. Louhab, H. Ait Oulahyane, M. Talea, and A. Bakali, "Novel sdn architecture for smart mpls traffic engineering-diffserv aware management," *Future Generation Computer Systems*, vol. 87, pp. 115–126, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17323725

[S41] P. L. Ventre, S. Salsano, M. Polverini, A. Cianfrani, A. Abdelsalam, C. Filsfils, P. Camarillo, and F. Clad, "Segment routing: a comprehensive survey of research activities, standardization efforts, and implementation results," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 182–221, 2020, [Accessed: 14.04.2023]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9253580

[S42] J.-R. Luttringer, T. Alfroy, P. Mérindol, Q. Bramas, F. Clad, and C. Pelsser, "Deploying near-optimal delay-constrained paths with segment routing in massive-scale networks," *Computer Networks*, vol. 212, p. 109015, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128622001748

[S43] T. Schüller, N. Aschenbruck, M. Chimani, and M. Horneffer, "Failure resiliency with only a few tunnels – enabling segment routing for traffic engineering," *IEEE/ACM Transactions on Networking*, vol. 29, no. 1, pp. 262–274, Feb 2021.

Appendices

A Trends and Challenges in Todays Network Landscape

A.1 OTTPs and Service Providers cooperation

The following section covers the definitions of over-the-top providers (OTTPs), internet service providers (ISPs), network service providers (NSPs), and their possible cooperation to solve problems relating to the increasing requirements of modern multimedia streamed over the internet. In this research project, we refer to the combination of ISPs and NSPs as telecommunications service providers (TSP). An NSP can function independently or concurrently act as an ISP and vice versa. In the context of OTT-related challenges, we use the term TSP to encompass the roles and responsibilities of both NSPs and ISPs as they share business problems, but the usage of ISP to refer to NSP or vice versa is erroneous.

In this section, we will describe the different types of over-the-top content providers, the challenges modern-day internet media and applications pose on the network infrastructure, and how OTT providers and TSPs can aim to cooperate. We also give a brief overview of the technical, regulatory, and policy considerations for such cooperations since it will further explain why modern content delivery processes pose challenges to the network infrastructure of the TSPs.

Over-the-top Services and the TSP-OTTP Problem

The Over-the-top (OTT) content providers are service platforms that provide the interface between the end users and the third-party content [25, 26]. As such, OTT providers (OTTPs) can be classified under the broad definition of any service or application provided to the end-user via the Internet [26].

The service providers that introduce the highest impact challenges and requirements for the network infrastructure are the services or applications that require either near-instantaneous connections, high bandwidth requirements, or both. On the other hand, TSP provides the interface between the service and content platform to the end users [25].

According to the study ordered by the European Telecommunications Network Operators Association (ETNO), most of the data traffic can be attributed to the major tech players such as Meta, Alphabet, Apple, Microsoft, Amazon, and Netflix[2]. Their claim is further supported and demonstrated in the Global Internet Phenomena Report of 2023 by Sandvine [27]. Sandvine identifies MAAMA (Microsoft, Alphabet, Meta, Amazon, and Apple) and Netflix as accounting for 48 % of internet traffic. Their collective contribution to network traffic has seen a slight downward trend as other services like TikTok and Disney+ have begun contributing more to the overall traffic volume, which continues to increase [27]. Among the traffic generated by these OTT providers mentioned above, video content constitutes 65.95 % of the total traffic volume.[27].

Real-time entertainment represents just one type of OTT service, and we can

further categorize them into various types such as:

1. Real-time communication Services
    - Examples: Skype, Viber, WhatsApp
2. Real-time entertainment
    - Can be further divided into video and audio.
      Examples: Netflix, Youtube, Spotify
3. Social Media
    - Examples: Instagram, TikTok, Facebook
4. Marketplace services
    - Examples: Amazon Prime, iTunes Store, Android Market
5. Cloud Storage Services
    - Examples: Dropbox, Google Drive, OneDrive
6. Online Gaming Services
    - Examples: PlayStation, Steam, Roblox
7. Web browsing
    - Standard Internet activities; HTTP

[25, 26, 2]

As the networking industry continues to face evolving challenges, TSPs are increasingly advocating for regulatory changes to help them address the mounting pressures arising from the growing traffic volumes. The escalating demand for high-quality and near-instantaneous content delivery by OTT services puts a significant strain on the infrastructure of TSPs, creating a pressing need for more efficient solutions and collaborative efforts between OTT providers (OTTP) and TSPs to ensure a seamless user experience. [2].

A.1.1 Models of cooperation between the service providers

The growth and evolution of OTT traffic not only present technical challenges but also raises regulatory and political issues that impact the business relationships between different service providers. This section will explore the challenges in more detail.

Policy and Regulatory Considerations for OTT-ISP Cooperation
Prior work concludes that directing partial profits of the OTT providers in developing the TSP network infrastructure would help alleviate the strain on the network infrastructure [2, 25, 28]. The OTTPs do take steps towards helping to alleviate their bandwidth demands by introducing high-efficiency protocols and encoding techniques and optimizing their content delivery by utilizing content delivery networks or network caching [2]. The following sections discuss the technologies implemented by OTTs relating to the quality of service, traffic engineering, and content delivery chain. Despite these efforts, the European Telecommunications Network Operators' Association (ETNO) considers these actions insufficient, as data traffic continues to increase exponentially [27, 2, 29].

One proposed solution to aid in the challenge posed by growing OTT demands is for the TSPs to diversify and evolve their business models by introducing new types of contracts for OTTs and consumers [25]. The service model of the TSPs often operates on a fixed-cost basis, but the evolving requirements of OTTs are increasingly justifying contracts with varying costs. [28, 25, 2].

Regulations and Rights
Regarding the idea of applying varying costs, both the United States of America and the European Union Parliament have passed regulations to ensure net neutrality [30, 28]. Net neutrality requires telecommunication operators to treat all internet traffic equally. Operators cannot impose restrictions on certain types of traffic; they must treat all subscription types equally and ensure that paid-for optimized services do not impair the general quality of the network service. [31, 30]. Policies that would infringe on the end-users internet rights would breach these regulations. The EU Regulation 2015/2120 passed in 2015 both impose the end users' rights but would still allow the TSPs to cooperate with the OTTPs on a paid-for optimized services[30, 28].

Peering Agreements Peering agreements enable two service providers to access each other's customers by using their respective networks [32]. A vital feature of these agreements is that they typically operate under Settlement-Free-Interconnection (SFI) or Settlement-Free-Peering [32, 33]. Related to the potential future contract types offered by TSPs, the debate over peering arrangements between OTTPs and TSPs mainly arises from the issue of OTTPs utilizing SFI as a legacy right to access the TSP's network without compensation [2, 34, 33]. A legal precedent emerged from a lawsuit between major OTT player Netflix and the largest broadband internet provider SK Broadband. In 2021, the court ruled that Netflix must acknowledge network usage as an expense, and the ISP can justifiably request payment for peering (Paid-peering), even if it had not done so previously [2].

Technical Aspects of Peering Agreements
With network peering, TSPs and OTT providers can establish direct connections between their networks, bypassing intermediary networks and reducing latency for end-users. This improved connectivity can enhance the quality of service (QoS) for

OTT content delivery while benefiting the TSPs by optimizing network utilization and reducing transit costs. By cooperating, both parties can achieve better network performance and user experience [33].

In the process of establishing a peering agreement between a TSP and an OTT provider, several technical aspects need to be considered to ensure efficient and secure connectivity. First, both parties must identify appropriate peering points or locations where their networks can interconnect. These points can be at Internet Exchange Points (IXPs) or data centers, providing direct connections between their respective networks [33]. Next, they need to define routing policies to govern traffic flow between interconnected networks, such as the selection of specific routes or traffic prioritization based on content type or user preferences. Defining these policies ensures optimal use of network resources and helps maintain a high-quality user experience [35].

Managing peering traffic is another crucial aspect, allowing the TSP and the OTT provider to gain insights into the performance of their interconnected networks. The management includes sharing relevant data, such as network performance metrics, content popularity, and user behavior, which can help both parties make informed decisions about network optimization and content distribution. All the information shared between the TSP and the OTT provider must be transmitted via secure communications to ensure the privacy and integrity of the data. By working together on these technical aspects, TSPs and OTT providers can achieve a successful peering agreement that benefits both their networks and their end-users [36].

A.1.2 NMS requirements posed by OTTs

In this section, we addressed the challenges TSPs face due to the rapid growth of internet traffic and the impact of OTTPs' traffic flows on the overall network infrastructure. We also explored the policies and regulations related to TSP-OTT cooperation. Moreover, we discussed the technical aspects of peering agreements between TSPs and OTT providers, which involve setting up peering points, establishing routing policies, and monitoring peering traffic.

The requirements for network management systems (NMS) arising from the OTT-TSP cooperation discussed in this section can be found in Appendix B.

A.2 Quality of service

Definition of Quality of Service (QoS)

The National Institute of Standards and Technology (NIST) describes the quality of service (QoS) as: *The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements [37].*

Overview of the Importance of QoS in network services

The importance of QoS and the mentioned service level agreements are especially important with the rapid growth of OTTPs.

The customer chain of **end user-ISP-NSP-OTTP** sets many demands and expectations on the quality of service each party in the chain expects.

The OTTP-TSP challenges discussed earlier in Section A.1 induce some problems for the QoS and further motivates the need for cooperation. If the OOTP growing bandwidth and demands for lower latency strain the network infrastructure to the point where the NSP can no longer fulfill the service level agreement (SLA) of the ISP, the quality of service of the end-user and the OTTPs will as well suffer.

Network management systems serve as essential tools for service providers to monitor their QoS metrics and, when required, generate reports demonstrating compliance with their agreed-upon SLAs [16, 38].

A.2.1 QoS metrics and parameters

The main QoS parameters are :

- Bandwidth
  - The speed of a link
- Latency
  - The time a packet requires to reach the end destination.
- Jitter
  - Irregular packet speeds on the network, often caused by congestion, can lead to distortions or gaps in the delivered content.
- Packet loss
  - The amount of lost data in transmission. Also, often results of congestion, and QoS-aware systems can decide what packets to drop if there is congestion. [39]

A.2.2 QoS techniques and mechanisms

Traffic shaping

Traffic shaping is a feature designed to assure that traffic is provided the committed rate by allotting higher priority to it if it falls short of the promised rate [40].

Packet Prioritisation

Traffic shaping enables dynamic treatment of QoS when guarantees are not fulfilled, while flow-based forwarding allows different treatment or prioritization for various application flows[16].

A.2.3 QoS standards and protocols

Resource reservation

Resource reservation or resource reservation protocol (RSVP) is part of the transport layer protocols [39]. The protocol reserves resources across the network and allows the delivery of specifically defined levels of quality of services for different application data streams [39].

Integrated Services (IntServ) The Integrated Services (IntServ) QoS architecture model reserves resources explicitly for the end-to-end path, and all routers store information on the network service state [16, 28]. IntServ uses the RSVP protocol to carry out this reservation process [39, 16]. Developers created Differentiated Services (DiffServ) to address scalability and complexity issues of IntServ [16, 28].

Differentiated Services

DiffServ is a framework that functions based on aggregating flows and employs a step-by-step method at each hop [16]. DiffServ sorts incoming traffic into predefined categories, using the Type of Service (ToS) header field as the foundation. Packets in the same category are subjected to the same handling [16]. However, Diffserv's simplicity as a QoS architecture poses challenges in providing quantitative QoS for individual data flows and offering guarantees [16, 28].

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching MPLS is a protocol that aims to make the transmission of packets to their destination endpoint more efficient [41]. To do so, MPLS uses a packet labeling technology to reduce the need for complex routing tables.[16, 28]. "Multiprotocol" refers to the fact that the protocol is not dependent on any specific routing protocol to operate but is an overlay that allows forwarding different types of data [41]. The use of MPLS with the ToS header of Diffserv is a common practice in private networks as the predetermined route pathing allows for better transmission and QoS compared to traditional IP routing [28, 41].

A.2.4 Quality of Experience

As the quality of Service metrics are not directly linked with the end-user satisfaction of the service, quality of experience metrics can be used to assess the quality of a multimedia service [34].

Mean Opinion Score

The Mean Opinion Score (MOS) is a subjective user-centric Quality of Experience metric [34, 16]. As user satisfaction can not be guaranteed strictly by using QoS network metrics, a subjective way for the user to communicate their satisfaction is needed [16]. MOS is mainly used for audio, audiovisual, and video services but is not limited to only the quality of experience of this type of media [16, 34]. For example, the user's satisfaction with a system's quality is after a video call.

A.2.5 QoS management and monitoring

As discussed in the previous section, the rise of OTT providers and the demand for near-instantaneous traffic have heightened the importance of QoS, prompting the adoption of innovative technologies like Software Defined Networks (SDN). SDN, which we will explore in later sections, offers a streamlined approach to network management by decoupling the control plane and data plane [16]. With SDN, network owners can maintain a top-down view from a central controller, dynamically optimizing and allocating resources and flow management [16]. Implementing these functionalities requires a carefully designed network management framework. As the theoretical background outlines, network management is a complex combination of different networking applications such as QoS management, traffic engineering, content delivery optimizations, and so on [16, 39, 42].

A.2.6 NMS requirements posed by QoS and QoE

In this section, we discussed Quality of Service (QoS) and Quality of Experience (QoE) and their increased importance in the current and upcoming networking landscape. From our review, we have compiled a list of requirements that the aforementioned trend poses on NMS; see Appendix C.

A.3 Network Caching and Content Delivery Networks

Network caching serves as a solution to the OTT-TSP problem by strategically storing content closer to the end-user's locations, thereby reducing latency and enhancing their overall experience. [43]. This form of cooperation can also reduce the operational expenses of the TSP, thus alleviating the financial problems highlighted in earlier sections [44].

A.3.1 Types of network caching

Content delivery networks (CDN) first emerged in 1998 to address the challenge of transmitting large amounts of data over long distances [43]. Proxy servers and CDNs address two issues: the TSPs use a proxy or surrogate servers to store the most frequently or recently used content. Web servers use content delivery networks to store content specified or configured to be cached by the administrator [43].

Content providers, or in some cases the TSP, place the servers responsible for the content delivery as close to the user to provide low latency content delivery [45]. A CDN compromise of a hierarchy of cache servers and surrogate servers (SS), which the content provider provides [43, 45]. It is common practice to place the lowest server in this hierarchy at the edge of the user network, inside the TSP network. [45].

CDNs are complex distributed networks with many components collaborating with different network providers to facilitate the content delivery chain [43].

The collaboration between these content delivery chain nodes can be divided into the following four steps:

1. Surrogate server caches the content of the origin server

2. Routers deliver the content request of the end-user to the surrogate server responsible for delivering the content

3. The requested content is distributed from the origin server to the surrogate server through the use of various network elements

4. Logs and accounting information is provided to the origin server utilizing an accounting mechanism [43]

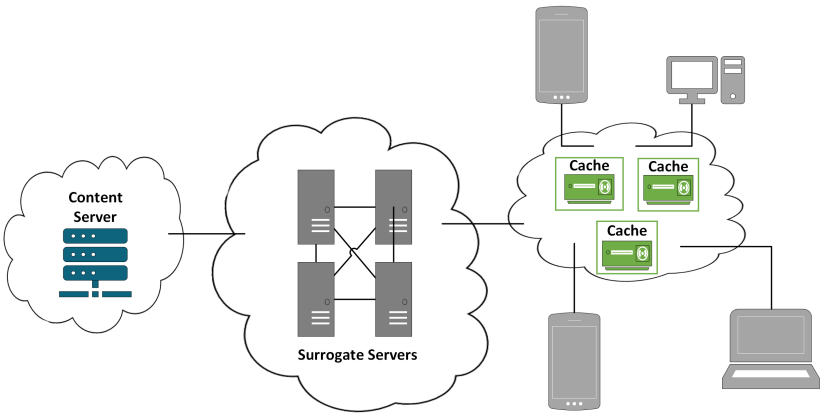

Figure 19: Typical CDN hierarchy, [45]

Surrogate servers and Proxy caching
The role of the surrogate servers in a CDN is to aim to alleviate the workload of the origin server by delivering the requested content on the origin server's behalf [43]. The typical topology of a CDN and the hierarchy of content servers, surrogate servers, proxy caches, and end-user devices can be seen in Figure 19.

As the end user requests content from an OTTP, the request is routed to the closest cache responsible for the content delivery [45]. The main benefit of appropriately placed proxy servers for the ISP is reduced bandwidth consumption. For the OTTP or web service, the main benefit is the reduced latency for their customers [43].

The administrators of the CDN can take two main approaches in the implementation of the deployment of their surrogate servers.

- The multiple ISP approach deploys many surrogate servers on as many global service provider points of presence as possible. The multi-ISP deployment approach aims to get the content as close to the user as possible. The benefit of this approach is that the CDN can provide the users content from the network of that user's ISP.

- The second approach is the singular ISP approach, which deploys multiple servers at the network's edge. A service provider with a global presence can utilize this approach to achieve adequate coverage without depending on

other ISPs [43]. The relative disadvantage of this approach is that the large numbers and the widely distributed network result in each of the surrogate servers getting fewer hits, which leads to poorer CDN performance [43].

Distributed caching is an alternate form where the caching nodes of the content delivery share the content to be delivered. When a content request arrives at one of the nodes, it will either deliver it from the node's locally stored files or by fetching the files from a node with the content [46, 47].

A.3.2 Strategies for network caching

Multiple caching policies can be employed, with the optimal choice often contingent upon the nature of the content and user behavior patterns. As content popularity and user behavior evolve, one might need to adapt the selected strategy accordingly. Two widely implemented object caching strategies include the Least Recently Used (LRU), and Least Frequently Used (LFU) methods.

The LRU-based strategy capitalizes on the locality of reference observed in content request streams, systematically removing the least recently accessed content from caching servers [48]. In contrast, the LFU-based strategy hinges on an item's popularity, gauging it through the frequency of use. By monitoring these popularity values, the LFU approach enables more informed caching decisions that adapt to content demand shifts. [48].

A.3.3 Implementations of network caching

Network caching was previously done by utilizing caching specialized hardware as the caching servers. The challenges in the rapid growth of network infrastructure and advancements in computing hardware have pushed this type of device out of favor. Software-based caching accommodates various devices, and modern server hardware can be customized to suit specific use cases. Software-based caching approaches are device agnostic and run efficiently in virtualized environments, making scaling and deploying the tools more accessible. Software-based and virtualized implementations are easier to scale up or down depending on the need than physical appliances.

Cloud-based Caching

Cloud-based caching or cloud-based content delivery networks (CCDN) are where the servers responsible for the caching or content delivery are hosted in a cloud environment outside of the company [49]. Compared to CDNs, CCDNs have better scalability, flexibility, elasticity, and reliability [49]. Because the content provider does not have to implement the caching infrastructure, the capital expenditure is lower. The operational expenditure is also significantly lowered as the OTTP has outsourced the maintenance to the CCDN provider [49]. The strengths mentioned above make CCDNs more affordable and allow the content provider to react to changes in demand more efficiently[49, 45].

A.3.4 Performance and optimization

Main Criteria for CDN

Metrics for how well a caching strategy and techniques work include:

- Performance and accuracy of the predication and estimation models of:
  - End-user content requests
  - Content access patterns
- Cost
- Scalability
- Traffic Load Balancing
- Fault tolerance

Monitoring CDN

A well-designed CDN monitoring strategy ensures effective utilization of CDN services by reducing problem detection time and significantly improving mean time to resolution. As organizations adopt multi-CDN approaches and use geo-specific CDNs with real-time performance-based routing, CDN monitoring becomes essential for assessing CDN performance and evaluating new CDN vendors.

CDN monitoring offers vital benefits such as benchmarking CDN performance to identify patterns and optimization opportunities and holding CDN vendors accountable for SLA breaches using aggregated performance data. It also enables quick detection and fixing of performance issues at the edge or origin for a superior end-user experience and efficient management of performance incidents, resulting in faster issue detection and lower mean time to resolution.

Building an effective CDN monitoring strategy involves several crucial steps. The first step is checking DNS resolutions with synthetic monitoring to emulate client DNS queries, detect and resolve DNS or identify configuration issues or DDoS attacks. The second step is monitoring CDN mapping and comparing performance data between CDN and origin servers to identify mapping anomalies and sub-optimal peering policies and verify if end users are served from the nearest edge server.

Additionally, it is essential to check the cache hit ratio using synthetic monitoring to measure cache hit and miss ratios, which helps evaluate CDN efficiency and latency. Another aspect is measuring end-user-to-edge location latency and edge-to-origin data center latency to track performance degradation, identify bottlenecks, and ensure optimal load balancing. Finally, monitoring and comparing metrics relevant to image optimization is essential to ensure CDN vendors' additional services are functioning and the correct end-user experience is provided [50].

A.3.5 Information-Centric- and Content-Centric Networking

Information centric networking (ICN)

Information centric networks (ICN) is an alternative network communication model. Instead of a host-centric paradigm is moved to information-centric networking [47]. In the current host-centric Internet paradigm, two network endpoints can start communication only if they know their respective IP addresses, either via domain name system (DNS) or the explicit IP address [47, 51]. In an ICN paradigm, the endpoints could initiate communication and send requests by using only the content name, regardless of where the content is, without knowing where it resides [47]. Disconnecting request sending and content transferring in this way offers benefits such as reduced latency and decreased network load. [47].

Content centric networking (CCN)

Respectively content-centric networking (CCN) is a promising architecture for the Future Internet [47]. The general principle of CCN is adopting content-based communication instead of the traditional host endpoint-to-host endpoint paradigm. The CCN paradigm divides the user's content into chunks, and a unique identifier based on the user name and the content name is attached to these chunks [47]. The name utilizes Uniform Resource Identifier (URI).

The steps to initiate CCN communication starts with a CCN client requesting content by injecting an interested packet into the network. The interest packet is forwarded until it reaches a CCN node or the origin server. If the interest packet meets a CCN node with the content available, the CCN node will deliver the content; if not, the interest packet is forwarded, and the client will receive the requested content. At the same time, the CCN nodes store a copy of the just requested content for future use [47].

A.3.6 Challenges of Network Caching

In this section, we discussed network caching, content delivery networks (CDNs), Information-Centric Networking (ICN), and Content-Centric Networking (CCN) and their impact on the networking landscape. From our review, we have compiled a list of requirements that the aforementioned trend poses on NMS; see Appendix D.

So far, we have examined the high-level challenges in the modern network environment, including the OTT-ISP problem, QoS, QoE, network caching, and content delivery networks (CDNs). In the following three sections, we will delve into state-of-the-art network techniques, such as Network Function Virtualization (NFV), Software Defined Networks (SDN), and Traffic Engineering with Segment Routing (SR-TE). These technologies actively assist network service providers in managing the challenges posed by emerging trends in the network environment while also addressing the limitations of traditional network technologies.

A.4 Network Function Virtualization

Network Function Virtualization (NFV) is a transformative technology that aims to revolutionize how network services are designed, deployed, and managed. It is

an architectural approach that decouples network functions from dedicated hardware, enabling them to run as software on general-purpose servers, switches, and storage devices. This shift from proprietary hardware to a virtualized environment allows network operations more flexibility, scalability, and cost savings. A group of network operators first introduced the NFV concept in a white paper published in 2012. Since then, it has gained significant traction in the telecommunication industry, including fixed access network service providers [52, 53].

This section aims to provide a comprehensive understanding of NFV and its closely related concept, Service Function Chaining (SFC), its architectures, and their potential impact on fixed access networks. At the end of this section, we will also outline the requirements that NFV and SFC impose on network management systems to ensure effective management and integration of these technologies.

A.4.1 Architecture

Overview of NFV architecture components

Similar to the transition from dedicated caching hardware to software caching on servers, Network Functions Virtualization (NFV) employs a structured architecture to effectively replace traditional hardware-based network devices with software-based counterparts operating on standard servers.

This architecture consists of layers and blocks, each having specific roles and responsibilities. These layers and blocks collaborate to create, manage, and allocate resources to virtual network functions (VNFs) such as virtual firewalls or routers, allowing for selection from various vendors [53].

The NFV architecture is classified into two groups for a seamless implementation: the High-Level ETSI NFV Framework and the Low-Level ETSI NFV Framework (see Figure 20 for a visual representation). The High-Level framework comprises three functional blocks: the Network Function Virtualization Infrastructure (NFVI) block, the VNFs block, and the Management and Network Orchestration (MANO) block. These blocks provide hardware resources, virtualization layers, and software resources for implementing VNFs. In contrast, the Low-Level framework delves deeper, dividing the three basic building blocks into more specific roles and responsibilities. [53].

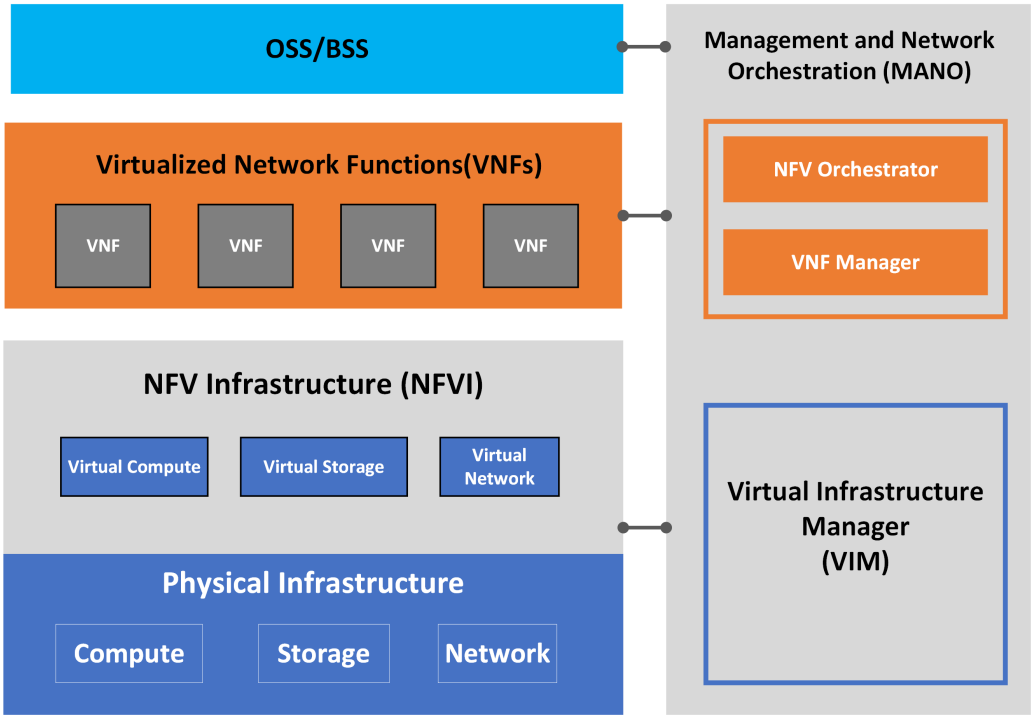

Figure 20: Overview of the NFV architecture. [54]

NFV Infrastructure (NFVI)
The NFV Infrastructure (NFVI) is the foundational component of the NFV architecture, supplying the necessary hardware and software resources for deploying and running Virtual Network Functions (VNFs). A virtualization layer, typically a hypervisor, is also included within the NFVI, which allows for the abstraction of hardware resources and creates an environment for VNFs to run as virtual machines or containers.

The NFVI is managed by the Virtual Infrastructure Manager (VIM), a Management and Orchestration (MANO) framework component. The VIM oversees the allocation and management of NFVI resources, such as computing, storage, and networking hardware. Additionally, the VIM handles power management, health checking, resource utilization monitoring, fault information collection, and resource management tasks like scaling and tearing down virtual machines [53].

Management and Orchestration (MANO)
Management and Orchestration (MANO) is an essential component of the NFV architecture, responsible for overseeing the lifecycle management of VNFs and the allocation of NFVI resources. As the central hub of the NFV architecture framework, MANO facilitates seamless communication and coordination between the NFVI and VNF blocks. MANO enables efficient end-to-end service orchestration, resource management, and automated VNF lifecycle management in an NFV environment [53].

Virtual Network Functions (VNFs)
Virtual Network Functions (VNFs) are software-based implementations of traditional network middleboxes, such as firewalls, routers, and load balancers, that run on NFV Infrastructure (NFVI). VNFs are modular, scalable, and interoperable, allowing network operators to deploy and manage them more efficiently than their hardware-based counterparts. VNFs can be instantiated on-demand, scaled in or out as needed, and updated or replaced without disrupting the overall network service. By adopting VNFs, network operators can benefit from increased flexibility, reduced operational costs, and faster deployment of new network services. The utilization of VNFs is central to the NFV concept, enabling the transformation of network operations from proprietary hardware-based systems to flexible, software-driven environments [55].

A.4.2 Service Function Chaining

Definition and concept of SFC
Service Function Chaining (SFC) is an approach that allows network operators to deliver end-to-end functionality to users by orchestrating a series of ordered Service Functions (SFs) within a network service. These SFs (e.g., VNFs) execute specific processing tasks on incoming packets. For example, a ”Network protection” service might necessitate VNFs such as a firewall, Deep Packet Inspection (DPI), and a virus scanner. SFC streamlines the deployment and management of network services by decoupling the relationship between service functions and the underlying network topology. This separation empowers operators to effectively deploy, scale, and manage services in response to evolving network conditions and demands, eliminating the need for complex manual configuration. The Internet Engineering Task Force (IETF) has developed a formal SFC architecture based on the ETSI NFV framework, enabling the creation of optimized, dynamic, and automated SFC systems [10].

SFC architecture and components
The SFC architecture comprises three distinct planes: management, data, and control, which interact to ensure efficient orchestration and forwarding of network traffic (Figure 21). The management plan includes the SFC manager, SFPath manager, and service function manager, who is responsible for installing, maintaining, and terminating service functions. The data plane consists of the classifier and service functions, with the classifier identifying and classifying traffic before forwarding it into the Service Function Path (SFP). The control plane, which establishes and manages the path between the classifier and service functions, encompasses the policy controller, SFC controller, SFP controller, and user profile. These components generate or select specific service function chains and allocate appropriate paths, satisfying capacity and QoS requirements for service functions, and their connecting links [10].

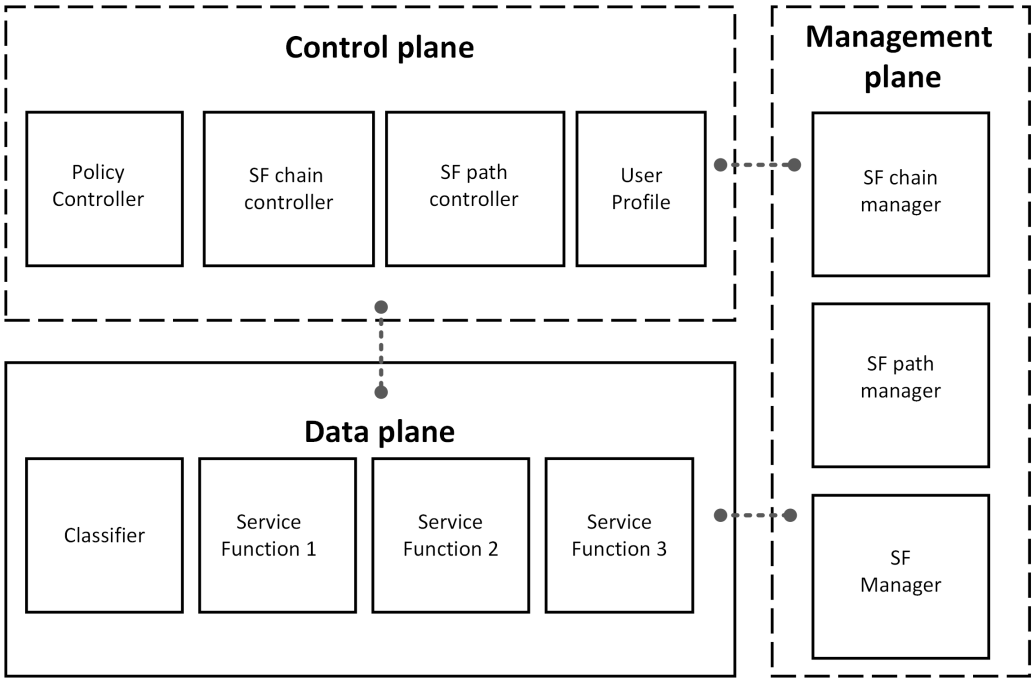

Figure 21: Overview of the three SFC planes.
[10]

Service Function Path (SFP)
The Service Function Path (SFP) is a key component of the SFC architecture, representing the ordered sequence of service functions that network traffic must traverse. SFPs are dynamically created and managed by the SFC controller, allowing for the flexible deployment and modification of service chains based on network requirements and policies [10]

Service Function Forwarder (SFF)
The Service Function Forwarder (SFF) is responsible for forwarding network traffic between service functions within an SFC. The SFF uses the Service Function Path (SFP) and Network Service Header (NSH) information to determine the appropriate forwarding actions, ensuring the correct traversal of traffic through the service chain [10].

Network Service Header (NSH)
The Network Service Header (NSH) is a metadata encapsulation protocol used to carry information about the service chain and the traffic flow. NSH encapsulates the original network packet, providing the context for the Service Function Forwarder (SFF) to forward the traffic to the appropriate service functions in the specified order [10].

SFC use cases in NFV
Service Function Chaining (SFC) offers significant benefits when used in con-

junction with Network Function Virtualization (NFV), enhancing the flexibility and agility of network service provisioning for Network Service Providers (NSPs). By employing SFC in an NFV environment, NSPs can dynamically create, modify, and manage complex service chains without requiring manual configuration. This ability to automate and optimize service provisioning leads to more efficient resource allocation and improved network performance, ultimately benefiting providers and end-users. By integrating SFC with NFV, NSPs can ensure seamless service orchestration, granular traffic management, and enhanced security, delivering a more robust and efficient networking experience that caters to the ever-evolving needs of the modern digital landscape [56].

Challenges and limitations of SFC
Service Function Chaining (SFC) in conjunction with Network Function Virtualization (NFV) presents various challenges that must be addressed for successful implementation and performance optimization. One of the primary challenges is dynamic online chaining, where service requests arrive at unknown times and with unknown durations. This challenge calls for developing algorithms that can handle real-time changes, such as adding or deleting Virtual Network Functions (VNFs) from a service request and re-composition, re-mapping, and re-scheduling of service chains [56].

Security is another crucial challenge in NFV and SFC architectures, as they are vulnerable to security attacks. An attack on a virtualized function could cause the entire service chain to fail. Open problems in this field include evaluating the dependability of products from multiple vendors, configuring VNFs adaptively to minimize network security risks, defending against Distributed Denial of Service (DDoS) attacks, detecting compromised components, and mitigating their impacts [10].

Distributed approaches are another area that needs further exploration. Most proposed approaches in NFV and SFC are centralized, where a single node is responsible for running the algorithm. Centralized approaches suffer from poor scalability and single points of failure and may only sometimes be feasible, especially in multi-service provider environments [10].

A.4.3 Deployment Models

In the context of NFV deployment models, the centralized, distributed, and hybrid models each offer distinct advantages and drawbacks. The centralized model provides simplified network management but may suffer from scalability issues and single points of failure. The distributed model, on the other hand, improves scalability and resilience but may require more complex management and higher operational costs. Finally, the hybrid model combines the benefits of both centralized and distributed models, offering a balance between network management simplicity and improved performance [57].

S. Park et al. [57] suggest that a dynamic deployment model using machine learning can be employed to overcome the limitations of the aforementioned NFV deployment models. This approach enables the network to adapt to changing traf-

fic patterns and demands by predicting the optimal VNF deployment in real-time, considering cost and Quality of Service (QoS) metrics. By training a machine learning model on simulation data obtained from an Integer Linear Programming (ILP) solution, the dynamic deployment model proposed by S. Park et al. can predict optimal VNF deployment and Service Function Chaining (SFC) for a predefined future point with high accuracy.

Furthermore, combining the dynamic deployment model with centralized, distributed, and hybrid models can enable service providers to benefit from the strengths of each approach, leading to more efficient and adaptive network management [57].

A.4.4 Benefits of Network Functions Virtualization

Network Functions Virtualization (NFV) has revolutionized the deployment and management of network services, offering numerous advantages to fixed-access network service providers. According to Chayapathi et al. (2016) in their book "Network Functions Virtualization (NFV) with a Touch of SDN," [58] NFV addresses many limitations associated with traditional network equipment and provides multiple benefits, such as cost reduction, resource optimization, improved agility, and enhanced scalability. In this sub-section, we will discuss the various advantages of NFV for fixed access network service providers, based on the insights provided by Chayapathi et al. (2016)[58] to better understand the transformative impact of this technology on network infrastructure and operations.

Cost reduction and resource optimization
One of the main benefits of NFV for fixed access network service providers is the potential for cost reduction and resource optimization. By virtualizing network functions, providers can consolidate hardware and reduce the need for specialized appliances, which in turn decreases capital expenditures. Virtualization also allows for more efficient use of computing, storage, and networking resources, leading to better overall utilization and reduced operational costs. Furthermore, NFV can result in more efficient power consumption and decreased physical space requirements, further contributing to cost savings[58].

Agility and scalability
Fixed access network service providers can benefit from the increased agility and scalability offered by NFV. Virtualized network functions can be deployed, scaled up or down, or decommissioned quickly and easily, allowing providers to adapt rapidly to changing market conditions and customer needs. This flexibility helps providers avoid significant hardware investments and lengthy deployment processes, enabling them to be more responsive and competitive in the market[58].

Simplified network management
NFV enables service providers to streamline network management and operations, as virtualized functions can be controlled and monitored from a centralized loca-

tion. This centralization reduces the complexity of managing diverse hardware appliances and simplifies the network management process, improving operational efficiency and reducing maintenance costs. Moreover, standardized virtualized functions can further simplify network management by promoting uniformity and consistency across the network [58].

Improved reliability and performance
Virtualizing network functions can enhance the reliability and performance of fixed access networks. NFV allows for the easy deployment of redundant instances of virtualized functions, ensuring service continuity during hardware failures, software issues, or other disruptions. Additionally, service providers can reduce latency and improve overall network performance by deploying network functions closer to end-users, resulting in a better user experience and increased customer satisfaction [58].

A.4.5 Use Cases in Fixed Access Networks

There are several use cases for NFV in fixed-access networks that can significantly improve service providers' operations and service offerings. Some of the most common and impactful use cases include:

Virtual Customer Premises Equipment (vCPE)
vCPE enables the virtualization of customer premises equipment functions, such as home routers and set-top boxes, reducing the need for physical devices at customer locations. By implementing vCPE, service providers can simplify device management, reduce maintenance costs, and accelerate the deployment of new services and features [59]

Network Slicing
Network slicing, although commonly associated with 5G infrastructure, offers significant benefits for fixed-access networks as well. This technology leverages the principles of software-defined networks (SDN) and network functions virtualization (NFV) and allows network managers to create multiple virtual networks on top of a shared physical network infrastructure. These virtual networks can then be customized to meet the specific requirements of services, customers, applications, or devices [60].

Network slicing helps operators meet service level agreements (SLAs) and address capacity issues when designing networks. By deploying networks designed for peak usage, operators can ensure that the network is not under-utilized during off-peak hours. On the other hand, creating networks with the lowest usage times in mind helps service providers handle peak hours or unexpected usage demands, preventing outages and maintaining customer satisfaction[60].

Virtual Content Delivery Networks (vCDNs)
The use of NFV in virtual Content Delivery Networks (CDN) can be very ben-

eficial for fixed access Network Service Providers (NSPs) as it addresses several challenges associated with delivering video content over the internet. The massive growth of high bandwidth traffic, particularly video, has been driven by the shift from broadcast to unicast delivery via IP, an increasing number of devices used for video consumption, and enhanced video quality in terms of resolution and frame rate. Integrating vCDN into NSP networks can effectively and cost-effectively manage this traffic, ensuring content delivery with low latency and consistently high quality [59].

By adopting vCDN, fixed access NSPs can overcome some of the limitations associated with non-virtualized approaches. For example, capacity designed for peak hours is underutilized during off-peak times, wasting energy and generating heat. Additionally, reacting to unforeseen capacity needs with dedicated physical appliances is difficult [59].

The Table 3 below illustrates various network elements and their corresponding functions, highlighting the potential application for NFV across a wide range of fixed access network components:

Network Elements	**Functions**
Switching Elements	Broadband network gateways, carrier-grade NAT, routers
Customer premises equipment	Home routers, set-top boxes
Tunneling gateway elements	IPsec/Secure sockets layer (SSL) virtual private network gateways
Traffic analysis	Deep packet inspection (DPI), QoE measurement
Assurance	Service assurance, SLA monitoring, testing, and diagnostics
Signaling	Session border controllers, IP multimedia subsystem (IMS) components
Control plane/access functions	AAA servers, policy control and charging platforms, DHCP servers
Application optimization	Content delivery networks, cache servers, load balancers, accelerators
Security	Firewalls, virus scanners, intrusion detection systems, spam protection

Table 3: Network Elements and Functions applicable by NFV [61]

A.4.6 Challenges of NFV Deployment

Security

Virtual Machines (VMs) or containers might need elevated privileges to support certain virtual network functions (VNFs), which can create security vulnerabilities for the host system and peer VMs or containers. NFV environments are dynamic and distributed, allowing the instantiation of VNFs across the virtualized infrastructure at various locations such as the edge, core, or operator's data center. This

dynamic nature extends to monitoring throughout the operator's network as well [62].

Co-residency in NFV poses unique challenges because it can occur between multiple layers, like between VNFs and the virtualization layer or between the virtualization layer and physical hosts. Furthermore, VNF co-residency on the same physical host, caused by either placement or migration, may result in side-channel or resource depletion attacks due to shared physical resources like CPU, memory, or cache [62].

Combining Software-Defined Networking (SDN), discussed in the next section, with NFV could help alleviate some security concerns by offering more precise and centralized control over network resources and service chain functions extending throughout the operator's network [62].

Complexity and Compatibility

Another challenge following the shift to NFV is the transition in the network setup context. The "NFV marketplace" will encompass a wide array of network functions, management software, and platform software, with some being proprietary and others available in the public domain. These multiple options can introduce compatibility and interworking issues that may critically impact dependability, particularly during abnormal situations. Unlike functions offered by a single vendor, no entity will have complete insight into the entire software. Moreover, it is essential to remember that providing and maintaining a highly dependable configuration will be the network operator's responsibility, which could be challenging regarding available competence during a transition phase. The increased flexibility and adaptability of NFV also contribute to the complexity and potential for faults in design, implementation, configuration, and operation [63].

A.4.7 Conclusion

In conclusion, Network Function Virtualization (NFV) presents a transformative opportunity for fixed access network service providers, offering numerous benefits such as cost reduction, resource optimization, improved agility and scalability, simplified network management, service innovation and differentiation, and enhanced reliability and performance. By deploying NFV in their networks, service providers can adapt to changing market demands and customer requirements more effectively, improving service quality and increasing revenue opportunities.

However, as discussed throughout this section, there are challenges and limitations to NFV deployment in fixed access networks, including performance and latency concerns, integration with legacy systems, security, and privacy considerations, and the need for standardization and interoperability. Addressing these challenges is essential for successfully adopting and implementing NFV in fixed-access networks.

In addition, integrating NFV with other emerging technologies, such as Software-Defined Networking (SDN), will create new opportunities for service providers to optimize their networks and deliver even more advanced services. These synergies

between NFV and other technologies will also help address some of the existing challenges and limitations, paving the way for more widespread adoption of NFV in fixed access networks.

A.4.8 NMS requirements posed by NFV

In this section, we have discussed the concepts of Network Function Virtualization (NFV) and Service Function Chaining (SFC) and their potential impact on the networking landscape. With the adoption of NFV and SFC, network management systems (NMS) need to adapt to these technologies' unique requirements and challenges. From our review, we have compiled a list of requirements that the aforementioned trend poses on NMS, see Appendix E.

A.5 Software Defined Networks (SDN)

Software Defined Networking (SDN) is a relatively new networking paradigm that has emerged over the past decade. Unlike traditional IP/MPLS networks, which have a tightly-coupled control plane and data plane see Figure 22, SDN allows for a separation of the two planes, making the network more flexible, scalable, and efficient. The separation is accomplished by consolidating the control plane into a single software-based controller, which manages the behavior of multiple data plane elements, such as switches and routers [64].

In this section, we will provide a comprehensive overview of SDN, including its architecture and key concepts, popular protocols, deployment models, benefits, and challenges. We will also examine some of SDN's common applications and use cases in fixed access networks and conclude with a list of requirements the technique imposes on network management systems.

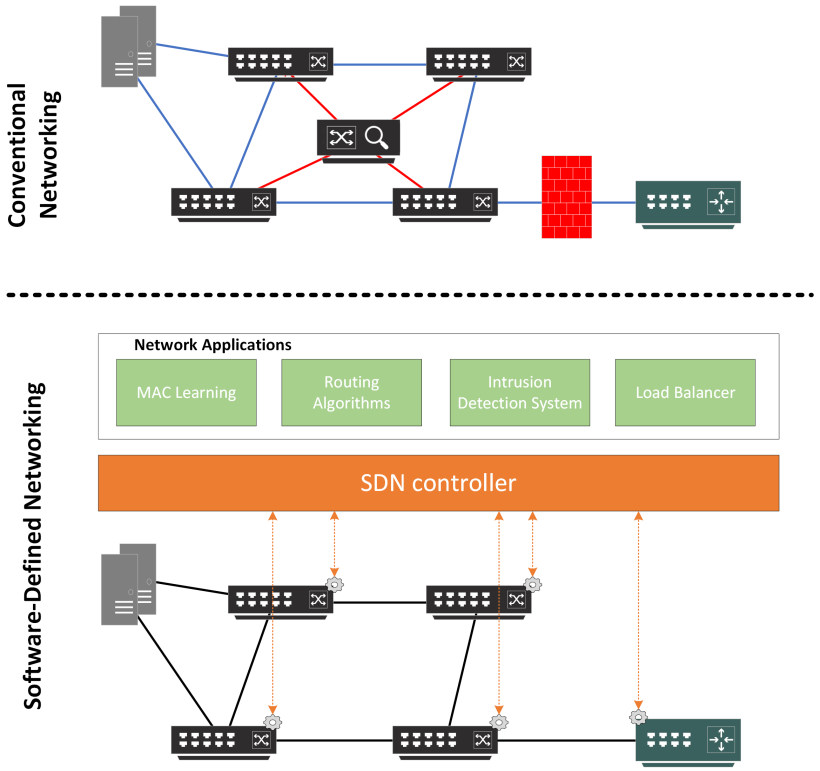

Figure 22: Instead of multiple control planes bound with data planes, SDN uses one centralized control plane to interact with and control all network devices underneath it.

[65]

A.5.1 Overview of the SDN Architecture

In the SDN architecture, the traditional network's three planes, the application, control, and data planes, are still present. However, instead of being housed in individual network devices' operating systems, the application and control planes have been centralized in one or more locations. The data plane and the device's operating system remain on the individual network devices, with an application programming interface (API) allowing them to interact with an SDN controller [66].

This separation of the control and data planes provides several advantages, such as the ability to manage the network in a more centralized and programmable manner, which facilitates more straightforward configuration and management of complex network environments. Moreover, SDN allows for greater automation, improved traffic engineering, enhanced security, and better utilization of network resources [66].

Additionally, having a centralized view of the network topology enables better visibility and understanding of the network as a whole. With a centralized view of the network topology, network administrators can also implement policy-based routing, quality of service (QoS) management, and other advanced network services, all of which can improve the end-user experience and increase customer

satisfaction [66].

SDN Controller
At the core of the architecture is the SDN controller, which acts as the system's "brain" by utilizing four APIs to interact with the planes above and below it and other controllers. Multiple controller types have emerged, supporting either centralized or distributed architectures. Available on the market are both open-source and commercial SDN controllers, and according to a comparative study on market trends for SDN controllers, published in 2021 by Neto et al. [67], the top six SDN controllers are:

1. ONOS (Open Network Operating System) - A Linux Foundation project and a leading open-source SDN controller widely used for building next-generation SDN/NFV solutions. It has a rich set of South-bound Interface (SBI) protocols and low hardware requirements.

2. OpenDaylight - Another Linux Foundation project, OpenDaylight is a widely used open-source SDN controller that serves as the basis for various proprietary controllers. Its service abstraction layer offers extensive protocol support, including OpenFlow, OVSDB, NETCONF, BGP, P4, LISP, SNMP, PCEP, and others.

3. Cisco ACI (Application Centric Infrastructure) - A proprietary SDN controller from Cisco, offering complete native Layer 2-7 integration and support for Virtual Extensible LAN (VxLAN) as an extensible overlay/network logic protocol and NFV using Generic Routing Encapsulation (NV-GRE).

4. Juniper Contrail - A proprietary SDN controller from Juniper Networks, providing end-to-end dynamic configuration, optimization, and control for various cloud infrastructures. It supports Network Functions Virtualization (NFV) and integrates with most cloud services.

5. HP VAN SDN Controller - A proprietary SDN controller from HP with strict hardware requirements and a rich API with comprehensive documentation. However, it only supports OpenFlow in its SBI, limiting its applicability.

6. Huawei Agile Controller - A proprietary SDN controller from Huawei, based on ONOS and part of its CloudFabric Solution. It has strong interoperability with third-party platforms like VMware vCenter and extensive support for OpenStack platforms. However, it requires large server-sizing hardware due to strict hardware specifications.

In addition to these top six SDN controllers, multiple other controllers with smaller market shares exist, such as Beacon, Ryu, POX, NOX, and Floodlight [66, 68].

What distinguishes SDN controllers is mainly the choice of protocols for the APIs, support for distributed architecture, and whether they are open or proprietary

[67]. Figure 23 offers an overview of the SDN architecture, including popular controller types and common API protocols.

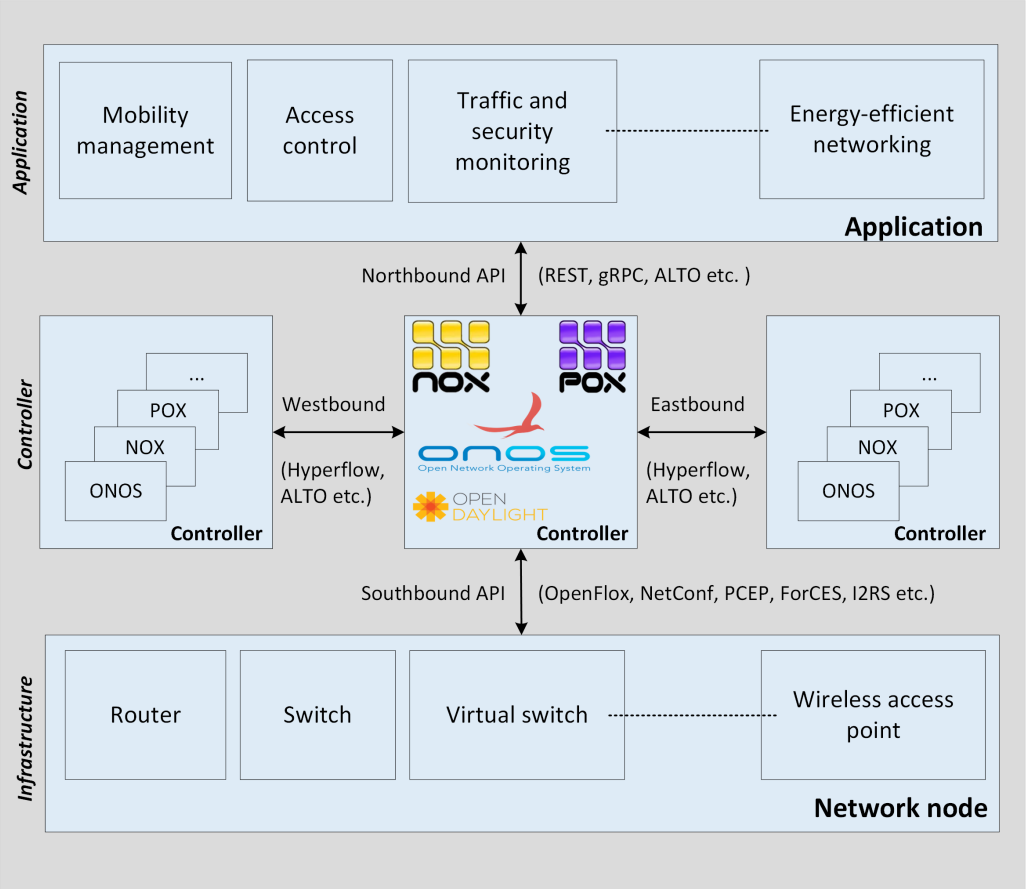

Figure 23: Overview of the SDN architecture and how the controller's four interfaces communicate with the different planes.
[64]

In the following sections, we will examine in more detail the four APIs used by SDN controllers and the relevant protocols required for their functions.

A.5.2 South-bound API protocols

The South-bound API in SDN handles communication between the SDN controller and the network devices, such as switches and routers. It enables the controller to manage, configure, and monitor the network infrastructure, translating high-level policies into specific device configurations [64].

OpenFlow
OpenFlow is the most popular South-bound protocol used in SDN networks. The Open Networking Foundation (ONF) created it to provide a standard interface between the controller and the data plane elements. OpenFlow allows the controller

to direct network traffic flow by configuring the forwarding tables on network switches and routers [64].

In an OpenFlow-based network, the data plane elements, such as switches and routers, are configured to send all their flow table lookup requests and packet processing decisions to the controller. The controller, in turn, makes decisions about how to forward packets based on network policies and rules. The decisions are returned to the data plane elements, which update their flow tables accordingly [64].

One of the advantages of OpenFlow is that it is vendor-neutral, meaning it can be used with switches and routers from different vendors as long as they support the protocol. This allows network administrators to build more flexible and scalable networks that are not tied to specific hardware vendors [64].

While OpenFlow is the most widely adopted south-bound protocol, other open alternatives are to be found that can either provide similar functions or additional ones. These protocols include BGP-LS, PCEP, ForCES, Interface to the Routing System (I2RS), NETCONF and RESTCONF, and commercial solutions such as Cisco ONE and Nuage Virtualized Services[69].

BGP-LS

BGP-LS (Border Gateway Protocol - Link-State) is an innovative south-bound protocol that facilitates communication between network devices and controllers by exchanging topology information and link-state data. This advanced protocol enhances network visibility and control, making it particularly valuable in large-scale data center networks and service provider environments [70].

A significant advantage of utilizing BGP-LS lies in the ability of service providers to collaborate and exchange crucial link-state and traffic engineering (TE) information with external components, including Path Computation Elements (PCEs) and SDN controllers. This cooperation provides well-informed decision-making processes for path optimization, resource allocation, and network congestion management, ultimately enhancing Quality of Service (QoS) in situations necessitating near-instantaneous communication [70].

PCEP

PCEP is an older technology that has been repurposed for SDN. PCEP use in SDN is primarily for Label Switched Path (LSP) path computation in the context of Multiprotocol Label Switching (MPLS) networks, enabling the path computation element (PCE) to communicate with network elements to calculate and configure the optimal path for a given traffic demand. The main components of the PCE environment include a PCE server, a PCE client (PCC), and the PCE Protocol. PCEP allows a network operator to delegate control of LSPs to a centralized controller, with the PCE server providing path computation, state maintenance, and infrastructure and protocol support services.

If the network infrastructure does not support OpenFlow, upgrading the entire network may be necessary or implementing NFV. In contrast, with PCEP-based

controllers, only edge routers must support PCEP, while the rest of the network can still use conventional network equipment.

In conclusion, When combined with BGP-LS, PCEP can be particularly useful for load balancing at the LSP level, while OpenFlow excels at flow level control [69, 70].

ForCES

ForCES (Forwarding and Control Element Separation) is a standard developed by IETF that proposes models for separating IP control and data forwarding elements, a transport mapping layer, and a logical function block library. However, its lack of clear language abstraction definition and controller-switcher communication rules has hindered its widespread adoption. Unlike OpenFlow, which requires routers and switches to support OpenFlow, ForCES does not change the essential network architecture and can run on traditional devices by simply adding networking/forwarding elements [64].

NETCONF, RESTCONF and YANG

Model-Driven Software Engineering (MDSE) has emerged as a critical framework in the networking domain, enabling the creation of portable models that can describe various aspects of network functionality. The model-driven approach is extensively used for network devices, services, policies, and APIs in the networking domain. The preferred protocols for implementing this approach are NETCONF and RESTCONF, with YANG (the widely-used data modeling language) [68].

Another reason for the increased popularity of Netconf and Restconf is that they are increasingly taking over many tasks from the legacy Simple Network Management Protocol (SNMP) due to their increased security, greater flexibility, more granular control, and better support for complex network configurations. Furthermore, these protocols are designed to work seamlessly with today's SDN environments and are better suited for the growing demands of dynamic and programmable networks [71].

NETCONF is an IETF network management protocol that provides a standardized set of Create, Retrieve, Update, and Delete (CRUD) operations for accessing configuration and operational data stores. It also supports Remote Procedure Calls (RPC) and Notification operations, utilizing XML-based data encoding for configuration data and protocol messages.

RESTCONF, on the other hand, is a REST-like protocol that offers a programmatic interface over HTTP for accessing data defined in YANG using the data stores outlined by NETCONF. RESTCONF modifies resources representing configuration data using HTTP methods such as DELETE, PATCH, POST, and PUT [68].

YANG, initially developed to model configuration and state data in network devices, is a tree-structured data modeling language capable of describing various network constructs, including services, policies, protocols, and subscribers. In addition to data definitions, YANG incorporates constructs for modeling Remote

Procedure Calls (RPCs) and Notifications, making it an ideal Interface Description Language (IDL) in a model-driven system [68].

I2RS
I2RS (Interface to the Routing System) is the last south-bound protocol covered. I2RS is an initiative by the Internet Engineering Task Force (IETF) to develop a dynamic, programmatic interface for controlling and monitoring the routing systems within a network. I2RS complements traditional routing protocols, such as BGP, OSPF, and IS-IS, by enabling real-time modifications to the routing state based on specific application needs or network conditions. The I2RS architecture consists of I2RS Agents running on network devices and I2RS Clients implemented on SDN controllers, orchestrators, or applications. Communication between I2RS Clients and Agents is facilitated using protocols like NETCONF or RESTCONF and relies on YANG data models to define the structure and semantics of the information exchanged.

Although I2RS has not yet gained widespread adoption, it provides a valuable tool for network operators and administrators seeking to enhance their control over routing systems, particularly in Software-Defined Networking (SDN) environments where dynamic and adaptable network control is essential [72].

A.5.3 North-bound protocols

The North-bound interfaces allow the SDN controller to communicate with applications, orchestration systems, and other higher-level services, allowing applications to request and manipulate network resources and services [64]. Common North-bound protocols include REST API, gRPC, and in some cases, NETCONF and RESTCONF.

REST
REST (Representational State Transfer) API is a popular choice for north-bound interfaces in SDN architectures due to its simplicity, flexibility, and widespread adoption. It is an architectural style for designing networked applications and relies on standard HTTP methods (e.g., GET, POST, PUT, DELETE) for communication between the SDN controller and higher-level applications, orchestration systems, or other services. REST APIs use simple and human-readable URLs for resource identification and are typically based on standard data formats like JSON or XML for exchanging data. One of the main advantages of REST APIs is that they are platform- and language-agnostic, allowing for seamless integration between different system components. Additionally, since REST APIs are stateless, they can be easily scaled to accommodate large-scale network deployments. In the context of SDN, REST APIs enable applications to request and manipulate network resources, configure network devices, and monitor network performance [73].

gRPC Remote Procedure Call gRPC (gRPC Remote Procedure Call) is an open-source, high-performance framework developed by Google as an alternative to REST. It is designed to run over HTTP/2.0 and improves performance compared to traditional REST-based communication. gRPC provides a remote procedure call with a single connection through the multiplexed stream function, offering faster processing than REST. Furthermore, gRPC uses Protocol Buffers (PB) as its Interface Definition Language (IDL) and serialization format, generating compact binary messages that enable faster transmission and reduced overhead compared to text-based formats like JSON or XML [74].

The key advantage of gRPC is its support for multiple programming languages, making it easy to integrate with various components of an SDN system. It operates by calling methods located on the server, allowing the client to implement a lightweight communication method for efficiency.

By leveraging gRPC as a north-bound interface, SDN controllers can provide a high-performance and flexible communication channel for applications, orchestration systems, and other services, especially in larger networks with multiple switches [74].

ALTO - Application-Layer Traffic Optimization
The ALTO protocol, developed by the IETF, has a significant role in fostering cooperation among service providers. By offering an abstract view of the network state, ALTO enables service providers to share crucial information about their networks without revealing sensitive internal details or policies. This selective information sharing is vital in maintaining a competitive edge while allowing for collaborative optimization efforts.

Service providers in cooperation can use ALTO's network abstractions to gain a broader understanding of the combined network state. This enhanced understanding enables them to make informed decisions regarding load balancing, traffic engineering, and resource allocation, ultimately resulting in improved network performance and user experience. Furthermore, ALTO can support the exchange of information among SDN controllers, facilitating efficient communication and cooperation among different service providers in a more streamlined manner [75].

A.5.4 Other protocols and techniques

gRPC Remote Procedure Call and gRPC Network Management Interface (gNMI)
Telemetry refers to the streaming of monitoring data in network operations, aiding network monitoring and troubleshooting. Several novel protocols have surfaced in recent years, providing less packet overhead compared to Simple Network Management Protocol (SNMP), both in synchronous and asynchronous monitoring. gRPC Remote Procedure Call (gRPC) and gRPC Network Management Interface (gNMI) are two such protocols, providing efficient and novel alternatives to SNMP and even modern protocols such as NETCONF and RESTCONF.

gRPC is a high-performance RPC framework that uses HTTP/2 and protocol buffers encodings, suitable for real-time monitoring and telemetry in network operations. It has emerged as a cloud-native solution for transport network control.

gNMI, built on top of gRPC, can configure and monitor network elements based on already defined YANG data models. Both gRPC and gNMI support a ”subscription” model, allowing the Network Management System (NMS) to subscribe to telemetry data streams from network devices, enabling real-time updates on network state and performance without frequent polling or SNMP-based queries. This reduces overhead and improves scalability, making gRPC and gNMI efficient solutions for managing and monitoring network devices in modern network environments [76, 77, 78].

Flow Monitoring Techniques
Flow monitoring is an exceptionally resource-efficient technique, especially when contrasted with traditional monitoring methods such as SNMP. It is instrumental in evaluating application performance and ascertaining the Quality of Service (QoS) for essential business applications like video conferences and VoIP. This technique grants network administrators the capability to monitor the travel routes of crucial data packets within the network and confirm that the right service classes are being employed. Additionally, by assessing the network's response to the incorporation of new applications, changes in configurations, or variations in user counts, flow monitoring helps understand their impact.

One of the standout benefits of flow monitoring is its ability to detect anomalous traffic patterns and potential security risks within the network. This is achieved through the internal monitoring of network traffic, which aids in spotting threats that might have eluded perimeter security measures. Notably, flow monitoring is effective in recognizing substantial traffic increases that may be indicative of security hazards such as data leaks, malware, or DDoS attacks [79].

Among various flow monitoring solutions on the market, the top three are NetFlow, sFlow, and IPFIX.

NetFlow Conceived by Cisco in the late 1990s, NetFlow is a protocol for monitoring network traffic flows. It records data about network traffic, termed ”traffic flows”, which are groups of packets that share attributes like source and destination addresses, ports, and protocol type. Network devices gather this flow information and forward the data to a centralized ”flow collector.” Paired with a ”flow analyzer,” this system offers a wealth of insights via visualizations, statistics, and both historical and real-time reporting.

There are two predominant versions of NetFlow: v5 and v9, the latter also referred to as Flexible NetFlow or FNF. NetFlow v5 has certain constraints, including its fixed fields for exporting data and not being compatible with contemporary technologies such as IPv6, MPLS, and VXLAN. NetFlow v9 rectifies these shortcomings by enabling custom templates and being compatible with the latest technologies. In addition, several vendors have developed their proprietary versions, like Juniper with jFlow and Huawei with NetStream. These adaptations often generate flow records that are compatible with NetFlow collectors and analyzers[79].

sFlow Emerging as an advanced flow technology for bolstering Quality of Service (QoS) in Software Defined Networking (SDN) ecosystems, sFlow is a protocol dedicated to the collection, monitoring, and analysis of network traffic flow data. In contrast to NetFlow's stateful tracking of flows, sFlow employs a methodology wherein it samples full packet headers from a particular flow at set intervals. This method cuts down on the bandwidth and CPU power needed by the devices that are collecting the data, but it might make the data less accurate. Nonetheless, sFlow procures more extensive data than NetFlow, including entire packet headers and even fragments of packet payloads[79].

sFlow, a sampling-based protocol, is scalable and affords continuous, real-time insights into network traffic. This enables network administrators to discern patterns, trends, and irregularities which could affect network performance or security. Through sFlow, SDN controllers can adeptly identify and tag large flows, enabling network administrators to fine-tune network performance and promptly re-allocate flows to make more effective use of available bandwidth. As the rate of bandwidth utilization becomes progressively critical, even a minor lag in identifying large flows can lead to a substantial decline in overall performance. In response to this challenge, sFlow presents an expeditious solution for the detection and management of large flows [80].

Unlike NetFlow, sFlow transmits data snippets swiftly as they are gathered and doesn't keep data on the network device. This makes sFlow advantageous for high-speed networks due to its capacity to process larger volumes of data. However, fine-tuning the sampling rate is critical and can be challenging since it varies from network to network, often requiring a trial-and-error approach. [79].

IP Flow Information Export (IPFIX)
IPFIX, or IP Flow Information Export, is similar to NetFlow but was developed as a universal solution for collecting and analyzing critical network data. Unlike NetFlow, which is primarily tailored for Cisco devices, IPFIX is compatible with a broader range of devices from different vendors, and that makes it a good choice for organizations seeking a NetFlow-like solution for non-Cisco devices [81].

A notable advantage of IPFIX over NetFlow is the ability to organize and analyze data during the collection process. IPFIX users can customize their requests, directing the system to complete specific tasks, such as organizing information or performing fundamental data analysis. Additionally, IPFIX can integrate more information into its exporting process, eliminating the need for additional devices to handle complex aspects of data collection and facilitating more efficient network tests [81].

Choosing between IPFIX and NetFlow can be challenging, but in a multi-vendor environment, IPFIX's flexibility stands out as a significant differentiator. Companies like Barracuda Networks, Nortel, Xirrus, and Juniper Networks utilize IPFIX. However, the customization possibilities of IPFIX might be overwhelming for less demanding users. NetFlow's simpler design may be more suitable for those who have standardized on Cisco devices [13].

Finally, one of the main reasons for Cisco introducing v9 (Flexible NetFlow)

was to address the above disparity. v9 is a generalized extension compatible with various systems, including NetFlow and IPFIX. While Flexible NetFlow cannot match all of IPFIX's capabilities, it is closing the gap [13].

P4 programming language
Although P4 is still relatively new and not yet widely adopted, it is worth mentioning due to its potential in the state-of-the-art networking space. As P4 continues to mature, it may play a crucial role in developing more flexible, efficient, and programmable networks, particularly in SDN architectures.

P4 is a high-level, domain-specific programming language designed for specifying forwarding plane behavior in programmable network devices. Developed by the P4 Language Consortium, it enables network administrators to define custom packet processing rules and actions, allowing for greater flexibility and control over the network. P4 can be used with various SDN architectures and protocols to integrate existing network management and control systems seamlessly. Its simplicity and versatility make it suitable for various applications, including In-Band Network Telemetry (INT) for efficient network monitoring and anomaly detection. P4 also excels in offloading tasks traditionally run on middleboxes or expensive equipment to the data plane, enabling the efficient collection of statistics and triggering actions upon specific events [82].

A.5.5 SDN controller deployment

Centralized controller architecture, where a single SDN controller manages the entire network, offers the advantage of simplified network management and control due to its unified view of the network. However, this approach can face challenges in terms of reliability, scalability, and latency, especially in large-scale or geographically diverse networks.

In contrast, distributed controller architecture provides several benefits. It enhances reliability and fault tolerance, as the failure of a single controller does not result in a complete loss of network control, ensuring continued operation and maintaining network stability. It also improves scalability, as the distributed nature of the controllers allows for more efficient handling of large-scale networks and high traffic loads, preventing potential bottlenecks and performance issues that may arise with a centralized controller.

Furthermore, distributed controllers can better handle network latency and geographical diversity, as they can be strategically placed closer to the network devices they manage, reducing communication delays and providing faster response times [66].

For distributed architecture to work, the controllers must use their East/Westbound interfaces. These interfaces are used for communication and coordination between SDN controllers. Some common protocols used for East/West communication between SDN controllers include specific East/West-bound architecture such as HyperFlow and previously mentioned ALTO protocol but also use South- and North-bound protocols such as BGP-LS, PCEP, NETCONF, RESTCONF, gRPC, and custom Ad Hoc protocols depending on the controller implementation

[66].

Hyperflow
HyperFlow is a distributed control plane architecture designed for OpenFlow, inspired by the NOX controller. In the HyperFlow architecture, multiple controller replicas are physically distributed across a geographical area, forming a logically centralized environment. HyperFlow uses a publish-subscribe messaging system to send event messages between controllers, making it necessary to maintain persistent storage of events to avoid reordering during network partitioning. It employs WheelFS, a distributed file system, to provide this functionality.

Each controller in HyperFlow can only program the switches it directly controls; to control others, it publishes a message containing the source controller identifier, target switch identifier, and local command identifier. Controllers periodically send messages to indicate their presence in the network. If a controller fails to send a message within three advertisement intervals, it is considered to have failed, and the associated switches must migrate to another controller to continue operation.

In the context of east-west interfaces, HyperFlow serves as a communication and synchronization mechanism among SDN controllers in a distributed architecture, ensuring all controllers have up-to-date network information for decision-making and resource management [66].

A.5.6 Benefits of Software-Defined Networking

Implementing Software-Defined Networking (SDN) in fixed access networks presents numerous advantages for service providers. These benefits range from cost reduction and network scalability to service agility, operational flexibility, and improved reliability. The following paragraphs provide an overview of these advantages, demonstrating the value of integrating SDN into fixed access networks.

Cost Reduction
SDN allows service providers to reduce capital and operational expenditures by leveraging commodity hardware and simplifying network management. This approach reduces the reliance on expensive, proprietary hardware and enables easier maintenance and upgrades. In addition, SDN's centralized overview and automation capabilities lead to more efficient network operations and reduced labor costs [64].

Network Scalability
SDN enables service providers to rapidly scale their networks up or down in response to changing demand. SDN's centralized control and programmability make it possible to manage network resources more efficiently, ensuring optimal utilization and avoiding over-provisioning. This adaptability allows providers to meet customer needs better while minimizing infrastructure investments [64].

Service Agility and Automation
SDN empowers service providers to quickly deploy and customize new services through automation, resulting in reduced time-to-market and a competitive edge. The programmable nature of SDN facilitates the development and implementation of innovative services, allowing providers to respond more effectively to changing market conditions and customer requirements. Automation simplifies network management processes, allowing providers to quickly adapt to network changes and efficiently allocate resources, which further enhances service agility [64].

Operational Flexibility
By centralizing and automating network management, SDN provides service providers with greater operational flexibility. This allows for easier configuration and maintenance of network devices, streamlined troubleshooting, and more efficient use of network resources. In turn, providers can deliver higher-quality services while minimizing operational complexity [64].

Improved QoS and QoE
SDN enhances QoS by employing various methods, including resource reservation, multimedia flow routing, inter-domain routing, and queue management, to name some. Furthermore, the OpenFlow protocol enhances QoS by providing flexible flow control and traffic management, allowing for efficient resource allocation and prioritization of critical network traffic [83].

Enhanced Telemetry and Network Visibility SDN, combined with In-Band Network Telemetry (INT), offers improved telemetry and network visibility in fixed access networks for Network Service Providers (NSPs). INT allows real-time collection of network state information directly from the data plane as packets are processed, providing detailed insights into traffic patterns and identifying potential issues before they escalate. This enhanced visibility enables NSPs to proactively monitor their networks, optimize performance, reliability, and resource utilization, and troubleshoot network failures more efficiently [84].

A.5.7 Challenges of SDN Deployment

Deploying SDN in fixed access networks has its challenges and limitations. One of the primary concerns is the need for substantial investment in updating existing network infrastructure. Many fixed access networks rely on legacy equipment that may need to be compatible with SDN technologies, requiring service providers to replace or upgrade their hardware and software to support SDN capabilities. This can be both time-consuming and costly, especially for smaller service providers with limited resources.

Interoperability is another significant challenge when deploying SDN in fixed access networks. SDN is still an evolving technology with multiple standards, protocols, and controller solutions available, which may not always be compatible with each other. Ensuring seamless integration between various SDN components

and between the SDN controller and existing network devices can be a complex task that requires careful planning and coordination [85].

Additionally, the introduction of SDN brings about new security concerns. The centralized control plane can be a single point of failure, making the network more vulnerable to attacks. Ensuring the security and integrity of the SDN controller and its communication with network devices is essential to prevent unauthorized access and maintain the stability of the network. Another security challenge with Software-Defined Networking (SDN) lies in its dynamic environment, where the ability to program the network and create dynamic flow policies can also lead to security vulnerabilities. Ensuring the enforcement of network security policies becomes crucial in this context [86].

Finally, the transition to SDN may involve organizational and cultural challenges. Adopting SDN requires a shift in mindset, moving from traditional networking approaches to a more software-centric, programmable, and agile way of managing networks. This change may require retraining and upskilling of existing staff and adopting new processes and operational models.

A.5.8 Conclusion

In conclusion, Software-Defined Networking (SDN) has emerged as a game-changing approach that offers significant benefits for fixed-access network service providers. By separating the control plane from the data plane, SDN enables improved network management, programmability, and flexibility. As a result, service providers can reap the advantages of cost reduction, network scalability, service agility, operational flexibility, and improved reliability.

Several use cases for SDN in fixed-access networks have been discussed, including centralized network management and control, traffic engineering and optimization, and network automation. Each of these use cases highlights the potential of SDN to transform network operations, enhance service delivery, and improve overall network performance.

However, the implementation of SDN also comes with challenges, such as the need for substantial investment in updating existing network infrastructure, interoperability issues, security concerns, and organizational and cultural shifts. Overcoming these challenges is critical for service providers to fully realize the benefits of SDN in their fixed-access networks.

A.5.9 NMS requirements posed by Software Defined Networks

In this section, we have discussed Software Defined Networks (SDN) and their potential impact on the networking landscape. With SDN's increasing adoption, network management systems (NMS) must adapt to SDN's unique requirements and challenges. From our review, we have compiled a list of requirements that the aforementioned trend poses on NMS; see In Appendix F.

A.6 Segment Routing and Traffic Engineering

In the previous sections, we have discussed how the growth of Internet traffic poses significant challenges for network service providers (NSPs). To address these challenges, NSPs can physically expand their networks, which can be expensive, or optimize the utilization of available resources using, for example, by applying traffic engineering [87].

Traffic engineering (TE) is a critical aspect of communication networks, as it involves strategies to optimize the performance of networks and greater utilization of resources. D. Nadeau defines traffic engineering as ”a process whereby a network operator can engineer the paths used to carry traffic flows that vary from those chosen automatically by the routing protocol(s) in use in that same network, in an effort to steer traffic through the network, which may result in more efficient use of network resources, protect against network node or link failures, as well as provide certain customers with custom services such as guaranteed bandwidth connections” [88].

In this section, we will discuss the importance of traffic engineering, with a focus on the use of Segment Routing (SR-TE) and Software-Defined Networking (SDN). However, we will also briefly discuss other TE technologies and consider why SR might not always be the best choice for traffic engineering, as established protocols like OSPF/IS-IS can sometimes provide better TE solutions [89].

A.6.1 Traffic Engineering

IP networks possess inherent mechanisms to manage themselves, such as a host implementing the Transmission Control Protocol (TCP) adjusting it's sending rate to the available bandwidth and routers recalculating paths in response to topology changes. However, these mechanisms alone do not guarantee efficient network performance. Traffic engineering aims to enhance user performance and optimize network resource usage by adapting the routing of traffic according to the prevailing demands [89]

Traffic engineering is a crucial aspect of fixed access networks for NSPs, who must accommodate increasing customer demands for connectivity while optimizing the utilization of available resources. NSPs can physically expand their networks or use traffic engineering to improve service quality and network efficiency. With the growing demand for high-quality service delivery, NSPs need to ensure that network resources are utilized effectively, and traffic engineering can help manage network congestion, minimize end-to-end delay, and reduce packet loss. This can lead to more efficient use of available network resources and improved quality of service delivery. To achieve these goals, NSPs need to choose their performance objectives carefully, taking into account the specific needs of their customers and the capabilities of their network infrastructure [90, 91].

The importance of traffic engineering for service quality and network efficiency
Traffic engineering (TE) plays a crucial role in ensuring service quality and network efficiency. One of its primary performance objectives is congestion mini-

mization, which directly impacts delay, jitter, and packet loss in operational IP networks. By employing techniques such as sharing network resources among multiple traffic streams, reallocating network resources, and denying access to congested resources, TE systems can effectively minimize congestion and achieve better network utilization [90, 91].

Another key performance objective of TE is end-to-end (E2E) delay minimization, which is essential for critical real-time communications. Techniques like Constrained-Shortest Path First (CSPF), where E2E delay is used as a constraint for path selection, can help achieve this goal. Packet loss minimization is also a vital network-related performance objective tackled by TE, which can be addressed by over-provisioning the network to increase resilience and providing redundant resources for use in case of failure.

In addition to the above objectives, TE also aims to optimize resource utilization, which has a significant impact on network operators' ability to serve a higher number of service demands without increasing costs. By addressing these performance objectives, traffic engineering ensures that network resources are used effectively, leading to improved service quality and network efficiency [90, 91].

Traffic engineering techniques and algorithms

Earlier routing protocols in the ARPANET and the Internet were not suitable for TE as they lacked the flexibility and resource awareness required for effective traffic engineering [90, 91]. With the growth of Internet traffic, various strategies have been developed to optimize routing in a network. Traditional IP routing protocols like OSPF and IS-IS have been used in large networks throughout the Internet for many years. These protocols initially lacked the features needed for traffic engineering, but they were later enhanced to support TE functions by optimizing the setting of static link weights and reconfiguring the routers with new weight settings as needed. This approach treats traffic engineering as a network operations task rather than the responsibility of the underlying routing protocol. Working with the traditional OSPF and IS-IS protocols has many practical advantages, including protocol stability, low overhead, diverse performance constraints, compatibility with traditional shortest-path IGPs, concise representation, and the ability to use default weights and backup routes in case of topology changes or link failures [92].

The introduction of Multiprotocol Label Switching (MPLS) brought a new paradigm for traffic engineering, focusing on different aspects such as metric optimization, multicommodity flow problems, and other techniques. The Path Computation Element (PCE)-based architecture for MPLS and Generalized MPLS (GMPLS) networks, proposed by the Internet Engineering Task Force (IETF), extends packet switching capabilities of MPLS to an open set of networking and switching methods. This architecture introduces a dedicated element for path computation, enabling the application of complex algorithms such as Constrained-Shortest Path First (CSPF). As a result, the PCE-based architecture has been widely adopted for traffic engineering in various contexts, including intra-domain, inter-domain, and inter-layer scenarios, effectively taking over from the previous traditional IP routing protocols [90, 91].

In recent years, more advanced traffic engineering approaches have been introduced. Segment Routing (SR) is an innovative traffic engineering technology that leverages source routing and MPLS, enabling greater flexibility and scalability in network routing. In addition to SR, centralized control mechanisms like Software-Defined Networking (SDN) have emerged, providing the possibility for short-term or even online traffic engineering. These modern technologies facilitate more dynamic and efficient network management, paving the way for improved network performance and resource utilization and establishing a strong link to the new networking technologies such as NFV, SFC, and SDN [87].

A.6.2 Segment Routing

Segment routing (SR) is a networking technique that divides a larger network into smaller, manageable segments, optimizing data transmission efficiency and improving overall network performance. This approach aims to reduce congestion and latency in the network by distributing traffic across multiple paths and subnetworks, thereby minimizing the impact of bottlenecks and maximizing resource utilization.

Segment Routing is based on the loose source routing concept, where a node can include an ordered list of instructions, called segments, in the packet headers. These segments guide the forwarding and processing of packets along their path in the network. The network path toward a destination can be divided into segments by adding intermediate waypoints, forming a segment list, or creating an SR Policy. Each segment may enforce topological requirements, such as passing through a node, or service requirements, like executing an operation on the packet [90, 91].

Comparison with traditional routing techniques
Segment Routing offers several advantages compared to traditional routing techniques, such as distance-vector, link-state, and path-vector algorithms. Traditional routing algorithms typically focus on finding the shortest path between source and destination nodes, while SR provides a more flexible approach by allowing nodes to specify an ordered list of instructions in packet headers. This flexibility enables advanced traffic engineering and service chaining, which are difficult to achieve with traditional routing techniques [90, 91].

One key advantage of SR over traditional routing is its ability to reduce the amount of state information maintained in network nodes. In traditional routing techniques, each node along a path must maintain state information, which can lead to scalability problems in the control plane and data plane. In contrast, SR requires only the ingress node to store the association between a flow and its path, reducing the amount of state information required in the network [90, 91].

Another benefit of SR over traditional routing is its support for Equal Cost MultiPath (ECMP) routing. Traditional routing techniques like MPLS-TE do not easily exploit ECMP, as they often use a single path for each flow, which can lead to congestion and suboptimal resource utilization. SR, on the other hand, allows multiple paths within each segment, enabling more efficient load balancing and better utilization of network resources.

Furthermore, SR simplifies network architectures by allowing the combination of overlay and underlay networking services and features using only IPv6 technology (in the case of SRv6). Traditional routing techniques often require the use of different protocol layers, which can increase complexity and make network management more challenging [90, 91].

A.6.3 Segment Routing Protocols and Technologies

Segment Routing relies on a set of protocols and technologies to enable flexible and efficient traffic engineering, service chaining, and load balancing in modern networks. The primary SR technologies are Segment Routing over MPLS (SR-MPLS) and Segment Routing over IPv6 (SRv6), which utilize different data planes to carry segment lists in packet headers and process them accordingly [90, 91].

MPLS-based segment routing
SR-MPLS operates over the well-established MPLS data plane, requiring no changes to the MPLS forwarding plane. It simplifies the traditional MPLS control plane by reducing the per-flow state information that needs to be maintained in network nodes. This reduction is achieved through the use of global SIDs, which eliminates the need for explicit path signaling and reduces the amount of state information required at each hop in the network. As a result, the overall complexity of the control plane is reduced, leading to improved scalability and easier management of network resources. SR-MPLS is particularly beneficial for operators with existing MPLS infrastructure, as it allows them to leverage their current deployment while enjoying the advantages of Segment Routing, such as increased flexibility, better traffic engineering capabilities, and more efficient use of network resources [90, 91].

IPv6-based segment routing
SRv6 relies on a new kind of IPv6 routing header called the SR Header (SRH), which carries segment lists and enables advanced traffic engineering and service chaining. The SRv6 is gaining popularity because it supports the SRv6 Network Programming Model, providing exceptional flexibility in designing and operating network services. SRv6 is an appealing option for operators deploying new networks or considering the future evolution of their network architectures, for instance, by incorporating virtual network functions and service chains into the network. This approach also streamlines the collaboration between SDN controllers and the underlying network, as it reduces the volume of routing information needed to manage network paths [90, 91].

Segment routing control plane architectures
The control plane for Segment Routing is responsible for complementing the functionality of the data plane and providing a complete solution for SR. It can be based on a fully distributed approach or rely on a centralized SR controller based on SDN principles. A hybrid approach can also be used where both approaches

coexist. The definition of the control plane for Segment Routing has started from the SR-MPLS data plane and has been adapted to the new data plane [90, 91].

The control plane can use the regular IGP routing protocols (OSPF, IS-IS) to support basic operations for the SRv6 data plane, while extensions are still needed to distribute IGP-Adjacency segments and other SR configuration information. The original design goal of the control plane for Segment Routing was to support the fully distributed approach, where routers are capable of making autonomous decisions, allowing the same functionality of a traditional MPLS network to be offered without a centralized SDN controller for its operations. However, there is now a trend to focus on a hybrid approach, in which distributed routing protocols coexist with an SR controller, aligned with the vision of Software Defined Networking, which aims to centralize the control plane function in SDN controllers [90, 91].

In conclusion, the Segment Routing architecture can be deployed by seeking the right balance between distributed and centralized control. The distributed control is used by the routers to exchange reachability information and evaluate the shortest paths in a traditional way, with no need to interact with the centralized controller. The centralized controller is in charge of making decisions about the SR policies that implement advanced features or services such as Traffic Engineering, VPNs, or Service Function Chaining, allowing the clear decoupling of the data plane operations from the service logic operating in the control plane [90, 91].

Key performance indicators for segment routing and traffic engineering
Segment routing and traffic engineering rely on several key performance indicators (KPIs) to evaluate the efficiency and effectiveness of the implemented solutions. In the context of SRv6, a specific type of segment routing, various KPIs have been proposed and studied in the literature. P. L. Ventre et al. [93] discuss the following important KPIs for segment routing:

Throughput: One of the primary KPIs for segmented routing is throughput, which represents the maximum rate at which data can be transferred through the network without causing packet drops. In the context of SRv6, throughput can be characterized using metrics such as No-Drop Rate (NDR) and Partial Drop Rate (PDR).

Latency: Latency measures the time taken for a packet to travel from the source to the destination within the network. It is a crucial indicator of network responsiveness and has a direct impact on user experience. In SRv6 evaluations, latency measurements can be obtained by injecting timestamps with high resolution.

Packet loss: Packet loss is another important KPI that indicates the percentage of packets that fail to reach their destination. In segmented routing, it is crucial to minimize packet loss to ensure reliable data transmission and maintain network performance.

Resource utilization: Efficient resource utilization is vital for segmented routing and traffic engineering. By optimizing the use of resources such as CPU, hardware, and network capacity, it is possible to improve network performance and minimize costs. In the context of SRv6, resource utilization can be assessed

by measuring CPU savings achieved through various implementation strategies, such as offloading SRv6 processing to network interface cards (NICs).

These KPIs provide valuable insights into the performance of segmented routing and traffic engineering solutions, allowing network operators to make informed decisions regarding the deployment and optimization of their networks.

A.6.4 SDN and Segment Routing for Traffic Engineering

In recent years, the combination of Software Defined Networking (SDN), Segment Routing (SR), and Traffic Engineering (TE) has emerged as a powerful approach to managing network traffic and improving network performance [94]. SDN enables the centralized control of the network, allowing for per-flow routing based on TE goals. SR can be used in centralized, distributed, or hybrid environments. In a distributed scenario, segments are allocated and signaled by routing protocols like IS-IS, OSPF, or BGP, while in a centralized scenario, an SR controller (SDN controller) allocates and instantiates the segments [95].

The integration of these technologies offers several benefits. For instance, SR reduces the complexity of both control and user planes by eliminating the need for per-flow state maintenance within the network. This is done by enforcing a packet's path through an ordered list of processing/forwarding functions called segments, which can include logical and physical elements such as packet filters, network nodes, or network links. The combination of SR and SDN centralizes the control plane, allowing for efficient network management and programmability.

One application of SR is Traffic Engineering, where SR can facilitate the setup, modification, and tear-down of TE paths within a network domain while operating only at the network's border. By focusing on a centralized approach and integrating with the application layer, SR can adapt to various application requirements. Applications can have diverse needs; some are delay-sensitive (e.g., financial transactions and VoIP), others require high bandwidth (e.g., data center replication), and some need low jitter (e.g., video streaming). A centralized SDN controller can react in an agile way to the application routing in the network, allowing for better performance and resource utilization [95].

In summary, the integration of SDN, SR, and TE offers numerous advantages, including simplified route enforcement, reduced network complexity, and centralized control for better network management. This powerful combination paves the way for improved network performance and resource utilization, offering new opportunities for network operators and administrators to enhance their network infrastructures [94].

A.6.5 NMS requirements posed by Segment routing and Traffic Engineering

In the previous section, we have discussed the concepts of Traffic Engineering (TE) and Segment Routing (SR) and their potential impact on the networking landscape, especially with the rising trend of SDN. With the increasing adoption of TE and SR, network management systems (NMS) need to adapt to the unique requirements and challenges posed by these technologies.

From our review, we have compiled a list of requirements that the aforementioned trend poses on NMS; see In Appendix G.

A.7 AI/ML in Network Management

As modern networks continue to evolve and increase in complexity, operators face significant challenges in managing their infrastructures. The rise of cloud computing, bandwidth, and latency demands, along with the implementation of cutting-edge technologies like software-defined networking (SDN) and network functions virtualization (NFV), have led to greater scalability and agility but also added layers of complexity to network systems [34].

The shift towards off-site cloud hosting of services has further increased the dynamism of network environments, allowing them to adapt more easily to changing requirements. However, this also makes network management increasingly difficult, as operators must now navigate multiple service level agreements (SLAs) and ensure high-quality service (QoS) and user experience (QoE) for customers [96].

One of the most pressing concerns for operators is the inefficiency and limitations of human-machine interaction. Current methods of network management often involve slow, error-prone, and expensive processes, and integrating different platforms presents a significant challenge due to the diverse configurations and the need for agile, personalized services. The lack of efficient, extensible standards-based mechanisms for providing adaptable services further contributes to high operational expenditures (OPEX) in network management [97].

This section will explore the role of artificial intelligence (AI) and machine learning (ML) in addressing these issues and enhancing the management of complex, dynamic network environments.

A.7.1 Leveraging AI/ML for Network Management

The EMA Research Report on Network Performance Management for Today's Digital Enterprise from 2019 emphasizes that advanced IT analytics (or AIOps) is the second-largest driver, after IoT, influencing an IT organization's network performance management (NPM) tool strategy. This suggests that network managers are increasingly integrating their data into analytics tools or directly incorporating AIOps capabilities into their tools to enhance their value [98].

Artificial intelligence in network management takes advantage of big data, analytics, and machine learning to optimize and streamline operational workflows. The process can be divided into two primary stages: data collection and application of analytics and machine learning capabilities. The initial step involves gathering a wide range of data from various sources, including [99, 100]:

- Historical performance and event data
- Streaming real-time operations events
- System logs and metrics
- Network data, including packet data

- Infrastructure data

Once the data has been collected, analytics and machine learning capabilities are employed to:

- **Distinguish significant event alerts from the 'noise'**: AIOps sifts through IT operations data, separating crucial abnormal event alerts (signals) from the rest (noise).
- **Pinpoint root causes and suggest solutions**: AIOps can correlate abnormal events with other event data across environments, identifying the cause of an outage or performance problem and recommending remedies.
- **Automate responses, including real-time proactive resolution**: AI can automatically direct alerts and suggested solutions to appropriate IT teams or even create response teams based on the problem's nature and the solution. In many cases, it processes results from machine learning to initiate automatic system responses that address problems in real time before users even notice them.
- **Continuously learn to improve the handling of future problems**: AI models enable the system to learn about and adapt to changes in the environment, such as new infrastructure provisioned or reconfigured by DevOps teams.

A.7.2 NMS Requirements Imposed by AI/ML

In this section, we have discussed the significance of AI and ML in network management and how they can greatly enhance the efficiency and effectiveness of managing complex, dynamic network environments. As AI and ML technologies become increasingly crucial in network management, network management systems (NMS) must evolve to incorporate features that support their effective integration and utilization. Based on the insights from the preceding discussions, we aim to identify and outline the essential features and requirements that an NMS must possess to effectively integrate and leverage AI/ML technologies.
In Appendix H, we compile requirements and features for leveraging AI and ML in network management systems.

A.8 Energy Management, GreenIT and ESG Monitoring for Network Service Providers.

Energy management and monitoring, GreenIT, and Environmental, Social, and Governance (ESG) considerations have become increasingly important for businesses, and Network Service Providers (NSPs) are no exception. Energy management and monitoring involve the systematic tracking, analysis, and optimization of energy consumption within an organization. GreenIT refers to the implementation of environmentally friendly technologies and practices within the information

technology (IT) sector. ESG is a set of non-financial factors that assess a company's sustainability and ethical impact, which includes energy usage, environmental impact, and other social and governance factors. The purpose of this section is to discuss the importance of energy management and monitoring, GreenIT, and ESG considerations for NSPs and to explore the challenges and opportunities they present. The scope of this section will cover key concepts, challenges, and strategies to enhance energy efficiency, environmental sustainability, and ESG performance within the context of fixed access networks [101, 102].

A.8.1 Energy Management and Monitoring Challenges

Fixed access networks, which provide wired connectivity to homes and businesses, face unique energy management and monitoring challenges due to their power consumption and infrastructure requirements. A significant portion of the energy consumed in fixed access networks is attributed to network equipment, such as routers, switches, and optical line terminals (OLTs), as well as the powering and cooling of data centers. As the demand for high-speed internet and data services continues to grow, network service providers must expand their infrastructure, which can lead to increased energy consumption and a larger carbon footprint [103].

To address these challenges, NSPs must focus on optimizing the energy efficiency of their fixed access networks by implementing innovative technologies, architectures, and management practices. For instance, they can deploy energy-efficient network devices, utilize passive cooling solutions, and leverage network virtualization to reduce power consumption. Additionally, service providers can adopt renewable energy sources to power their networks and data centers, further minimizing their environmental impact. By prioritizing energy management and monitoring, GreenIT, and ESG considerations, NSPs can not only reduce operational costs but also improve their corporate social responsibility and overall sustainability performance [104].

A.8.2 Energy Management and Monitoring Techniques

Energy management and monitoring techniques in fixed access networks are essential for achieving sustainability goals and minimizing environmental impacts. Key approaches include network upgrades, adaptive power management, and the integration of renewable energy sources.

Network upgrades are a fundamental aspect of energy management in fixed access networks. By replacing older, less energy-efficient equipment with modern, energy-saving devices, Network Service Providers (NSPs) can significantly reduce their energy consumption and carbon footprint. Additionally, network upgrades often involve the deployment of advanced technologies and architectures that optimize network performance and capacity while minimizing energy use [105, 104].

Adaptive power management is another essential technique for managing energy consumption in fixed access networks. This approach involves dynamically adjusting the power consumption of network devices and servers based on real-time demand and usage patterns. For instance, adaptive power management can include techniques such as adjusting the power output of devices during periods of

low network traffic or implementing sleep modes for idle equipment. By tailoring power consumption to actual network needs, NSPs can significantly reduce energy waste and lower their operational costs [106].

A.8.3 Role of NFV and SDN in Energy Management

The role of Network Function Virtualization (NFV) and Software-Defined Networking (SDN) in energy management, monitoring, and optimization is becoming increasingly significant as Network Service Providers (NSPs) seek more efficient and flexible network solutions. These technologies enable greater control over network resources, more efficient use of infrastructure, and the automation of various network functions, all of which can contribute to improved energy efficiency and optimization [107].

Virtualization is a critical aspect of NFV that allows NSPs to run multiple network functions on a single physical server, reducing the need for dedicated hardware and lowering energy consumption. By consolidating network functions onto fewer devices, virtualization enables NSPs to optimize resource usage and minimize power consumption. Additionally, the ability to scale network functions up or down according to real-time demand allows for more efficient use of resources and further energy savings [105].

Resource pooling is another essential aspect of NFV and SDN that contributes to energy management and optimization. With resource pooling, multiple network functions can share the same physical resources, such as processing power, memory, and storage. This approach allows for better resource utilization and reduces the need for redundant, energy-consuming hardware. By dynamically allocating resources based on network demand, NSPs can minimize energy waste and optimize their infrastructure for peak efficiency [105, 107].

Network automation, enabled by SDN, plays a significant role in energy management and optimization as well. SDN allows NSPs to centrally control and manage their networks through programmable interfaces and policies, which can be used to implement energy-saving strategies. For example, SDN can facilitate the automated powering down of network devices during periods of low demand or the routing of traffic through more energy-efficient paths. By automating these processes, NSPs can reduce energy consumption, lower operational costs, and improve overall network performance [107].

In summary, NFV, and SDN technologies are instrumental in improving energy management, monitoring, and optimization in fixed access networks. Through virtualization, resource pooling, and network automation, NSPs can achieve greater energy efficiency, reduce their environmental impact, and create more flexible, sustainable networks.

A.8.4 ESG Factors in Fixed Access Networks

ESG factors in fixed access networks encompass a wide range of environmental, social, and governance issues that directly or indirectly impact network operations and performance. Among these factors, carbon footprint, waste management, and regulatory considerations stand out as crucial components of a sustainable and

responsible network infrastructure [102].

Carbon footprint refers to the total greenhouse gas (GHG) emissions generated by network devices, servers, and other equipment throughout their lifecycle. This includes emissions from energy consumption during operation, as well as those associated with manufacturing, transportation, and end-of-life disposal or recycling. Reducing the carbon footprint of fixed access networks is not only environmentally responsible, but it also helps organizations comply with increasingly stringent regulations aimed at mitigating climate change [107].

Waste management is another critical ESG factor in fixed access networks, as the disposal of obsolete or malfunctioning equipment can have significant environmental impacts. Proper waste management entails the safe and environmentally-friendly disposal of electronic waste (e-waste), as well as the recycling or repurposing of materials whenever possible. Organizations must also consider the social implications of waste management, such as potential health hazards for workers involved in recycling processes or the impact on communities near waste disposal sites [107, 102].

Regulatory considerations play an essential role in shaping ESG practices within fixed access networks. Governments and regulatory bodies are implementing policies and guidelines that promote energy efficiency, reduce GHG emissions, and encourage responsible waste management. Network Service Providers must be aware of these regulations and ensure their operations are in compliance to avoid potential penalties and reputational damage. Additionally, adhering to regulatory requirements can help NSPs identify opportunities for improving their environmental performance, reducing operational costs, and enhancing their overall ESG profile [102], [108].

A.8.5 ESG Reporting and Performance Measurement

ESG Reporting and Performance Measurement are essential components of a comprehensive approach to energy management, Green IT, and ESG considerations for Network Service Providers (NSPs). By tracking, measuring, and reporting on various ESG metrics, NSPs can demonstrate their commitment to sustainability, assess their progress towards ESG goals, and compare their performance with industry peers [102].

ESG metrics are quantitative and qualitative indicators used to evaluate an organization's environmental, social, and governance performance. For NSPs, relevant ESG metrics may include energy consumption, carbon emissions, waste management practices, employee well-being, and corporate governance structures. By monitoring and analyzing these metrics, NSPs can identify areas for improvement, set targets for future performance, and make informed decisions about their sustainability initiatives [102].

Reporting frameworks provide guidelines and best practices for ESG reporting, ensuring that organizations disclose their ESG performance in a consistent, transparent, and comparable manner. Some widely recognized ESG reporting frameworks include the Global Reporting Initiative (GRI), the Sustainability Accounting Standards Board (SASB), and the Task Force on Climate-related Financial

Disclosures (TCFD). By adopting these frameworks, NSPs can ensure that their ESG reports meet the expectations of various stakeholders, including investors, customers, and regulators [109].

Industry benchmarking is a valuable tool for NSPs to assess their ESG performance relative to their peers. By comparing their ESG metrics with those of other organizations in the industry, NSPs can gain insights into their competitive position and identify best practices that could be adopted to enhance their sustainability efforts. Benchmarking can also help NSPs set realistic targets for improvement and track their progress over time, enabling them to demonstrate their commitment to ESG goals and drive continuous improvement [108].

A.8.6 Conclusion

In conclusion, energy optimization, GreenIT, and ESG considerations are essential for Network Service Providers (NSPs) seeking to improve their environmental sustainability and social responsibility. Fixed access networks face unique challenges due to their power consumption and infrastructure requirements, but innovative technologies, architectures, and management practices can help NSPs optimize energy efficiency and reduce their carbon footprint. NFV and SDN play a significant role in energy management, monitoring, and optimization by enabling greater control over network resources, resource pooling, and network automation. ESG factors such as carbon footprint, waste management, and regulatory compliance also play a crucial role in a sustainable and responsible network infrastructure. ESG reporting and performance measurement are essential components of a comprehensive approach to energy management, GreenIT, and ESG considerations. By tracking, measuring, and reporting on various ESG metrics, NSPs can demonstrate their commitment to sustainability, assess their progress towards ESG goals, and compare their performance with industry peers. In summary, focusing on energy optimization and ESG considerations not only reduces operational costs but also improves corporate social responsibility and overall sustainability performance.

A.8.7 NMS requirements posed by Energy Management, GreenIT, and ESG Monitoring

In this section, we have discussed the importance of energy management, Green IT, and Environmental, Social, and Governance (ESG) considerations for Network Service Providers (NSPs). As these factors gain increasing prominence, network management systems (NMS) need to evolve and incorporate features that support effective monitoring and management of networks with a focus on energy efficiency, sustainability, and ESG performance.

Based on the insights from the preceding discussions, we have compiled requirements and features for energy management and monitoring, GreenIT, and ESG considerations in network management systems, see Appendix I.

Requirements:

B Partner Company

SLA measurements and reports:		
No.	**Feature**	**Requirement**
1	a) SLA report generation b) Customer-specific SLA information, uptime, logs, and comments	The system should be able to automatically generate a customer SLA report with SLA information, uptime, logs, and comments for all events during the reporting period.
2	Customizable reporting time periods	The SLA report must be producible for any defined time period.
3	SLA weighting for prioritization of hosts	The SLA part of the report should be able to handle weighting. For instance, if hosts A and B both have SLA of 99.98%, it should be possible to indicate that host A is more important than B with a weighting parameter.
4	Automatic SLA calculation based on group membership	The system should automatically calculate SLA levels based on group membership.
5	Customizable SLA levels according to the client's terms	SLA levels must be customizable according to the client's own terms.
Other reports:		
No.	**Feature**	**Requirement**
6	Scheduled report generation	The system should have the ability to generate scheduled reports.
7	Reporting of custom time periods	All reports should be producible for any defined time period.
8	Reporting active switch ports	The system should be able to report the number of active switch ports.
9	Reporting monitored elements per group or customer	The system should be able to report the number of monitorable objects, such as switches, routers, and servers, per group or customer.
10	Reporting monitored elements per model type	The system should be able to report the number of monitorable objects per model type.
11	Reporting unmanaged elements	The system should be able to report the number of unmanaged objects.

12	Ranking of the nodes based on errors or load	The system should be able to generate alert reports with top nodes, such as the top 10 nodes with the most problems or the top 10 most loaded links.
13	Bandwidth utilization reports	The system should manage to generate bandwidth utilization reports.
14	Exporting of hosts and services as CSV files	Export functions to extract hosts/services as a CSV file.
15	Graphical trend reports (min 1-year timespan)	The system should be able to generate graphical trend reports based on statistics over a longer period of time, at least 1 year.
Mapping and Visualization		
No.	**Feature**	**Requirement**
16	Support for topologies with different views and layers	NMS should support three layers, with a different view for each entity.
17	Network asset placement on a geographical map based on GPS coor- dinate	Objects should be able to be entered on the map based on GPS coordinates.
18	Customizable user view	The user view should be customizable.
19	a) Graphing of all monitored network elements b) Large-scale graphing capacity of minimum 100.000 ports and 5000 switches c) Graphing of all monitored services	The system must be able to handle graphing of all monitored objects such as switches (approx. 5,000), ports (min 100,000 ports), servers, and services.
20	a) Easy-to-use management system for both logical and geographical topologies b) Capability to revert changes to the map management system using an undo function	Easy-to-use system for managing maps, logical and geographical. (preferably with undo function!).

Discovery and Monitoring		
No.	**Feature**	**Requirement**
21	Automatic discovery function with support for CDP, LLDP, OSPF, BGP	The system should have an automatic discovery function with support for CDP, LLDP, OSPF, BGP.
22	Large-scale, real-time concurrent monitoring capacity (minimum 6000 switches and 8000 APs)	The system must handle at least 6000 switches plus 8000 access points.
23	a) Server hardware monitoring for Windows and Linux OS b) Server services monitoring for Windows and Linux c) Server processes monitoring for Windows and Linux OS d) Server Memory monitoring for Windows and Linux OS e) Server CPU monitoring for Windows and Linux OS	The system must be able to monitor hardware, services, processes, memory, CPU on servers with both Windows and Linux OS.
24	Monitoring common server protocols such as HTTP/HTTPS, SSH, FTP, SNMP, DNS, DHCP, SMTP	The system should be able to monitor various protocols such as FTP, HTTP, SSH, etc.
25	Distributable remote polling agent to report routing conflicts	The system should be able to monitor a customer network via a ”remote poll” to avoid possible routing conflicts.
26	Optional SNMP OIDs monitoring	It must be possible to monitor optionally specified SNMP OIDs.
27	Automatic scanning of hosts with IP range and black-list support	The system should be able to conduct automatic scanning via IP range with the possibility of defining a ”black-list”.

28	Search feature for hosts and services	All hosts/services must be searchable.
29	Network element identification by address	The system should use the address of the objects for identification, not the node name or name of BRF.
30	Monitoring Cisco QoS quality	The system should be able to monitor Cisco QoS quality.
31	Monitoring Cisco Multicast quality	The system should be able to monitor Cisco Multicast quality.
32	Monitoring Cisco VoIP quality	The system should be able to monitor Cisco VoIP quality.
33	Monitoring state on BGP/OSPF/IS-IS links	The system should be able to monitor the state on BGP/OSPF/IS-IS links.
34	Monitoring access points via the Wireless Controller	The system should be able to monitor access points via the Wireless Controller.
35	Monitoring end-to-end services	The system must be able to monitor how the client is experiencing the service.
36	Support for network element groups.	
Alerting and notifications:		
No.	**Feature**	**Requirement**
37	SMS and email alerting capability	The system must be able to send SMS and e-mail alarms based on the regulations defined by the company. This should also work in the event of an outage on the master server.
38	Error event correlation	If a main node goes down, the objects below should not alarm.
39	Event commenting functionality	Users should be able to comment on individual events.
40	Temporary interruption scheduling	Users should be able to specify a temporary interruption as a planned job.
41	SNMP trap processing with customizable rules	SNMP traps must be able to be processed and managed with rules: info alarm, red alarm, SMS alarm, email.
42	Event processing with customizable rules	Different types of events must be able to be processed and managed with rules -¿ info alarm, red alarm, SMS alarm, email.
43	a) Color-coding and labeling of alarms b) Filtering of alarms based on label	Different types of alarms must be color-coded and filtered in different views.

44	Configurable notification settings based on time of day and type of event	Automatic acknowledgment of selected events during a specific time (for example not call out support at night if the event is only for a millisecond or the event is something that can wait until next morning).
45	Support for different alarm delays based on network element group	The system should support different alarm times (delay) based on groups.
46	Customizable SNMP rules with MIB import support	Ability to import MIBs and modify/add rules for SNMP traps (customize the monitoring and alerting system by defining additional rules for SNMP traps).
Scalability and redundancy:		
No.	**Feature**	**Requirement**
47	Support for backup servers	The system must be able to run on redundant servers located in physically different facilities.
48	API and integration support	Open system that makes it possible to easily integrate with other systems.
49	Built-in backup and restore functionality	
Security:		
No.	**Feature**	**Requirement**
50	Customer-specific access control for their respective topology and alarms	Customers' access rights to map views and alarms should be limited, meaning they can monitor their object but not other customer's ones.
51	Encrypted management traffic for all protocols	All management traffic must be encrypted, independent of the underlying protocol (ssh, telnet, etc).
Customer support and localization:		
No.	**Feature**	**Requirement**
52	Built-in chat support.	
53	Enterprise customer service.	
54	Has web API.	
55	On-site hosting.	
56	Cloud-based with servers located only in Sweden.	

C OTTPs and Service Providers cooperation

OTTP-TSP Co-operation Driven NMS Features		
No.	**Feature**	**Requirement**
1	Peering Point Management	The NMS should be able to manage and monitor peering points or locations where TSP and OTT networks interconnect, such as Internet Exchange Points (IXPs) or data centers.
2	Routing Policy Configuration	The NMS should allow for the definition and modification of routing policies that govern the flow of traffic between interconnected networks. This may include route selection, traffic prioritization based on content type, or user preferences.
3	Traffic Monitoring	The NMS should provide real-time monitoring and analysis of peering traffic to help both TSPs and OTT providers assess the performance of their interconnected networks.
4	Data Sharing	The NMS should facilitate secure and efficient sharing of relevant data between TSPs and OTT providers, including network performance metrics, content popularity, and user behavior.
5	Secure Communications	The NMS should ensure secure communication and data sharing between TSPs and OTT providers to protect sensitive information and maintain network integrity.
6	Reporting of Peering Agreement	The NMS should generate customizable reports and visualizations for both TSPs and OTT providers, allowing them to track their peering agreement.

D Quality of Service

Essential Quality of Service Protocol Requirements		
No.	**Feature**	**Requirement**
1	Support for the DiffSev protocol	Differentiated Services (DiffServ) is a simplistic QoS model protocol that operates on flow-aggregation and utilizes the hop-by-hop process
2	Support for the RSVP protocol	Resource Reservation Protocol (RSVP) is a protocol used by Integrated Services (IntServ) QoS architecture model for the reservation in which resources explicitly for the end-to-end path and all routers store information of the network.
3	Support for the MPLS protocol	Multiprotocol Label Switching (MPLS) is a technology that aims to reduce the need for complex routing tables via the use of labeling techniques by introducing a layer on top of traditional routing.

Additional Quality of Service Requirements		
No.	**Feature**	**Requirement**
1	Quality of Experience-aware mechanisms	The Network Management Server implements Quality of Experience-aware mechanism
2	Support for SDN to allow flexible modern-day QoS	The support for SDN protocols such as OpenFlow can be seen as a value-added requirement. Or further QoS/QoE can be seen as a value-added feature of SDN.
3	Northbound API support	Northbound API support allows for automation of SLA reporting utilizing SDN. Allows for a wide range of network policies.

E Network Caching and Content Delivery Networks

Network Caching		
No.	**Feature**	**Requirement**
1	Cache Content Management	Provide visibility into the content stored in cache servers, allowing administrators to track frequently accessed content, manage cache storage policies, and monitor cache hit and miss ratios.
2	Cache Server Configuration and Optimization	Enable administrators to configure cache server settings, such as content refresh rates and eviction policies. It should also analyze cache performance, enabling the definition and modification of cache placement strategies based on content popularity and access patterns, ensuring efficient content delivery and minimal latency for end-users.
3	Load Balancing and Fault Tolerance	Monitor the load on cache servers, balance traffic and content requests across servers and detect and handle server failures.
4	Cache Server Health Monitoring	Monitor cache server health, providing alerts and notifications for potential issues, such as high resource utilization, downtime, or performance degradation.
5	Cache Traffic Analysis	Provide insights into traffic patterns between cache servers, origin servers, and end-users, helping administrators understand content delivery efficiency and identify areas for improvement.

Content Delivery Networks (CDN)		
No.	**Feature**	**Requirement**
1	CDN Distribution Optimization	Analyze content distribution throughout the CDN, monitoring content popularity and access patterns to inform and optimize cache placement and content delivery strategies.

Content Delivery Networks (CDN)		
No.	**Feature**	**Requirement**
2	CDN DNS Resolution Monitoring	Monitor DNS resolution using synthetic monitoring to emulate client DNS queries, detect and resolve DNS issues, and identify configuration issues or DDoS attacks.
3	CDN Mapping	Monitor CDN mapping, comparing performance data between CDN and origin servers to identify mapping anomalies and sub-optimal peering policies and verify if end-users are served from the nearest edge server.
4	CDN Latency Monitoring	Measure end-user-to-edge location latency and edge-to-origin data center latency to track performance degradation, identify bottlenecks, and ensure optimal load balancing.
5	CDN Image Optimization Monitoring	Monitoring and comparing metrics relevant to image optimization to ensure CDN vendors' services work as expected for the end-user.

Information-Centric Networks (ICN) and Content-Centric Networks (CCN)		
No.	**Feature**	**Requirement**
1	Content Name-based Communication	Ability to manage and monitor communications initiated using content names in an ICN or CCN paradigm, allowing endpoints to request content without knowing the specific location of the content.
2	ICN and CCN Traffic Analysis	Provide insights into traffic patterns within ICN and CCN architectures, helping administrators understand content delivery efficiency, network load, and latency, as well as identifying areas for improvement.
3	CCN Content Chunk Management	Support the management and monitoring of content chunks in CCN, tracking the unique identifiers attached to content chunks, and monitoring the availability and distribution of content across CCN nodes.

F Network Function Virtualization

VNF Deployment		
No.	**Feature**	**Requirement**
1	Instantiation	Support the creation of new VNF instances in the network. This includes selecting the appropriate virtualization platform, allocating resources (CPU, memory, storage, and network interfaces), and launching the VNF software on the allocated resources.
2	Configuration	Support configuration of VNFs settings and parameters. This may include setting up network interfaces, routing rules, and security policies.
3	Integration with existing network services	Provide seamless integration of the newly deployed VNF with existing services in the network, and ensure data flow between the functions.
4	Automation and orchestration	Support automation and orchestration of VNF deployment tasks.
VNF Discovery		
No.	**Feature**	**Requirement**
5	Automatic discovery of deployed VNFs	Ability to automatically detect the presence of all VNFs in the network (e.g. by scanning for known VNF signatures, monitoring virtualization platforms for new VNF instances, or integrating with other management systems that deploy and manage VNFs).
6	VNFs reporting	Ability to create a report on all VNFs in the network, or group/type of VNFs, containing information about each VNF, such as its type, version, configuration, location, and resource utilization.
7	Discovering relationships with the underlying physical infrastructure	Ability to map VNFs' relationships with the underlying physical infrastructure. This includes the connections between VNFs and the physical servers, switches, routers, and other devices that support them.

8	Tracking VNF dependencies	VNFs often rely on other VNFs or physical network functions to operate correctly. The NMS should be able to identify and track these dependencies.
9	Visualization and monitoring	Provide a visual representation of the discovered VNFs and their relationships with the underlying physical infrastructure.
VNF Scaling		
No.	**Feature**	**Requirement**
10	Monitor the performance and resource utilization of VNFs	Collect performance metrics and resource usage data for each VNF, such as CPU usage, memory consumption, network throughput, and latency.
11	Analyze and predict performance requirements	Ability to analyze the collected data and predict the future performance requirements of the VNFs, taking into account factors like traffic patterns, user demand, and network conditions.
12	Automatically scale VNFs based on requirements and constraints	Capability to automatically scale the VNFs up or down based on the analyzed performance requirements and any predefined constraints. This could involve adding or removing resources, such as CPU, memory, or network bandwidth, or creating additional instances of the VNF to distribute the load.
13	Implement scaling policies and rules	Allow network administrators to define and implement scaling policies and rules for the VNFs. These policies can specify the conditions under which VNFs should be scaled, the maximum and minimum resource limits, and other parameters.
VNF Decommissioning		
No.	**Feature**	**Requirement**
14	Data migration	Support, before decommissioning a VNF, the migration of its data to other instances or network services to ensure that no critical information is lost.
15	Resource release	Once the VNF is no longer needed, then release its allocated resources back to the underlying virtualization platform or resource pool.

16	Automatic update of network configuration	Automatically update the network configuration after decommissioning to reflect the removal of the VNF from the network.
Network Slicing Support		
No.	**Feature**	**Requirement**
17	Support for network slicing	Allowing the creation of multiple virtual networks on top of a shared physical infrastructure, to meet specific requirements of services, customers, applications, or devices.
Service Function Chaining Requirements		
No.	**Feature**	**Requirement**
18	Dynamic Service Chaining	Ability to dynamically create, modify, and delete SFCs based on changing network conditions and service requirements.
19	SFC monitoring	Ability to monitor the performance and status of individual SFs and the entire SFC.
20	SFC Analytics	Capability to analyze SFC performance, for identifying bottlenecks, failures, or optimization opportunities.
21	SFC Traffic Steering	Support for policy-based traffic steering through specific SFCs.
22	SFC Security Enforcement	Ability to monitor and enforce security policies within, and across, SFCs.

G Software Defined Networks

Essential Protocol Support	
Feature	**Requirement**
OpenFlow:	OpenFlow is fundamental in SDN and essential for efficient communication and control across various OpenFlow versions in the NMS.
BGP-LS:	BGP-LS support is crucial in the NMS for exchanging link-state information between SDN controllers and traditional routing protocols.
PCEP:	PCEP support enables optimized path computation and communication in MPLS and GMPLS networks within the NMS.
NETCONF/YANG:	Support for NETCONF and YANG allows streamlined remote configuration and management of network devices in the NMS.
RESTCONF:	RESTCONF support in the NMS provides a RESTful interface for remote network device configuration and management.
REST:	Supporting RESTful APIs ensures seamless communication with various web technologies and tools within the NMS.
gRPC:	gRPC support is essential for efficient communication with SDN controllers or devices using protocol buffers in the NMS.
HyperFlow:	HyperFlow support in the NMS is essential for efficient communication and synchronization between distributed SDN controllers, maintaining a consistent view of the network state and improving scalability and reliability.
Protocol Support for Additional Value	
Feature	**Requirement**
ForCES:	ForCES support in the NMS, helps manage the separation of control and forwarding planes in network devices and can be valuable in specific use cases or network architectures, but in a lot of cases OpenFlow is enough.
I2RS:	I2RS support, while promising, is not yet widely adopted; however, it enables dynamic interaction between applications and the routing system within the NMS, potentially providing additional benefits as its adoption grows.

ALTO:	ALTO support, while not essential for every network, allows the NMS to exchange network topology and resource information among SDN controllers, facilitating informed decision-making for traffic optimization and resource allocation in networks that require advanced traffic engineering.
P4:	P4 programming language support, although not essential for all networks, enables network administrators to define custom forwarding plane behavior in the NMS and offers added flexibility in network management, especially in environments with specialized forwarding requirements.
Telemetry and Analytics	
Feature	**Requirement**
gNMI:	Support for the gRPC Network Management Interface (gNMI) allows the NMS to subscribe to telemetry data streams from network devices, offering efficient data collection and low latency.
NetFlow:	Support for NetFlow enables the collection of traffic flow information for analysis and reporting, and is widely adopted but might be less efficient than gNMI for certain use cases.
sFlow:	Support for sFlow enables the collection of traffic flow information for analysis and reporting, offering sampling-based monitoring that can be more scalable than NetFlow in high-speed networks.
IPFIX:	Support for IPFIX and IP Flow Information Export (IPFIX) protocols enable the collection of traffic flow information for analysis and reporting. While it is useful and more flexible than NetFlow, it might be redundant if the underlying infrastructure already uses NetFlow.
Flow Management and Monitoring:	
Feature	**Requirement**
Flow monitoring:	Real-time monitoring of flow entries, flow statistics, and performance metrics for individual flows in the SDN network.
Flow rule management:	The ability to create, modify, and delete flow rules in SDN devices directly from the NMS.
Flow rule conflict detection:	Detection of conflicting flow rules and automatic resolution or notification to network administrators.

Essential Controller Support	
Feature	**Requirement**
ONOS (Open Network Operating System):	A Linux Foundation project and a leading open-source SDN controller, widely used for building next-generation SDN/NFV solutions. It has a rich set of Southbound Interface (SBI) protocols and low hardware requirements.
OpenDaylight:	Another Linux Foundation project, OpenDaylight is a widely used open-source SDN controller that serves as the basis for various proprietary controllers. It offers extensive protocol support in its service abstraction layer, including OpenFlow, OVSDB, NETCONF, BGP, P4, LISP, SNMP, PCEP, and others.
Cisco ACI (Application Centric Infrastructure):	A high-cost, proprietary SDN controller from Cisco, offering full native Layer 2-7 integration and support for VxLAN as an extensible overlay/network logic protocol and NFV using GRE (NV-GRE).
Juniper Contrail:	A proprietary SDN controller from Juniper Networks, providing end-to-end dynamic configuration, optimization, and control for various cloud infrastructures. It supports Network Functions Virtualization (NFV) and integrates with most cloud services.
HP VAN SDN Controller:	A proprietary SDN controller from HP, with strict hardware requirements and a rich API with excellent documentation. However, it only supports OpenFlow in its SBI, limiting its applicability.
Huawei Agile Controller:	A proprietary SDN controller from Huawei, based on ONOS and part of its CloudFabric Solution. It has strong interoperability with third-party platforms like VMware vCenter and extensive support for OpenStack platforms. However, it requires large server-sizing hardware due to strict hardware specifications.
Additional Controller Support	
Feature	**Requirement**
Beacon:	Support for integration with the Beacon SDN controller, an easy-to-use Java-based platform with an emphasis on modularity and extensibility.

Ryu:	Support for integration with the Ryu SDN controller, a lightweight, component-based controller that enables rapid development of custom network applications.
POX:	Support for integration with the POX SDN controller, a Python-based platform suitable for research and educational environments.
NOX:	Support for integration with the NOX SDN controller, a pioneering controller that laid the foundation for several other platforms.
Floodlight:	Support for integration with the Floodlight SDN controller, a Java-based platform with a focus on performance and scalability.

H Segment Routing and Traffic Engineering

Network Discovery and Representation		
No.	**Feature**	**Requirement**
1	Discover and represent all SR-enabled network elements	Discover and represent all routers and switches that support segment routing in the network.
2	Discover and represent the links between all SR network elements	Discover and represent the connections between all segment routing-capable routers and switches.
3	Discover and represent segment identifiers (SIDs)	Discover and represent the unique labels assigned to segments in the network, which are used to define the path a packet should follow through the network.
Traffic Engineering and Management		
No.	**Feature**	**Requirement**
4	Create and modify traffic engineering policies	Define new traffic engineering policies using segment routing features, or modify existing policies. This may include specifying the desired path through the network using SIDs, setting priority levels for different types of traffic, and defining how traffic should be distributed across multiple paths.
5	Traffic steering through specific paths and links using segment routing features	Provide traffic steering based on SR features such as Throughput, Latency, and Packet loss.
6	Path computation	Analyze the network topology and the segment routing configuration to calculate the most efficient paths for data packets, considering factors such as link capacity, latency, and current traffic load.
7	Path optimization	Dynamically adjust computed paths based on real-time network conditions.

Performance Monitoring and Analysis		
No.	**Feature**	**Requirement**

8	Real-time monitoring	Continuously collecting and analyzing network performance and traffic data, providing network operators with up-to-date information about the state of the network.
9	Monitor segment routing-based network performance - Throughput	Measure throughput in SR-Paths to help network operators understand how much traffic is being carried and whether the network is capable of handling the current load.
10	Monitor segment routing-based network performance - Latency	Measure the latency in SR-paths, which is an important metric because it can impact the quality of experience for users, especially in time-sensitive applications like voice and video communications.
11	Monitor segment routing-based network performance - Packet loss	Detect and quantify the number of data packets that are lost while being transmitted across SR paths.
12	Monitor segment routing-based network performance - Resource utilization	Monitor the usage of network resources, such as link bandwidth, router/switch CPU and memory, and other relevant components for SR-paths. By monitoring resource utilization, network operators can identify potential bottlenecks or issues that may be impacting network performance.
Routing Flexibility and Control		
No.	**Feature**	**Requirement**
13	Ad-hoc routes support	Enable network operators to create and manage ad-hoc routes, which are temporary or customized paths created to meet specific needs or address particular situations. These routes might be used to bypass network failures, optimize traffic flow, or meet specific performance requirements.
14	Dynamic traffic management	Enable network operators to dynamically steer traffic based on real-time network conditions.

Integration and Compatibility		
No.	**Feature**	**Requirement**

15	Segment Routing over MPLS (SR-MPLS)	Integrate with SR-MPLS to support various vendor solutions and devices.
16	Segment Routing over IPv6 (SRv6)	Be compatible with SRv6 to manage IPv6-based networks utilizing segment routing features.
17	Programmability with IPv6 in SRv6	Manage and interact with SRv6-based networks, supporting the programmability features offered by IPv6 in the context of segment routing. By utilizing IPv6 extension headers and SRH (Segment Routing Header), SRv6 enables network operators to define and manipulate the forwarding paths and behaviors within the network, providing greater flexibility and control.
18	Open Shortest Path First (OSPF) with Segment Routing Extensions	Work with OSPF and its segment routing extensions for managing network topologies and routing paths. OSPF is a popular interior gateway protocol (IGP) used for routing within an autonomous system. Segment routing extensions for OSPF have been developed to provide segment routing capabilities.
19	Intermediate System to Intermediate System (IS-IS) with Segment Routing Extensions	Be compatible with IS-IS and its segment routing extensions. IS-IS is another popular IGP protocol used for routing within an autonomous system. Like OSPF, segment routing extensions for IS-IS have been developed to support segment routing.
20	Border Gateway Protocol (BGP) with Segment Routing Extensions	Integrate with BGP and its segment routing extensions. BGP is an exterior gateway protocol used for routing between autonomous systems. BGP can also be extended to support segment routing, enabling more flexible routing policies and traffic engineering.

I Artificial Intelligence and Machine Learning

AI/ML-driven Network Management Features		
No.	**Feature**	**Requirement**
1	Big data capabilities from diverse sources	Capability to gather and consolidate data from a wide variety of sources such as logs, metrics, real-time events, network devices, and service ticketing systems.
2	Advanced data analytics	Analyze collected data such as traffic patterns, resource utilization, network performance metrics, and incidents using AI algorithms.
3	AI/ML-driven anomaly detection	Utilize AI/ML algorithms to identify and flag unusual events, patterns, or trends in the analyzed data.
4	Adaptive learning capabilities	Leverage machine learning models to continuously learn from the data, improving the accuracy and efficiency of anomaly detection and network management processes over time.
5	Automated root cause analysis	Use AI/ML algorithms to correlate abnormal events across different data sources, focusing in on the root cause of performance problems or incidents.
6	Proactive problem resolution	Implement AI/ML-driven automation to proactively address detected anomalies or issues, reducing the time to resolution and minimizing the impact on network performance.
7	Capacity planning and optimization	AI/ML features to forecast future capacity requirements and optimize resources based on historical and real-time data. This can improve network performance and reduce costs by ensuring that resources are allocated efficiently.

J Energy Management, GreenIT, and ESG Monitoring

Energy, GreenIT and ESG monitoring		
No.	**Feature**	**Requirement**
1	Energy usage monitoring	Provide real-time and historical data on energy consumption of network devices, servers, and other equipment, allowing for identification of patterns and potential inefficiencies.
2	Carbon footprint estimation	Enable estimation of the carbon footprint (also referred to as Greenhouse Gas (GHG) emissions tracking, carbon emissions estimation, CO2 emissions monitoring) of network infrastructure and servers, based on energy consumption data and relevant emission factors.
3	Hardware lifecycle tracking	Track the lifecycle of network devices and servers, including procurement, usage, and end-of-life management, to help assess the environmental impact of equipment disposal and recycling.
4	Cooling and power efficiency monitoring	Monitor the efficiency of cooling systems and power distribution units (PDUs) in data centers, enabling identification of potential areas for improvement and energy savings.
5	Integration with energy management systems	Integrate with energy management systems, such as building management systems (BMS) or data center infrastructure management (DCIM) solutions, for a more comprehensive view of energy consumption and efficiency.
6	Customizable ESG metric dashboards	Offer customizable dashboards for visualizing ESG metrics, enabling stakeholders to quickly assess the performance of the network infrastructure and servers against ESG goals and targets.
7	Automated ESG reporting	Support automated generation of ESG reports based on predefined templates, complying with relevant reporting frameworks (e.g., GRI, SASB) and regulatory requirements.

Energy, GreenIT and ESG monitoring		
No.	**Feature**	**Requirement**
8	ESG Alerting and notifications	Provide alerts and notifications for deviations from predefined ESG thresholds or targets, enabling timely intervention to address potential issues.
9	Integration with ESG data sources	Integrate with external ESG data sources, such as energy utilities or emissions reporting systems, for a more comprehensive view of the organization's ESG performance.
10	Benchmarking and analytics	Support benchmarking of ESG performance against industry peers and historical data, as well as predictive analytics for forecasting future ESG performance based on current trends and patterns.