Performance Metrics and Monitoring Tools for Sustainable Network Management

Literatür Makalesi/Review Article

İbrahim Özden DUMAN[1], Uğur ELİİYİ[2]

[1] Department of Computer Science, Graduate School of Natural and Applied Sciences, Dokuz Eylül University, İzmir, Turkey
[2]Department of Business, Faculty of Economics and Administrative Sciences, İzmir Bakırçay University, İzmir, Turkey
networker1903@gmail.com, ugur.eliiyi@bakircay.edu.tr
(Geliş/Received:14.08.2020; Kabul/Accepted:13.12.2020)
DOI: 10.17671/gazibtd.780504

***Abstract*—** Network infrastructures comprise the backbone of our modern life, ranging in scale from relatively micro-level settings of offices or university campuses, to macro-level structures such as smart cities or national defense systems. Consequently, effective management of the quality and sustainability of provided services and network infrastructures has grown to be essential for modern service providers. Considering standard features like reliability, availability and maintainability, several questions are identified in this study for network performance management and investment levels of sustainable network infrastructures. We describe various stages of the performance management processes, along with corresponding software tools to measure network efficiency and sustainability for information and communications technologies. Fundamental key performance indicator categories and their definitions are also compiled according to their functions within the network management context. Depending on the importance of services provided on a network, it is necessary to develop different performance management systems for monitoring the infrastructure for different practitioners. The development of required management systems will be possible by integrating the comprehensive compilation of indicators and software tools presented in this study.

***Keywords*—** network infrastructure, key performance indicator, network management, network efficiency, network sustainability, performance monitoring.

Sürdürülebilir Ağ Yönetimi için Performans Metrikleri ve İzleme Araçları

***Özet*—** Ağ altyapıları, görece mikro ölçekli ofis veya üniversite kampüslerinden makro ölçekli akıllı şehirler veya ulusal savunma sistemleri gibi yapılara kadar değişen büyüklükleri ile modern yaşamımızın omurgasını oluşturmaktadır. Buna bağlı olarak sağlanan hizmetlerin ve ağ altyapılarının kalitesinin ve sürdürülebilirliğinin etkin yönetimi modern hizmet sağlayıcılar için vazgeçilmez hale gelmiştir. Bu çalışmada güvenilirlik, kullanılabilirlik ve sürdürülebilirlik gibi standart özellikler göz önünde bulundurularak ağ performans yönetimi ve sürdürülebilir ağ altyapılarının yatırım seviyeleri için çeşitli sorular belirlenmiştir. Aynı zamanda ağ verimliliğini ve sürdürülebilirliğini ölçmek için kullanılabilecek yazılım araçlarıyla birlikte performans yönetimi süreçlerinin çeşitli aşamaları açıklanmıştır. Bilgi ve iletişim teknolojileri için temel anahtar performans göstergesi kategorileri ve tanımları çalışmamızda ağ yönetimi bağlamındaki işlevlerine göre derlenmiştir. Bir ağ üzerinde sağlanan hizmetlerin önemine bağlı olarak farklı uygulayıcılar için altyapının izlenmesine yönelik farklı performans yönetim sistemlerinin geliştirilmesi gereklidir. İhtiyaç duyulan yönetim sistemlerinin geliştirilmesi bu çalışmada kapsamlı bir şekilde derlenmiş gösterge ve yazılım araçlarının entegre edilmesi yoluyla mümkün olabilecektir.

***Anahtar Kelimeler*—** ağ altyapısı, temel performans göstergesi, ağ yönetimi, ağ verimliliği, ağ sürdürülebilirliği, performans izleme.

1. INTRODUCTION

Due to ongoing development of information and communications technologies (ICT), many things have changed in the daily life of societies around the globe. People rely more and more on technology, both in their personal lives and in the cities where they live. This heavy reliance and the ever-increasing demand for digitalized services brought together a matching and continuous increase in the supply of such services; and accordingly rendered the digitalization of more and more analogue services as inevitable. Consequently, many things have become easier in the everyday life. Today, people can access the information they need from the comfort of their homes with a few keystrokes via the internet. The once intricate and lengthy process of correspondence (by letters, telegrams and post) is now at light speed and performed with much fewer words. Accessing any required services and goods has become so much easier via the developing technology and the adaptation of the economic market to the new rules of this technology.

As a direct result of this growing demand and supply of digitalization, the quality and sustainability of provided services and network infrastructures have become critical. In order to ensure customer satisfaction, the service provider is required to deliver and maintain services of a certain quality. The maintenance of a standard quality level is especially challenging as the Quality of Experience (QoE) is highly relative and based on personal user experience [1].

Any component within the network infrastructure of a provided service may affect quality. In the process of conveying digitalized services to people's homes, the number and variety of such components are massive, comprising of all constituents within the electrical infrastructure, the system infrastructure and the network infrastructure. In order to deliver the required services, a secure and stable communications network infrastructure should be built and continuously improved in accordance with requirements of growing demand. Communications network infrastructure has many components such as cable substructure, network devices, servers, connection speed etc. In order to be able to accurately measure factors affecting the performance of a service within a network infrastructure, it is necessary to evaluate the performance of all its components.

If a sustained quality of service is aimed while fulfilling requirements of the service recipients, the communications network infrastructure needs to be designed, planned and installed based on gathered information and necessary levels of related performance indicators. If an infrastructure investment is made without estimating the needs of the supplied service, either excessive budget or under-allocation of resources may result in subpar service quality. The same unwanted consequences may also occur if the investment is made without considering how long the service will be provided for. With the above motivation, we focus on a comprehensive compilation of key performance indicators (KPI) for sustainable communications network management in this study, through a characterization of the metrics for devices within the network infrastructure. We also identify and establish factors that affect the quality of service within communications networks. In this respect, our study is intended to be a guide for industry practitioners and researchers within this area.

For a better understanding, we identify some example questions to be answered for obtaining a healthy infrastructure and an appropriate investment level in Section 2. We also review the related literature on performance metrics for communications network infrastructure. In Section 3, various management functions of the network infrastructure are presented, along with related software tools. A compilation of crucial KPIs for the ICT infrastructure and their definitions are presented in Section 4. Finally, conclusions and possible research extensions are discussed in the last section.

2. EXAMPLE QUESTIONS AND ASSOCIATED LITERATURE

In order to initiate the best-fitting infrastructure for the intended service and to evaluate its compulsory financial requirements, the questions in the following subsection need to be answered carefully.

2.1. Questions for Infrastructure Design

We include an example service as online ticket sales, and provide illustrative answers to the posed questions for designing the network infrastructure.

- What is the service to offer? (e.g. online ticket sales)
- How many people are expected to be served on average daily? (e.g. 1000 people)
- How many people are expected to be served on average daily within the next year? (e.g. 2000 people)
- What data size will a single process require on the application? (e.g. 200 kbit)
- How many people are expected to be served at the same time? (e.g. 200 people)
- How much bandwidth will be consumed by the people served at the same time? (e.g. 20 Mbit)
- How much data storage needs to be allocated daily? (e.g. 10 GB)
- What are the expectations for CPU (Central Processing Unit) consumption and RAM (Random Access Memory) usage when the service is used at its maximum level? (e.g. 60% and 20 GB, respectively)
- How much traffic will the maximum service generate in the internal network? (e.g. 400 GB/s)
- How much reading speed is expected on the storage with maximum service? (e.g. 2 GB)

The answers to the above and other relevant questions should be obtained for each service provided. The collected

aggregate information provides a basis for the investment estimate for the infrastructure, together with scalability forecasts for the yearly demand increase. An average five-year planning horizon should be respected for infrastructure planning. This is due to the fact that, even if the offered services might differ or evolve during this time period, new services can be offered without the need for substantial additional investment. This issue is of critical importance in terms of manageability, time, and budget savings.

While planning the infrastructure, it is also necessary to consider the following questions for design and planning of the central system room.

- How many cabinets will be needed?
- How much physical space will be needed for the cabinets in the system room within five years?
- How many racks will be needed in the cabinets within a year?
- How many racks will be needed in the cabinets within five years?
- Where (on which floor) should be the system room located?
- How much cooling will be needed in five years of growth?
- How much voltage or current will be needed within a year?
- How much voltage or current will be needed cabinets within five years?
- How will the energy redundancy be provided?
- How will the redundancy provided be able to back up the five-year power requirement?

According to the answers of the above and any other relevant question, the electrical design, needs of the UPS (Uninterruptable Power Supply), generator needs, the number and shape of cabinets, and the cooling system needs can be determined. In addition, open-source or commercial software applications can be used for managing the central system rooms for monitoring energy and cooling information.

2.2. Relevant Literature

The literature on performance monitoring and performance indicators for the network infrastructure is rather scarce. In this section, we include the most relevant existing work within the context of our study.

McGill [1] investigated a class of network performance measures, regarded as Quality of Service (QoS) parameters. Measurement difficulties of user satisfaction and application performance were mentioned in the study. The author stated that performance problems experienced in the application were not generally known until the user complained. The study aimed to obtain some quality of experience (QoE) indicators via using the current network performance measures (QoS values), and stated that these new measures offer a more user- or application-centric means of assessing the network performance. The author also identified the difficulties of demonstrating QoE as a KPI, and suggested monitoring of more than one metric so that network problems can be predicted.

Another study involved performance indicators for the case of the city of London [2]. Five performance keys were defined in the study as network connectivity, data center capability, electrical power supplies, security and resilience, and finally skills. The aim was to create a suitable model for the ICT infrastructure planning and development for sustainable cities. The study focused on networks, data centers and energy consumption. Formulas were provided to evaluate capacity, utilization and energy consumption, as well.

Another study focused on calculating system accessibility [3]. The authors stated that the accessibility of the system is the first and foremost critical issue to be considered in practice. The study also included definitions for MTBF (Mean Time between Failures) and MTTR (Mean Time to Repair) as measurement tools, and stated that the probability of failure of a system can usually be measured using these measures. As a result of their analysis, the authors have reached the following conclusions: (1) The higher the MTBF value, the higher the reliability and usability of the system. (2) MTTR affects availability; if a system takes a long time to recover from a failure, the system will have a low availability. (3) High availability can be achieved if MTBF is too large compared to MTTR.

A framework for developing Key Performance Indicators (KPIs) for measuring the ICT service quality (ICTSQ) was proposed in [4]. In addition, the authors conducted a study that provided a list of KPIs of relevance to measure ICTSQ. One of their primary objectives was to measure the performance of information and communication technologies with the prepared KPIs. Properties of good indicators were defined also in [5]. The authors claimed that the infrastructure capacity was created or increased in constant increments, often for practical and cost-efficiency reasons. They also provided examples of indicators for the existing infrastructure and explained technical difficulties about these indicators.

Green KPIs for information technology (IT) infrastructures were developed in [6]. Three layers were identified in their study as the technical layer, the information layer and the business layer. Specific metrics for these layers were designed. In particular, the study focused on energy efficiency and KPIs related to energy efficiency. Another article examined some widely used metrics such as reliability, fault tolerance, reliability and security [7]. The study also provided a systematic approach for determining the complementary properties of these metrics. The metrics at the infrastructure level were classified as measurable and not measurable, and a method was proposed to determine the information security metrics.

Performance metrics were identified as important decision tools in the design, analysis, operation and management of

telecommunication systems in [8]. It was stated that the metrics are used as BPIs (Basic Performance Indicators) and are vital for defining SLA (Service Level Agreement). While BPI metrics are often chosen by customers to increase system or service adoption rates, the authors emphasized that SLA metrics were developed to control contractual agreements between service providers and end users. Frameworks related to the development of metrics were also examined. A compilation and classification of metrics used in network engineering were attempted, however, as many metrics are in use, a full compilation has not been considered as practical. Instead, the most frequently used metrics were identified and gathered under certain headings.

As a result of the review of literature and analysis of existing work, our study is the first in literature to compile a large variety of performance indicators in a systematic fashion to the best of our knowledge. Therefore, we intend for it to bring a significant contribution to the related literature.

3. MANAGEMENT OF THE NETWORK INFRASTRUCTURE

Trained manpower is essential for monitoring a network infrastructure and for timely response to problems. It is also necessary to provide uninterruptedness and redundancy in the skilled crew. Establishing such a Network Operation Center (NOC) crew, in which each person is licensed in a specific area, is critical. While designing the skill sets for the members of the crew, a person with expertise in a specific area can also be used as a substitute specialist in a different area. Hence, each member of the crew will have one core and one secondary specialization and each device in the infrastructure will have master and backup experts.

As an example, let crew member X be the master specialist of device A and the backup specialist of device B. In this case, when the master specialist of device B is not available for any reason, crew member X is able to manage and monitor device B and uninterrupted service can be supplied, as malfunctions are intervened rapidly. In this manner, dependency on stakeholders who are active in the establishment and management needs of the infrastructure are reduced. Once a system depends less on stakeholders and is better known by its decision makers, the quality of service levels increases inevitably.

It is also critical to ensure the continuity of the crew's knowledge via continuous training for the devices and technology within the network. In addition, using a ticket system to effectively monitor network problems, and applying SLA times can ease operations and facilitate business cycles. In order to manage the network effectively, it is necessary to perform the steps in the following subsections with the help of a software tool or manually.

3.1. Fault Management and Configuration Management

In order to ensure effective management and continuity of network components, errors occurring in the system must be stored and classified according to their criticality. Certain Simple Network Management Protocol (SNMP) management tools (e.g. Zabbix [9]) can be used to effectively monitor fault management.

All changes to the setting and configuration of the files within network devices and services must be recorded with great care. This will allow the network to make immediate returns to back-up configurations in potential threat situations and faults. For example, Figure 1 depicts some example displays of KPIs on an SNMP tool running on a metropolitan city network infrastructure.

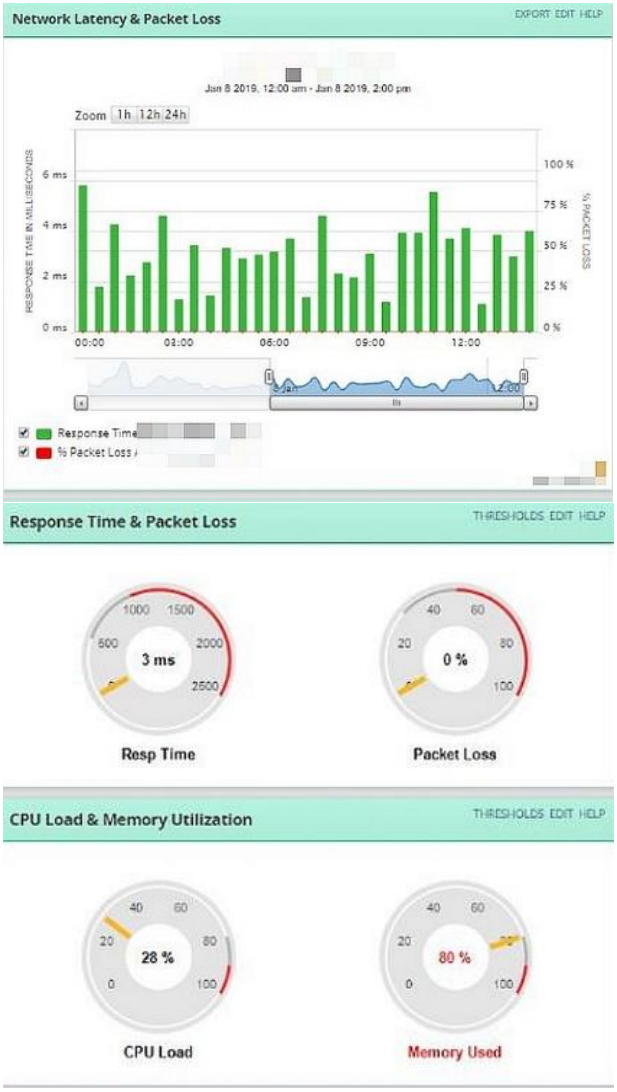

Figure 1. Example displays of KPIs on an SNMP tool

In Figure 1, it can be observed that the response time obtained through the SNMP software increases between 09:00 and 12:00, which are the working hours. However, no packet loss is observed, and the use of CPU and RAM seems to be normal during this period. Through such continuous monitoring of custom KPIs with appropriate

software, possible threats and problems can be predicted and timely precautions can be taken. The general condition of the network infrastructure can also be assessed by evaluating the data obtained from the indicators on a daily, weekly, monthly, and yearly basis.

3.2. Accounting Management

The usage rates of network-related links can be regularly monitored through accounting management. Hence, the usage rates of lines and specific users can be identified. Open source products such as MRTG, Cacti, Nagios and Zabbix can be used for these purposes. In particular, Zabbix can be used for Network monitoring, and MRTG for bandwidth monitoring.

In addition, the data traffic that flows through the network can be analyzed based on IP and protocol. Netflow developed by Cisco is used for such operations. The same technology is available under different names such as Juniper-Jflow and HP-Sflow, as well.

The benefits of the flow protocols can be identified as follows:

- The impact of new services on the network is visible.
- It is possible to identify users who use bandwidth the most (top talkers).
- Inappropriate internet traffic can be detected and unnecessary new investment can be prevented.
- DoS attacks can be detected.

3.3. Performance and Security Management

Performance monitoring of all network components with parameters such as service, device, link, Round Trip Time (RTT), package loss or delay is one of the most important steps in network management. This step must be effectively followed by the NOC team for service quality and customer satisfaction. It is also very critical to provide software and systems such as antivirus, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) by following the patches for all network and system components in the infrastructure. The traffic in the network should be checked via a Firewall, as well. The physical security of places where devices are located should be ensured. Particularly, the physical safety of devices that are dispersed to different points within a city should be warranted, as the security of these endpoints will pose a risk to central security. Compliance with the ISO (International Organization for Standardization) 27001 certification to facilitate operations can be of great benefit in managing the overall security of the infrastructure.

Tables 1 through 5 provide an extensive list of commercial and free software tools for performance management. Software tools that facilitate management of the above steps are listed in these tables, as well as tools for monitoring environmental factors such as energy and

Table 1. Data center management software

Data Center Management Software	**Type**	**Features**
OpenDCIM (Free) [10]	Data center infrastructure management	Web Based
		Asset Tracking
		Capacity Management
		Fault Tolerance Tracking
		Tracking of Cable
		Power Connections
dcTrack (Paid) [11]	Data center infrastructure management	Environment Monitoring
		Energy Management
		Power Management
		PDU Management
		Thresholds and Alerts
		Smart Rack View
		Real-Time Dashboards
Power IQ (Paid) [12]	Data center energy management and power monitoring	Asset Management
		Capacity Management
		Change Management
		Energy Management
		Environment Management
		Power Management
		BI & Analytics
		Connectivity
		Power Management
		Security
Txture (Paid) [13]	Data center energy management	Application Portfolio
		Application Capability
		Technology Portfolio
		Solution Architecture

Table 2. Helpdesk and log management software

Helpdesk and Log Management Software	**Type**	**Features**
OTRS (Free) [14]	Helpdesk ticket tracking system	Ticket Management
		Security & Permissions
		Automation & Processes
		Time Management
		Customer Management
		Knowledge Management
		Reporting
Request Tracker (Free) [15]	Helpdesk ticket tracking system	Assets
		Time Tracking
		Task Priority
		Translation
GLPI (Free) [16]	Helpdesk ticket tracking system	ITIL V2 Compatible
		Asset Management
		Data Quality Control
		Software Inventory
		License Management
		Knowledge Base
Kiwi syslog (Free) [17]	Log management software	High-Traffic Alerts
		Real Time Statistics
		Daily Statistics
ELK Stack (Free) [18]	Log management software	Alerting
		Security
		Monitoring
		Machine Learning
		SQL Search

cooling that can be effective in operations. The brand name of the related software as well as information on the management type and key features provided are presented. The paid/freeware distinctions are also included.

Table 1 exhibits the prominent data center management software with their available features, whereas Tables 2 through 5 provide software applications for other functions of the network infrastructure. These include helpdesk and log management, network monitoring, application and flow monitoring, and security management. Using the software in these tables, potential problems in the network regarding resolution times, general status, application accessibility rates and security risk scores can be monitored. In addition, these software tools can provide ICT managers with decision support on equipment to be used for administrative purposes, staff performance, etc.

Table 3. Network monitoring software

Network Monitoring Software	**Type**	**Features**
MRTG (Free) [19]	Network monitoring	Monitoring Network Devices
Cacti (Free) [20]	Network monitoring	User Management
		Monitoring Network Devices
Zabbix (Free) [9]	Network monitoring	Monitor Anything
		Network Monitoring
		Servers Monitoring
		Applications Monitoring
		Services Monitoring
		Web Monitoring
		Storage Devices Monitoring
		Virtual Machines Monitoring
		KPI/SLA
		Security
Solarwinds (Paid) [21]	Network monitoring and management	Network Management
		System Management
		Database Management
		Configuration Management
		Network Automation Manager
		IT Security
		Netflow Traffic Analyzer
		Application Performance Optimization
		Flow Monitoring
ManageEngine (Paid) [22]	Network monitoring and management	Network Performance Monitoring
		Hardware Monitoring
		Server Monitoring
		Firewall Log Management
		Network Configuration Management
		Application Management
		IP Address Management
		Netflow
		Flow Monitoring
Cisco Prime (Paid) [23]	Network monitoring and management	Data Center Management
		Network Monitoring
		Intelligent WAN Management
		Netflow
		Application Performance Monitoring
		UCS (Unified Computing System) Support

Table 4. Application and flow monitoring software

Application and Flow Monitoring Software	**Type**	**Features**
Nagios (Free) [24]	Service and application monitoring	Network Flow Monitoring
		Server Monitoring
		Application Monitoring
FlowScan (Free) [25]	Flow monitoring	Network Flow Monitoring
NPROBE (Free) [26]	Flow monitoring	Packet Capture
		Traffic Recording
		Network Probe
		Traffic Analysis

Table 5. Security management software

Security Management Software	**Type**	**Features**
Apache Metron (Free) [27]	Security analytics	Real-Time Big Data Security
		Threat Intelligence
		PCAP Replay
		Evidence Store
		Hunting Platform
		Security Data Lake
		Pluggable Framework
Cyphon (Free) [28]	Security threat intelligence	Aggregate Data
		Custom Alerts
		View Incidents by Criticality Level
		Categorize and Prioritize
		Investigation
		Ticket Create, Block IP etc.
GOSINT Framework (Free) [29]	Security threat intelligence	Searching/Sorting İndicators
		Investigation
		Threat İntelligence
AlienVault OSSIM (Free) [30]	Security management	Asset Discovery
		Vulnerability Assessment
		Intrusion Detection
		Behavioral Monitoring
		SIEM Event Correlation
Security Onion (Free) [31]	Security management	Security Monitoring
		Log Management
		Includes many security tools
Bro IDS (Free) [32]	Network intrusion detection and prevention	Intrusion Detection System (IDS)
		Traffic Analyzer
		Statefull
		Forensics
Snort (Free) [33]	Network intrusion detection and prevention	Intrusion Prevention System (IPS)
		Intrusion Detection System (IDS)
		Realt-Time Analyze
		Packet Logging
Suricata (Free) [34]	Network threat detection	IDS / IPS
		Automatic Protocol Detection
		Lua Scripting
Ossec (Free) [35]	Host-based network intrusion detection system	Host Based IDS
		Real-Time Analystics
		File Integrity Monitorinig
		Log Monitoring
		Rootcheck
		Process Monitoring

Besides the tools presented in Table 3, interoperable measurement frameworks such as perfSONAR are deployed for the detection and diagnosis of anomaly events that may cause capacity bottlenecks for crowded services [36].

In addition to employing the software provided in this section, compliance with certifications such as ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information and Related Technology) in operations of the NOC crew can enable the ICT services to be provided at a more professional level [37, 38].

4. KEY PERFORMANCE INDICATORS FOR SUSTAINABLE NETWORK MANAGEMENT

It is more difficult to ensure the continuity of a system than to install it. In systems that cannot be tracked, there is usually no information about application performance of the NOC until a customer (using the service) complains. For a system to be sustainable, it must be measurable and traceable. As what gets measured gets managed, traceability and measurability are key issues in assuring system sustainability.

In today's technology it is not sufficient to manage the ICT infrastructure at the device level only. Applications such as database, http, video, etc. also need to be monitored [1]. For example, the impact of different tunneling mechanisms may vary for different application types [39]. While the performance of indicators is difficult to follow on the application side, performance monitoring on network devices is often easier. In order to manage the ICT infrastructure well and to use it efficiently, it is imperative to design customized KPIs for the infrastructure and the provided services. Such indicators are designed to improve the performance of the infrastructure and keep it at a certain level, as well as facilitating further development of infrastructure investments and policies. The designed KPIs should be compatible with the advancing technology. The interruption tolerance of the services should also be considered while designing the KPIs.

Conforming to the answers to the following basic questions can lead designers to compile an effective and sustainable list of KPIs to monitor:

- What to measure?
- Why to measure?
- Who to measure?
- How to measure?

In addition, good indicators should have the following properties:

- Easy calculation
- Data availability and quality
- Simplicity and transparency

While designing the indicators, the main challenges to be addressed by the service providers are as follows.

- Extending the life of an implemented solution
- Increasing the continuity of a solution
- Ensuring flexibility and agility in new types of services
- Ensuring flexibility in system capability and capacity at a low cost
- Warranting system, hardware and software continuity
- Securing continuity of the human resources
- Ensuring budget continuity

In the following subsections, we present a comprehensive compilation of the principal KPIs along with their definitions for managing sustainable network structures.

4.1. KPIs for the ICT Infrastructure

Several indicators are used for assessing ICT infrastructure performance. We present the definitions of the most crucial ones in this section [40, 41].

Availability:

Availability of an ICT infrastructure is defined as the ratio of the period in which the provided service is not interrupted in a time interval to the total duration of that interval. In other words, it is the uptime divided by the total of uptime and downtime of a system. It is one of the most important indicators and directly affects customer satisfaction. However, it is not realistic to expect the same availability rates for all components in a system or network. For example, 99.9% continuity in the backbone can be expected, but this level of availability might not be required or realized at the endpoints. This indicator can be calculated weekly, monthly and annually using the following formula:

Availability=MTBF/(MTBF+MTTR), where

MTBF: Mean time between failures, calculated as the total hours of operation divided by the total number of failures; and *MTTR*: Mean time to restore function (repair).

The *MTBF* is a frequently recommended indicator for the success of equipment regarding functional performance and capacity adequacy. The *MTTR* can be divided into several components according to the number of stops/failures within the system. By analyzing the components corresponding to stops separately, it can be easier to find solutions to problems through incremental improvements in each stop. Note that, as the *MTBF* value approaches infinity or when *MTTR* is near zero, availability will approach to 100%. For an accurate calculation of *MTTR*, it is vital to consider the failover time's effect on the *MTTR* in cluster configurations on the devices. While these mere seconds may not be important for small centers, they

could be very significant for large data centers trying to provide 99.9% availability to their customers.

It is also possible to estimate the yearly interruption hours of the infrastructure using a desired uptime rate. For example, up to how many hours can the interruptions be allowed per year to achieve a 99.9% availability guarantee? As there are 365x24 = 8,760 hours per year, the maximum yearly total of interruptions should be 8,760x0.1% = 8.76 hours. The desired uptime of devices can also be considered as a sub-KPI of availability.

Reliability:

Reliability measures the possibility that any component, device or service may be interrupted in a unit of time. The most frequently used function in life data analysis and reliability engineering is the reliability function. The function gives the probability of a device performing its intended purpose under given operating conditions and environments for a specified length of time without any failures. As such, reliability is a function of time, in that every reliability value has an associated time value. In other words, one must specify a time value with the desired reliability value, i.e. 95% reliability at 100 hours. Note that the delays due to high traffic within the storage will decrease the reliability ratio.

Capacity Utilization:

This KPI is used to monitor the rate at which devices in the infrastructure are used. More effective results can be achieved by creating thresholds for capacity utilization regarding the criticality of the servers and the network devices. The capacity utilization in terms of time can be calculated using the following formula:

Capacity Utilization = Used Time / Total Time

Note that, the capacity utilization should not only be recorded for devices but also for components within each device, such as CPUs, RAMs, links or buffers.

Capacity utilization can also be calculated as:

Capacity Utilization = Actual Output / Potential Output

Link Capacity Utilization:

This KPI can be considered as a sub-KPI of *capacity utilization*. It is a very important metric, which affects the performance of the services offered. The high rate of link usage on the backbone or at the node transition points spreading to different locations in a city will affect the overall performance. As an example, 100% linking at the at the end nodes in the field will affect the system performance negatively, even if the use of link on the backbone network device in the central system room is as low as 30%.

Latency:

The *latency* is the total delay in the transmission of a message over a connection, i.e. it is the time interval between the stimulation and response. It typically refers to delays in transmitting or processing data, which can be caused by a wide variety of reasons. The delay of a few seconds does not cause any problems during the load of an internet page or during the opening of an application, whereas such latencies might cause problems for delay-sensitive applications such as video conferencing or financial transactions.

Latency is also computed as the sum of *transmission and propagation delays*, which are defined below.

Transmission Delay:

The *transmission delay* (or *store-and-forward delay*, also known as *packetization delay*) is defined as the elapsed time for the transmission of an m bit-data to the transmission link. In other words, it is the delay caused by the data-rate of the link. It is usually expressed as:

$TD = m/r$,

where m is the number of data bits sent, and r represents the data rate in bits per second indicating the bandwidth of transmission.

It is obvious from the formula that a connection of 100 Mbps will generate a much less delay for the same amount of data from a 10 Mbps connection. Hence, increasing the transmission capacity reduces the transmission delay.

Propagation Delay:

This delay defines the time taken for data in the transmission channel to reach to the destination point, i.e. it is the amount of time it takes for the head of the signal to travel from the sender to the receiver. The *propagation delay* is equal to the distance (d) between the sender and receiver (in meters), divided by the speed (s) of the electromagnetic wave (in meters per second):

$PD = d/s$.

For example, if the source and destination are in the same building at 200 m from one another, the propagation delay will be around 1 microsecond. However, if they are located in different countries at a distance of 20,000 km, the delay will be in the order of 0.1 seconds. Hence, the main reasons for delay are usually long links and low data rates. The amount of data that the line stores or carries can be computed as the data rate multiplied by the propagation delay.

Queuing Delay and Processing Delay:

The *queuing delay* is defined as the waiting time of packages in front of other packages. Each point passed has a certain processing and packet sending capacity. If more packages are received than capacity, they are kept in memory as they cannot be processed immediately. This is called *queuing delay* due to the wait in line to be processed. In short, it is the time it takes for the packet to be sent from the link and depends on the number of pending packages. If there is no pending packet, the delay will be zero.

Queuing delay is directly related with traffic intensity on the network, which is La / R, where a is the average arrival rate of packets (packets/s), R is the transmission rate (bps), and L is the average packet length (bits). As traffic intensity approaches 1, the queue delay time increases and packet drops start after a certain threshold, as shown in Figure 2.

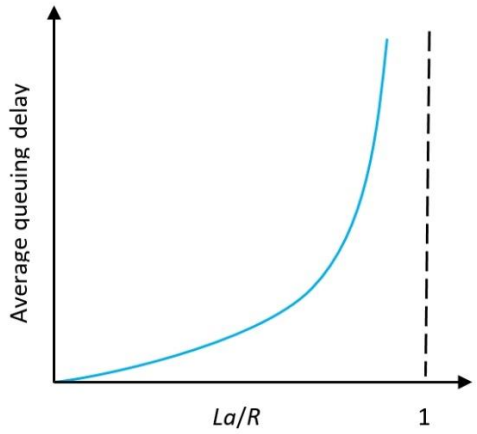

Figure 2. Traffic intensity vs. average queuing delay

The *processing delay* (*PrD*) is the time it takes routers to process the packet header. Processing delay is a major element in the overall network delay, as well.

Nodal Delay:

The *nodal delay* is the sum of transmission, propagation, queuing and processing delays in a network. The contribution of these delay components can vary significantly. Algebraically, the nodal delay (*ND*) is expressed as:

$$ND = TD + PD + QD + PrD$$

End-to-End Delay:

The *end-to-end delay* is the total time it takes for a packet to be sent through a network. As each router may have its own delay, this KPI only yields an estimation, and is formulated as follows.

$$End\text{-}to\text{-}End\ Delay = n(TD + PD + PrD),$$

where n is the number of links (number of routers - 1).

The *end-to-end delay* differs from the *round-trip time* (*RTT*), since only a one-direction path from the source to the destination is measured.

Round-Trip Time:

The *round-trip time (RTT)* is the duration it takes for a network request to go from a source to a destination and back again to the starting point. The *RTT* is measured in milliseconds (ms). It is an important KPI in controlling the health of a connection, and is commonly utilized by network administrators to diagnose the speed and reliability of their network connections.

RTT is simply the time between the transmission of the target and the acknowledgement (ACK). The *ping* utility, which is available on effectively all computers, is a method of estimating *RTT*. Besides, alternative architectures are proposed for passively measuring this indicator more accurately [42].

Throughput:

The *throughput* is one of the most important KPIs to be monitored for internet networks and critical devices. This KPI defines the total amount of data transferred per second in a network and can directly affect the performance of offered services. Suppose a file transfer from point A to point B. In such a case, *throughput* (in bits/s) is the rate at which host B receives the file at any time, computed as:

$$Throughput = sa/t,$$

where s is the number of successfully sent packets, a is the average packet size, and t is the total time spent in delivering all packages. Figure 3 depicts an example for computing throughput on a network.

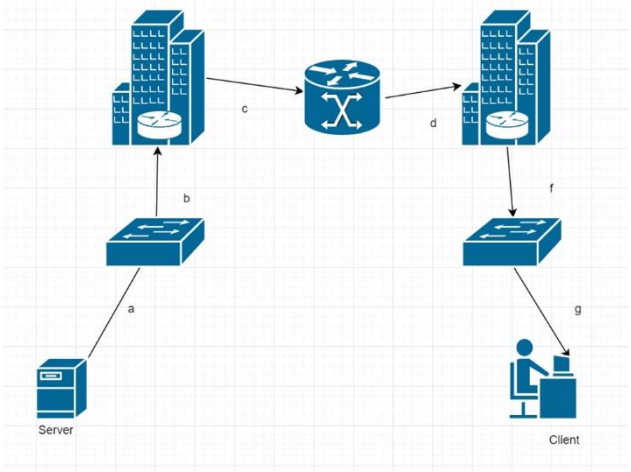

Figure 3. An example for throughput

In Figure 3, a, b, c, d, e, f and g represent the throughput values of the links between devices. If d <c, this means that the link with throughput c is sending traffic to the network at its own bandwidth, however the link with throughput d will not be able to match it at the same rate and the queueing process starts on the router. If d > c on the other hand, there will be no queueing on the router. In the connection between the server and the client, the smallest throughput among all links will determine the throughput value of the connection.

Throughput can be tested with iPerf [43] or JPerf [44] software. As the software's server application is run on the server side and the client runs the client application, throughput testing can be performed. Figure 4 illustrates sample throughput values taken from the same metropolitan city network as in Figure 1.

Figure 4. Monitoring throughput on an SNMP tool

In Figure 4, the blue plot shows the download amount, whereas the green one illustrates the amount of upload. It is observed that the amount of download is doubled on some days of the week. When such a change is observed, the reason for this change should be investigated in order not to have any performance problems. Unmonitored and unexplored changes might cause unpredictability for the network administrator. It is possible to follow throughput with MRTG and Cacti software, as suggested in Table 3.

Jitter:

The *jitter* is basically wave distortion. The definition of jitter in the network domain is the difference in delay times of the packets. Jitter expresses the difference between the time elapsed during the transmission of packets of the same type between the source and the target. Namely, it is the deviation from true periodicity of a presumably periodic signal.

Jitter is a meaningful metric for audio and video services as these services are sensitive to delay. It is a problem when the receiver cannot receive even intervals because of network congestion, incorrect queuing, etc. while the sender is sending packets at even intervals.

Packet Loss:

The *packet loss* is the performance metric that expresses whether a packet is successfully transmitted to the point it was supposed to. It occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is calculated as a percentage of the packets lost with respect to the packets sent. The header sequence number in the packets is used to keep track of the connection between two points. The formula for this KPI is:

Packet Loss (%) = 100 (Number of Packets Lost / Number of Packets Sent).

Service Load:

The *load* refers to the amount of data (traffic) being carried by the network. One can evaluate the network congestion and performance using the load on the service devices. As an example, it is possible to see the load status of the provided link in Cisco Switch using the following command:

Show interface eth1/1.

Bit Error Rate:

The *bit error rate (BER)* is used to determine whether data is transmitted reliably from one point to another via the digital communication link. *BER* is calculated by comparing the transmitted sequence of bits to the received bits and counting the number of errors. The ratio of how many bits received in error over the number of total bits received defines *BER*. This KPI is affected by many factors including lost packets and jitter.

Service Quality:

The term *service quality* may include many parameters. For example, if a customer is guaranteed a 100Mbit internet connection by a service provider and the average download falls to 20Mbits, one cannot talk about the quality of this service. This KPI can in fact be deemed as a composite of all other KPIs in this section. To be able to measure the *Quality of Service (QoS)* quantitatively, several related KPIs should be computed, such as packet loss, bit rate, throughput, transmission delay, availability, jitter, etc. Hence, the *QoS* provides a representation of the overall performance of a service.

The Two-Way Active Measurement Protocol (TWAMP), which is an open protocol for measuring network performance between any two devices, can be used for measurement in the above service provider example. Several KPIs such as RTT, latency, service load and throughput can be followed via TWAMP.

The KPIs described in this section for evaluating the ICT infrastructure performance along with other related indicators can be seen in Table 6.

4.2. Other KPI Categories

The previous section presented many KPIs specific for the ICT infrastructure. There are also numerous KPIs that can be categorized under the headings in Table 7, such as KPIs specifically designed for the system room performance, KPIs regarding human resources or the NOC.

In this section we compile main KPIs under these headings. Under the *ICT (general)* category, some composite indicators can be counted as:

- Availability
- Reliability
- Scalability
- Security
- Interoperability
- Maintainability
- Recoverability
- Documentability
- Sustainability

Table 6. KPIs for the ICT infrastructure

KPIs for the ICT Infrastructure	
Availability	Packet Drops
Reliability	Packet Queue
Link Capacity	Nodal Delay
Latency	End-to-End Delay
Throughput	Internet Bandwidth
Jitter	Total Internet Bandwidth
Lost Packets	Traffic Sent
RTT (Round Trip Time)	Traffic Received
Load	Unplanned Unavailability
BER (Bit Error Rate)	MTTD (Mean Time to Detect)
Service Quality	Max Internet Utilization
Packet Errors	Min Internet Utilization
Packet Discards	Transfer Speed
Propagation Delay	Application Response Time
Queueing Delay	Buffer
Reachability	Serialization Delay

Table 7. Other KPI categories for ICT

ICT (general)
ICT Equipment
ICT VOIP/Video
Backup and System Room
Demand for ICT
Human Resources / Helpdesk / NOC
IoT Devices
Safety and Security
Energy

As these general measures are composite and usually very difficult to monitor and control, the KPIs explained in the previous section are most commonly used as their estimators. Under the *ICT Equipment* category, the following KPIs should be utilized for monitoring performance:

- Capacity, RAM and CPU utilization
- Average storage utilization and capacity
- Maximum and minimum storage utilization
- Server processor, RAM and storage usage
- Server network usage and network capacity
- Number of physical servers, routers and firewalls
- Number of layer 2 and layer 3 switches
- Service life of facilities, hardware and cabling
- Number of installed ports
- Average storage disk read/write times
- Average storage disk transfer rate
- Maintenance cost

KPIs for the most commonly used *ICT VOIP/Video* performance are as follows:

- MOS (Mean Opinion Score)
- Voice network availability and performance
- Time of voice network return to service
- Voice network utilization
- CBR (Constant Bit Rate)
- VBR (Variable Bit Rate)

For evaluating the performance of the *Backup and System Room*, decision makers can employ the following KPIs:

- Backup capacity
- Percent success rate of backup operations
- Average time to restore backup
- Network equipment config backup
- Critical data backup
- Cost of system room infrastructure
- Percent usage of data center floor area
- Percent usage of data center cabinet space
- Total data center floor area and cabinet space
- Average data center rack utilization
- Cooling and cooling capacity
- Air quality and CO_2 footprint
- Power connectivity
- Temperature of the system room and the hardware
- ICT equipment software version

The temperatures in the system room can be monitored both for the room and for each device via data center management software with the help of the SNMP protocol. Figure 5 shows an example monitoring of the *Cooling* KPI. It is very important for continuity to monitor temperature and cooling of the system room and the devices in it.

Demand for ICT can be measured or estimated using the following indicators.

- Throughput peak demand
- Total internet bandwidth demand
- General network demand
- Server network, processor and RAM demand
- Daily application storage and processing demand

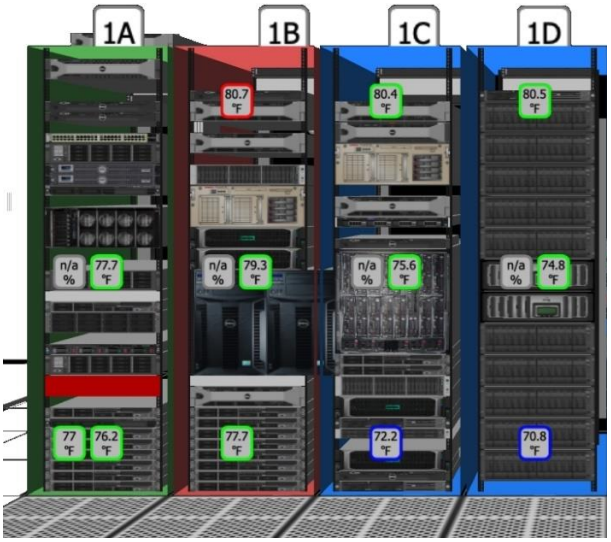

Figure 5. Monitoring cooling on the DC Management Software [11]

KPIs for *Human Resources / Helpdesk / NOC* are numerous and listed below. Important information regarding the performance of the call center and the network operation taskforce can be obtained periodically through a statistical evaluation of these measures [45].

- Number of hours spent in IT training
- Number of technical experts
- Number of helpdesk tickets per year
- Percent helpdesk availability
- Helpdesk response performance
- Technical support availability
- Work order request/customer assistance performance
- Number of customers with multiple tickets
- Average number of incoming calls
- Average rate of incoming calls
- Average speed to answer incoming call
- Percent calls transferred
- Percent callers with satisfaction surveys
- Percent of dropped calls
- Problem/incident queue rate
- Average problem/incident closure duration
- Average problem/incident response time
- Percent of incorrectly assigned incidents
- Percent of escalated / repeated service requests
- Percent of incidents resolved remotely
- Number of service requests older than 30 days
- Number of incidents per known problem
- Percent of problems with a root cause identified
- Time until root cause identification
- Security incident response time
- Percent of downtime due to security incidents
- Percent of successful software upgrades
- Number of urgent releases / hotfixes
- Number of complaints
- Average cost to solve an incident
- Percent rate of getting help from third parties

Sensor health, sensor availability, sensor reachability and the number of sensors are the basic KPIs for *IoT Devices* in the ICT infrastructure. As a crucial category, *safety and security* should be closely monitored using the following metrics [46].

- Amount of hazardous operational waste
- Asset utilization
- Total downtime and total uptime
- Total repair time and total maintenance cost
- Infected host
- Audit log
- Email spam messages stopped/detected
- Number of detected network attacks
- Number of viruses in network
- Frequency of security audit
- Number of DNS requests
- Number of exploits and vulnerabilities detected
- Number of urgent changes
- Number of TCP and UDP packets on firewall
- Number of connections and sessions on firewall
- New session rate and throughput on firewall
- Amount of daily log and http/https traffic
- Security incident response time
- Top source and destination
- Top services and applications
- Top used ports, top source traffic country
- Top bandwidth consumed hosts
- IPS/IDS connection rates
- Number of dropped critical risks
- Number of required security updates
- Security risk score

The last KPI, *security risk score*, is a composite measure.

As a final category, *energy* KPIs are used to assess the energy efficiency of the ICT infrastructure on hand, especially for monitoring grid performance in the context of smart cities [47] or of wireless sensor networks using hierarchical routing protocols [48]:

- Efficiency of power delivery system
- Efficiency of power consumption
- Energy peak demand
- Power rating of ICT devices
- Power rating of non-ICT devices
- Power rating of future ICT devices
- UPS energy losses and battery capacity
- Lighting power requirement
- Expected critical load peak power
- Total electrical power requirement

- Cooling power capacity
- Server power utilization
- Total network power rating
- Energy consumed for lighting
- Energy consumption in the network
- Total ICT equipment energy usage
- MHz per watt, bandwidth per watt and capacity per watt
- Cost of electricity
- Critical peak load
- Generator capacity vs. required capacity
- Generator cooling energy usage
- Annual energy use of the server, storage, network equipment and data center
- Energy usage per cabinet

4.3. Software-Defined Networking

Software-defined networking (SDN) technology can be defined as the management of all devices from a software control layer by physically separating the control layer and the data layer in network devices. As a logical by-product of computing virtualization, SDN has its origins in 1990s' research, and has more recently been commercialized, standardized, and widely implemented [49].

By deploying SDN, dependency on network engineers decreases, network management can be easier and desired features can be easily integrated into the network structure via centralized software. This technology provides network engineers with flexibility on scripts, especially with advantages of Python support and socket programming. Communication between switches and controller in SDN is provided via the OpenFlow [50] protocol. One of the most well-known and advanced SDN controllers is the OpenDaylight [51]. This controller can be used in real environments with the use of products that support these projects. The Pox [52] and Ryu [53] controllers, and the Open vSwitch [54] virtual switches can be preferred for research. Besides these software, performance tests emulating SDNs can be easily performed, especially on the Mininet [55] platform.

Some practical advantages of SDN are identified as:

- The ability to direct applications according to line performance over a single software,
- Ease of management, provided that all operations related to the network can be followed through the software,
- Flexibility for adding new features to the network infrastructure through programmable features,
- The ability for the network traffic to be managed and optimized centrally [56].

The following indicators should be monitored continuously for managing the performance in SDN.

- OpenFlow protocol throughput
- Out-of-order OpenFlow packet rate
- Retransmission OpenFlow packet rate
- Average OpenFlow Packet
- Minimum idle CPU on OpenFlow controller
- Minimum idle RAM on OpenFlow controller
- Latency

In the hierarchical network topology, the logical placement of the SDN controller can be seen in Figure 6.

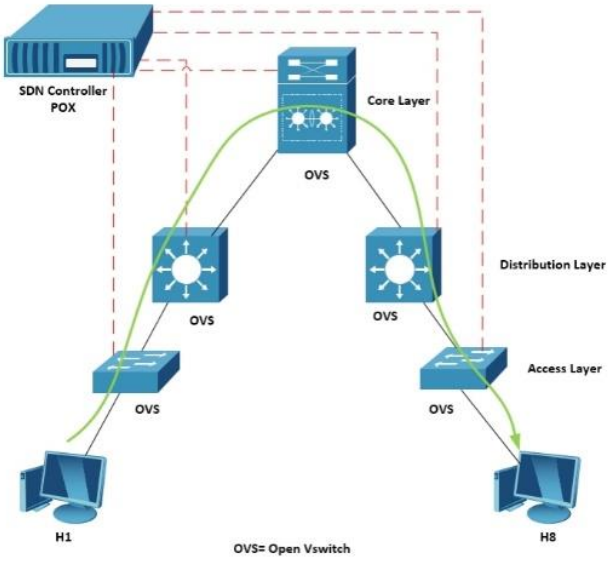

Figure 6. A three-tier test topology for Mininet

5. CONCLUSION

As a direct result of growing demand and supply of digitalization, the quality and sustainability of provided services and network infrastructures has become critical. In order to ensure customer satisfaction, the service provider is required to deliver a smooth digital experience with minimum interruptions. Therefore, communications networks on which these services are built become the focus of attention in terms of monitoring, maintaining and quick recovery scenarios.

In this study, by identifying questions for managing a sustainable network, various stages of the performance management processes are presented along with available software tools. Relevant performance metrics from the literature are also compiled into functional categories including crucial KPIs in a comprehensive manner. Depending on the priorities of provided services, different performance management systems for monitoring network infrastructures might be developed by integrating various indicators and tools.

Considering combined digital services within the smart systems context, the performance management issues presented in this paper could be extended with simulation

tools. Such smart systems may include IoT, smart cities, blockchains, automated vehicles and such, which are connected through cyber-physical application layers. In addition, effective machine learning methods from the literature could be applied for better performance assessment and more intelligent preventive measures. Sustainability requires clever and timely decisions directed by the most appropriate metrics available. In this respect, the compilation of tools in this study could be a guide for academicians as well as practitioners within the ICT sector.

REFERENCES

[1] S. McGill, **Network performance management using application-centric key performance indicators**, Phd Thesis, University of Central Florida, College of Engineering and Computer Science, 2007.

[2] A. Adepetu, E. Arnautovic, D. Svetinovic, O. Weck, "Complex urban systems ICT infrastructure modeling: a sustainable city case study", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(3), 363–374, 2014.

[3] H. Rohani, A. K. Roosta, **Calculating total system availability**, Information Services Organization KLM-Air France, Amsterdam, 2014.

[4] N. R. N. Haizan, A. R. Alinda, A. R. Azizah, "The KPI development framework for ICTSQ measurement", **3rd International Conference on Information and Financial Engineering** 12, Shanghai, China, 274–279, 19-21 August, 2011.

[5] A. Schiff, J. Small, M. Ensor, **Infrastructure Performance Indicator Framework Development**, National Infrastructure Unit, The Treasury, New Zealand, 2013.

[6] B. Celebic, R. Breu, "Using green KPIs for large IT infrastructures' energy and cost optimization", **3rd International Conference on Future Internet of Things and Cloud**, Rome, Italy, 645–650, 24-26 August, 2015.

[7] M. Al-Kuwaiti, N. Kyriakopoulos, S. Hussein, "A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability", *IEEE Communications Surveys & Tutorials*, 11(2), 106–124, 2009.

[8] S. M. Al-Shehri, P. Loskot, T. Numanoglu, M. Mert, "Common metrics for analyzing, developing and managing telecommunication networks", *arXiv*:1707.03290, 2017.

[9] Internet: Zabbix, Network monitoring, www.zabbix.com, 21.02.2020.

[10] Internet: openDCIM, Data center infrastructure management, opendcim.org, 15.02.2020.

[11] Internet: Sunbird, dcTrack data center infrastructure management, https://www.sunbirddcim.com, 15.02.2020.

[12] Internet: Raritan, Power IQ data center energy management and power monitoring, www.raritan.com, 15.02.2020.

[13] Internet: Txture, Data center energy management, txture.io, 15.02.2020.

[14] Internet: OTRS, Helpdesk ticket tracking, otrs.com, 16.02.2020.

[15] Internet: Best Practical, Request Tracker, Helpdesk ticket tracking, bestpractical.com, 16.02.2020.

[16] Internet: GLPI, Helpdesk ticket tracking, glpi-project.org, 16.02.2020.

[17] Internet: Kiwi Syslog, Log management, www.kiwisyslog.com, 21.02.2020.

[18] Internet: Elk Stack, Log management, elastic.co, 21.02.2020.

[19] Internet: MRTG, Network monitoring, mrtg.com, 21.02.2020.

[20] Internet: Cacti, Network monitoring, cacti.net, 21.02.2020.

[21] Internet: SolarWinds, Network monitoring and management, solarwinds.com, 21.02.2020.

[22] Internet: ManageEngine, Network monitoring and management, manageengine.com, 21.02.2020.

[23] Internet: Cisco, Cisco Prime network monitoring and management, cisco.com/c/en/us/products/cloud-systems-management/prime.html, 21.02.2020.

[24] Internet: Nagios, Service and application monitoring, nagios.com, 22.02.2020.

[25] Internet: CAIDA, Flow monitoring, FlowScan,caida.org, 22.02.2020.

[26] Internet: ntop, NPROBE flow monitoring, www.ntop.org, 22.02.2020.

[27] Internet: The Apache Software Foundation, Apache Metron security analytics, metron.apache.org, 28.02.2020.

[28] Internet: Cyphon, Security threat intelligence, cyphon.io, 28.02.2020.

[29] Internet: GOSINT, Security threat intelligence, gosint.readthedocs.io, 28.02.2020.

[30] Internet: AT&T, AlienVault OSSIM security management, cybersecurity.att.com/products/ossim, 18.07.2020.

[31] Internet: Security Onion, Security management, securityonion.net, 28.02.2020.

[32] Internet: Zeek Network Monitoring Project, Bro IDS network intrusion detection and prevention, github.com/bro, 28.02.2020.

[33] Internet: Snort, Network intrusion detection and prevention, snort.org, 28.02.2020.

[34] Internet: Suricata, Network threat detection, suricata-ids.org, 28.02.2020.

[35] Internet: OSSEC, Host-based network intrusion detection, www.ossec.net, 28.02.2020.

[36] Calyam, M. Dhanapalan, M. Sridharan, A. Krishnamurthy, R. Ramnath, "Topology-aware correlated network anomaly event detection and diagnosis", *Journal of Network and Systems Management*, 22(2), 208–234, 2014.

[37] Axelos, **ITIL Foundation, ITIL 4 Edition**, TSO, London, UK, 2019.

[38] Internet: ISACA, COBIT, www.isaca.org/resources/cobit, 15.01.2020.

[39] A. Kwizera, C. Koçak, "Performance evaluation of tunneling mechanism in MIPv6 over IPv4", *Bilişim Teknolojileri Dergisi*, 10(3), 327–334, 2017.

[40] A. N. Katov, **Energy Efficient Mechanism for Next Generation Networks: Adaptive Resource Allocation**, Master Thesis, Aalborg University, 2014.

[41] Internet: KPI Library, KPIs in information technology, kpilibrary.com/categories/itman, 10.05.2020.

[42] F. Abut, "A distributed measurement architecture for inferring TCP round-trip times through passive measurements", *Turkish Journal of Electrical Engineering & Computer Sciences*, 27(3), 2106–2120, 2019.

[43] Internet: iPerf, Throughput measurement, https://iperf.fr, 25.04.2020.

[44] Internet: A. Grove, JPerf Java performance and scalability testing, sourceforge.net/projects/jperf, 25.04.2020.

[45] M. Jibril, **Information & communications technology service - Review of KPI's**, Breckland: Breckland Council, 2005.

[46] T. Raza, M. Bin Muhammad, M. A. A. Majid, "A comprehensive framework and key performance indicators for maintenance performance measurement", *ARPN Journal of Engineering and Applied Sciences*, 11(20), 12146–12152, 2016.

[47] E. Personal, J. I. Guerrero, A. Garcia, M. Pena, M., C. Leon, "Key performance indicators: A useful tool to assess Smart Grid goals", *Energy*, 76, 976–988, 2014.

[48] I. Ouafaa, K. Salah-ddine, L. Jalal, E. Said, "The comparison study of hierarchical routing protocols for ad-hoc and wireless sensor networks: A literature survey", *Bilişim Teknolojileri Dergisi*, 9(2), 71–79, 2016.

[49] National Academies of Sciences, Engineering, and Medicine. **Information Technology Innovation: Resurgence, Confluence, and Continuing Impact**, Washington, DC: The National Academies Press. https://doi.org/10.17226/25961, 2020.

[50] Internet: OpenFlow, SDN communications protocol, opennetworking.org, 01.12.2020.

[51] Internet: OpenDaylight, Open-source SDN controller, www.opendaylight.org, 01.12.2020.

[52] Internet: Pox, Open-source SDN controller, noxrepo.github.io/pox-doc/html/, 01.12.2020.

[53] Internet: Ryu, Open-source SDN controller, ryu-sdn.org, 01.12.2020.

[54] Internet: Open vSwitch, Open-source SDN controller, www.openvswitch.org, 01.12.2020.

[55] Internet: Mininet, Open-source SDN Emulator, www.mininet.org, 01.12.2020.

[56] A. Yassine, H. Rahimi, S. Shirmohammadi, "Software defined network traffic measurement: Current trends and challenges", *IEEE Instrumentation & Measurement Magazine*, 18(2), 42–50, 2015