International Journal of Engineering Research and Reviews ISSN 2348-697X (Online)
Vol. 10, Issue 3, pp: (29-32), Month: July - September 2022, Available at: www.researchpublish.com

The History and Future of Network Monitoring

Marek Zidek[1], Peter Magdina[2], Ali J. Alkhalaf[3]

Affiliation: Dhahran, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.7060322

Published Date: 08-September-2022

Abstract: **Network monitoring is one of the main tools in the internet space to ensure a continuous operation of the network. Demands are constantly increasing: we cannot imagine our lives today without computers or the internet; this is true both for our work life and our private lives. Almost all job sectors have been digitized during the last 20 years. What our parents could not have imagined, we are experiencing first-hand today, and will be an integral part of our children's lives. How could humanity undergo such a drastic change in telecommunications and computer technology in just 20 years? In addition to the positives, this technological revolution brought pitfalls in the form of technology abuse from cybercriminal activities. Another big concern is - how will we manage all those computer resources and internet services as they cannot be left unattended or otherwise they would break down. Introduce network monitoring, a technological field working in parallel with other functions to fulfill this role. Today we will take a closer look at this field to understand its irreplaceable role in the IT world and what the future holds for it.**

Keywords: **network monitoring, AI, internet, optimization, cyber security.**

I. INTRODUCTION

In order to know what the future holds, we must first look into the history. Computer networks are currently one of the most dynamically developing industries. Network Monitoring Systems (NMSs) are now the standard solution for collecting and processing information about networks. Over time, more complex networks are being deployed with an amplified amount of information required to tackle more complex problems and events occurring in these networks. With this growing complexity of services provided on today's networks and amount of information to be processed, the requirements for monitoring systems' functionality and features are also increasing.

II. DISCUSSION

Dawn of Computers until Early 90s

In the early era of computers, there was no monitoring or monitoring was limited to internal services (processes) of computers. End-Users were connected via serial connection to the mainframe system, with minimal data transfer over the network. Monitoring tools were primitive, and since most systems were batch-oriented, there was no real-time input or output data. Systems were under physical monitoring of trained technical staff, who keep it in a healthy condition by observing lights or sound indicators.

In a later stage, serial terminals were replaced by Unix systems, which moved away from batch processing and towards an interactive input and real-time data. Needs to transfer real-time data to a central location helped expand the networks connecting this new type of computer terminals.

In the early 90s, introduction of massive computer networks and the dependence of companies on continuous feeds of real-time data led to the development of network monitoring tools and protocols. The technical teams quickly understood the importance of monitoring these networks to avoid slowness, disruptions and outages.

Early 2000s

The basic challenge of the early 21st century was the fact that for more and more organizations, the internet was no longer an alternate or an optional outlet for doing business. It was now their main, and sometimes only, platform.

Along with all of the standard functional and performance issues, many of which could be and often were better handled by hosting service providers, the need arose to monitor a growing list of what were, essentially, business-related metrics. It was as important to know the sequence of data traffic flow from one page or an element within a page to the next, the pattern of traffic over time, and the geographic source of traffic as it was to know whether the server was handling the traffic adequately or not.

By the beginning of the 21st century, however, it was becoming apparent that the monitoring requirements of websites and internet-based services were not the same as those of a typical office LAN. This initially led to the development of a generation of monitoring tools, such as Cacti, Nagios, and Zabbix, that supported standard internet protocols, could be used on multiple platforms, were often quite scalable, and typically had Web-based interfaces.

These tools, however, were still generally focused on functional and performance metrics, with a strong emphasis on server and communication hardware-related issues. They extended the reach of older network monitoring tools, but they retained much of those tools' basic nature. The first decade of the 21st century would see the growing need for a new kind of monitoring tool.

Modern Network Monitoring Functionality

The monitoring system can be imagined as a control element that observes the entire network and constantly checks the quality of services provided on this network[i]. Events from the network are collected, processed and used to provide information about the network or network components health.

One example is network links provided by telecommunications operators. To provide services of sufficient quality and reliability, it is necessary to detect problems and remediate them very quickly to reduce disruptions and meet SLA requirements. The detection and identification of problems in these big, complex networks cannot be provided effectively by humans due to the network size and frequency of events in them, this must be provided by an automated network monitoring system. The monitoring system subsequently notifies technical staff to remediate the detected problem.

This process is not unlike monitoring bank security, in which the outputs of security sensors and cameras are collected by an automatic surveillance system. The systems trigger an alarm whenever it detects an unexpected event. In this case, the security personnel are responsible for resolving the problem.

So, we can sum it up like this:

Network monitoring is an invisible protector of the computer network. Whenever something happens to the network, the monitoring mechanism reports and suggests a solution. Today's monitoring mechanisms are much more advanced than the first generations, but there is still a room for improvement. It is quite possible that they will improve as a result of the evolution of artificial intelligence.

The Evolution of Monitoring Systems

With all that being said, it should be noted that efficient monitoring is becoming increasingly difficult. Not only because of the volume of data, but also the number of connections. Many of the so-called silent failures remain undiscovered. This category mainly includes configuration errors, routing anomalies, and unexpected minor faults on routers. Even these minor errors can lead to more catastrophic network failures.

Therefore, just like network monitoring, measuring the operating characteristics of the network is essential to gauge the performance of the network and whether it behaves as expected or not. Introducing this extra step aids in preventing future failures when some indication is noticed on the network. There are two types of this measurement:

1. Active Measurement:

This type of measurement is implemented by sending test packets (probes) into the monitored network. This is the most optimal way to test the flow of network traffic with two or more boundary points. Using this type, the round-trip time (RTT), average loss rate, connection bandwidth, and packet throughput can be determined with a high accuracy. At the IP level, packets are a mechanism for determining the quality and performance of computer network operations.

2. Passive measurement:

This type requires no change to the existing traffic and runs on network components (routers, switches, etc.) with built-in protocols such as NetFlow, SNMP, and RMON. Passive measurement is performed periodically, and based on the evaluation of the collected metrics, the condition and performance of the network is determined. Additional advantages of passive network measurement include providing useful information about the network infrastructure and network users and introducing minimal disruption to the network operations.

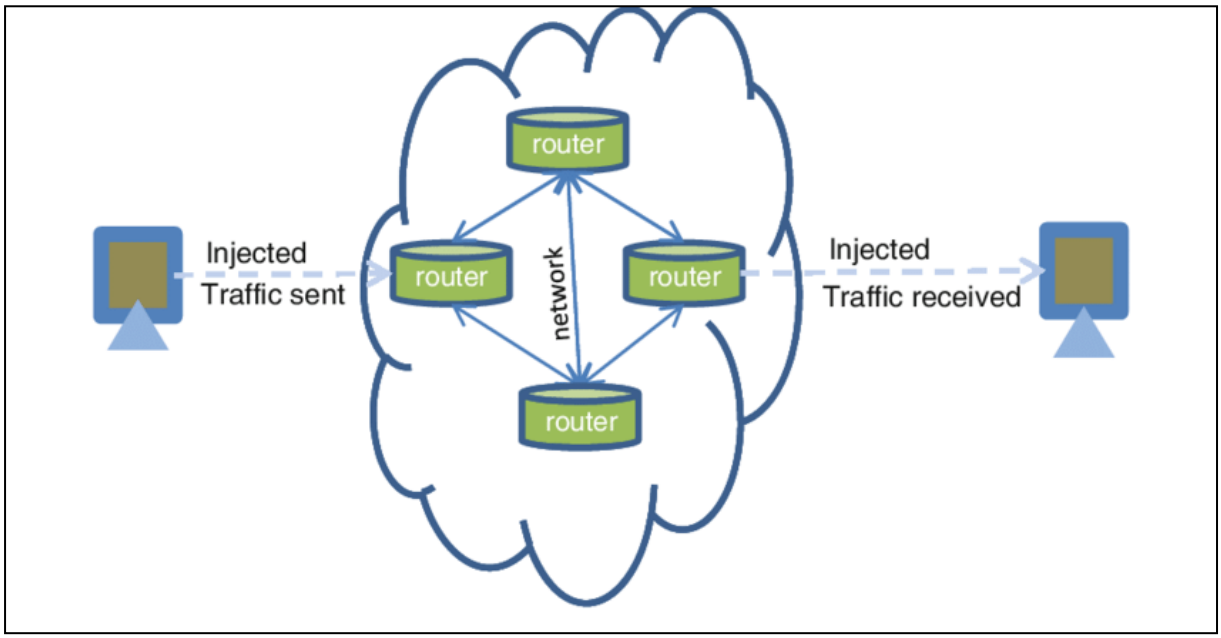

Fig 1: Active Network Monitoring

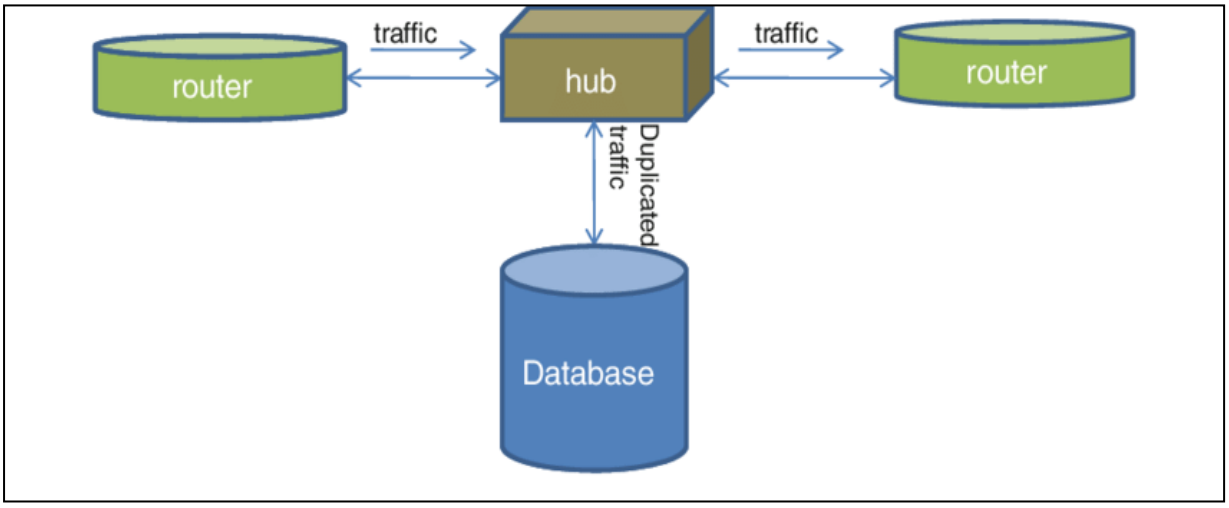

Fig 2: Passive Network Monitoring

III. CONCLUSION

Advanced Artificial Intelligence will gradually replace Older Monitoring Mechanisms

Today, we already encounter various autonomous bots, even during normal use of the internet. They work on the principle of algorithms, which can range from very simple to more complex. These bots serve to monitor, protect and manage networks. It is more than likely that AI will improve and eventually completely replace human repetitive input and output. Odds are in favor of AI, not only in the field of network monitoring, but also in all other activities. The main task of AI is learning and problem solving, which is the essence of network monitoring.

As the need for high network performance increases, so does the risk of various undetectable anomalies that affect said performance, and extreme pressure on the network requires increased control. Artificial intelligence as network monitoring will become more and more essential to discover unseen anomalies and service dependencies. Growing AI independency and flexibility is crucial to keep up with this rapid growth in network size and requirements.

Today's top network monitoring software include Pulseway, which has a really wide coverage: routers, switches, firewalls, wireless LAN controllers, and servers[ii]. Nessus is also known by many professionals, as well as Nagios, OpManager, Spiceworks, Cacti, which is really easy to use, even for beginners, NetFlow and many others. Most of these tools provide an AI component to compliment the classical way of monitoring networks and kickstart the age of autonomous monitoring.

With the development of the latest generations of phones and the use of smartphones at work, the monitoring and protection of these devices, along with the network, will also increase. With the arrival of 5G networks and IToT devices, new challenges await network monitoring tools, and it is necessary to adapt to them. Are there any hidden pitfalls to using fully autonomous artificial intelligence? Of course, there are; with every progress comes some risks.

REFERENCES

[1] L. DeCarlo – „AI, analytics, automation fuel the future of network management“, https://www.techtarget.com/searchnetworking/feature/AI-analytics-automation-fuel-the-future-of-network-management

[2] Z. Ayop, M. Aiman, M. Hamka, S. Anawar – „A Usability Study on Mobile Server Monitoring Applications“, p. 76 – 79, https://www.researchgate.net/profile/Siti-Nurul-Mahfuzah-Mohamad/publication/329884762_ICT_HUMAN_Book_Chapter/links/5c2062dba6fdccfc7064b661/ICT-HUMAN-Book-Chapter.pdf#page=77