Challenges of the System and Network Administration

VALEAGH BAILEY[1], BHARAT S.RAWAL[2]
[1]Computer Science Department Capitol Technology University, Laurel, USA (e-mail: (vrbaile@captechu.edu)
[2]Computer Science Department Capitol Technology University, Laurel, USA (e-mail: bsrawal@captechu.edu)

ABSTRACT

In IT, as larger networks are developed, more challenges appear. Two important groups of individuals that are responsible for the computer systems and overseeing the network are system and network administrators or 'admins'. Although the system and network administration consist of different roles, overlapping will most likely exist with the two of them working so closely together. Many challenges must be faced head on in system and network administration every day. What is the problem? What tools are needed for testing to discover the root cause? How can we overcome network efficiency issues? These are questions that these administrators must be ready for 24/7. This paper discusses the challenges that develop when working with networks (particularly larger ones), some available tools that can be used in reaching solutions, and the challenges involved in implementing the solutions. There will be additional research provided that gives details of implementation testing performed on a large enterprise and the process of achieving high efficiency.

KEYWORDS System administrator; network administrator; work practices; performance management; network efficiency; network management.

I. INTRODUCTION

The use of the Internet has drastically increased in the last two decades [6]. As technology and networks continue to advance and grow at a rapid speed, system and network admin must continuously research and find the most efficient ways to tackle all the challenging issues that come to them from various directions [4]. End users run into performance issues all the time and want a quick fix, but it can be time consuming when trying to locate the root cause and may take additional assistance from elsewhere to get things back up and running properly.

System admins must prepare him or themselves by improving their skills to be able to solve problems because it is their responsibility to ensure that the computer system is properly functioning and meeting the organization's needs. Problem solving is a process that at times requires critical thinking, therefore, it can be extremely difficult. System admins must do everything in their power to make sure that the computer systems are kept up and running for the sake of the organization.

There are also complex problems that network admin must approach. Network admin monitors networks and ensures that everything runs just as it was designed to. To have effective network management, it is of high importance for network monitoring to existing [18]. A lot of troubleshooting takes place in this role and is more of a learned skill. Some of the issues that network admin face evolves around physical connectivity, slow networks, duplicate IP addresses, weak Wi-Fi signals, VLAN problems, and excessive CPU usage.

System and network admin perform a great deal of research and troubleshooting techniques that may direct them to investigate similar network problems such as incorrect VLAN assignment, DNS issues, or even IP address conflict. Although their tasks are different, the roles of both system and network admin are interchangeable and deal with server and network problems that require immediate attention along with solutions.

The research in this paper proposes that there are far more issues in larger enterprises, particularly due to much larger networks, which could cause some issues with network efficiency, but the possibility to achieve higher efficiency is there. It is not uncommon for businesses to struggle with network efficiency, but like any other process, some steps can be taken to improve network efficiency.

The following is how the rest of the paper is structured: The introduction is covered in section I, and the related work is covered in section II. Then, section III system architecture Section IV analytical model. Section V presents a discussion. Finally, section XI concludes the research paper.

II. RELATED WORKS

Many challenges surround the system admin today that require a ton of critical thinking and decision making. The system admin is under the radar to keep computer systems up and functioning to their full potential. Despite the many challenges that come, system admin is required to solve problems under pressure while paying close attention to many systems at a time, meet tight deadlines and expect calls 24/7. Just know that throughout the entire course of every project, decision-making is involved daily [11].

Ineffective software can make it difficult when it comes down to test. Due to the lack of updated software, system admin must often wonder if some things are worth testing. Many organizations do not have additional funds to purchase quality software. Therefore, system admin is forced to use tools that are outdated and ineffective.

Server errors can occur when there is a lack of storage space. The response from the servers become extremely slow and may cause login problems. Many systems admin has come face to face with this problem during some of their most intense work assignments. Therefore, it is important to keep server hardware and software updated to minimize encounters with server error problems.

Often, the system admin runs into issues trying to read someone else's code. When there is a lack of simplicity, comprehension, or logic in the code, usually no one wants to deal with it. Many have found that it is so much easier to just write their own block of code than to fix the previous admin's code. Either way, it will be tedious and time-consuming.

The most common complaint that system admin hears from employees is that they have no internet connection. The internet is a major resource used daily by the admin for research and to reach testing tools. This affects their ability to work on the tasks at hand of current projects. Also, if there is no internet connection, there is no access to the company's site resulting in possible financial loss and disgruntled customers.

As a system admin, time management is a challenge that can be very stressful and harmful. First, every project has a deadline. These deadlines become almost impossible to meet when there is a lack of resources available, whether it be inside tools or other IT personnel outside the organization. Not only that, while trying to complete assigned tasks, system admin may have to stop often to assist colleagues with questions or take on more urgent matters that come up. Prioritizing could make a huge difference when dealing with time management.

Just as the system admin is faced with many challenges, the network admin also has many problems and are under pressure to always keep the networks up and secure. The most challenging aspect in modern IT may possibly be network administration. Network admin is responsible for ensuring that an organization's computer networks are secure and working well.

The physical connection is one problem that the network admin deals with. With all the different cables in the closets connected to the hardware, it is not unusual when others to come in to do work on their equipment to accidentally knock cables loose. Although it is a simple fix, it can break the network until the issue is found. There can also be damaged cables from sharp edges, which is why you must be careful when pulling the cables while performing other work around them. Locating damaged cables can be a little more time consuming if they are above the ceilings.

End users often complain about having slow network issues. These issues usually come from added applications or a switch port that is failing. Large organizations will have more traffic which in turn can cause cloud applications to produce slow responses. However, downloading high-definition videos can also reduce network speed. Network admin has network monitoring tools to assist in situations such as these.

A weak Wi-Fi signal is an issue that may arise often after an office move. Network admin often finds the causes for this to be interference or object blocking. Bluetooth or microwave ovens can cause interference. A Wi-Fi signal can be blocked by large objects made of metal such as file cabinets. The network admin has Wi-Fi testing tools that can be used to identify the problem.

Having too many open applications can cause excessive CPU usage. Many times, an individual can have so many open applications that resources may start to leak. It is important to ensure that you have up-to-date antivirus to avoid a virus from consuming resources.

One of the top network admin's challenges is security. Whenever possible, anonymous users should be prevented at all costs [16]. There are many threats that can gain access to the network and phishing emails are one of the main sources used. Phishing emails may appear to come from someone in your organization, however, they are fraudulent email messages with the goal of using the victim's computer to steal sensitive information [15]. Employees are tricked to believe that the emails are from a known source from inside of the organization and are safe to access, and as soon as they click on the links provided, threats enter the network. Once hackers can get in and steal targeted information, they then clear traces of their work making it hard to investigate and track causing the organization great losses [8]. Traffic can be protected by encryption, which is supposed to help guarantee that a user's sensitive information is kept private, but this solution makes it hard to watch over the network activity [21]. The tools that can improve security must all correlate and work together which could be difficult. The performance will be impacted any time security-related functionalities are integrated in any system [1].

Having duplicate IP addresses is an issue in the networking world for both the system and network admin. If there are duplicate IP addresses, reliable access does not exist for systems. Dynamic Host Configuration Protocol (DHCP) assigns addresses for most network devices. These addresses change each time a system is booted up on the local area network (LAN). However, some are assigned a static IP address which is a permanent address. The issue comes in if or when someone decides to assign a static IP without informing the network admin and disrupts the network when DHCP assigns the same address to another device.

System and network admin are also challenged with

VLAN misconfiguration problems. The switch configurations must be compatible with the other switches. Many of the admin has found it useful to copy the switch configuration into a notepad, update the information for the new switch and paste the configuration in the new switch to avoid misconfiguration.

Print problems are also troublesome problems for the system and network admin. An active printer may have pending print jobs just sitting and waiting for some reason. Another issue is when a user cannot connect to the printer. It is up to the system admin to troubleshoot printer server issues, while the network admin focuses on the physical aspects to diagnose the problem.

When DNS failures exist, it can be challenging to access the internet as well as other key applications. This can default from faulty DNS server configuration. Furthermore, slow DNS lookups can occur. If DNS lookups are slow, there can be a slow link along the path, or the server can be slow or overloaded.

Challenges could be easily addressed if networks remained the same. However, networks continue to grow every time a new network device needs to be added. There is an increase in the potential point of failure whenever additional connections are added with each new device. Over the past decade, there has been a huge increase in distributed denial of service (DDoS) attacks due to increases in additional devices connecting to the Internet and exploitation of vulnerabilities [5], [17], [20], [22]. When a DDoS attack occurs, an attacker can cause the switches to become overwhelmed by flooding them with malicious flows [2]. To do so, the attacker must mirror all the traffic by maintaining the exact flow rules of the traffic being mirrored. After such an attack, identification of a hacked application is hard to determine because incorrect parameters can be established in the application [3]. Therefore, it is an important factor for the admin to keep the network protected from unauthorized parties [14].

There is usually a challenge with having the available budget to meet the needs of network services. It can be expensive any time admin may need to increase bandwidth by getting new hardware, upgrading cables, enabling new protocols on existing infrastructure by upgrading the configuration, or hiring experts to assist with setting up and managing different network features. However, these costs can be minimized by cloud computing, which consists of online storage, sites, and applications [7]. Because the cloud is not an on-site infrastructure, this will allow an organization to save on hardware and pay only for resources being used [10]. It is important to keep in mind that security and privacy issues do become major concerns when data is outsourced to a third party [12].

Admin typically uses an intrusion detection system (IDS) for monitoring networks, which is a popular defense system [19]. A lot of confidential data is stored and shared across networks. All network flow can be controlled monitored and maintained with an IDS. Network admin will be alerted by the IDS whenever there is any irregular behavior or threat attacks taking place within the networks [9].

A network intrusion prevention system (IPS) is another monitoring tool that the admin uses to monitor malicious activity on networks and prevent it. It still can be challenging to identify an attack in time even with an IDS or IPS [13]. Satisfactory or acceptable penetration testing should be performed to identify vulnerabilities. Furthermore, the admin should ensure that the appropriate software and hardware are installed according to the organization's requirements. A good network security governance should be developed as well [23].

III. SYSTEM ARCHITECTURE

Network architecture is positioned around the organization of a system's computers and the distribution of tasks between the computers. Peer-to-peer (P2P) and client/server are among the most popular network architectures used. P2P is very well-known and mainly used for file sharing. Whereas, in a client-server network, requests and services are requested from the network via network clients, and the requests or services are managed and provided by one or more network servers.

Many of the threats and challenges that the system and network admin are faced with evolve around network security, network performance, time management, growth, and cost or available budget. Table I gives an overview of these components, the threats, and challenges that could develop, and possible solutions to try to avoid or fix the issues. As the networks continue to grow with each organization, costs increase while productivity decrease. Ways to overcome network problems that develop from growth will be discussed in the latter part of this paper.

Make sure to identify every issue that exists at that moment. After gathering information pertaining to the network issues, take the time to come up with reasons that could be possible causes. Work toward testing those possibilities to see if that resolves the issues. After confirming your thoughts on the causes, you are now ready to come up with a plan to address and solve the problem(s).

Make sure to identify every issue that exists at that moment. After gathering information pertaining to the network issues, take the time to come up with reasons that could be possible causes. Work toward testing those possibilities to see if that resolves the issues. After confirming your thoughts on the causes, you are now ready to come up with a plan to address and solve the problem(s). The next step is where the plan is implemented. It is possible that you may be able to complete the work on your own, or you may require assistance from users or other colleagues. Once the solution has been implemented, perform testing to ensure that the issue has been resolved. If all is good, document the issue with all the information of the troubleshooting steps taken down to the solution that fixed the issue(s). This information will be viable for the next admin that may run into a similar network issue.

TABLE 1: Threat Model

Components	Threats/Challenges	Solutions
Network Security	Insider attacks/Hacking Phishing emails	Data protection tools Encryption User training Updated malware Security tools (IDS, IPS)
Network Performance	Slow networks Internet connectivity/downtime Financial losses	Network monitoring tools
Time Management	Meeting deadlines when trying to complete assigned work and assisting colleagues when needed Lack of resources Limited control	Prioritizing Improve network management tools Increase personnel Have a third party available to assist with network management
Growth	Increase in devices/traffic Increase in a potential point of failure Increase in DDoS attacks	Introduce design tools Internet monitoring tools Backup and failover capabilities for network
Cost/Available Budget	Need for new hardware Upgrading cables Upgrading configuration Hiring experts for assistance	Cloud computing (online storage, sites, and applications)

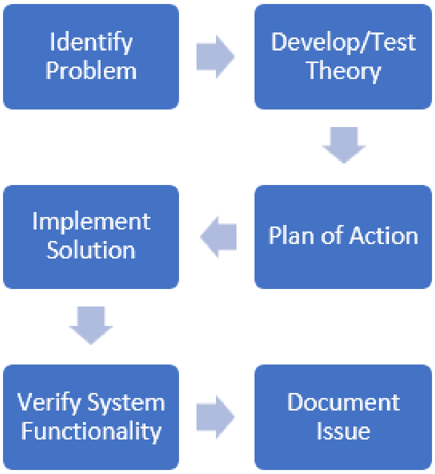

FIGURE 1: Network Troubleshooting Flowchart

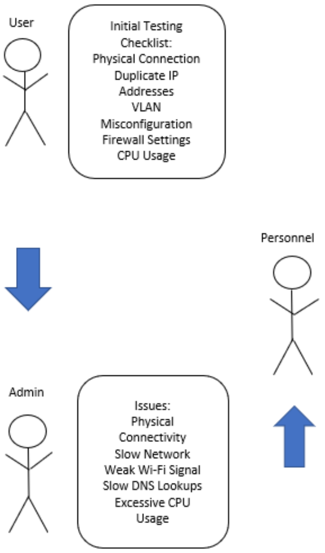

FIGURE 2: The system interaction

Users run into networking issues quite often and reach out to the admin for assistance. Admin will perform research and try to pinpoint the root cause of the problem. Diagram I show some common issues that users contact the admin to help fix. Admin has some basics to check and if there is a dead end, then there is the option for admin to get some additional assistance from other personnel such as other admin, service providers, or third-party to help resolve the problem at hand.

$a(t) \Rightarrow Network \Rightarrow r(t)$

Examining the network shown in the figure above:

a(t) = action or input

r(t) = reply or output

Assuming that all initial conditions are zero, this network function is defined as the ratio of the reply or output of the network to the action or input applied.

$E(s) \Rightarrow Network(Ts) \Rightarrow R(s)$

T(s) in the s domain is used to denote the network function. Therefore, the network function can be defined as T(s) = R(s)/E(s). The transforms of r(t) and e(t) are R(s) and E(s). The reply for any type of action can be obtained once the T(s) of the network function is known. However, one must specify the output terminals to determine the network function.

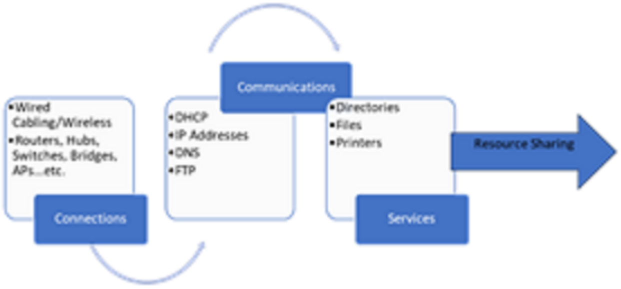

FIGURE 3: The system interaction

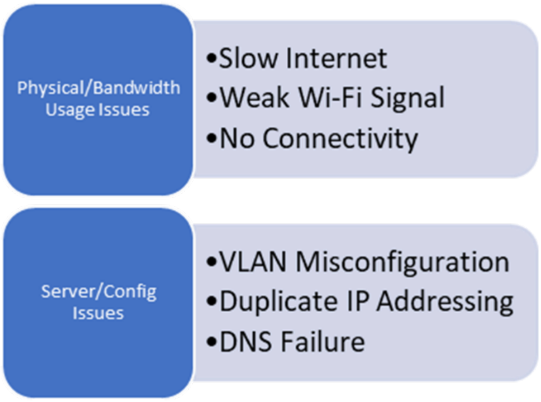

FIGURE 4: The system interaction

IV. ANALYTICAL MODEL

Networks consist of the connection of multiple computers, servers, and other devices utilizing a channel that allows information to be exchanged. The network operating system manages the computer network resources, and its most important function is to support multiple input requests at the same time in a multiuser environment. Some beneficial features of computer networks are resource sharing, simultaneous access, cost reduction, and communication medium.

There are three basic requirements for a network to function. Connections, communications, and services must all be provided for proper functionality as shown in the chart below. Network devices can be connected via wired cabling or wirelessly. These devices use a variety of network protocols to communicate with computer systems. This is the phase where rules are established for the computers to talk and understand one another. What the computer shares with the world is defined in services.

The next chart shows the challenges of a network that can block functionality. Although many of the barriers are quick fixes, they could be very detrimental. The process carried out by a computer network system is expected to function to produce a reliable and secure network that is useful for business operations.

The main goal of computer network systems is to ensure a high-quality network with quick recovery that provides continuous access and operations with no gaps. However, it will always be challenging to avoid barriers because devices will have the possibility of being faulty or failing at some point. Therefore, it is very likely that in the future there may be a decrease in hardware and an increase in cloud software.

V. DISCUSSION

Over the years, there have been many improvements to system networking, however, they still are not resistant to new problems. Therefore, it is not only important to be able to identify and troubleshoot as quickly as possible, but also to analyze ways to prevent these problems from reoccurring. Although there are several tools available to the system and network admin for troubleshooting, the greatest challenge lies in the growth of networks in larger organizations. Continuous growth causes an increase in costs and a decrease in productivity. A solution to the rising costs is cloud computing, rather than continuing to budget for hardware, cable, and configuration upgrades. Moving to cloud computing will be beneficial by providing remote access, ease of availability, and real-time collaboration, in addition to cost savings. Users benefit from cloud computing because they would no longer have to use an app via computer or buy any versions configured for a specific device. Cloud computing will have fewer maintenance issues, and storage and upgrades will no longer be existing problems since the latest updates will automatically be available and ready for use without any actions from the user. Innovation is enabled and there is no need for anyone to go out to find resources for development and testing . I believe that in the future, cloud computing will allow many companies to do away with hardware and turn to cloud software for a more improved, secure network.

VI. CONCLUSION

System and network administration are both very challenging roles. Admins spend most of their days troubleshooting issues with users and analyzing ways to improve their systems' performance and reliability. This line of work requires a lot of critical thinking and attention to detail under pressure. It could easily become an extremely intense day for admin. This review covers the many challenges that arise in system networks, available tools used to reach solutions, and the challenges involved in implementing the solutions.

REFERENCES

[1] Sicari, Sabrina, Alessandra Rizzardi, and Alberto Coen-Porisini. "Security&privacy issues and challenges in NoSQL databases." Computer Networks (2022): 108828.

[2] Goud, Konda Srikar, and Srinivasa Rao Gidituri. "Security Challenges and Related Solutions in Software Defined Networks: A Survey."

[3] Daneshmand, Behrooz, and Tu Anh Le. "Software-Defined Networking: A New Approach to Fifth Generation Networks–Security Issues and Challenges Ahead." In 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 307-313. IEEE, 2022.

[4] Gupta, B. B., Joshi, R. C., & Misra, M.. Defending against distributed denial of service attacks: issues and challenges. Information Security Journal: A Global Perspective,(2009) 18(5), 224-247.

[5] Chaganti, Rajasekhar, Bharat Bhushan, and Vinayakumar Ravi. "The role of Blockchain in DDoS attacks mitigation: techniques, open challenges and future directions." arXiv preprint arXiv:2202.03617 (2022).

[6] Ahmad, Suhail, and Ajaz Hussain Mir. "SDN Interfaces: Protocols, Taxonomy, and Challenges." (2022).

[7] Singh, Miss Ankita, Mr Vedant Naidu, and Deepali Shah. "Issues and Challenges in Data Integrity and Data Storage Security in Cloud Computing." Journal homepage: www. ijrpr. com ISSN 2582: 7421.
[8] Chen, Zhiyan, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, Hussein T. Mouftah, and Petar Djukic. "Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats." ACM Computing Surveys (CSUR) (2022).
[9] Khan, Amjad Rehman, Muhammad Kashif, Rutvij H. Jhaveri, Roshani Raut, Tanzila Saba, and Saeed Ali Bahaj. "Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions." Security and Communication Networks 2022 (2022).
[10] Grabowski, Cezary. "Technical challenges of creating an IT system in microservices architectural style using cloud services."
[11] Afkhamiaghda, Mahdi, and Emad Elwakil. "Challenges review of decision making in post-disaster construction." International Journal of Construction Management (2022): 1-10.
[12] Hassan, Junaid, Danish Shehzad, Usman Habib, Muhammad Umar Aftab, Muhammad Ahmad, Ramil Kuleev, and Manuel Mazzara. "The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges—A Systematic Literature Review (SLR)." Computational Intelligence and Neuroscience 2022 (2022).
[13] Marchang, Jims, and Alessandro Di Nuovo. "Assistive multimodal robotic system (AMRSys): security and privacy issues, challenges, and possible solutions." Applied Sciences 12, no. 4 (2022): 2174.
[14] Laaychi, Abdelaziz, Mariam Tanana, and Saiida Lazaar. "Security issues of the Web of Things: challenges and solutions." In E3S Web of Conferences, vol. 351, p. 01013. EDP Sciences, 2022.
[15] Srivastava, Gautam, Rutvij H. Jhaveri, Sweta Bhattacharya, Sharnil Pandya, Praveen Kumar Reddy Maddikunta, Gokul Yenduri, Jon G. Hall, Mamoun Alazab, and Thippa Reddy Gadekallu. "XAI for Cybersecurity: State of the Art, Challenges, Open Issues and Future Directions." arXiv preprint arXiv:2206.03585 (2022).
[16] Masoumzadeh, Amirreza, Hans van der Laan, and Albert Dercksen. "BlueSky: Physical Access Control: Characteristics, Challenges, and Research Opportunities." In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, pp. 163-172. 2022.
[17] Tripathi, S. et al,. Hadoop based defense solution to handle distributed denial of service (ddos) attacks. Journal of Information Security (2013)Vol. 4 No. 3
[18] Ding, Damu, Marco Savi, Federico Pederzolli, and Domenico Siracusa. "Design and Development of Network Monitoring Strategies in P4-enabled Programmable Switches." In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, pp. 1-6. IEEE, 2022.
[19] Mosemann, Faith. "Assessing Security Risks with the Internet of Things." (2022).
[20] Dahiya, A., et al. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Generation Computer Systems, (2021) 117, 193-204.
[21] Sicari, Sabrina, Alessandra Rizzardi, and Alberto Coen-Porisini. "Security&privacy issues and challenges in NoSQL databases." Computer Networks (2022): 108828.
[22] Gaurav, A., et al. . A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs. Technological Forecasting and Social Change, (2022) 177, 121554.
[23] Awang, Norkhushaini, Ganthan Narayana Samy, and Noor Hafizah Hassan. "Prioritizing Cybersecurity Management Guidelines using Analytical Hierarchy Process (AHP) Decision Technique." Open International Journal of Informatics 10, no. Special Issue 1 (2022): 1-10.