IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

STRATEGIC ANALYSIS OF LAN-BASED COMPUTER NETWORK MAINTENANCE: ENHANCING EFFICIENCY, RELIABILITY AND SECURITY

[1]Adam Musa Safiyanu, [2]Yakubu Awal Jibrin, [3] Sani Danjuma
[1,2,3]Department of Computer Science, Nasarawa State University, Keffi.
Nasarawa State.

Abstract

As society continues to advance, Internet technology has become an integral part of daily life and work. The widespread adoption of Internet technology has introduced various external interferences into computer systems during daily operations, leading to a range of network failures. Strengthening regional network maintenance and management is essential to reduce the likelihood of computer network failures and ensure the normal and secure operation of computer systems. This paper delves into strategies for enhancing LAN maintenance to mitigate computer network failures.

Index Terms - **LAN Maintenance, Computer Network, Network Failure**

I. Introduction

1 Introduction

The rapid convergence of computer and network technologies has ushered in a revolutionary era, fundamentally altering the landscape of how people work, communicate, and navigate their daily lives. This transformative fusion of capabilities has propelled computer network technology into the very heart of modern society. Its defining attributes—convenience, cost-efficiency, and speed—have not only reshaped industries but have also become inseparable from the daily routines of individuals worldwide. In this digital age, the pivotal role played by computer networks in facilitating the transmission, storage, and processing of data cannot be overstated [1]. They have become the backbone of our interconnected world, seamlessly linking individuals, organizations, and nations. Whether it's sharing vital information across continents in seconds, conducting complex financial transactions, or enabling remote collaborations, computer networks are the invisible threads weaving our global tapestry together. Given the pervasive influence of computer networks in people's lives, the maintenance of these intricate systems takes on paramount importance. Any disruption or fault in these networks can have far-reaching consequences, affecting not only business operations but also the daily routines and interactions of individuals [2]. The uninterrupted flow of data and communication has become a lifeline, underpinning the functioning of modern society. Consequently, the custodians of these networks, the network management departments, are entrusted with a weighty responsibility. They must stand as vigilant guardians, relentlessly ensuring the seamless operation of these digital lifelines. To achieve this, they must intensify their efforts in analysing, monitoring, and maintaining computer network infrastructure. The increasing complexity of modern networks, coupled with the ever-evolving landscape of cybersecurity threats, demands a proactive and sophisticated approach to network management. In this dynamic environment, the realm of network management is not merely about reacting to issues as they arise but about predicting and preventing disruptions before they occur. It involves a continuous cycle of assessment, optimization, and innovation, guided by the imperatives of reliability, security, and efficiency. The fate of businesses, the flow of information, and the quality of daily life hinge on the competence and dedication of those tasked with this mission [2.3].

2. Definition of LAN

A Local Area Network (LAN) is defined as a network comprising several computers connected through standard network cards or wireless network cards, routers, and hubs. It facilitates rapid sharing and exchange of information among users within its coverage area. LANs are typically linked to a central processing unit via dedicated data circuits, forming a comprehensive information processing system. LANs are characterized by their small coverage areas, high operating speeds, and regular distribution. Their stability and suitability for internal information transmission make them ideal for campuses and related enterprises. Hence, analysing issues in LAN management and maintenance is imperative [1].

3. Timely Network Card Inspection for LAN Problems

3.1 Check Network Cable Connection

When no faults are detected in the network card, maintenance personnel should verify the status of the connection between computer equipment and network cables. The process involves opening the Network Neighbourhood and checking for other accessible computers within the network. If other computers are visible, the connection between the computer device and the network cable is deemed normal. Conversely, the absence of visible computers indicates a faulty network cable connection. In such cases, maintenance personnel can use network cable testers for further diagnostics. For LANs with longer cables, shielded circuitry should be employed to prevent electromagnetic interference during testing [2].

3.2 Proper Server Hard Disk Configuration

The efficiency of a LAN's data transmission speed is profoundly impacted by the performance of the server's hard disk, not the number of users browsing the network. Hence, when configuring computer equipment, it is imperative to select high-speed, high-capacity hard disks to enhance LAN speed. Additionally, selecting the appropriate server interface model ensures optimal LAN operation. Permission from the relevant authorities allows maintenance personnel to install hard disk display cards in LAN servers, further improving network hard disk performance [3].

3.3 Driver Inspection

Following hard disk inspections, maintenance personnel must scrutinize computer drivers for damage or installation errors. Most users employ the Windows operating system. If no driver issues are detected during inspection, maintenance personnel should uninstall the network adapter, perform a hardware scan to detect new hardware, and then reinstall the computer's driver to resolve driver-related problems.

3.4 Proper Switch Configuration

Switches are critical data exchange components in LAN operations. Consequently, computer maintenance personnel should meticulously configure switches during LAN maintenance to bolster data transmission capacity. When handling extensive data transfers, ensure that the network card's operation speed in the switch aligns with the duplex setting. Network parameter setup must adhere to these rules to prevent issues [4].

4. Computer Network Breakdown Maintenance Mode

Currently, LAN-related computer network failures significantly impact network stability. Network failures typically fall into two categories: physical faults and logical faults. Physical failures encompass issues with computer components such as hard disks, memory, and displays, as well as connection equipment like power lines, network cards, network cables, and routers. Software failures include problems with network protocols, network equipment configurations, settings, and viruses. Given the critical role of computer networks, timely fault analysis and maintenance are paramount to ensuring their seamless operation.

From the analysis, network faults can be categorized into hardware and software issues. Analysing network faults should begin by examining these two aspects: starting with server analysis before checking workstations, and from the external network to the internal network, first verifying external equipment effectiveness and then addressing internal problems. The analysis should also follow the software-to-hardware sequence, starting with software and then investigating hardware issues. A case study illustrates these general analysis methods and steps[5] .

5. Daily Computer Network Maintenance Mode

5.1 Proper Host Network Address Parameter Setting

Logical faults often disrupt network usage when the host's IP address doesn't match other computers in the LAN. Therefore, maintenance personnel must employ network neighbourhood software to inspect IP addresses and address discrepancies promptly [6].

5.2 Verification of Host’s Network Protocol

The host's network protocol is pivotal in the LAN. Incorrect selection can hinder network connectivity. Thus, proper configuration of the host's network protocol to align with other hosts is imperative. When network connectivity issues arise, maintenance personnel can verify the correctness of the host's network protocol and make necessary repairs using network neighbourhood and local connection tools [7].

Regular Firewall and Security Updates Maintaining a secure network is paramount in today's digital landscape. To ensure the safety of your network, regular updates of firewall rules and security protocols are essential. Maintenance personnel should schedule routine checks to confirm that firewalls are up to date and that security measures are current. Any vulnerabilities or outdated security settings should be promptly addressed to prevent potential breaches

Continuous Bandwidth Monitoring Efficient network performance relies on proper bandwidth allocation. Regularly monitoring bandwidth usage helps identify potential bottlenecks or overutilization of network resources. Maintenance personnel should employ network monitoring tools to track bandwidth usage trends and make necessary adjustments to optimize network performance. This proactive approach can help prevent network slowdowns and ensure smooth operation.

Backup and Recovery Testing Data loss can be catastrophic for any organization. To safeguard against data loss due to network failures or other unforeseen events, regular backup and recovery testing should be part of the network maintenance routine. Maintenance personnel should periodically test the backup systems to ensure they are functioning correctly and can quickly restore data in case of emergencies.

Documentation and Network Diagram Updates Accurate documentation is crucial for efficient network maintenance. Maintenance personnel should update network diagrams and documentation regularly to reflect any changes or additions to the network infrastructure. This documentation serves as a valuable resource for troubleshooting and future network planning.

By incorporating these additional aspects into your daily computer network maintenance mode, you can enhance the reliability, security, and performance of your network while ensuring that it remains up to date with the evolving technology landscape.

6. Consideration in LAN Maintenance

During LAN maintenance, it's crucial to keep network maintenance logs up-to-date, including comprehensive records for future reference. Additionally, establish comprehensive component documentation that encompasses system analysis, maintenance records, maintenance plans, and other aspects. This documentation aids in recording and addressing LAN issues effectively. Network maintenance personnel should also bolster their network security awareness, timely implement patch programs, and enhance antivirus software performance to mitigate LAN network faults [8].

Robust Network Maintenance Logs: The cornerstone of effective LAN maintenance is maintaining up-to-date network maintenance logs. These logs should not only record routine maintenance activities but also capture critical incidents, changes, and upgrades. A well-maintained log serves as a valuable reference point for diagnosing issues and tracking the network's evolution over time.

Comprehensive Component Documentation: In tandem with maintenance logs, it's imperative to create comprehensive component documentation. This documentation should encompass detailed system analysis reports, maintenance records, maintenance plans, and any relevant network diagrams. Such documentation serves as a roadmap for understanding the network's architecture, making it easier to pinpoint and address problems swiftly.

Proactive Issue Recording: Encourage network maintenance personnel to adopt a proactive approach to issue recording. Instead of merely documenting problems after they occur, implement a system for proactive monitoring and alerting. This way, potential issues can be identified and addressed before they escalate into significant network faults.

Security Awareness: In today's cybersecurity landscape, network security should be a paramount concern. Network maintenance personnel should continually bolster their network security awareness. Regular training and awareness programs can help staff recognize and respond to security threats effectively. This proactive stance reduces the likelihood of security breaches that can disrupt LAN operations.

Patch Management: Timely implementation of patches and updates is pivotal for LAN stability and security. Maintain a well-structured patch management program that ensures critical security updates are promptly applied. This practice minimizes vulnerabilities that malicious actors could exploit.

Antivirus Software Optimization: Antivirus software plays a crucial role in protecting your LAN from malware and other threats. Ensure that your antivirus solutions are optimized for performance. Regularly update virus definitions and conduct system scans to identify and remove potential threats promptly [8].

7. Conclusion

In today's information age, computer networks are indispensable tools for work and daily life. To ensure efficient network utilization, timely and effective resolution of network faults is imperative. Network failures can lead to significant inconveniences and even substantial losses for users. Therefore, enhancing the diagnosis and maintenance of network faults is essential. However, safeguarding the secure and efficient operation of a local area network is a long-term endeavour that requires dedication and ongoing effort.

References

1. Liu, J. (2021, February). Analysis of Computer Network Maintenance Strategy Based on Lan. In *Journal of Physics: Conference Series* (Vol. 1744, No. 3, p. 032131). IOP Publishing.
2. Chakravarty, P. K. (2015). Computer networking technologies and application to IT enabled services.
3. Antonio Carzaniga, Basic concepts in Computer Networking, September 19, 2014.
4. Teodora Bakardjieva, Introduction to Computer Networking.
5. Peter L. Dordal, An Introduction to Computer Networks, Release 1.8.07, June 16, 2015.
6. Bob Dickerson, Computer Networks, January 2005.
7. Russell Anthony Tantillo, Network Security through Open Source Intrusion Detection Systems, May 2012.
8. http://web.net/~robrien/papers/mpconclusion.html
9. http://www.computerhope.com/jargon/i/ip.htm