Network Fault Effectiveness and Implementation at Service Industry in Indonesia

Fahrurrozi Lubis, Muharman Lubis

1Universitas Sumatera Utara, Jalan Dr. T. Mansur No. 9, Padang Bulan, Medan, 20155
2Telkom University, Jalan Telekomunikasi No. 1, Bandung, 40257
Email: fahrurrozi.lubis@usu.ac.id

Abstract. The efficiency of network administrators have been decreased concurrently due to complexity and heterogeneous of network built in certain environment of company. Actually, large heterogeneous network has created a crisis and conflict for many organizations. Available network tools and solutions are not only expensive but also difficult to install, configure, manage and maintain. This paper discusses the implementation of network fault in the service industry to match with the expectations of stakeholders to be able to achieve the higher efficiency and to carry out proactive processes although the practical truth is often the opposite way.

1. Introduction

In the past decade, network fault practices have been largely owned by high development costs but the rapid development of the next decade towards larger and more complex networks has led to a large proliferation of network technology solution. Network management is a set of activities, procedures and tools related to the operation, management, maintenance, and provision of computer networks. Operations worry about keeping their networks and services functioning efficiently, usually by monitoring networks and solving any problems before affecting users. Administration revolves around keeping the network under control, and includes tasks such as monitoring network resources and tasks. Maintenance is related to repairs, enhancements and measurements to optimize the network such as configuration settings. Finally, offer deals by changing networks to deal with new requirements or services. Organizations recognize that productivity benefits and benefits created by network technology with majority companies are beginning to expand their existing networks after new technologies are introduced. Without realizing the pain of managing unplanned networks, organizations have created complex and heterogeneous networks within organizations. There has been tremendous expansion in the distribution of networks around the world. Network errors can cause downtime and network degradation and thus affect network user performance. The purpose of error and fault evaluation is to detect, record, notify users of problems, and remedy problems remotely to keep the network running effectively. Fault efficiency involves identifying network errors and isolating problems. After the problem has been identified, the solution must be resolved and tested and applied to all systems or only system errors.

Corporate network management becomes more difficult and hard due to complexity and homogeneity. The most common and serious problems in the network are connection failures or crash implementation. Intermittent problems that can also occur as a result of excessive traffic and traffic cause network and package delays, which results in a decrease in performance. Management functions can be implemented explicitly by human operators, but in such cases, most of the functions will be
carried out from a number of remote sites. As organizations today rely heavily on computing networks in everyday transactions and business, there is a huge demand for network and system managers to ensure that the network operates smoothly, without obstacles or interruptions. The task of a network administrator is to maintain the company's IT infrastructure and correct problems that may arise at all. Thus, this study wants to explore the efforts that have been made by the service industry in the problem solving or error effectiveness process to detect, isolate and correct errors in each network, and compensate for changes in the environment, and keep checking error logs, and receipt of notification work Error detection, error tracking and identification, implementation of diagnostic sequence tests, reporting conditions for errors, and location and tracking errors through inspection and processing of information gathering in company databases.

2. Network Effectiveness Practices

Some of the key challenges in network effectiveness that should be considered carefully related the attempt to balance the pace of technological progress, maintaining continuous communication in respective channel and the analysis of problems related to optimization based on intuition and skills on particular context. The ability to maintain the network topology as simple as possible is required to reduce the costs of managing network effectiveness for collecting important data for submission to relevant executive management [1]. The process must be more self-managed and self-organized, so that it is economically viable while its solutions should remain simple and elegant, as evidenced by the development of the Internet to be applied within the heterogeneous networks on a large scale. As time goes on with the development of various application to solve problem occurred, a large number of industries rely on network connections for business and safety problems [2]. Communications and coordination within the networks are vulnerable to increased penetration threats, which the individuals or even governments are susceptible to be attacked, so the current requirement to implement network safety measures to prevent illegal modification, serious damage or leakage of information become extremely critical, especially to increase efficiency of network effectiveness [3].

Fault management is the discovery of network errors and debugging, which can be broken into hardware and software errors. Therefore, the hardware errors may occur due to damage, incident, malfunction, broken or improper installation while the software errors can occur due to misconfiguration, incorrect designs, improper use of programs or incorrect information, such as an incorrect routing table that can cause slow or erroneous service [4]. Thus, the network management process regarded that the information that cannot be used by users are categorized as trash. In addition, the server and the computer system must have sufficient capacity to meet the requirements of users to access information on the Internet. However, information availability can be disrupted by cyber-attacks, natural disasters and environmental factors [5]. At same time, the increasing reliance of companies on networks means that services and the use of the network are continuing to develop and expanded. Thus, network management must evolve to follow evolution and become more sophisticated and intelligent in the process. In the past, it has been affected only by staff skills but when networks become more dynamic and complex lead to the necessity to utilize a good network management program such as the use of artificial intelligence to solve some administrative problems [6].

Current and emerging communications networks and computers are expected to provide a high level of reliability by achieving near-immediate recovery if one or more network elements fail [7]. Although various network management tools has many promising opportunities, many risk factors can hinder its future growth. It is not surprising that security and interoperability are the biggest obstacles or even errors in network systems due to compatibility and communication problems. Another important obstacle [8] is the absence of a clear return on investment (ROI), immaturity of technology, old equipment and so on. Management techniques are needed to deal with the complexity of computer networks to detect and monitor the behaviour of system resources. At present, the management system operates in the central station where data is transferred from the client to the server and vice versa. This can cause inefficiency if the network size is too large [9]. Monitoring network resources and
services, isolating and identifying problems during a failure, repairing them by sending technicians to the site most of the time or downloading certain configuration files remotely to correct configuration problems is common in the service industry [11].

3. Research Method
This study draw the conclusion by examine the implementation of network management in the selected of 6 (six) companies that operate at service industry through group delegation to identify what is called as standard and continuous monitoring. The process of observation utilized field notes, which are coding sheets to adjust with the fundamental theories based criteria and to anticipate activities that can be very critical to understand the contextual setting. This research method has been selected to provide an essential meaning of a phenomenon, situation and behaviour by explaining in detail the network characteristics. The network management standard in this case study was referenced to IETF RFC 6632 and ITU-T M.3703 that help the system developers and user to select appropriate standard fault management protocols and data models to address relevant management needs [12, 13]. To be precise, the company or PT.A has delivered service in the telecommunication service while PT.B in housing industry, then PT.C in packaging industry, next PT.D has provided internet service, later PT.E in consultant industry and lastly PT.F has presented service in the energy field. Then, the measurement of the score based on the interpretation of observation in the field.

4. Analysis and Discussion
Since managing corporate networks is tedious, time-consuming, and error-prone, network administrators rely heavily on tools to support their daily activities. The chosen network management tool must support all activities or some tools can be integrated to provide this service. In general, errors can be identified by requesting diagnostic tests and status updates from resources that trigger an alert. Before fixing a problem, network administrators might want to divert traffic from these resources to ensure a minimum loss of service. After the error has been identified and analysed, corrective action can be taken. This administrator might include a damaged hardware or debug replacement. Some debugging can be done automatically, with error management programs starting independently in script mode when certain problems occur. As a whole, network fault management comprises a variety of functions. Here are some examples of actions and services performed by fault management systems to keep the network operational such as the definition of thresholds for potential failure conditions, the constant monitoring of system status and usage levels and continuous scanning for threats, such as viruses and Trojans. Meanwhile, the network administrator should conduct general diagnostics, provide the remote control of system elements with including workstations and servers from a single location as well as have the alarms mechanism that notify administrators and users of impending and actual malfunctions. In addition, the process of tracing the locations of potential and actual malfunctions should be fulfilled in the easiest way such as automatic correction of potential problem-causing conditions, automatic resolution of actual malfunctions and detailed logging of system status and actions taken. Thus, this study establish the description of required activities to evaluate the process of fault management in respective company through implication, parameter and level.

| No. | Process       | Description                                                                 | Implication                                                        |
|-----|---------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------|
| 1.  | Fault Prediction | Determine the possibility of structural imperfection within network device and system that might happen before the event take place through certain technique or methods | Present measurable step to accelerating slip or transient in the networking device and system in anticipate every possible bad case scenarios |
| 2.  | Fault Detection | Identification of unpermitted interruption of feature or ability to execute standard function under specified operating conditions | Early detection of system or device faults can help avoid further abnormal event progression |
| 3.  | Fault Localization | Produce the output of ranked list of suspicious                              | Focus the attention on the suspicious lists such                      |
code locations at which the program may be defective as lines, statements or declarations instead of debugging the network system

4. Fault Diagnosis
Analyze the root causes by identify the cause and effect of specific or combination faults within the system frame to be resolved in eventual event
Support the process of accurately reproduce the result that keep track of extensible the unprecedented event lead to faults

5. Fault Isolation
Trace the faults to be secluded to the other process to present the clear condition of what is happening within the current network system
Suggest or keeping apart the network fault that is identified from the other activities process

6. Fault Recovery
Evaluate the effect of the fault on the service and autonomously implement restoration in order to minimize degradation or disruption
System initialization at different level through activation of a backup software, a fallback software load, download of a software unit, etc.

7. Error Correction
Reconstruction of the original with changing the inaccuracy due to the channel noise in the transmission process within the network system
Enable the reliable delivery of the data over unreliable channel or medium through consistency and integrity checks

8. Event Correlation
Build reactive applications for the event notification service and the workflow moderator, which allows consumers to subscribe to syndicated event patterns
Present an additional dimension to data management and increases the scalability or performance of distributed systems

9. Problem Resolution
Describe the measurable action to avoid, prevent, anticipate and migrate the problem, either by minimalize errors or optimize procedure in network fault management
Improve the sustainability of the network service through systematic troubleshooting process and judgment procedure

10. Restoration of Service
Monitor the network failure points or bad configuration to return the activities in the normal network operations, even improve the quality of the network services
Prevent the disruption of the network system that bringing down the performance of organizational assets and facilities

11. Alarm Acknowledgment
Maintenance function that aids the operator in his day-to-day management activity of his network as the indicator of certain problem
Allow the same information to be managed in term of current responsibility for handling

12. Clearing of alarms
Consequences of corresponding faults need to be repaired, which the procedure dependent to the scope
Generate implicit request to optimize the service in specific threshold

13. Examination of Error Logs
Facilitate the routine to check the generated message in the network system indicated the status or the occurrence of events
Clarification the entity that originated the content of the message

| Table 2. The Matrix Score of Evaluation in Fault Management |
|----------------------------------------------------------|
| Parameter | Level |
| No indicator that organization has implemented fault management | 0 |
| Manual workforce has been executed based on certain instruction | 1 |
| Organization conduct monitoring process of certain activities | 2 |
| Employ certain known standard technique in fault management | 3 |
| Automatically executed by the agent in the network environment | 4 |
| Assessment of fault management has been executed in certain period | 5 |

Actually, there are many techniques that can be used in fault prediction such as regression tree method, s-plus, multinomial model, SMOTE, fault content method, genetic algorithm, Six CK metrics, Ant Colony Optimization, Goel-Okumoto, etc. [14]. On the other hand, there are several fault detection methods for overlapping errors namely data methods and signal models (limit and trend checking, data analysis/PCA, spectrum analysis and parametric model, pattern recognition), process model based methods (parity equations, state observers, parameter estimation, nonlinear models) and knowledge based methods (expert system, fuzzy logic) [15]. Meanwhile, there is insignificant differences between spectrum-based fault localization (SBFL) and mutation-based fault localization (MBFL), which there is also no significant relationship between the results for real and artificial faults [16]. Diagnosing and isolating network faults either wired or wireless, of course a difficult problem because of the interactions between the different network entities and the interactions between faults.
where the mechanism to assess still receive a little attention in the research community [17]. To design tolerant system errors, discovery and debugging errors are very important. Errors occur in programs when information is sent from one node to another node [18]. In addition, the recent evolution of ubiquitous computing has brought with it a significant increase of event monitoring capabilities by wireless devices and sensors, which require new, more sophisticated of event correlation over time and space [19]. Furthermore, event correlation can provide overall look of the traffic or event within the network system to represent the actual condition or pinpoint the important one, which can be classified into step by step decomposition, which are event filtering, event aggregation, event de-duplication, event masking, root cause analysis and action trigger [20].

Table 3. Observation of Respective Company in Implementing Fault Management

| No. | Process                | PT. A | PT. B | PT. C | PT. D | PT. E | PT. F |
|-----|------------------------|-------|-------|-------|-------|-------|-------|
| 1.  | Fault Prediction       | 5     | 1     | 1     | 4     | 3     | 3     |
| 2.  | Fault Detection        | 4     | 1     | 2     | 3     | 3     | 3     |
| 3.  | Fault Localization     | 4     | 0     | 1     | 3     | 3     | 2     |
| 4.  | Fault Diagnosis        | 4     | 1     | 1     | 4     | 3     | 2     |
| 5.  | Fault Isolation        | 3     | 1     | 1     | 4     | 3     | 3     |
| 6.  | Fault Recovery         | 5     | 1     | 2     | 4     | 3     | 4     |
| 7.  | Fault Correction       | 4     | 1     | 1     | 2     | 3     | 3     |
| 8.  | Event Correlation      | 2     | 1     | 1     | 2     | 1     | 1     |
| 9.  | Problem Resolution     | 5     | 2     | 3     | 4     | 3     | 4     |
| 10. | Restoration of Service | 4   | 2     | 3     | 4     | 3     | 4     |
| 11. | Alarm Acknowledgement  | 3     | 0     | 1     | 3     | 0     | 4     |
| 12. | Clearing of Alarms     | 3     | 0     | 1     | 3     | 0     | 4     |
| 13. | Examination of Error Logs | 4 | 1     | 2     | 4     | 3     | 4     |

From the evaluation metrics, this study conclude that PT. B still in the infant phase of implementing best practice of network management based on standard, while PT. A become the best among the others although there are certain process need to be improved such as event correlation, fault isolation, alarm acknowledgement and clearing alarms. Interestingly, the level of event correlation in each of company were not reached 3 as it showed the monitoring has been done due to several event or certain directive policy from executives. There are also three kind of activities that has not been implemented yet in the organization due to several reason such as there is no employee that has capabilities in network management or lack of skill within available environment. In recent years, identity theft has become one of the fastest growing crimes. The internet has facilitated this phenomenon because it is a very open portal and allows the tracking process of confidential information from certain users due to its availability in various social media applications for those who understand how to look for it [21]. Due to high cost of equipment, complexities of network structure and higher demand of larger bandwidth, it is not realistic to assume that all nodes are equipped with full monitoring capabilities, thus obtaining periodic information from nodes with high capabilities is critical for successful network fault management [22].

5. Conclusion

When the network becomes larger and more complex, it is more difficult to manage due to its heterogeneity and relationship in each process. The most common and serious problems in the network are connection failures or crash management especially to determine the recommended time and process for respective errors activities. Actually, network management solutions must be easy to implement and cost-effective, in which they must have a simple user interface, quick and easy implementation to eliminate huge load than can affect in the future process. Network administrators also should be able to use network management tool effectively to implement network monitoring, performance management, and remote device configuration from a central point to manage network devices in multiple locations in order to obtain effective and efficient process.
References

[1] Rao UH. 2011. Challenges of Implementing Network Management Solution. *International Journal of Distributed and Parallel Systems (IJPDS)* 2(5).

[2] Boutaba R and Xiao J. 2002. Network Management: State of the Art. *Springer Comm. Sys.*, 92 pp. 127-145.

[3] Ahmad B, Jian W and Ali ZA. 2018. Role of Machine Learning and Data Mining in Internet Security: Standing State with Future Directions. *Journal of Computer Networks and Communications*, 6383145.

[4] Lowman S. 2010. Central Issues in Network Management. Available at: https://www.lowmanio.co.uk/share/CentralIssuesinNetworkManagement.pdf

[5] Brar HS and Kumar G. 2018. Cybercrimes: A Proposed Taxonomy and Challenges. *Journal of Computer Networks and Communications*, 1798659.

[6] Lubis M and Azizah AH. 2018. Towards Achieving the Efficiency in Zakat Management System: Interaction Design for Optimization in Indonesia. *User Science and Engineering*, pp. 289–301.

[7] Awoyemi BS. 2018. Network Restoration for Next-Generation Communication and Computing Networks. *Journal of Computer Networks and Communications*, 4134878.

[8] Ray PP. 2018. Creating Values out of Internet of Things: An Industrial Perspective. *Journal of Computer Networks and Communications*, 1579460.

[9] Fonseca PCR and Mota ES. 20017. A Survey of Network Fault Management in Software-Defined Networks. *IEEE Communications Surveys & Tutorials*, 19(4), pp. 2284-2321.

[10] Toy M. 2014. Self-Managed Networks with Fault Management Hierarchy. *Procedia Computer Science* 36, 373-380.

[11] Branch JW and Gutierrez SA. 2010. System Monitoring and Fault Management Methods and Techniques. *Revista Avances en Sistemas e Informatica*, 7(2), 139-148.

[12] IETF. 2012. *An Overview of the IETF Network Management Standards*. Request for Comments: 6632, Internet Engineering Task Force, June.

[13] ITU-T. 2010. *Common Management Service – Alarm Management – Protocol Neutral Requirement and Analysis*. Telecommunication Standardization Sector: M. 3703 (06/2010). International Telecommunication Union.

[14] Sings PS, Panda RK and Sangwan OP. 2015. A Critical Analysis on Software Fault Prediction Techniques. *World Applied Sciences Journal* 33(3), pp. 371-379.

[15] Miljkovic D. 2011. Fault Detection Methods: A Literature Review. MIPRO/CTS, pp. 110-115.

[16] Pearson S, Campos Jose, Just R, Fraser G, Abreu R, Ernst MD, Pang D and Keller B. 2017. Evaluating and Improving Fault Localization. *Int. Conf. on Software Engineering*.

[17] Qiu L, Bahl P, Rao A and Zhou L. 2003. *Fault Detection, Isolation and Diagnosis in Multihop Wireless Networks*. Technical Report MSR-TR-2004-11, Microsoft Research.

[18] Sadi MS, Bachar PK, Ghosh P and Rahman MS. 2013. A New Error Correction Coding Approach. *Journal of Advances in Information Technology*, 4(3), pp. 142-147.

[19] Yoneki E and Bacon J. 2005. Unified Semantics for Event Correlation Over Time and Space in Hybrid Network Environment. *LNCS* 3760, pp. 366-384.

[20] Pandey NK, Zhang K and Weiss S. 2014. Distributed Event Aggregation for Content-based Publish/Subscribe Systems. *ACM DEBS*.

[21] Lubis AR, Fachrizal F, Lubis M and Tahir HM. 2018. Wireless Service at Public University: A Survey of Users Perception on Security Aspects. *Proc. of IEEE ICOIACT*.

[22] Premadi A. 2016. Network Management in Optical Communication. *Proc. of ICTIS*. 