2008

The OSI Network Management Model - Capacity and performance management

Chompu Nuangjamnong
Edith Cowan University

Stanislaw P. Maj
Edith Cowan University

David Veal
Edith Cowan University

10.1109/ICMIT.2008.4654552

This article was originally published as: Nuangjamnong, C. , Maj, S. P., & Veal, D. R. (2008). The OSI Network Management Model - Capacity and performance management . Proceedings of 4th IEEE International Conference on Management of Innovation and Technology . ICMIT 2008. (pp. 1266-1270). Bangkok, Thailand. IEEE. Original article available here

The OSI Network Management Model- Capacity and Performance Management

C. Nuangjamnong, S. P. Maj, D. Veal
School of Computing and Information Science, Edith Cowan University, Perth, Western Australia
(*cnuangja@student.ecu.edu.au, {p.maj, d.veal}@ecu.edu.au*)

Abstract - **With the rapid growth of large enterprise networks, capacity and performance management issues are becoming increasingly important to both business organizations and the telecommunication industry. Capacity and performance management techniques and methods provide guidance on how to plan, justify and manage network resources. Inappropriate planning for capacity and performance may lead to wasted resources resulting in unnecessary cost, or lack of resources resulting in poor network performance or even the unavailability of IT services. Moreover, it is not uncommon for networks to be equipped with devices from different vendors which potentially add to complexity. Resource management may be assisted by using a network management framework. The OSI Network Management Model (NMM) is the standard model and provides a conceptual framework for organizing a diverse range of network resources. This paper is an analysis of the OSI NMM to evaluate its use within large enterprise networks focusing upon capacity and performance management.**

Keywords – **Capacity planning, network management, performance management, the OSI Network Management Model**

I. INTRODUCTION

Network managers are facing increasing challenges to provide improved higher rates of system performance. Problems faced include unscheduled down time, lack of staff with appropriate expertise, insufficient tools, complex technologies, business consolidation, and competitive markets. The paper is a systematic evaluation of the OSI NMM.

A. Network capacity planning and network performance management

Network performance management is the practice of managing network service response time, consistency, and quality of individual and overall services [1]. Capacity planning of network resources is necessary in order to minimize adverse performance or even lack of IT availability which can result in negative impacts on business performance. Most network performance management problems involve capacity issues, which in turn affect network application demands. Therefore, business organizations need to collect relevant networking information as the basis for identifying potential problems, planning changes, and implementing new capacity and performance functionality into their networks. However, business organizations do not always perform trend analysis to enable a determination of the affect of network changes to future situations (figure 1) [2].

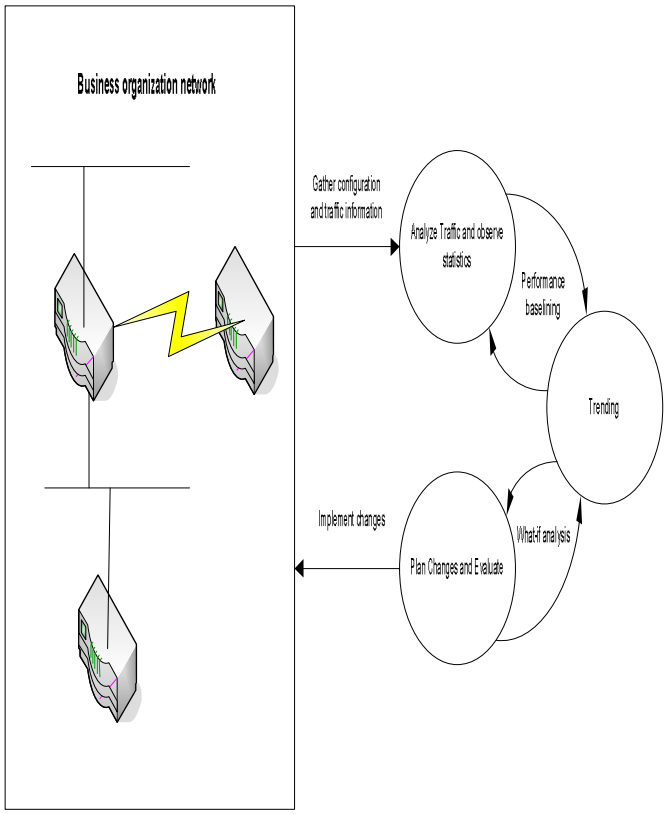

Figure 1. Network capacity and performance management processes

Network capacity and network performance management are the discipline of managing how networks function, the delivery of the lowest latency, highest capacity, and maximum reliability regardless of intermittent failures and limited bandwidth [1]. For example, various factors in network capacity and network performance management include central processing unit (CPU) power, memory performance and capacity, buffering, queuing and bandwidth. Failure to ensure the system as a whole is performing correctly is a core issue for managing network traffic. If these resources are insufficient this can result in networks operating non-optimally [1].

978-1-4244-2330-9/08/$25.00 ©2008 IEEE

With a variety of network systems, the functional process of network performance management consists of measuring, modeling, planning, and optimizing networks to ensure that they carry traffic with the speed, reliability, and capacity appropriate for the nature of the application and the cost constraints of the organization [3].

Cisco Systems [1] notes that there are five functional areas in network capacity and network performance management:

1. Service level management is a demonstrated methodology, which copes with network resources by defining a deliverable and creating two-way accountability for a service attachment.
   - User and business organization agreements
   - Case-by-case funding
2. Network and application provides 'what-if' analysis and defines the outcome of a planned change. Network changes can result in the collapse of the network causing many hours of production down time. Without a 'what-if' analysis business organizations can take significant risks to change-success and overall network availability.
3. Baselining and trending offer network administrators the ability to plan and complete network upgrades before a capacity problem results in network down time or performance problems.
4. Exception management identifies the methodology for resolving capacity and performance issues. For example, network administrators may receive an alarm indicating a high CPU load on a router; they can then login to the router to determine why CPU load is high. After that, they may reconfigure the router to reduce the CPU load. In some network management tools, there is a feature to enable the setting thresholds and alarms when a violation is detected.
5. Quality of Service (QoS) management relates to creating and monitoring specific traffic classes within the network. Traffic classes are created based on performance of service level agreements (SLAs) for the more business critical applications and specific application requirements. However, managing QoS configurations is still potentially a problematic, which can be due a lack of tools and/or suitable measurement methods [1].

B. The OSI Network Management Model

Rapid network developments in recent years coupled with the introduction of large number of new technologies and the expectation of new services, in possibly a multi-vendor environment, mandate an improvement in network management. One possible solution is the Open Systems Interconnection (OSI) Network Management Model (NMM). The OSI has developed a standard network management model [4], [5], [6]. This is known as the Network Management Model. This model provides a framework and guidelines for the control, maintenance and supervision of large networks [7], [8]. This model is also referred to as the *OSI Telecommunication Management Network Model* or *ISO NMM.*

According to the International Organization for Standardization [9], the OSI NMM defines a conceptual model for managing all communication "entities" within a network. There are three basic components comprising the elements of the management architecture to support a successful implementation of the OSI NMM:

- A functional component involved with the various activities performed in support of network management.
- A communication component which focuses upon how the information is exchanged between the managed systems.
- An information component involved with five major functional areas (fault, configuration, accounting, performance, and security management (FCAPS)) in IT management which facilitate rapid and consistent progress within each category's individual areas [9]:
  1. Fault management (F) is an event, which has a negative significance. This functional management is designed to detect, recognize, isolate, correct, and log faults that occur in the network. This function uses trend analysis to predict error with the intention that the network is always available and to keep network running effectively.
  2. Configuration management (C) is concerned with monitoring network systems and system configuration information; therefore, the effects on network operation of various versions of hardware and software elements can be tracked and managed.
  3. Accounting management (A) is involved with gathering of usage statistics of the users. These statistics on the network systems can be regulated which can minimize network problems and maximize the fairness of network access across all users.

4. Performance management (P) determines the efficiency of the current network, for example, the relationships to the investments initially undertaken to install the network. The network performance addresses the throughput, percentage utilization, error rates, and response time considerations. By collecting and analyzing performance data the network's health can be monitored. Trends analysis can indicate capacity and reliability issues, which can determine if a particular network problem is worthy of attention.

5. Security management (S) is the process of controlling access to assets in the network systems. This can identify sensitive network resources and determine mappings between these resources and user sets. This process also monitors access points to sensitive network resources and logs any inappropriate access to sensitive network resources [9], [10].

Using FCAPS it is possible to define and hence manage an organization's Information Technology (IT) infrastructure. Employees and customers rely on IT services where availability and performance are mandated, and problems can be quickly identified and resolved. Mean time to repair (MTTR) must be as short as possible to avoid system downtimes where a loss of revenue is possible [9], [10], [11].

C. Large enterprise network environment

Network management is frequently viewed as only a technical problem that does not include human factors. However, the ultimate responsibility for management exists with people and their requirements, not machines [12], [13]. A business must provide users with the ability to access, store and process the current network to obtain relevant information relevant to their needs. Such access may be be effected by the network's performance and capacity. Hence, the major components of large enterprise network management are the:

- End-users who are interested in the operation and use of the network.

- Network resources which are involved in physical and logical network components.

- Functional enterprise network management which relates to setting policies, network activities, and designing network structures.

- Human as well as the software and hardware elements involved in making decisions and network management tools which provide network capacity and performance management [13].

II. CONCEPUAL FRAMEWORK

This study has concentrated upon a quantitative research method because it directly relates to the use of the combination of functionalities within the OSI NMM in business organization networks. The purpose of this study is to analyze the possibility of using the OSI network management model within large enterprise networks by focusing on capacity and performance management. The results of the analysis of this study could be employed to reduce the complexity of network systems.

This study is based on a large enterprise network - the Network Technology Lab National Electronics and Computer Technology Center (NECTEC) in Thailand. NECTEC is used as a case study, focusing on a LAN that uses centralized network management in an e-Learning system. Consider the LAN which uses the OSI reference model as a framework to develop the OSI NMM. Figure 2 represents the components needed for network management when combined with the OSI reference model. These are:

- Network administrator refers to IT professionals who can operate network management functions.

- Network application refers to an automated tool which can use to monitor and control network activities.

- Network management protocol refers to protocol layer which can maintain network configurations and status of network systems.

- Network management agents provide communication services and cooperate with network management application.

- Network object entities define physical network resources that can be managed.

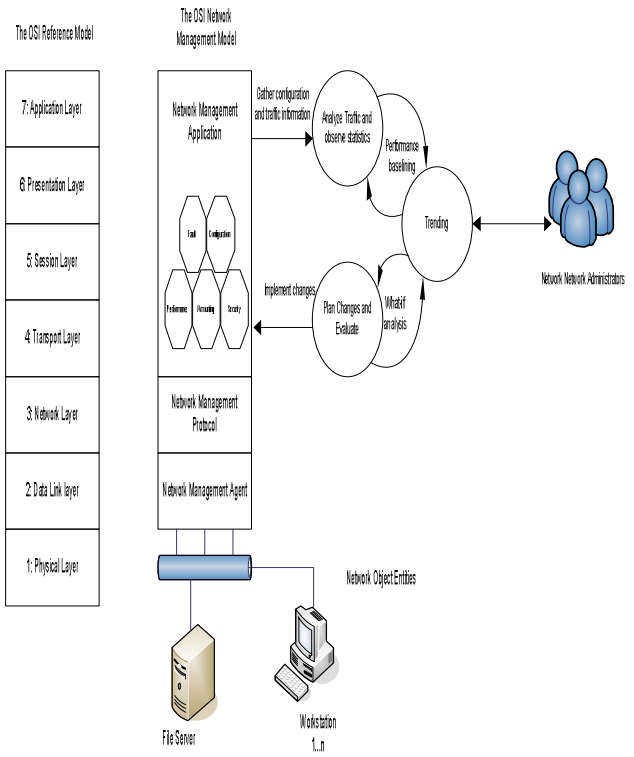

Figure 2. Integrated network capacity and performance management processes into the OSI NMM

NECTEC has a combination of multiple enterprise networks which is managed by Thai government; hence, those networks can be seen as a heterogeneous model which provides various services and information.

The variety of services on NECTEC networks need to utilize many different protocols; therefore, the general capacity and performance management based on the OSI NMM could be taken as:

- The ability to manage entire networks or subnetworks
- The ability to manage the combination of wide area networks (WAN) and local networks (LAN)
- The ability to manage a variety of network resources
- The ability to provide the basic management functions; fault, configuration, accounting, performance and security management

III. DISCUSSION

The results from an analysis of the OSI NMM reveal that it is possible to use and apply it to a large enterprise network. Also, the OSI NMM provides a single set of tools for managing and monitoring entire network's resources. This may be particularly important in a multi-vendor system. According to Koanantakool [14]:

"Enterprises with different types of networks will have the problem of dealing with multiple management tools, and each different type of network or brand of network equipment has different ways for managing those resources" [14].

This paper recommends the use of a single NMM in conjunction with FCAPS and hence addresses the following:

Fault management
- QoS management should reduce Mean Time To Recovery (MTTR) by monitoring and troubleshooting an extensive array of network technologies

Configuration management
- Service level management should support large or geographically dispersed environments with its distributed server architecture, including consolidated, enterprise-wide reporting and global configuration capabilities
- Network and application 'what-if' analysis should achieve proactive control of complex infrastructures, such as switched networks, load-balanced configurations, redundant segments and virtual circuits, to help network administrators fully understand how application traffic is transported across the enterprise network
- Baselining and trending should monitor traffic to optimize resources by identifying over- and under-utilized physical and logical segments, enabling network administrators to redistribute load and balance costs

Accounting management
- Network and application 'what-if' analysis should gain quantifiable business justification by understanding and reporting on which applications consume your network resources in order to postpone upgrades and justify growth and policy decisions
- Exception management should provide a cohesive and integrated view into all the applications and technologies that comprise the business services traversing today's enterprise networks

Performance management
- Service level management should proactively combat network congestion by reporting on bandwidth growth and forecasting capacity shortfalls
- Baselining and trending should determine baseline current traffic patterns to ensure new applications can be supported during peak activity periods

- Exception management should support and plan enterprise-wide network capacity with a unified performance management solution that will provide all data sources and areas of your network from the core to access layers, including higher speed networks such as 10 Gigabit Ethernet.

- QoS management should monitor curtail network misuse for better network utilization by identifying and reporting on non-business uses of the network

Security management

- QoS management should evaluate and optimize the QoS results by monitoring the new traffic patterns and testing the response times of the targeted applications

However, the OSI NMM characteristics are focused principally on monitoring, accounting, and controlling network environment (activities and resources), but they do not including planning and organizing network resources. Consequently, if the network is not planned and organized properly, any amount of monitoring, accounting, and controlling may be ineffective.

V. CONCLUSIONS AND FURTHER WORK

A preliminary analysis was conducted of a large enterprise network with particular attention being given to capacity and performance management. The system selected was the NECTEC. Results to date suggest that the OSI NMM substantially met the requirements of a network management system. However this paper recommends the integration of the OSI NMM with the FCAPS criteria in order to more substantially meet capacity and performance standards. Further work however is needed in order to address other human resource based factors such as skill sets, experience etc. Human factors must be recognized as essential for improving the management of network systems.

REFERENCES

[1] Cisco Systems, "Capacity and Performance Management," October 2005. [Online]. Available: Cisco Systems White Paper, http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008011fde2.shtml. [Accessed January 24, 2008]

[2] P. Weilnau, "Capacity Analysis Considerations for Web-based Applications," in *ISM: The power behind great IT decision*, October 2003. [Online]. Available: The Information Systems Managers Inc., http://www.techsearch.co.kr/down/perfman/white%20paper/CACWebApps.pdf. [Accessed January 18, 2008]

[3] NetQoS Inc, "Understanding Performance Management," in *Network Performance Daily*, October 2006. [Online]. Available: http://www.networkperformancedaily.com/2006/10/understanding_performance_mana.html. [Accessed March 4, 2008].

[4] IntelliGrid Architecture, "OSI Network Management Model," 2004. [Online]. Available: Electronic Power Research Institute, http://intelligrid.info/IntelliGrid_Architecture/New_Technologies/Tech_OSI_Network_Management_Model.htm. [Accessed January 12, 2008].

[5] Y. Yemini, "The OSI network management model," in *Communications Magazine, IEEE,* vol. 31, no. 5, pp. 20-29, May1993.

[6] N. Jailani and A. Patel, "FMS: A computer network fault management system based on the OSI standards," in *Malaysian journal of computer Science,* vol. 11, no. 1, pp. 22-31, June 1998.

[7] J. McCallum, "Cyber security: A crisis of prioritization, " in *Reports to the President – Archive*, February 2005, pp. 1-58. [Online]. Available: National Coordination Office for Networking and Information Technology Research and Development, http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf. [Accessed March 6, 2008].

[8] International Telecommunication Union 2008, "Handbook on new technologies and new services: Fascicle 2," *Network and service management,* 2008.

[9] International Organization for Standardization, "Information technology - Elements of management information related to the OSI Network Layer," *International Standards for Business, Government and Society,* 1998.

[10] J. Parker, "FCAPS, TMN & ITIL: Three key ingredients to effective IT management," in *Enterprise Management System,* pp. 5-7, May 2005. [Online]. Available: OpenWater Solutions, http://www.openwatersolutions.com/docs/FCAPS_TMN_%20ITIL.pdf. [Accessed March 8, 2008].

[11] Future Software Limited, "FCAPS," in *India: Flextronics Software Systems,* pp. 1-7, 2005. [Online]. Available: Flextronics Software Systems White paper, http://www.futsoft.com/pdf/fcapswp.pdf. [Accessed February 20, 2008].

[12] C. A. Joseph and K. H. Muralidhar, "Integrated Network Management in an Enterprise Environment," *IEEE Network Magazine,* vol. 4, no. 4, pp. 7-13, July 1990.

[13] R. Aronoff, M. Chernick, K. Hsing, K. Mills, and D. Stokesberry, "Network Management Functional Requirements," in *National Institute of Standards and Technology (NIST) Special Publication 500-175,* November 1989. [Online]. Available: Information Technology's NIST Special Publication 500: Information Technology Series, http://www.itl.nist.gov/lab/specpubs/sp500.htm. [Access January 26, 2008].

[14] T. Koanantakool, "IT Project into the Future," in *National IT projects in Thailand,* 1997. [Online]. Available: National Electronics and Computer Technology Center (NECTEC), http://www.nectec.or.th/it-projects/1997.html. [Accessed March 15, 2008].