NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN EVALUATION OF MANAGEMENT TECHNIQUES FOR SONET/SDH TELECOMMUNICATION NETWORKS

by

Wee Shoong Lim

September 2004

Thesis Advisor:	John C. McEachen
Second Reader:	Randy L. Borchardt

Approved for public release; distribution is unlimited

THIS PAGE IS INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) An Evaluation of Management Techniques for SONET/SDH Telecommunication Networks			**5. FUNDING NUMBERS**
6. AUTHOR(S) Lim, Wee Shoong			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

A study of SONET network management applications and the load they impart to the network is conducted to provide a better understanding of the capability of various management approaches. In this study, a SONET network is set up in the Advanced Networking Laboratory of the Naval Postgraduate School using four Cisco ONS 15454s. Next, two Element Management Systems, the Cisco Transport Controller and the Cisco Transport Manager, are deployed onto the SONET network. Subsequently, the network traffic of the Element Management Systems is captured and analyzed using a packet analyzer. Link utilization of the two tools is computed using the first–order statistics of the captured traffic distributions. In addition, the Hurst parameter is estimated using the variance–index plot technique (which uses higher–orders statistics of the modeled distributions) to determine the captured traffic's degree of self–similarity. Finally, the calculated utilization is extrapolated to obtain the link utilization for 2500 network elements (the maximum number supported by the Cisco Transport Manager). The result obtained is useful in determining the maximum number of network elements (Cisco ONS 15454s) that the Cisco Transport Manager can support from a network loading point of view.

14. SUBJECT TERMS Cisco Transport Controller, Cisco Transport Manager, Element Management Systems, Network Management, SNMP, SONET, SDH, Optical Networks, Self–similarity, Queuing Theory and Traffic Analysis.			**15. NUMBER OF PAGES** 75
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE IS INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN EVALUATION OF MANAGEMENT TECHNIQUES FOR SONET/SDH TELECOMMUNICATION NETWORKS

Wee Shoong Lim
Civilian, Ministry of Defense, Singapore
B.E. (Hons), Nanyang Technological University, Singapore, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Wee Shoong Lim

Approved by: John C. McEachen
Thesis Advisor

Randy L. Borchardt
Second Reader

John P. Powers
Chairman, Department of Electrical and Computer Engineering

THIS PAGE IS INTENTIONALLY LEFT BLANK

ABSTRACT

A study of SONET network management applications and the load they impart to the network is conducted to provide a better understanding of the capability of various management approaches. In this study, a SONET network is set up in the Advanced Networking Laboratory of the Naval Postgraduate School using four Cisco ONS 15454s. Next, two Element Management Systems, the Cisco Transport Controller and the Cisco Transport Manager, are deployed onto the SONET network. Subsequently, the network traffic of the Element Management Systems is captured and analyzed using a packet analyzer. Link utilization of the two tools is computed using the first–order statistics of the captured traffic distributions. In addition, the Hurst parameter is estimated using the variance–index plot technique (which uses higher–orders statistics of the modeled distributions) to determine the captured traffic's degree of self–similarity. Finally, the calculated utilization is extrapolated to obtain the link utilization for 2500 network elements (the maximum number supported by the Cisco Transport Manager). The result obtained is useful in determining the maximum number of network elements (Cisco ONS 15454s) that the Cisco Transport Manager can support from a network loading point of view.

THIS PAGE IS INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE IS INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE IS INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my gratitude to the following persons for offering assistance and support to make this thesis possible.

First and foremost, many thanks to Prof. John McEachen for being there and providing the necessary guidance, resources and advice. His encouragement and support had enabled a smooth research and writing process for me.

I would also like to thank Prof. Randy Borchardt for his time and effort in reviewing this thesis.

Special thanks also go to Lt. Matthew Klobukowski and Lt. James Young for their assistance to this study. Matt had set up the SONET network that formed the test environment while James provided the Mathcad program that generated the samples from the captured traffic for statistical analysis. His program had greatly reduced the time taken for me to perform the analysis.

I am also grateful to Mr. Kazuhiro Hara from NEC Corporation and Mr. Herbert B. Shulman from AT&T for their prompt replies to my queries.

Last, but not least, I would like to thank my wife, Aileen, together with Winnie, for being there to support me through my work.

THIS PAGE IS INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Since its introduction into telecommunications networks, fiber optic technology has enabled the telecommunications industry to provide better quality of service at huge cost savings to consumers. Subsequently, optical standards such as SONET/SDH were proposed and adopted to ensure interoperability between equipment of different vendors. Due to popular demand, the size of SONET/SDH networks has grown vastly, thus becoming increasingly difficult to manage. Therefore, it is critical to have management tools that can interface with SONET/SDH equipment to poll and acquire information from connected network elements (NEs). Consequently, management overhead traffic is injected into the network by the respective management tools and their connected NEs.

In this study, SONET network management applications, in particular Element Management Systems (EMSs), and the load they impart into the network are investigated to provide a better understanding of the capability of various management approaches. A SONET network was set up in the Advanced Networking Laboratory of the Naval Postgraduate School using four Cisco ONS 15454s.

During a preliminary market survey, it was found that most SONET/SDH equipment manufacturers build their own EMS to support their own products. In addition, there are few third–party EMSs that can interface with multi–vendor's products. Therefore, the two EMSs deployed onto the Advanced Networking Laboratory's SONET network are the Cisco Transport Controller (CTC) and the Cisco Transport Manager 4.6 (CTM 4.6).

The CTC was set up in the Cisco ONS 15454 to collect and monitor the NEs on the SONET network. The NEs' information was collated at one NE and forwarded to a CTC client that was connected to the NE through an Internet Protocol (IP) network. The same NE was also connected to a Sun Solaris workstation, which was configured with the CTM 4.6 server, through the same IP network. Subsequently, packet analyzers (Ethereal) were deployed on the IP network to passively capture the network traffic inbound and outbound from the CTC client and the Sun Solaris workstation.

In the first round of analysis using Ethereal, it was revealed that both the CTC and CTM 4.6 use a proprietary Socks protocol (which incorporated General Inter–Orb Protocol) that connects to TCP Port 1080. The CTM 4.6 also uses SNMP. Therefore, the captured traffic was divided into five categories: CTC's Socks traffic, CTM 4.6's Socks traffic, CTM 4.6's SNMP traffic, CTM 4.6's Socks and SNMP traffic, and CTM 4.6's Ethernet traffic. Then the categorized traffic underwent a data pruning process using Microsoft Access.

Next the interarrival times and packet sizes of the pruned data were analyzed statistically using Mathcad and Micrsoft Excel (as the plotting tool). Using first–order statistics, the link utilizations of the five categories of traffic were computed and linearly extrapolated to obtain the link utilizations of the same traffic for 50 NEs (the CTC's capacity) and 2500 NEs (the CTM 4.6's capacity). The results show that the CTC will utilize about 1.7% of the Section Data Communication Channel's (SDCC) capacity of 192 kbps when managing 50 NEs while the CTM 4.6 will utilize about 93% of the SDCC's capacity when managing 2500 NEs.

In addition, the Hurst parameter for the interarrival time distributions and the packet size distributions were estimated using the variance–index plot technique (which uses higher–orders statistics) to determine the degree of self–similarity. The results show that the CTC's traffic has a high degree of self–similarity while the CTM 4.6's traffic resembles M/M/1 traffic with a Hurst parameter value close to 0.5.

Finally, by plotting the mean network utilization versus the queue depth for the estimated Hurst parameters, utilizations for the CTC and the CTM 4.6 (taking into account the burstiness of the CTC and CTM 4.6's traffic) were obtained. The results show that, although the CTC's traffic is self–similar and bursty, the low link utilization (for managing 50 NEs) requires a small queuing buffer. On the other hand, a much larger queuing buffer is required to support the high link utilization of the CTM 4.6 (for managing 2500 NEs). Thus it is possible but not advisable to use the CTM 4.6 for managing 2500 NEs. Instead, it is recommended to use the CTM 4.6 for managing up to 1027 NEs, operating within a link utilization of 38% that can be supported by a relatively much smaller queuing buffer.

LIST OF SYMBOLS, ACRONYMS, AND/OR ABBREVIATIONS

Alcatel	Alcatel Network Systems
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AT&T	American Telephone and Telegraph Company
CCITT	International Telegraph and Telephone Consultative Committee
Cisco	Cisco Systems
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
CORBA	Common Object Request Broker Architecture
CPU	central processing unit
CTC	Cisco Transport Controller
CTM 4.6	Cisco Transport Manager 4.6
DCC	Data Communication Channel
EMSs	Element Management Systems
Fujitsu	Fujitsu Network Transmission Systems
Gbps	gigabits-per-second
GIOP	General Inter–Orb Protocol
GUI	Graphical User Interface
H	Hurst parameter
HTTP	Hypertext Transfer Protocol
IDs	Identifications

IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Standardization for Organization
ITU-T	International Telecommunication Union–Telecommunication Standardization Bureau
J2RE	Java 2 Runtime Environment
Java-RMI	Java Remote Method Invocation
JRE	Java Runtime Environment
kB	kilobytes
kbps	kilobits-per-second
log	logarithmic function
Lucent	Lucent Technologies
M/M/1	System with exponential interarrival and service times
MA	Mobile Agents
Mbps	megabits-per-second
ms	milliseconds
NEC	NEC Transmission
NEs	Network Elements
NML-EML	Network Management Layer–Element Management Layer
NMSs	Network Management Systems
NPS	Naval Postgraduate School
OAM&P	Operations, Administration, Maintenance, and Provisioning
ONS 15454	Optical Network System 15454
OS	Operating System

OSI	Open System Interconnection
PC	Personal Computer
PM	Performance Monitoring
q	queue depth
s	seconds
SDCC	Section Data Communication Channel
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SNMPv2	Simple Network Management Protocol Version 2
SONET	Synchronous Optical Network
TCC+	Timing Control Card Plus
TCP	Transport Control Protocol
TL1	Transaction Language 1
TMF	Telemanagement Forum
TNS	Oracle's proprietary communications protocol
T_S	service time
UDP	User Datagram Protocol
λ	mean arrival rate in items per second
µs	microseconds
ρ	mean network utilization

THIS PAGE IS INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

Since the telecommunications industry started using optical fiber for their telecommunications networks in the 1980s, they have been able to provide better network quality at a huge cost savings to their customers. These benefits have generated substantial research in optical fiber technologies and created many advances in optical networks [1].

As the large–scale deployment of optical fiber began, the industry realized the need for an optical standard to ensure interoperability of optical equipment from different vendors [1]. Using the standard proposed by Bellcore, the American National Standards Institute (ANSI) introduced the Synchronous Optical Network (SONET) standard in 1985. The International Telegraph and Telephone Consultative Committee (CCITT), predecessor of the International Telecommunication Union–Telecommunication Standardization Bureau (ITU-T), modified Bellcore's proposal and created the Synchronous Digital Hierarchy (SDH) standard as the international version of the same technology [2,3].

A major feature of SONET/SDH is its scalability, which helps these standards meet the quest for higher network capacity [1]. Both technologies have evolved over the years to support up to a data rate of 40 gigabits-per-second (Gbps) at the OC-768 optical level [3]. SONET/SDH thus forms most of the core backbone networks of the Internet due to demand for high–speed network transmission used by multimedia applications and bandwidth consuming software.

As SONET/SDH networks grow in size, managing them becomes increasingly difficult. Management tools that can interface with SONET/SDH equipment to capture the relevant network information are critical. The usual management method is to poll and acquire information from network elements (NEs). In this case, it is likely that management overhead traffic is injected into the network by the respective management tool and the NEs. Therefore, it would be interesting to find out the amount of management

traffic injected into the network, and to determine either the optimum number of NEs or the maximum number of NEs that can coexist on the network before it becomes overly congested with management traffic.

B. THESIS OBJECTIVE

The primary objective of this thesis was to study and analyze the performance of management tools, particularly Element Management Systems (EMS) that are used for managing SONET/SDH networks. A SONET network was simulated under laboratory conditions with EMSs running. The network load generated by the different EMSs utilizing different communication protocols were then captured and analyzed. The analysis was done on the packet size distribution and the interarrival time in between packets distribution. The main thrust was to model the network load generated by the EMS using the concept of self–similarity so as to determine the optimum number of NEs that could be deployed on a single SONET network running the EMS, with sufficient buffers for the payload traffic based on a specific bandwidth.

C. RELATED WORK

Network management is an area of great research potential. Many papers have been written on management protocols like the Open System Interconnection's (OSI) Common Management Information Protocol (CMIP), the Internet Engineering Task Force's (IETF) Simple Network Management Protocol (SNMP), and distributed object technologies like Common Object Request Broker Architecture (CORBA) and Java Remote Method Invocation (Java-RMI).

However, as networks expand, collecting information about them becomes an exceedingly complex task for a monitoring technique based on either management protocols or distributed object technologies. Recent research is focused on the potential of deploying Mobile Agents (MA) for network monitoring purposes [4].

Within the Naval Postgraduate School (NPS), the Advanced Networking Laboratory has been actively researching network management, particularly SONET/SDH networks. Recent work by Kok Seng Lim [5], which studied the effect of SNMP traffic on

Network Management Systems (NMS), showed that a NMS can effectively manage a network with less than 200 NEs.

D. SUMMARY

This thesis is organized as follows: Chapter II discusses the SONET network management tools and the various protocols used with focus on the Cisco Transport Controller (CTC) using General Inter–Orb Protocol (GIOP) and the Cisco Transport Manager 4.6 (CTM 4.6) using Simple Network Management Protocol Version 2 (SNMPv2). Chapter III describes the procedures for setting up the laboratory SONET network, the EMS, and the capturing of the network load used in this study. Chapter IV briefly reviews the probability theory relevant to this study and the concept of self–similarity. Chapter V presents the traffic analysis done on the captured traffic and discusses the results obtained. Chapter VI concludes the study and provides suggestions on further research areas.

THIS PAGE IS INTENTIONALLY LEFT BLANK

II. SONET NETWORK MANAGEMENT TOOLS

A. CHAPTER OVERVIEW

This chapter gives a short introduction of SONET network management tools and products. It then goes on to briefly discuss the common network management protocols. Subsequently, the chapter focuses the reader on two EMSs, the CTC and the CTM 4.6.

B. INTRODUCTION

SONET network management involving operations, administration, maintenance, and provisioning (OAM&P) is provided for in the SONET standard [6]. In order to utilize that capability provided by SONET, a NMS is required. However, the NMS works only at the upper level and manages the traffic on the network domain. It manages the NEs through the use of an EMS. "The role of the EMS is to control and manage all aspects of the" NEs in a network "domain and to ensure maximum usage of the devices' resources." [7] This typically includes gathering information on the network domain through interaction with each NE and issuing commands to the NE.

Most SONET equipment and EMS are vendor–specific. The six main SONET/SDH equipment manufacturers are Alcatel Network Systems (Alcatel), Fujitsu Network Transmission Systems (Fujitsu), Lucent Technologies (Lucent), NEC Transmission (NEC), Nortel Networks, and Tellabs [6]. Alcatel 1353 GEM, an EMS product by Alcatel, supports only Alcatel's line of NEs [8]. Similarly, Fijitsu's NetSmart 500 and 1500 software are EMSs built to support Fujitsu's Flashwave family of SONET equipment [9]. Likewise, Lucent's Navis® Optical EMS supports only Lucent's optical NEs [10]. In an email correspondence with Kazuhiro Hara of NEC, he informed that NEC does not have management tools that support other vendors' products and has no plans to develop any [11]. In the same way, the Tellabs 7190 Element Manager is built for managing Tellabs' 7000 series NEs [12]. The same vendors also supply NMSs to work in conjunction with their EMSs. Alcatel and Lucent's NMSs also provide for multi–vendor NEs' interface through the use of CORBA [13,14]. Nevertheless, there is no published

case study of anyone deploying SONET equipment with a NMS from different suppliers. The only known case is that of the American Telephone and Telegraph Company (AT&T), a telecommunications service provider company that utilizes multi–vendor SONET equipment. In an email correspondence with Herbert Shulman of AT&T, he stated that AT&T develops the management tool in–house [15].

C. NETWORK MANAGEMENT PROTOCOLS

Although each vendor builds their own software system for managing their own SONET equipment, standards with "specifications that have a cross–system and multi–vendor orientation" do exist [16]. Over the years, the International Standardization for Organization (ISO) and ITU-T have been developing several network management standards based on the OSI architecture. These standards use the common management information services (CMIS) with CMIP as the management protocol. The CMIS/CMIP pair is quite comprehensive, but its complexity in implementation partly renders it unpopular with SONET equipment vendors [6].

When SONET was first introduced, CMIS/CMIP was not an available solution for network management. The SONET equipment vendors' only choice was implementing the transaction language 1 (TL1). TL1 was developed to be a "man–machine language," with a human managing the network through a command–line terminal. Being vendor–neutral and easy to implement, TL1 became the popular choice for vendors. Nevertheless, it requires a separate communication link to the NEs being managed. This aspect and the fact that TL1 requires a human in the loop limit its usage in modern networks. [6]

Subsequently, the development of the Internet saw another network management protocol appearing on the scene. SNMP, the IETF's standard, was designed for managing nodes on an IP network. As the name implies, SNMP is simple and easy to implement. Nearly all devices support SNMP, and numerous management applications using SNMP are available. SNMP uses the "trap", which is essentially a message that reports a problem or event. The main drawback of SNMP is its use of a connectionless protocol, the user datagram protocol (UDP), for communications. SNMP version 1 is the dominant management protocol in the data communication world. However, it has certain limita-

tions such as weak security, and is unable to handle large volumes of management data efficiently. SNMPv2 incorporated more administrative structure and better security features. These cause complexity in implementation and incompatibility with SNMP version 1, thus making it unsuccessful in the market. [16]

In contrast to the management protocols discussed above, CORBA is not specifically developed for network management purposes. Primarily “a programming technology for distributed computing, CORBA enables components of various application programs to communicate with one another” [17] transparently. This prompted the Telemanagement Forum (TMF) to adopt it “as the preferred distribution technology” for network management and created standards that define CORBA objects and methods to be used at the network management layer–element management layer (NML-EML) interface. [17]

Figure 1 shows a typical network management architecture with CORBA implementations. The NML-EML interface in this case is referred to as a northbound CORBA interface. It is so named as the interface provides services upwards from the perspective of the EMS. Similarly, the southbound CORBA interface shown in Figure 1 provides services downwards with respect to the EMS. The Cisco products in this study use GIOP, which is a specific CORBA implementation.

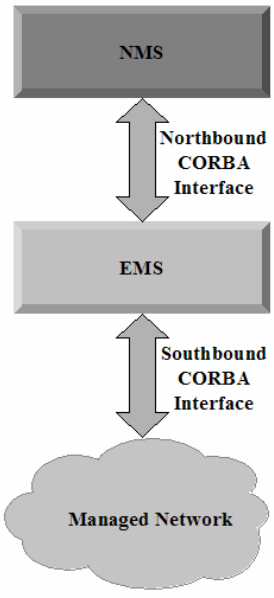


Figure 1. Typical network management architecture with CORBA implementations

D. CTC

"Cisco Systems (Cisco) more or less invented the router" [6] by integrating their routing technology and SONET technology on a single platform. Cisco is able to provide "multiservice optical networking" to the business community [18]. For this study, the Cisco Optical Network System 15454 (ONS 15454), with a capability for supporting time–division multiplexing and high–speed optical and gigabit networking, was used. The central processing unit (CPU) of Cisco ONS 15454 is the Cisco Timing Control Card Plus (TCC+). It performs NE management through an EMS CTC, which is stored in its non–volatile memory [19].

CTC is the EMS shipped with Cisco ONS 15454. It can manage up to 50 NEs concurrently. CTC is installed automatically onto the workstation that is connected to Cisco ONS 15454. It provides a graphical user interface (GUI) that contains "three primary views," namely, the network, node, and card views. The network view presents the entire network in graphical format for network management. It allows the user to install a location map, e.g., the United States map. The network topology is built by adding icons, representing nodes, onto the location map. The nodes' statuses are represented by the colors of their icons. The node view presents a node by displaying Cisco ONS 15454's shelf in graphical format showing all the cards in the node. The user is able to manage a node through this view. Similar to the network view, each card's color represents its status. The card view simply shows a specific card based on the user's selection. The user "performs card and port–specific maintenance tasks in this view." [19] The functions available are dependent on the card selected.

CTC connects to ONS 15454 using the SONET data communication channel (DCC); as such, it is able to search and discover other ONS 15454s connected to the DCC. Nevertheless, CTC is able to connect to ONS 15454 using an Internet Protocol (IP) connection. However, in this case it would be unable to perform the search and discover feature. CTC is also able to support a northbound CORBA interface for communication to a NMS. [19]

E. CTM 4.6

CTM 4.6 is the most advanced optical EMS for Cisco ONS 15000 series products. It uses CTC to collect network information, via SNMPv2, that is stored in an external database. The presence of the external database enables it to manage up to 2500 NEs.

Apart from providing all the capabilities of the CTC, such as GUI and management functions, CTM 4.6 is also able to collate extensive performance monitoring (PM) statistics across the network for display or export. Its ability to cope with heavy load scenarios allows Cisco to offer it as a high availability solution to customers. Like the CTC, CTM 4.6 also has an optional Gateway/CORBA component to support a northbound CORBA interface to integrate with a NMS [20].

F. SUMMARY

SONET network management tools and products were introduced in this chapter with brief discussion of common network management protocols. An overview of CTC and CTM 4.6 was also provided to give an insight to the products.

The next chapter describes the laboratory SONET network setup and the procedures performed to capture the network load for this study.

THIS PAGE IS INTENTIONALLY LEFT BLANK

III. LABORATORY SETUP AND PROCEDURES

A. CHAPTER OVERVIEW

This chapter describes the SONET network and equipment configuration in the laboratory. Next, the chapter will briefly recount the steps and challenges for setting up the equipment. Last but not least, the chapter will also discuss the procedures performed to collect data for analysis.

B. LABORATORY SETUP

Figure 2 shows a logical implementation of a SONET network in the Advanced Networking Laboratory.

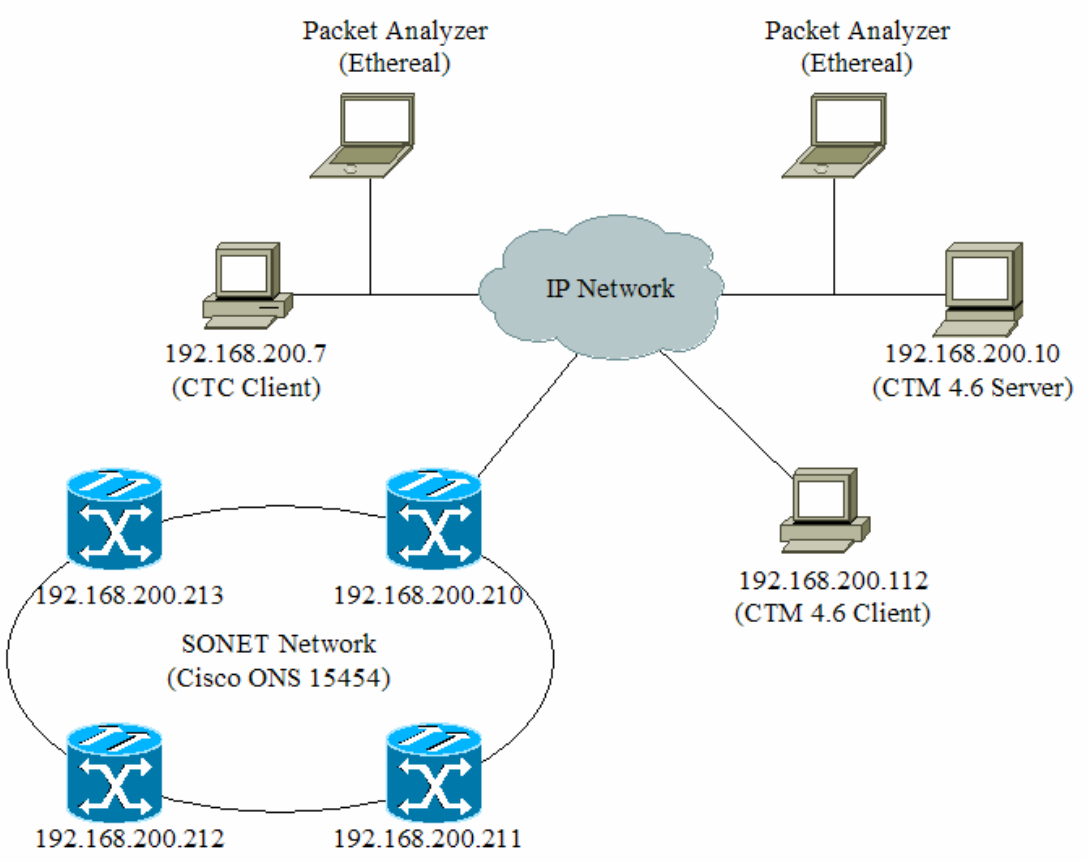


Figure 2. Logical implementation of the Advanced Networking Laboratory's SONET network

As can be seen from Figure 1, four ONS 15454s are connected in a ring to form a SONET network. One of the ONS 15454 is connected to an IP Network and forms the bridge between the SONET and the IP networks.

C. EQUIPMENT CONFIGURATION

1. Installing ONS 15454s

Lieutenant Matthew Klobukowski of the Advanced Networking Laboratory set up the SONET network by installing the four ONS 15454s and connecting them in the ring. In addition, he had assigned IP addresses and NE Identifications (IDs) to them as shown in Table 1.

NE ID	**IP Address**
Carmel	192.168.200.210
Pacific Grove	192.168.200.211
Monterey	192.168.200.212
Salinas	192.168.200.213

Table 1. Assigned NEs' IDs and IP addresses

This SONET network is configured to simulate a regional network across tens of miles. The NE ID represents the pseudo–location of the NE.

2. Installing CTC

CTC is a Java application that is downloaded automatically to a machine each time the machine connects to an ONS 15454. As such, CTC can only be launched through a web browser with a Java Plug–in. This web browser is required only during the intial launching. CTC version 4.1, as used in the Advanced Networking Laboratory, was found to be compatible only with Java Runtime Environment (JRE) version 1.3.1_02. It was found that the web browser is unable to launch CTC if Java 2 Runtime Environment (J2RE) version 1.4.2_04 was used.

For this study, CTC was launched on a Dell PowerEdge 2650 running Microsoft Windows 2003 Server, which is designated as a CTC client in Figure 1, to monitor the SONET network.

3. Installing CTM 4.6

The CTM 4.6 server software only runs on Sun Solaris 8 Operating System (OS) and requires Oracle 8i, an external database, during its operations. In addition, a personal computer (PC) is required to connect to the CTM 4.6 server as a CTM 4.6 client for user–related activities [20].

As a machine with Sun Solaris 8 OS was unavailable, the Sun Blade 1000 in the Advanced Networking Laboratory, previously configured with Sun Solaris 9 OS, was reconfigured with Sun Solaris 8 OS. Subsequently, Oracle 8i Enterprise Edition, CTM 4.6 server, CTM database schema, and CTM web server were installed onto the machine. Next the CTM 4.6 client was installed onto a PC running Windows XP.

As mentioned in Chapter II, CTM 4.6 uses SNMPv2 as the underlying management protocol. Therefore, SNMPv2 has to be enabled on the ONS 15454s. As shown in Figure 3, CTC was used to enable SNMPv2 on the NEs. Figure 3 also shows that SNMPv2 was configured to use the community name “AdvNetLab” and UDP port 162 for sending SNMPv2 traps to the CTM 4.6 server (IP address – 192.168.200.10). In addition, the “Maximum Trap per Second” was set to 0, which implies all traps are sent to the CTM 4.6 server.

Next, the NEs to be monitored by the CTM 4.6 server were added through the CTM 4.6 client and the performance monitoring option in the CTM 4.6 was enabled. Figure 4 shows the CTM 4.6 processes running on the server. The processes “CTM Server”, “SNMPTrapService”, and “SMService” indicate that the server is running properly. The NE–specific process is shown as “NEService–21” and the PM–specific process is shown as “PMService–2”. The “Apache Web Server” indicates that the web server option is installed and running and that the CTM 4.6 client is able to download information from the CTM 4.6 server through Hypertext Transfer Protocol (HTTP).

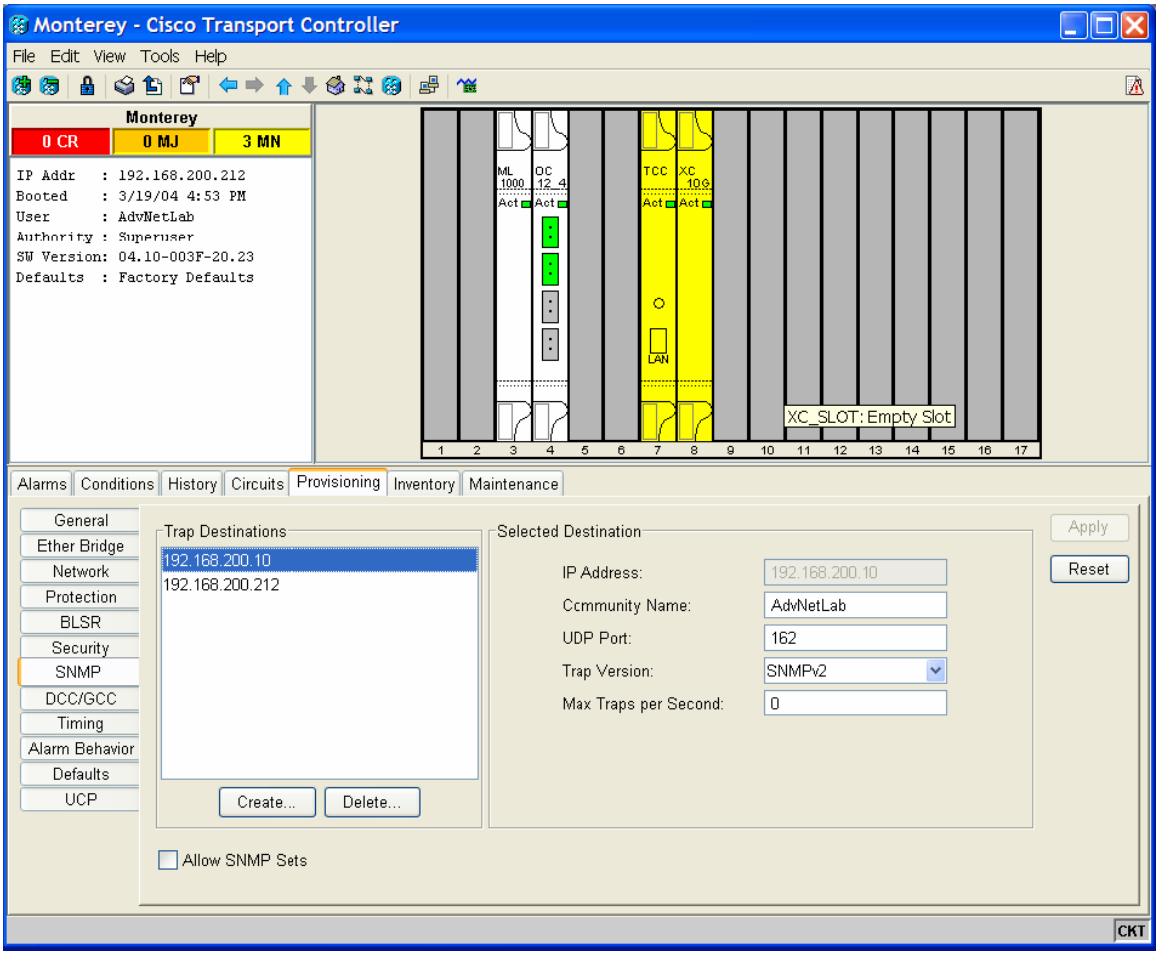


Figure 3. ONS 15454s' SNMPv2 configuration

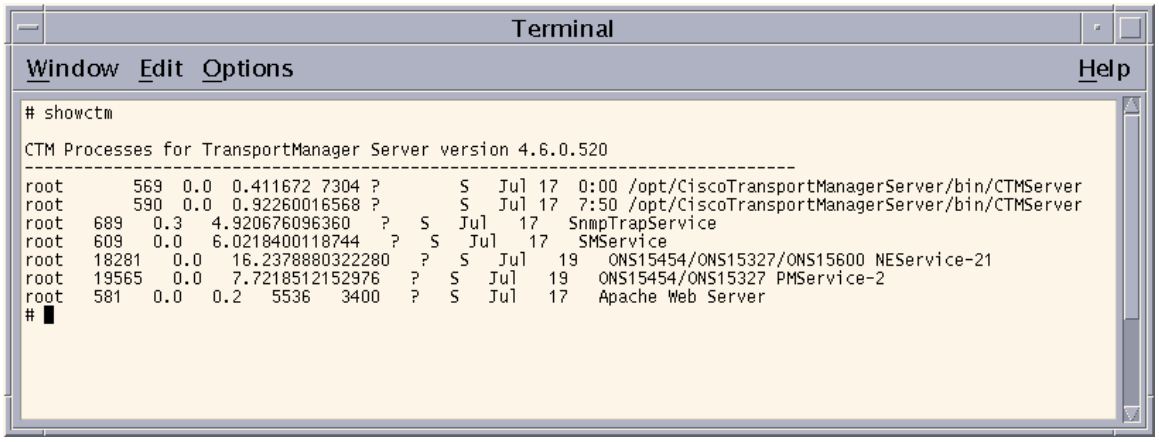


Figure 4. CTM 4.6 processes running on the server

D. DATA COLLECTION

Ethereal, an open–source packet analyzer freeware program, was used to capture the traffic for analysis. As can be seen from Figure 1, Ethereal was deployed to passively monitor the network interfaces of the CTC client and the CTM 4.6 Server.

1. Collecting the CTC's Traffic

As mentioned in Chapter II, the CTC connects to an NE, from which it can discover and manage other NEs through the DCC. Therefore, by capturing the data communications between the CTC and the connected NE, it is possible to determine the overhead traffic injected by the CTC and the managed NEs onto the DCC. Ethereal was placed on the network to capture the IP traffic inbound and outbound to the CTC client. This IP traffic is essentially the traffic on the DCC that is forwarded to the CTC client by its connected NE using the IP network. In this study, the CTC was left running for a period of 10 days to generate sufficient network traffic for analysis.

2. Collecting the CTM 4.6's Traffic

Similar to the way the CTC's traffic was collected, Ethereal was deployed to monitor the inbound and outbound communications from the CTM 4.6 server. SNMPv2 agents were configured to run on the ONS 15454s and report to the CTM 4.6 server. In this case, all the SNMPv2 traps were sent to the CTM 4.6 server through the IP network. Thus the traffic captured on the IP network is representative of the load generated by CTM 4.6 and the managed NEs.

E. SUMMARY

The Advanced Networking Laboratory's SONET network and the equipment were initially discussed in this chapter. Next the challenges encountered during the installation of the equipment were briefly described. The chapter concluded with a discussion of the data collection process.

The next chapter provides some background knowledge of probability theory used in the analysis of the data. The concept of self–similarity will also be briefly discussed.

THIS PAGE IS INTENTIONALLY LEFT BLANK

IV. PROBABILITY THEORY AND SELF–SIMILARITY

A. CHAPTER OVERVIEW

This chapter aims to provide a brief review of probability theory and the concept of self–similarity. The first part of the chapter briefly reviews the discrete random variable and its probability distributions. The second part of the chapter briefly states the queuing equations used in this study. The last part of this chapter provides an overview on the concept of self–similarity and discusses a technique used to estimate the Hurst value, a key parameter for determining the degree of self–similarity.

B. DISCRETE RANDOM VARIABLE

A discrete random variable, *X*, is defined by its probability distribution:

$$P_X(k) = \Pr[X = k] \tag{4.1}$$

$$\sum_{\text{all } k} P_X(k) = 1. \tag{4.2}$$

In addition, the discrete random variable, *X*, has the following characteristics:

Mean: $$E[X] = \mu_X = \sum_{\text{all } k} k \Pr[x = k] \tag{4.3}$$

Second Moment: $$E[X^2] = \sum_{\text{all } k} k^2 \Pr[x = k] \tag{4.4}$$

Variance: $$\text{Var}[X] = \sigma_X^2 = E[X^2] - \{E[X]\}^2 \tag{4.5}$$

Standard Deviation: $$\sigma_X = \sqrt{\text{Var}[X]} \tag{4.6}$$

Coefficient of Variation: $$\frac{\sigma_X}{\mu_X}. \tag{4.7}$$

As stated in [21], “the mean is known as a first–order statistic” while “the second moment and the variance are second–order statistics”. Two essential probability distributions used in queuing theory are discussed next.

1. Exponential Distribution

The exponential distribution used in queuing analysis has a probability distribution function, $F(x)$, and a probability density function, $f(x)$, given by:

$$F(x) = 1 - e^{-\lambda x} \tag{4.8}$$

$$f(x) = \lambda e^{-\lambda x}. \tag{4.9}$$

The mean of the exponential distribution is equal to its standard deviation:

$$\mu_X = \sigma_X = \frac{1}{\lambda}. \tag{4.10}$$

In queuing theory, the service time, that is the packet transmission time of a packet switched network, is often assumed to be exponential [21].

2. Poisson Distribution

The Poisson distribution is another distribution that is used in queuing analysis. It takes on the form:

$$\Pr[X = k] = \frac{\lambda^k}{k!} e^{-\lambda}. \tag{4.11}$$

The mean of the Poisson distribution is equal to its variance:

$$\mu_X = \sigma_X^2 = \lambda. \tag{4.12}$$

Figure 5 shows an example of the Poisson distribution with $\lambda = 4$. As shown in the figure, there are two maxima at $k = 3$ and $k = 4$, which correspond to $k = \lambda - 1$ and $k = \lambda$, respectively.

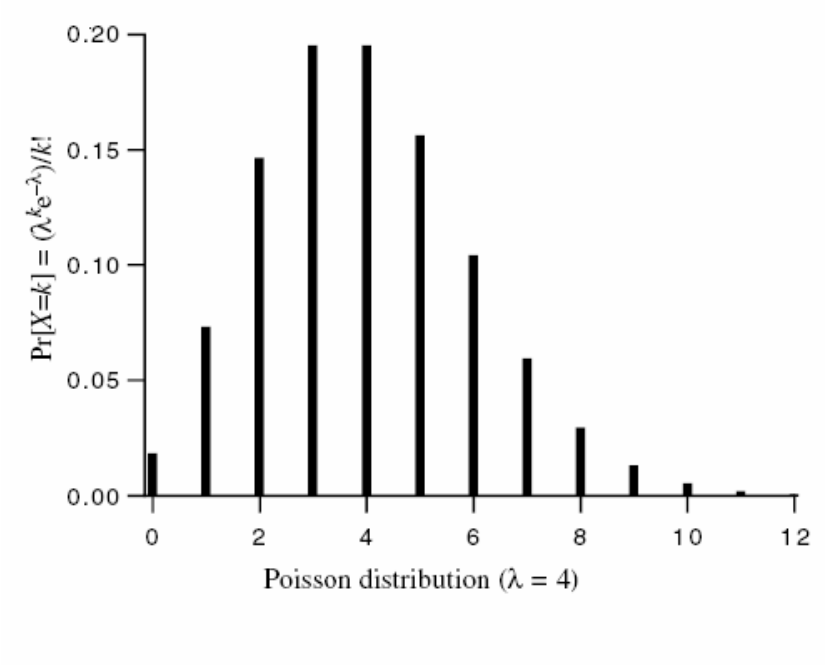


Figure 5. Poisson distribution with $\lambda = 4$ (After Ref. [21].)

In queuing analysis, the items arriving at the queue are usually modeled after the Poisson distribution pattern; thus from Equations (4.11) and (4.12):

$$\Pr\left[k \text{ items arrive in the time interval } T\right] = \frac{\left(\lambda T\right)^k}{k!} e^{-\lambda T} \tag{4.13}$$

$$E\left[\text{number of items to arrive in time interval } T\right] = \lambda T \tag{4.14}$$

$$\text{Mean arrival rate, in items per second} = \lambda. \tag{4.15}$$

If the interarrival times, the times between arrivals of items, are assumed to follow the exponential distribution, then from Equations (4.8) and (4.10):

$$\Pr\left[\text{Interarrival time} < t\right] = 1 - e^{-\lambda t} \tag{4.16}$$

$$E\left[\text{Interarrival time}\right] = \frac{1}{\lambda}. \tag{4.17}$$

Therefore, it can be seen from Equation (4.17) that the mean interarrival time is inversely proportional to the arrival rate [21].

C. QUEUING EQUATIONS

In this study, queuing theory is applied to calculate the utilization, ρ, of the SONET link. As such, the queuing equations in [21] that are used in the next chapter are briefly discussed below.

From Equation (4.17):

$$\lambda = \frac{1}{\text{Mean interarrival time}}. \tag{4.18}$$

As mentioned above, the service time, T_S, is the packet transmission time of a packet switched network. Therefore, T_S is related to the packet size and the link speed as:

$$T_S = \frac{\text{Mean packet size (in bytes)} \times 8}{\text{Link speed}}. \tag{4.19}$$

Knowing the arrival rate and the service time, ρ can be calculated through:

$$\rho = \lambda T_S. \tag{4.20}$$

D. SELF-SIMILARITY

The exponential and Poisson distributions provide a good estimate for the network traffic into a single–server queue. However, these models are unable to take into account the burstiness of the network traffic accurately. This has led to the idea of modeling network traffic using the concept of self–similarity. Based on fractals and chaos theory, the concept of self–similarity is becoming important in the description of network traffic [21]. In this subsection, the concept is briefly introduced to provide adequate information for analyzing the captured traffic.

1. Estimation of Self–similarity

A significant measure of self–similarity is the Hurst (H) parameter. A process is statistically self–similar if $0.5 \le H \le 1$. There are a number of ways to estimate H. In this study, H is estimated by analyzing the variances of aggregated processes, $x^{(m)}$, where m is an integer representing the number of samples considered in a given sample window.

As was stated in [21], for self–similar processes, the variances satisfy the following relationship for large values of *m*:

$$\mathrm{Var}(x^{(m)}) \propto \frac{\mathrm{Var}(x)}{m^{\beta}}, \tag{4.21}$$

where β is defined as:

$$H = 1 - \frac{\beta}{2}. \tag{4.22}$$

Taking the log on both sides of Equation (4.21):

$$\log\left[\mathrm{Var}\left(x^{(m)}\right)\right] \propto \log\left[\mathrm{Var}(x)\right] - \beta \log(m). \tag{4.23}$$

A variance–index plot is obtained by plotting log(*m*) versus $\log\left[\mathrm{Var}\left(x^{(m)}\right)\right]$ of Equation (4.23). The gradient of the variance–index plot is the approximate value of β. Next, Equation (4.22) is used to calculate *H*, which provides an indication of the degree of self–similarity [21,22].

2. Queue Depth for Self–similar Traffic

The queue depth of a network, *q*, is related to the mean network link utilization, ρ, and *H*:

$$q = \frac{\rho^{\frac{1}{2(1-H)}}}{(1-\rho)^{\frac{H}{(1-H)}}}. \tag{4.24}$$

For a system with exponential interarrival and service times (also termed as M/M/1), $H = 0.5$ [21].

E. SUMMARY

This chapter began by reviewing the characteristics of the discrete random variable and some related probability distributions. The exponential and Poisson distributions were briefly mentioned. Next the chapter briefly stated the queuing equations. Then the concept of self–similarity and the Hurst parameter, *H*, which is used to determine the degree of self–similarity, were introduced. Finally, the chapter described a technique to estimate *H* and provided the relationships between the queue depth, mean utilization, and the Hurst pararmeter, *H*.

The next chapter begins by describing the traffic analysis performed using a packet analyzer. The remainder of the chapter presents the statistical traffic analysis.

V. TRAFFIC ANALYSIS AND FINDINGS

A. CHAPTER OVERVIEW

This chapter starts by discussing the observations of the initial traffic analysis performed using a packet analyzer. Next, the chapter briefly describes the data pruning process and further discusses the findings of the traffic analysis performed using the statistical tools presented in Chapter IV. Last, the results from the traffic analysis are presented.

B. TRAFFIC ANALYSIS USING ETHEREAL

As mentioned in Chapter III, the CTC and the CTM 4.6's traffic are captured using Ethereal. In addition to monitoring the traffic, Ethereal is also able to decipher the traffic into commonly used (open standards) protocols. Figure 6 shows a screen shot of Ethereal deciphering the CTC's traffic.

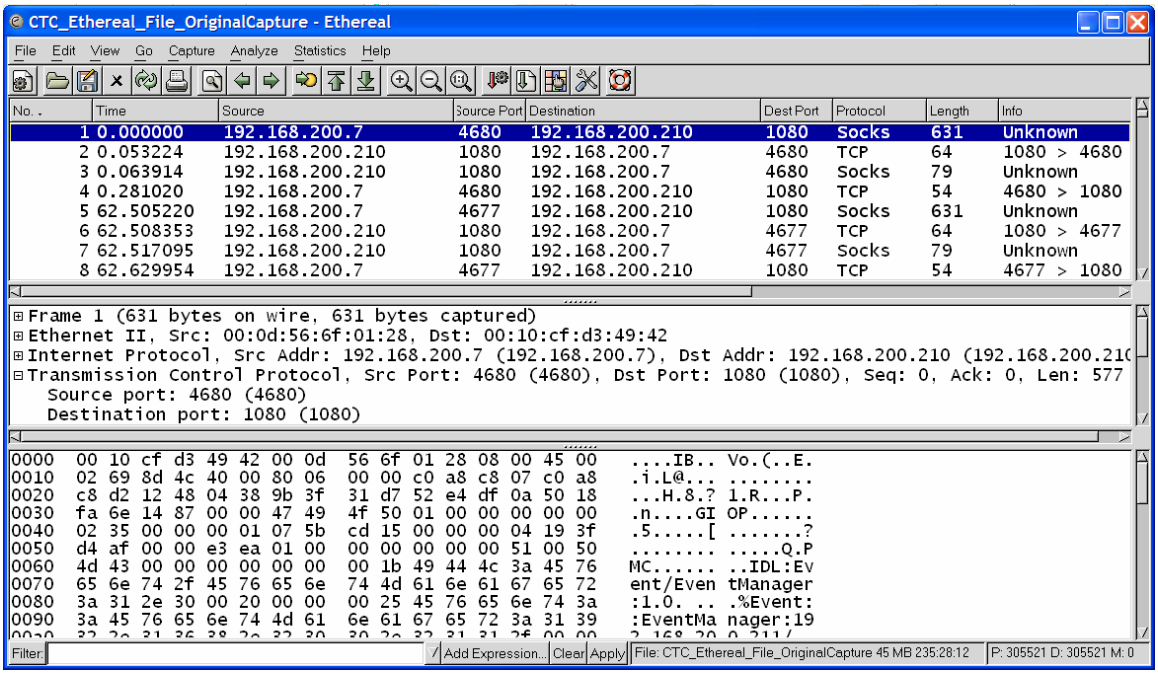


Figure 6. Screen shot of Ethereal deciphering the CTC's traffic

1. Observations Made on the CTC's Traffic

The CTC's traffic was captured between June 11, 2004 and June 20, 2004, over a period of 235.5 hours. Using Ethereal, it was observed that the CTC communicated with the managed NEs using Cisco's proprietary Socks protocol that connects to Transport Control Protocol (TCP) Port 1080 on the NEs. Although Ethereal cannot decipher the Socks protocol, it can be observed from the payload (data) section that this Socks protocol incorporated GIOP (a type of CORBA implementation). In addition, further analysis revealed that the CTC's user–commands (sent through the CTC client) were forwarded to the NEs using GIOP. Table 2 shows a summary of the type of traffic and the number of packets observed in the captured traffic. The Socks traffic is the data of interest (supposedly the actual traffic on the DCC), while the TCP overhead includes traffic for setting up TCP connections, tearing down TCP connections, TCP acknowledgment, and TCP retransmission. The other communications seen on the network are networking protocols like Address Resolution Protocol (ARP), UDP, and HTTP, etc., which are unrelated to this study.

Type of Traffic	Number of Packets
Socks communications between CTC and the managed NEs	124,784
TCP overhead for CTC's Socks communications	148,796
Other communications on the network	31,941
Total packets captured on the network	305,521

Table 2. Summary of the CTC's traffic captured between June 11, 2004 and June 20, 2004

2. Observations Made on the CTM 4.6's Traffic

The CTM 4.6's traffic was captured between July 20, 2004 and July 30, 2004, over a period of 257 hours. A summary of the captured traffic is as shown in Table 3. Similar to the CTC's traffic, the Socks traffic is the portion of the CTM 4.6's traffic that uses Cisco's proprietary Socks protocol. Similarly, the TCP overhead includes traffic for setting up TCP connections, tearing down TCP connections, TCP acknowledgments, and

TCP retransmissions. An additional protocol observed in this set of data is SNMPv2. Other traffic are communications that are unrelated to this study. These include other protocols observed on the network and the CTM 4.6 client's traffic (user commands), which are made up of GIOP and the Oracle database's TNS connections.

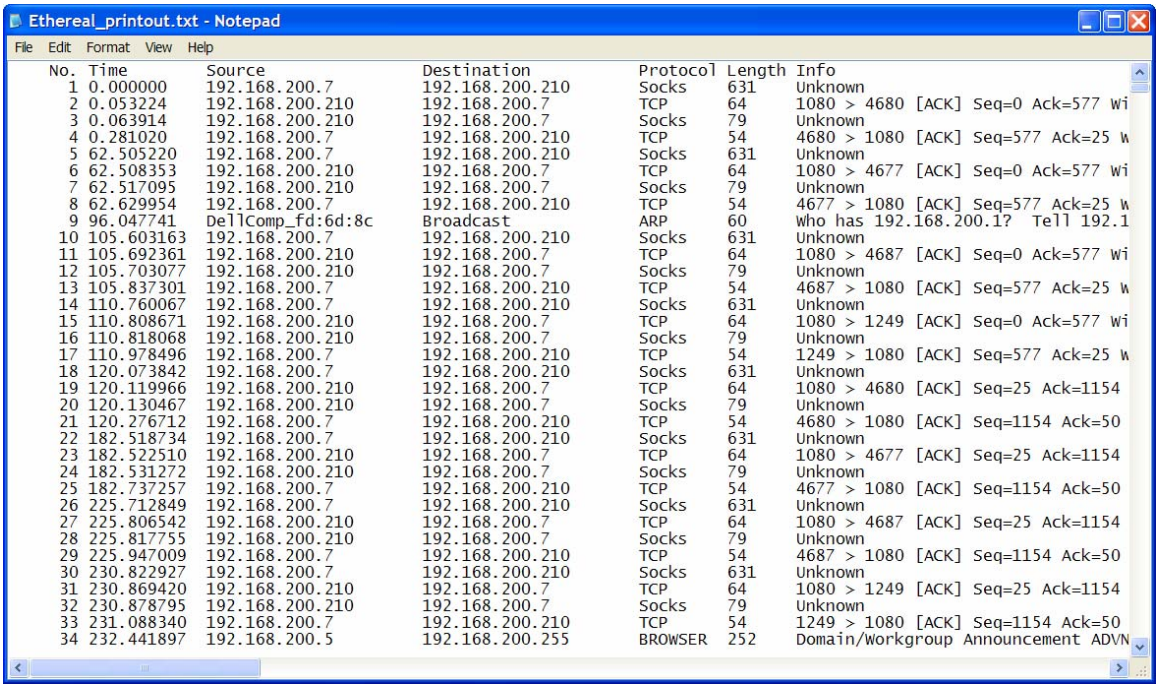
Type of Traffic	Number of Packets
Socks communications between CTM and the managed NEs	203,278
TCP overhead for CTM's Socks communications	260,461
SNMPv2 traffic	7,364
Other communications on the network	193,333
Total packets captured on the network	664,436

Table 3. Summary of the CTM 4.6's traffic captured between July 20, 2004 and July 30, 2004

Through Ethereal, it is observed that the CTM 4.6 mainly communicated with its managed NEs in the same manner as the CTC, and that the SNMPv2 traffic only forms 1% of the total traffic. This was unexpected as it was thought that the CTM 4.6 collects the NEs' information through the CTC using SNMPv2 as the underlying network management protocol. However, close inspection revealed that the CTM 4.6 performs a "GetBulk" operation to the NEs every 24 hours. This "GetBulk" operation enables the CTM 4.6 to collect large amount of data from the NEs efficiently through a single operation [5]. In addition to these "GetBulk" operations, SNMPv2 "trap" operations sent by the NEs were also observed.

C. DATA PRUNING

After identifying the types of network traffic that were captured, the next step was to extract those relevant to this study for further analysis. First, a summary of the captured data was printed out in text format (i.e., divided into columns) from Ethereal and saved into a flat file. A screen shot of the text print out from Ethereal is shown in Figure 7. The important fields are the "Time" and "Length" fields.



Ethereal_printout.txt - Notepad

File Edit Format View Help

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.200.7	192.168.200.210	Socks	631	Unknown
2	0.053224	192.168.200.210	192.168.200.7	TCP	64	1080 > 4680 [ACK] Seq=0 Ack=577 Wi
3	0.063914	192.168.200.210	192.168.200.7	Socks	79	Unknown
4	0.281020	192.168.200.7	192.168.200.210	TCP	54	4680 > 1080 [ACK] Seq=577 Ack=25 W
5	62.505220	192.168.200.7	192.168.200.210	Socks	631	Unknown
6	62.508353	192.168.200.210	192.168.200.7	TCP	64	1080 > 4677 [ACK] Seq=0 Ack=577 Wi
7	62.517095	192.168.200.210	192.168.200.7	Socks	79	Unknown
8	62.629954	192.168.200.7	192.168.200.210	TCP	54	4677 > 1080 [ACK] Seq=577 Ack=25 W
9	96.047741	DellComp_fd:6d:8c	Broadcast	ARP	60	Who has 192.168.200.1? Tell 192.1
10	105.603163	192.168.200.7	192.168.200.210	Socks	631	Unknown
11	105.692361	192.168.200.210	192.168.200.7	TCP	64	1080 > 4687 [ACK] Seq=0 Ack=577 Wi
12	105.703077	192.168.200.210	192.168.200.7	Socks	79	Unknown
13	105.837301	192.168.200.7	192.168.200.210	TCP	54	4687 > 1080 [ACK] Seq=577 Ack=25 W
14	110.760067	192.168.200.7	192.168.200.210	Socks	631	Unknown
15	110.808671	192.168.200.210	192.168.200.7	TCP	64	1080 > 1249 [ACK] Seq=0 Ack=577 Wi
16	110.818068	192.168.200.210	192.168.200.7	Socks	79	Unknown
17	110.978496	192.168.200.7	192.168.200.210	TCP	54	1249 > 1080 [ACK] Seq=577 Ack=25 W
18	120.073842	192.168.200.7	192.168.200.210	Socks	631	Unknown
19	120.119966	192.168.200.210	192.168.200.7	TCP	64	1080 > 4680 [ACK] Seq=25 Ack=1154
20	120.130467	192.168.200.210	192.168.200.7	Socks	79	Unknown
21	120.276712	192.168.200.7	192.168.200.210	TCP	54	4680 > 1080 [ACK] Seq=1154 Ack=50
22	182.518734	192.168.200.7	192.168.200.210	Socks	631	Unknown
23	182.522510	192.168.200.210	192.168.200.7	TCP	64	1080 > 4677 [ACK] Seq=25 Ack=1154
24	182.531272	192.168.200.210	192.168.200.7	Socks	79	Unknown
25	182.737257	192.168.200.7	192.168.200.210	TCP	54	4677 > 1080 [ACK] Seq=1154 Ack=50
26	225.712849	192.168.200.7	192.168.200.210	Socks	631	Unknown
27	225.806542	192.168.200.210	192.168.200.7	TCP	64	1080 > 4687 [ACK] Seq=25 Ack=1154
28	225.817755	192.168.200.210	192.168.200.7	Socks	79	Unknown
29	225.947009	192.168.200.7	192.168.200.210	TCP	54	4687 > 1080 [ACK] Seq=1154 Ack=50
30	230.822927	192.168.200.7	192.168.200.210	Socks	631	Unknown
31	230.869420	192.168.200.210	192.168.200.7	TCP	64	1080 > 1249 [ACK] Seq=25 Ack=1154
32	230.878795	192.168.200.210	192.168.200.7	Socks	79	Unknown
33	231.088340	192.168.200.7	192.168.200.210	TCP	54	1249 > 1080 [ACK] Seq=1154 Ack=50
34	232.441897	192.168.200.5	192.168.200.255	BROWSER	252	Domain/Workgroup Announcement ADVN

Figure 7. Screen shot of a text print out from Ethereal

Next, the flat file was imported into a Microsoft Access database table. As the import was done using fixed column's width, some of the fields were imported with an additional white space before the fields. A general "Replace" operation was performed in Microsoft Access to eliminate the additional white space.

Microsoft Access allows queries on the data based on a field. Thus a query was performed to select all the packets using the Socks protocol and the query result was cut and pasted into an empty database table. Additional queries were then performed on the new database table to select the unwanted data (like "TCP Retransmission" packets of the Socks protocol) for deletion. Finally, the pruned data was exported into text format, from Microsoft Access using "tab" as the delimiter and saved into another flat file. Similar operations were performed to extract other data of interest. Using this process, data for the following were generated: CTC's Socks traffic, CTM 4.6's Socks traffic, CTM 4.6's SNMP traffic, CTM 4.6's combined Socks and SNMP traffic, and CTM 4.6's Ethernet traffic (which includes all the TCP/IP traffic related to the Socks and the SNMP communications).

D. STATISTICAL ANALYSIS

As mentioned in Chapter IV, in queuing theory the interest lies in the interarrival times between packets and the packet sizes of the traffic. The interarrival times between packets are obtained by taking the differences in the arrival times (corresponding to the "Time" column in Figure 7) between two adjacent packets. The packet sizes are simply the packet lengths (corresponding to the "Length" column in Figure 7).

Using a Mathcad program written by Lieutenant James Young in the Summer 2003 EC4850 class, the interarrival times and packet sizes of the captured traffic were extracted and modeled as random variables. Next a set of data samples for each random variable was generated and exported to Microsoft Excel for plotting.

1. Interarrival Time Distributions

Using the generated data samples for interarrival times, the interarrival time distributions are plotted in Figures 8 to 12 using Microsoft Excel.

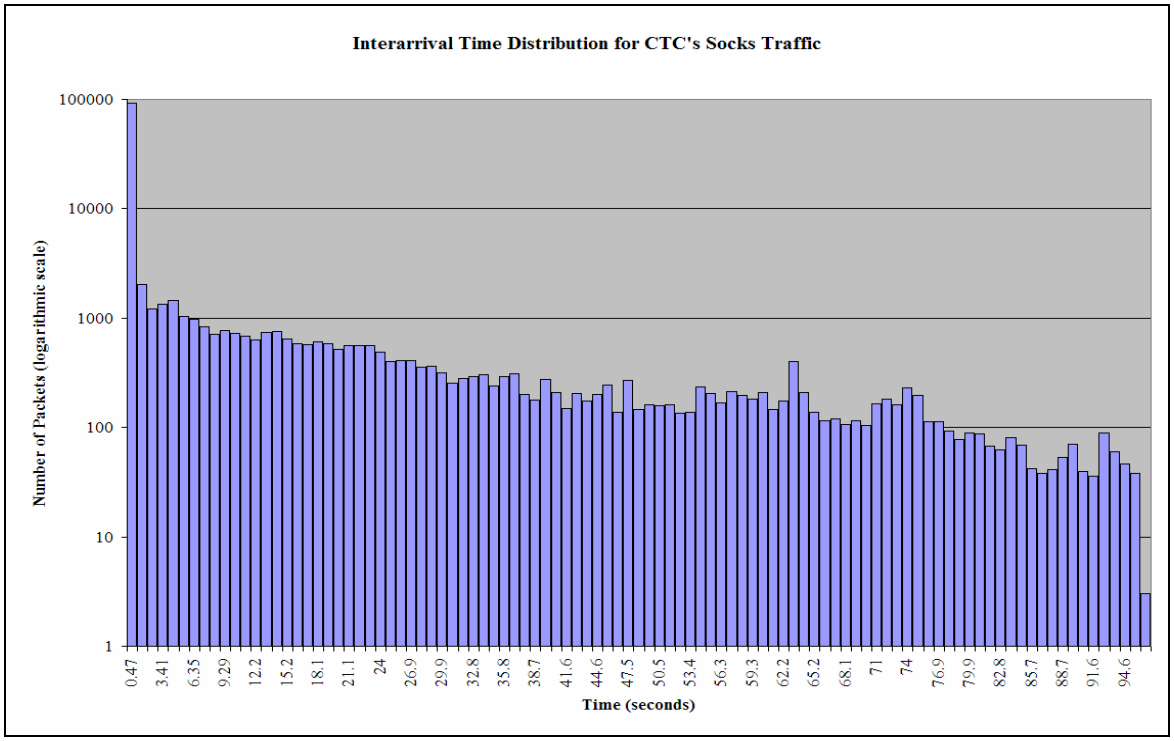


Figure 8. Interarrival time distribution for CTC's Socks traffic

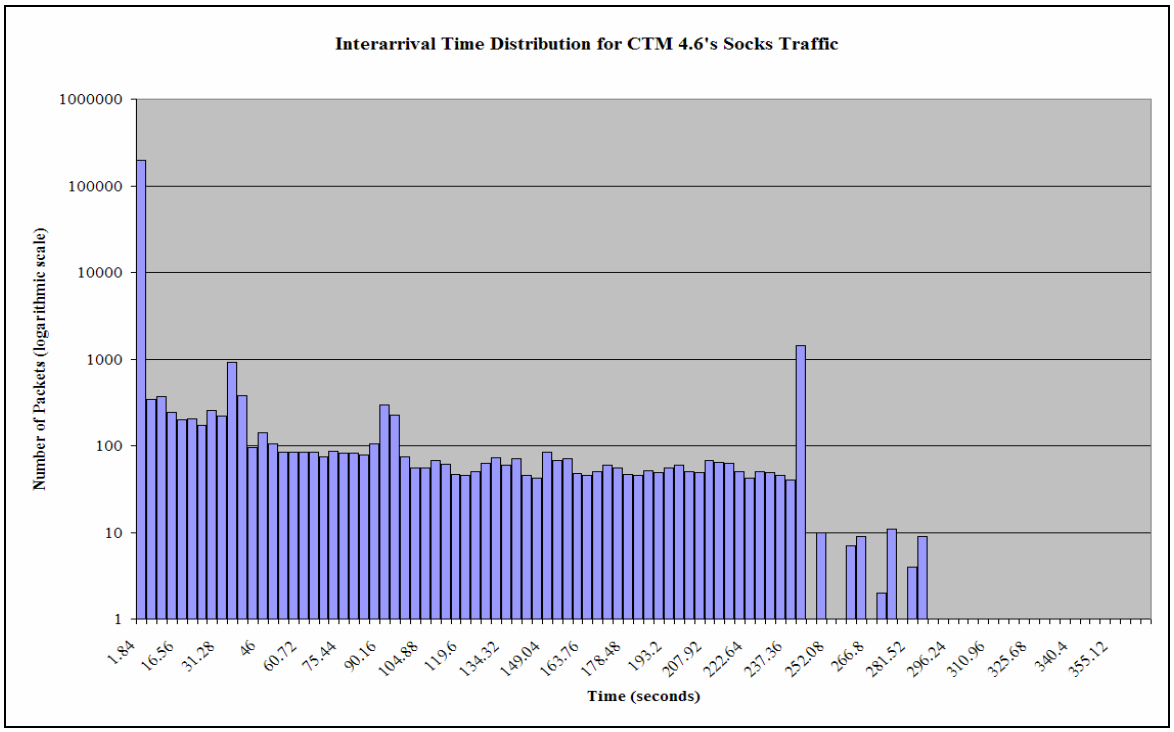


Figure 9. Interarrival time distribution for CTM 4.6's Socks traffic

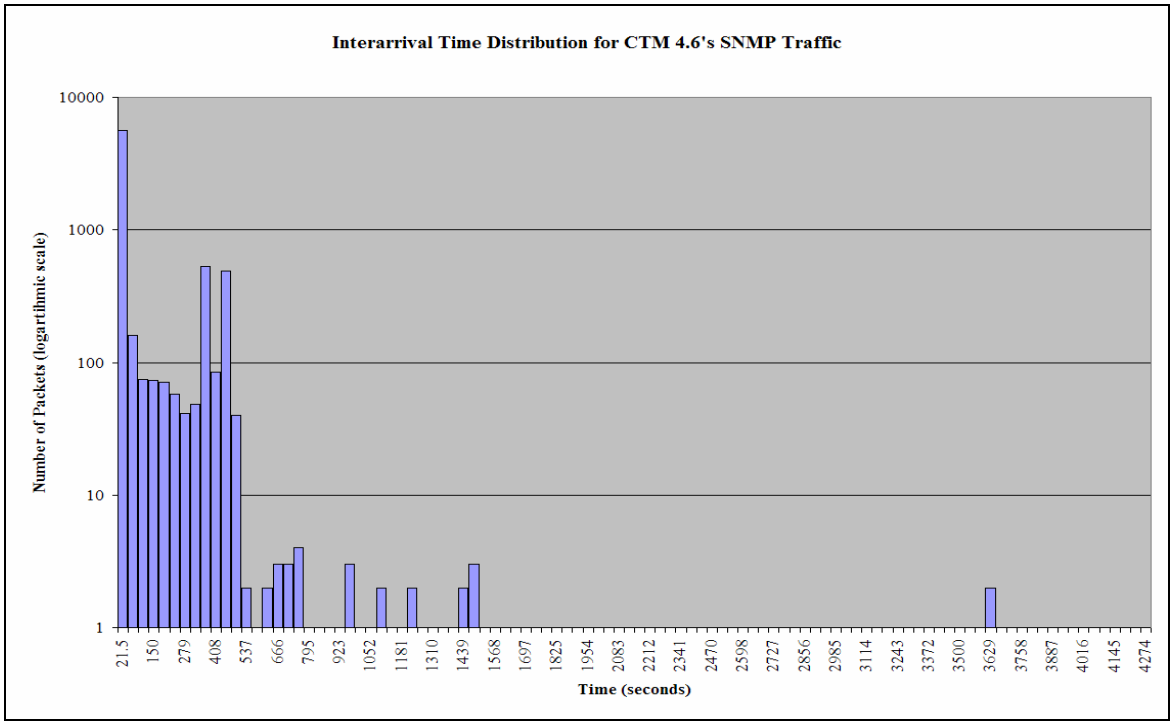


Figure 10. Interarrival time distribution for CTM 4.6's SNMP traffic

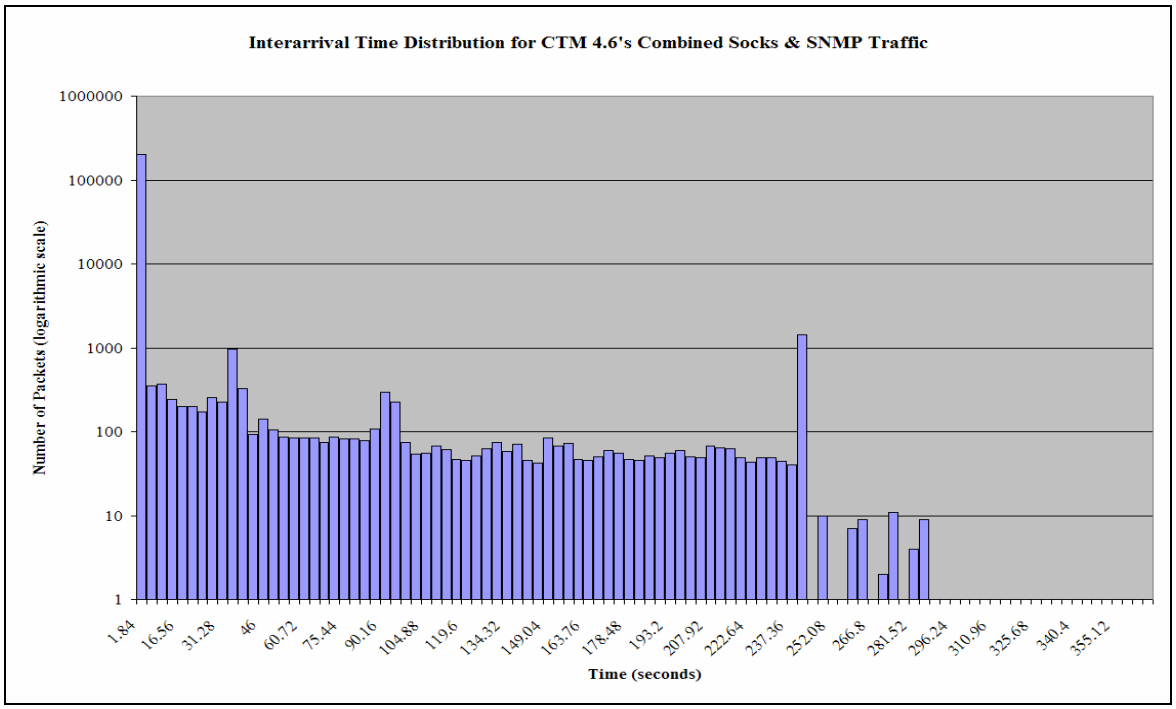


Figure 11. Interarrival time distribution for CTM 4.6's combined Socks & SNMP traffic

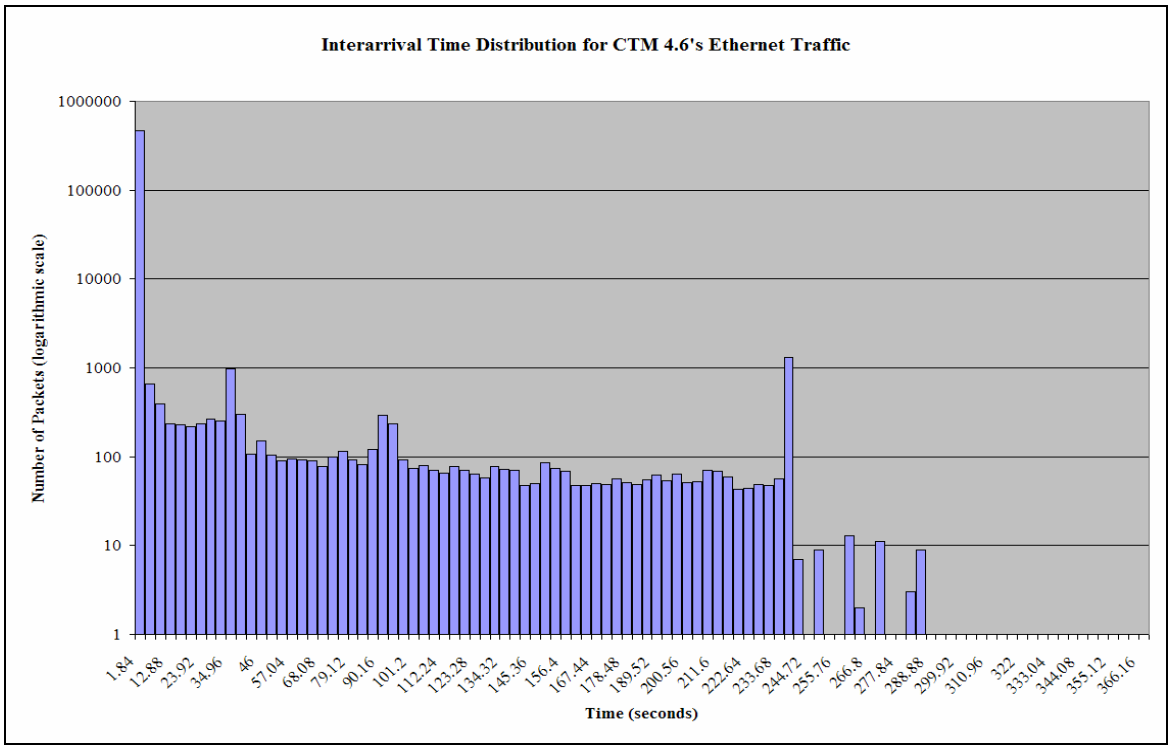


Figure 12. Interarrival time distribution for CTM 4.6's Ethernet traffic

From the figures, it can be seen that some of the distributions resemble that of the exponential distribution with a linear rate of decay, $\lambda \leq 1$, and the majority of the packets arrive within a relatively short interarrival time. Figures 8 and 10 also exhibit a long–range dependency characteristic (with a few samples that are relatively much larger than the rest) that suggests the CTC's Socks traffic and the CTM 4.6's SNMP traffic are self–similar and bursty [21]. Using Equations (4.3) to (4.7) in Mathcad, the mean, variance, and coefficient of variation of the interarrival time distributions are computed as shown in Table 4. Note in all cases the coefficient of variation implies a strong tail $(\sigma_t/\mu_t \geq 1)$.

Type of Traffic	**Mean (s)**	**Variance (s^2)**	**Coefficient of Variation**
CTC's Socks Traffic	6.793	273.854	2.436
CTM 4.6's Socks Traffic	4.553	772.087	6.103
CTM 4.6's SNMP Traffic	120.043	627080.020	6.597
CTM 4.6's Combined Socks & SNMP Traffic	4.394	745.556	6.215
CTM 4.6's Ethernet Traffic	1.965	323.759	9.159

Table 4. Tabulated statistics for the interarrival time distributions

Substituting the mean values in Table 4 into Equation (4.18), the values for λ are computed as shown in Table 5, which confirms that $\lambda \leq 1$.

Type of Traffic	**λ (s^{-1})**
CTC's Socks Traffic	0.147
CTM 4.6's Socks Traffic	0.220
CTM 4.6's SNMP Traffic	0.008
CTM 4.6's Combined Socks & SNMP Traffic	0.228
CTM 4.6's Ethernet Traffic	0.509

Table 5. Tabulated values of arrival rate, λ, for the interarrival time distributions

2. Packet Size Distributions

Similar to the plotting of interarrival time distributions, the samples of the packet size are used to plot the packet size distributions in Figures 13 to 17 using Microsoft Excel. Figure 13 shows that the packet size distribution of the CTC's Socks traffic is non–deterministic. Further, this suggests that the traffic is self–similar. On the other hand, the linear decay of Figures 14, 16 and 17 show a slight resemblance to the exponential distribution. Although a small peak is observed for packets of 550 bytes in size, the majority of the traffic is small in size (< 100 bytes). Figure 15 indicates that the CTM's SNMP traffic exhibits a long–range dependency that suggests the traffic is self–similar and bursty.

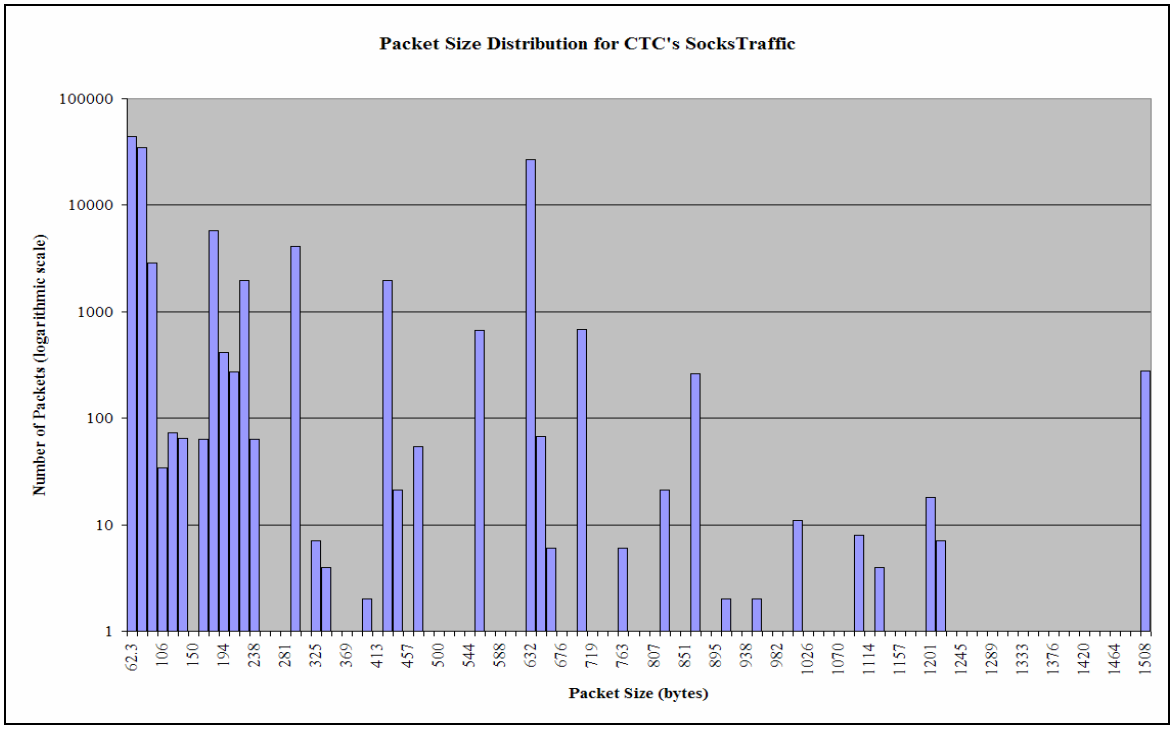


Figure 13. Packet size distribution for CTC's Socks traffic

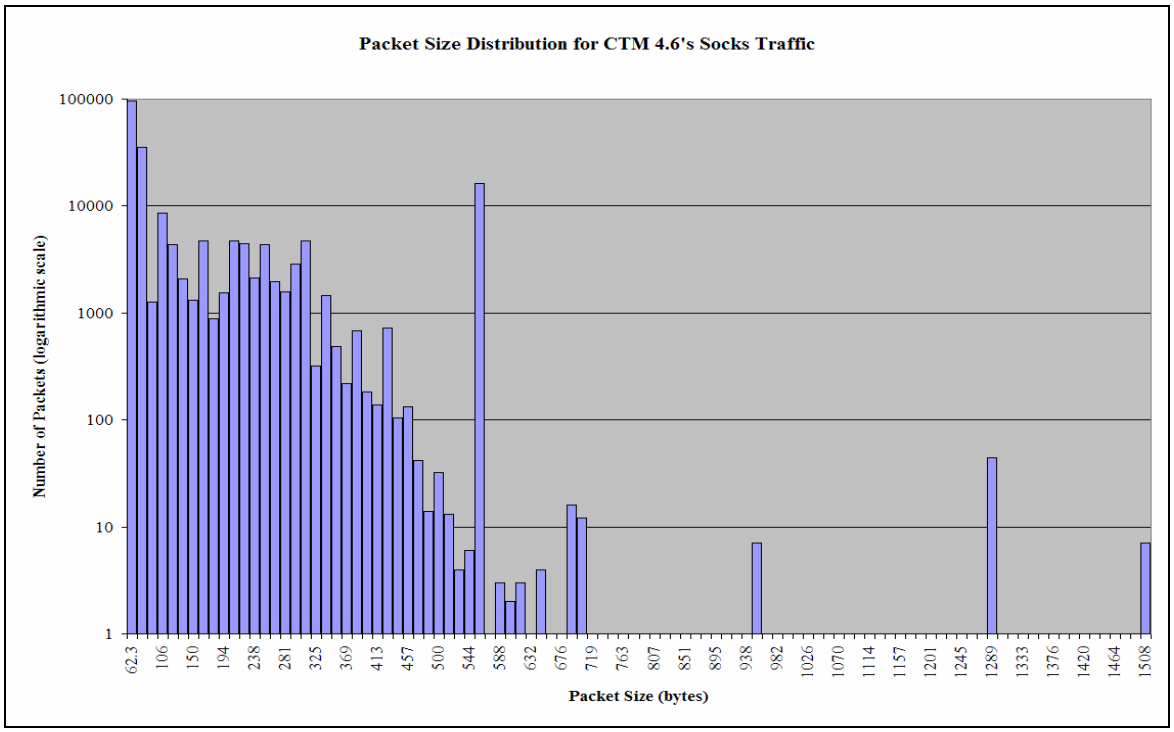


Figure 14. Packet size distribution for CTM 4.6's Socks traffic

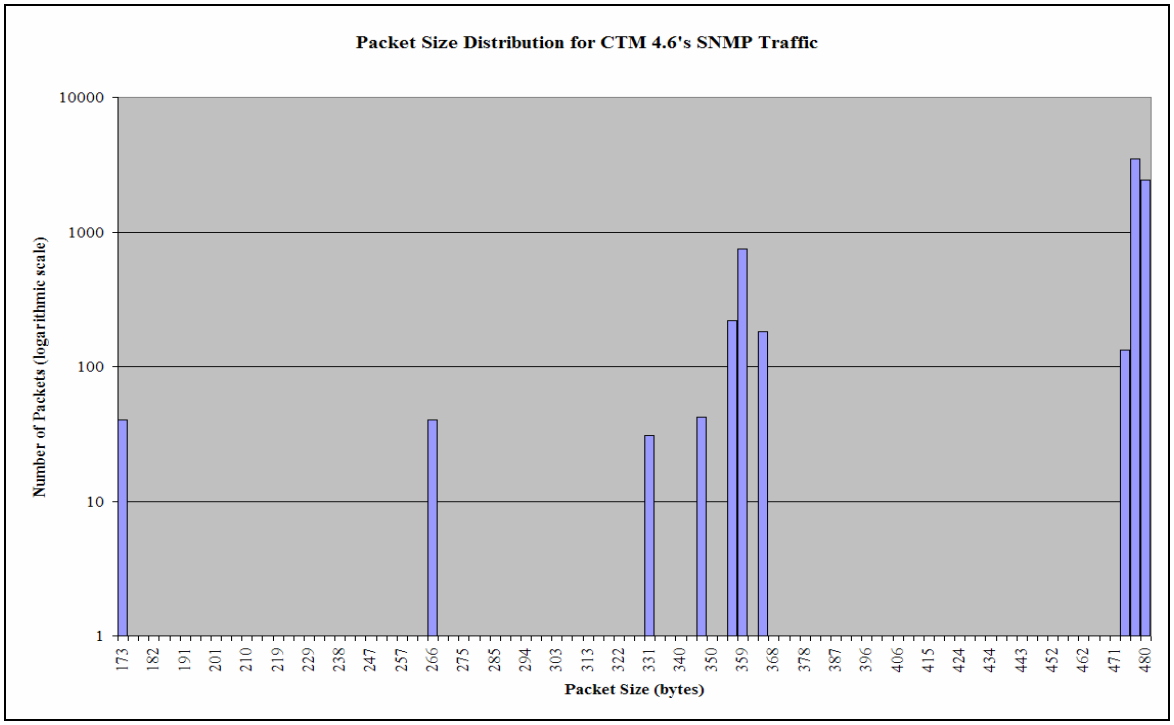


Figure 15. Packet size distribution for CTM 4.6's SNMP traffic

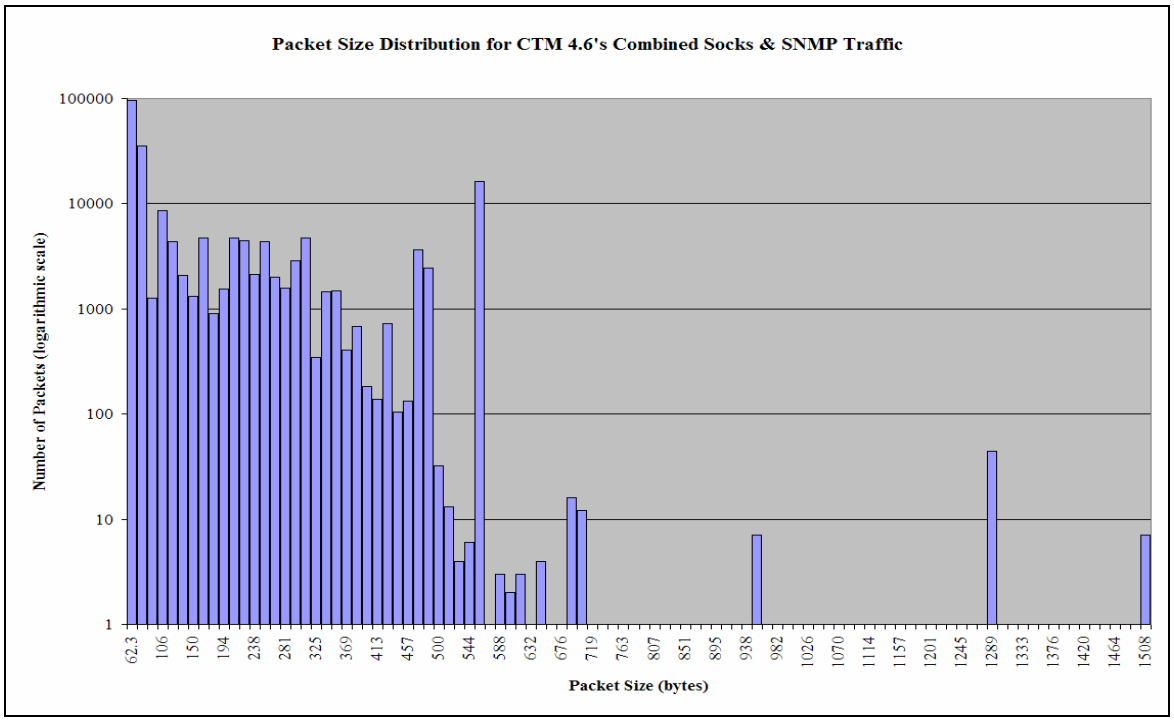


Figure 16. Packet size distribution for CTM 4.6's combined Socks & SNMP traffic

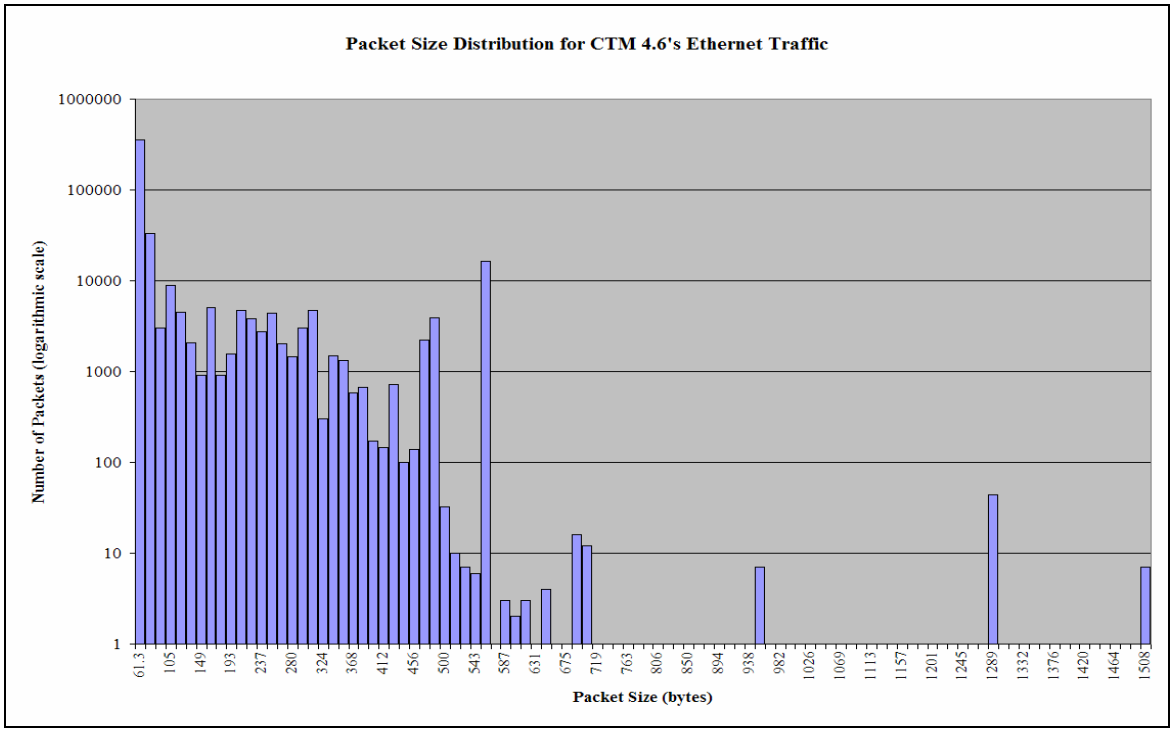


Figure 17. Packet size distribution for CTM 4.6's Ethernet traffic

As in the analysis of the interarrival time, the mean, variance, and coefficient of variation of the packet size distributions are computed using Equations (4.3) to (4.7) in Mathcad and tabulated in Table 6 below.

Type of Traffic	Mean (bytes)	Variance ($bytes^2$)	Coefficient of Variation
CTC's Socks Traffic	222.972	59095.784	1.090
CTM 4.6's Socks Traffic	145.053	21536.979	1.012
CTM 4.6's SNMP Traffic	455.214	2627.746	0.113
CTM 4.6's Combined Socks & SNMP Traffic	155.898	24121.782	0.996
CTM 4.6's Ethernet Traffic	102.678	13118.495	1.112

Table 6. Tabulated statistics for the packet size distributions

The mean values in Table 6 are then substituted into Equation (4.19) to calculate the values for T_S. In the calculations involving traffic that traverses on the Section DCC (SDCC), i.e., the CTC's Socks traffic, the CTM 4.6's Socks traffic, the CTM 4.6's SNMP traffic, and the CTM 4.6's combined Socks and SNMP traffic, the SDCC's link speed of 192 kbps is used. Likewise the Ethernet's link speed of 100 Mbps is used in the calculations for the CTM 4.6's Ethernet traffic. The results are tabulated in Table 7 below.

Type of Traffic	Type of Link/Speed	T_S
CTC's Socks Traffic	SDCC/192 kbps	9.291 ms
CTM 4.6's Socks Traffic	SDCC/192 kbps	6.044 ms
CTM 4.6's SNMP Traffic	SDCC/192 kbps	18.967 ms
CTM 4.6's Combined Socks & SNMP Traffic	SDCC/192 kbps	6.496 ms
CTM 4.6's Ethernet Traffic	Ethernet/100 Mbps	8.214 μs

Table 7. Tabulated values of service time, T_S, for the packet size distributions

3. Link Utilization

With the results in Tables 5 and 7, the link utilization can be computed using Equation (4.20). The link utilizations for four NEs are shown in Table 8. Next, the results in Table 8 are linearly extrapolated to obtain the link utilizations for 50 NEs (the maximum capacity of the CTC) and 2500NEs (the maximum capacity of the CTM 4.6), which are tabulated in Table 9.

Type of Traffic	Type of Link/Speed	Link Utilization
CTC's Socks Traffic	SDCC/192 kbps	1.37×10^{-3}
CTM 4.6's Socks Traffic	SDCC/192 kbps	1.33×10^{-3}
CTM 4.6's SNMP Traffic	SDCC/192 kbps	1.58×10^{-4}
CTM 4.6's Combined Socks & SNMP Traffic	SDCC/192 kbps	1.48×10^{-3}
CTM 4.6's Ethernet Traffic	Ethernet/100 Mbps	4.18×10^{-6}

Table 8. Tabulated link utilizations for four NEs

Type of Traffic	Type of Link/Speed	Link Utilization for 50 NEs	Link Utilization for 2500 NEs
CTC's Socks Traffic	SDCC/192 kbps	0.0171	0.855
CTM 4.6's Socks Traffic	SDCC/192 kbps	0.0166	0.830
CTM 4.6's SNMP Traffic	SDCC/192 kbps	1.98×10^{-3}	0.099
CTM 4.6's Combined Socks & SNMP Traffic	SDCC/192 kbps	0.0185	0.926
CTM 4.6's Ethernet Traffic	Ethernet/100 Mbps	5.23×10^{-5}	2.62×10^{-3}

Table 9. Linearly extrapolated link utilizations for 50 and 2500 NEs

From Table 9, it can be seen that the SDCC can potentially support the CTC's Socks traffic for 50 NEs with ease and for up to 2500 NEs with about 14% of spare capacity. However, the CTM 4.6, which has both Socks and SNMP traffic on the SDCC,

will utilize about 93% of the SDCC's capacity if it is managing 2500 NEs. The results also show that the link utilization of the CTM 4.6's Ethernet traffic is too low to create any impact. Nevertheless, this is based only on the analysis of first–order statistics and has not taken into account the burstiness of the traffic. This will be examined in the next subsection.

4. Estimation for Self–similarity

Using Mathcad, the data points for the variance–index plots were generated for values of m = 1, 10, 32, 100, 320, and 1000 that correspond to values of log(m) = 0, 1, 1.5, 2, 2.5 and 3. The variance–interarrival time plots for the different types of traffic are illustrated in Figures 18 to 22 while the variance-packet size plots for the different types of traffic are shown in Figures 23 to 27. In all the plots, the data points are joined using linear best–fit. The linear function of the straight line thus corresponds to Equation (4.23) and its gradient is β. With the values of β, the corresponding values of H are computed in Table 10 using Equation (4.22).

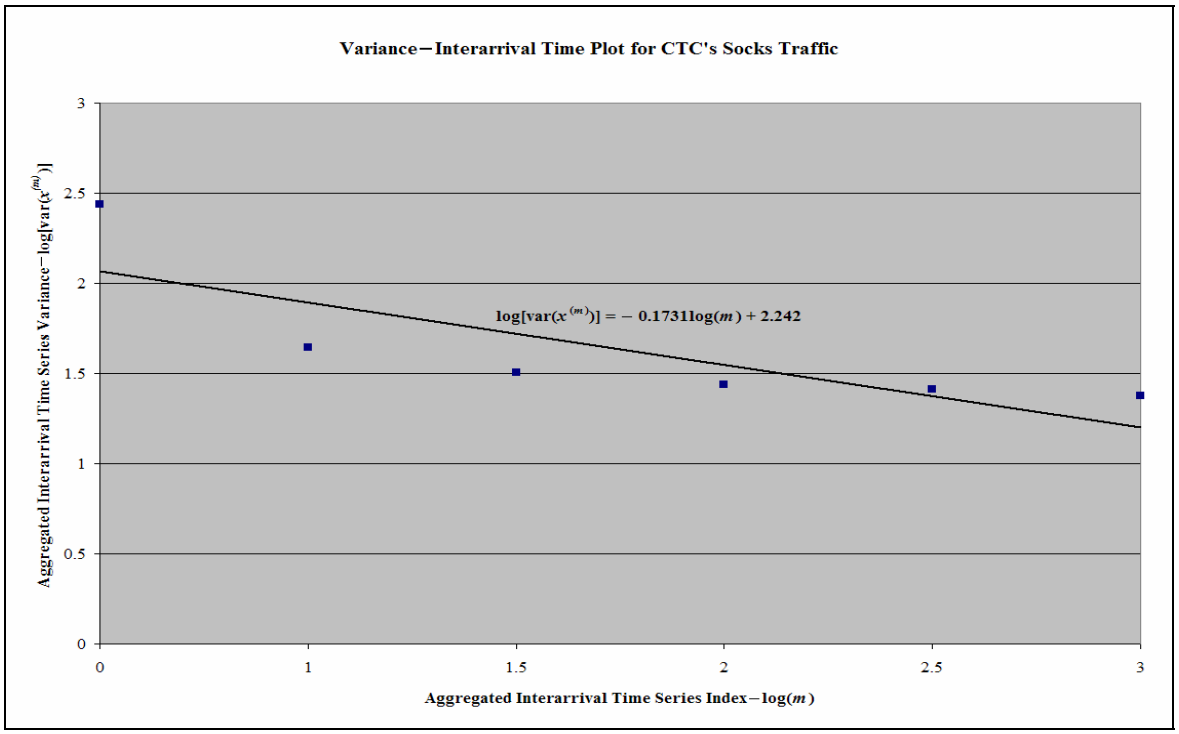


Figure 18. Variance–interarrival time plot for CTC's Socks traffic

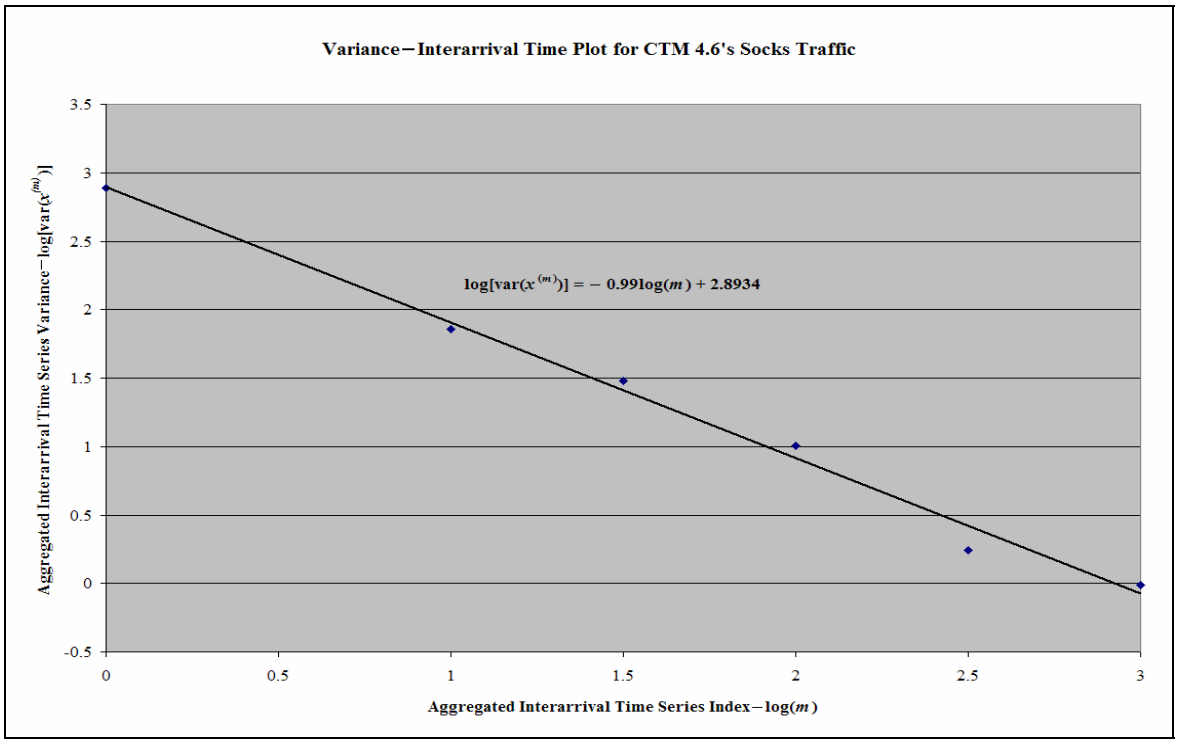


Figure 19. Variance–interarrival time plot for CTM 4.6's Socks traffic

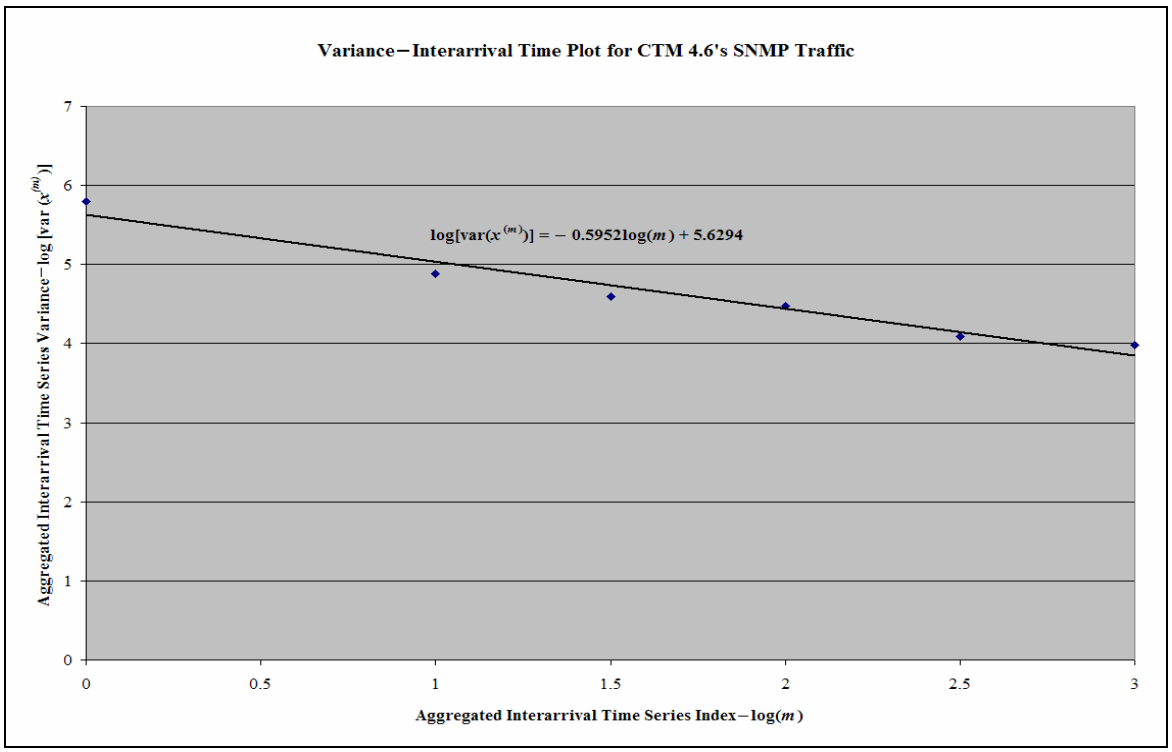


Figure 20. Variance–interarrival time plot for CTM 4.6's SNMP traffic

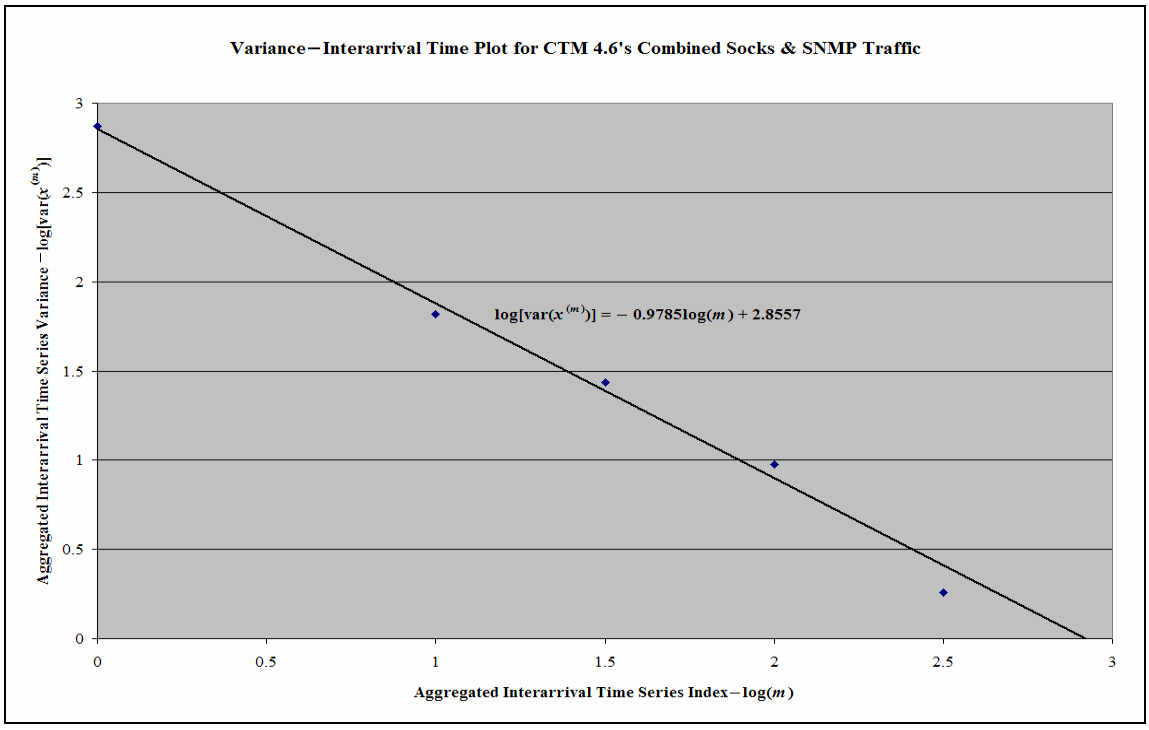


Figure 21. Variance–interarrival time plot for CTM 4.6's combined Socks & SNMP traffic

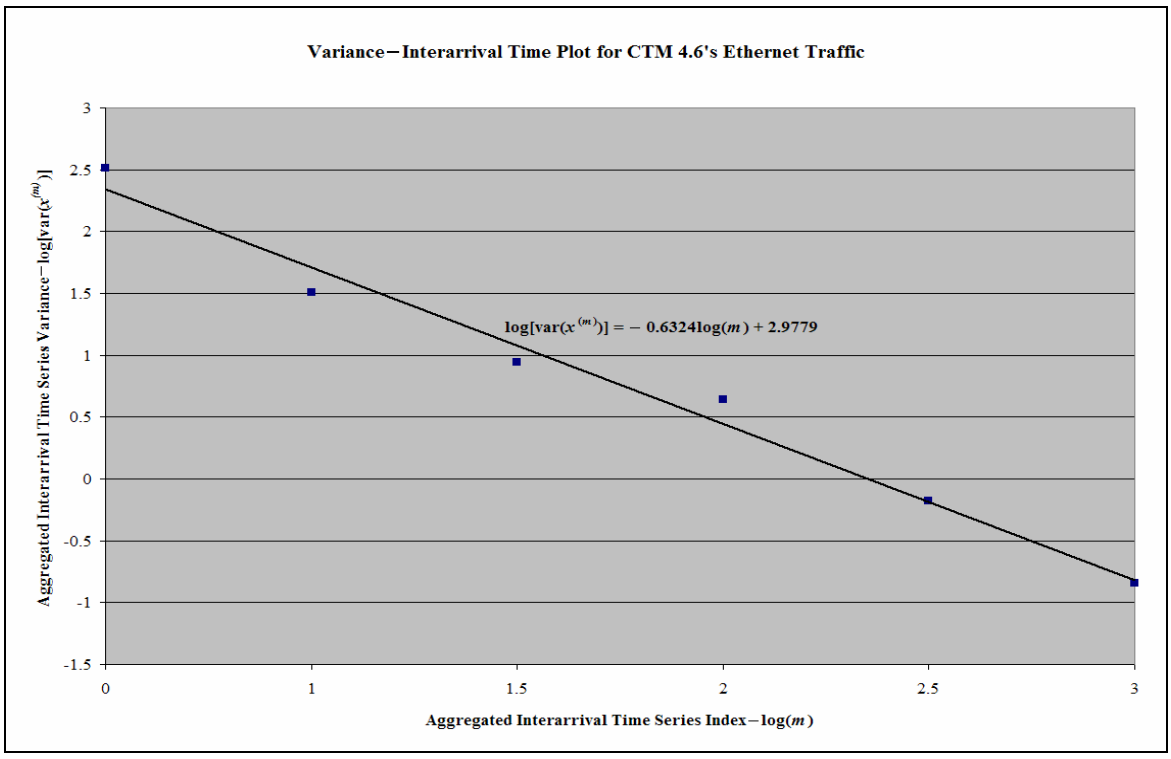


Figure 22. Variance–interarrival time plot for CTM 4.6's Ethernet traffic

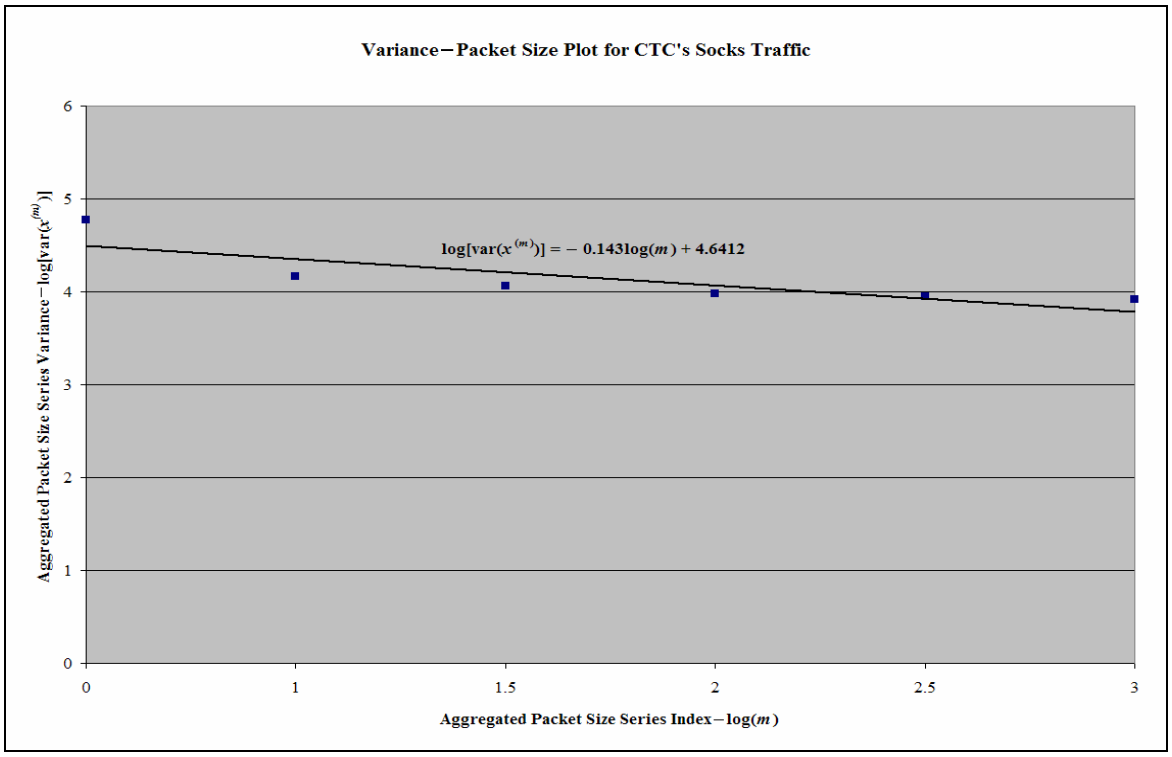


Figure 23. Variance–packet size plot for CTC's Socks traffic

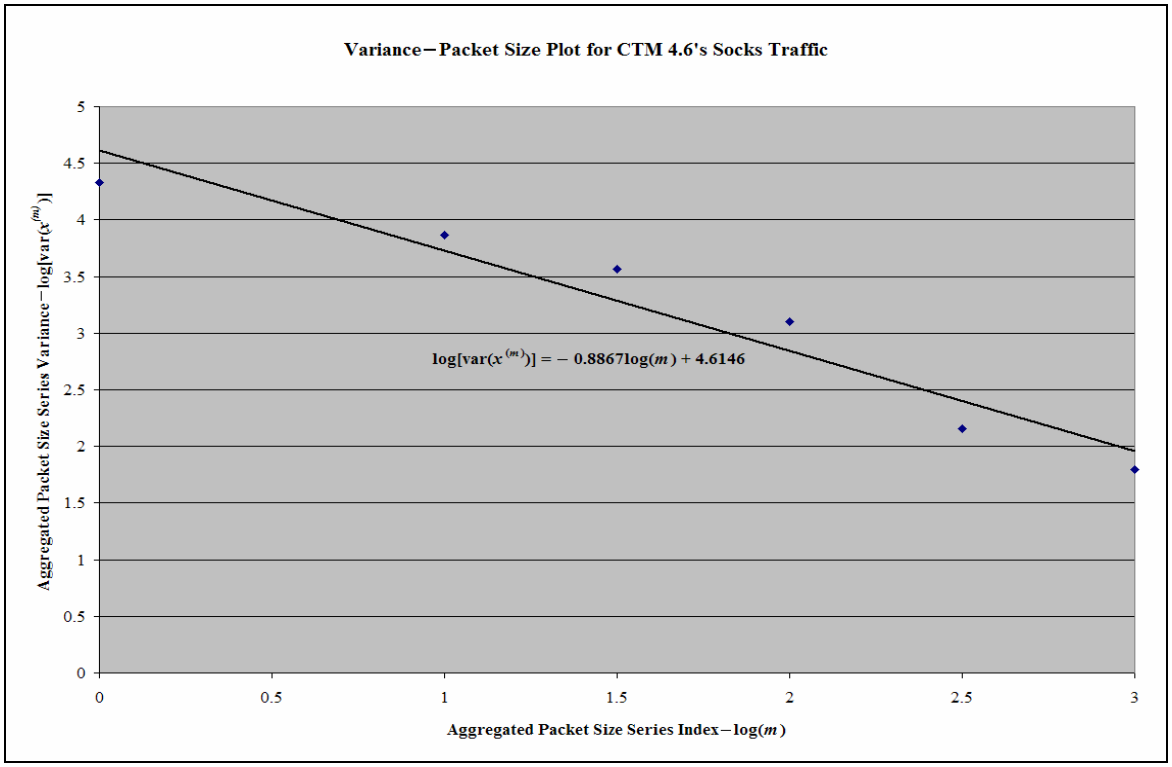


Figure 24. Variance–packet size plot for CTM 4.6's Socks traffic

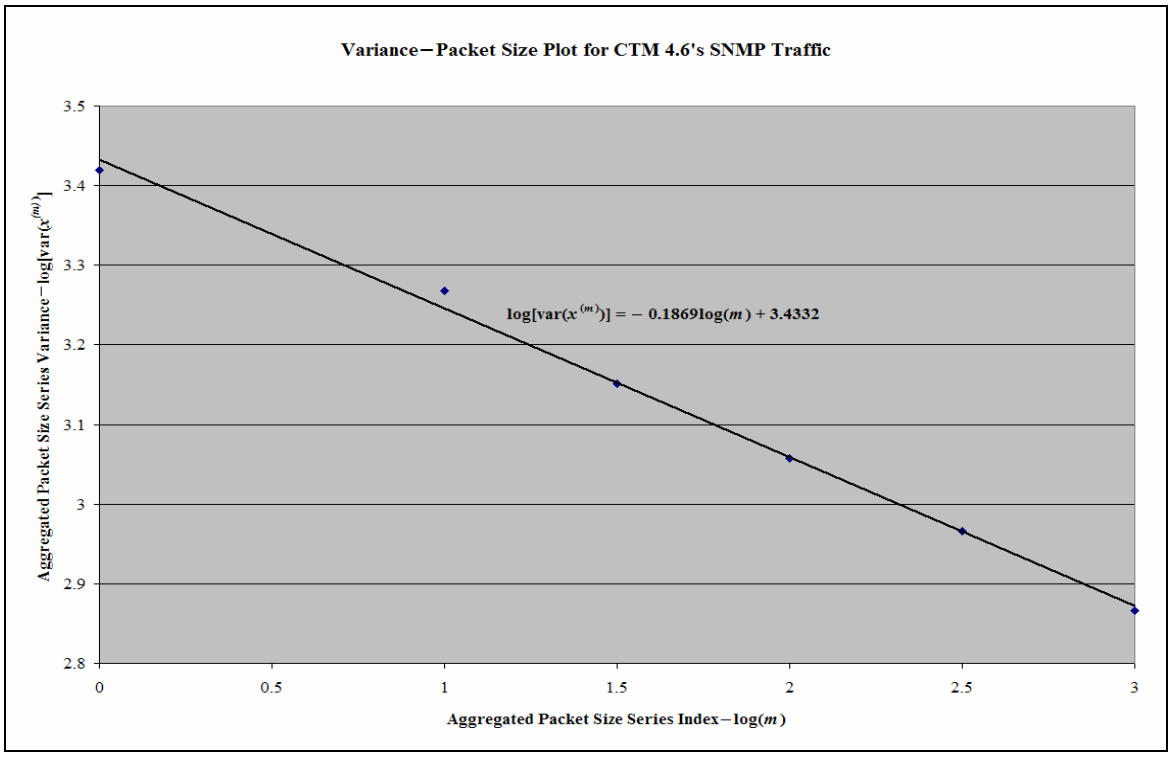


Figure 25. Variance–packet size plot for CTM 4.6's SNMP traffic

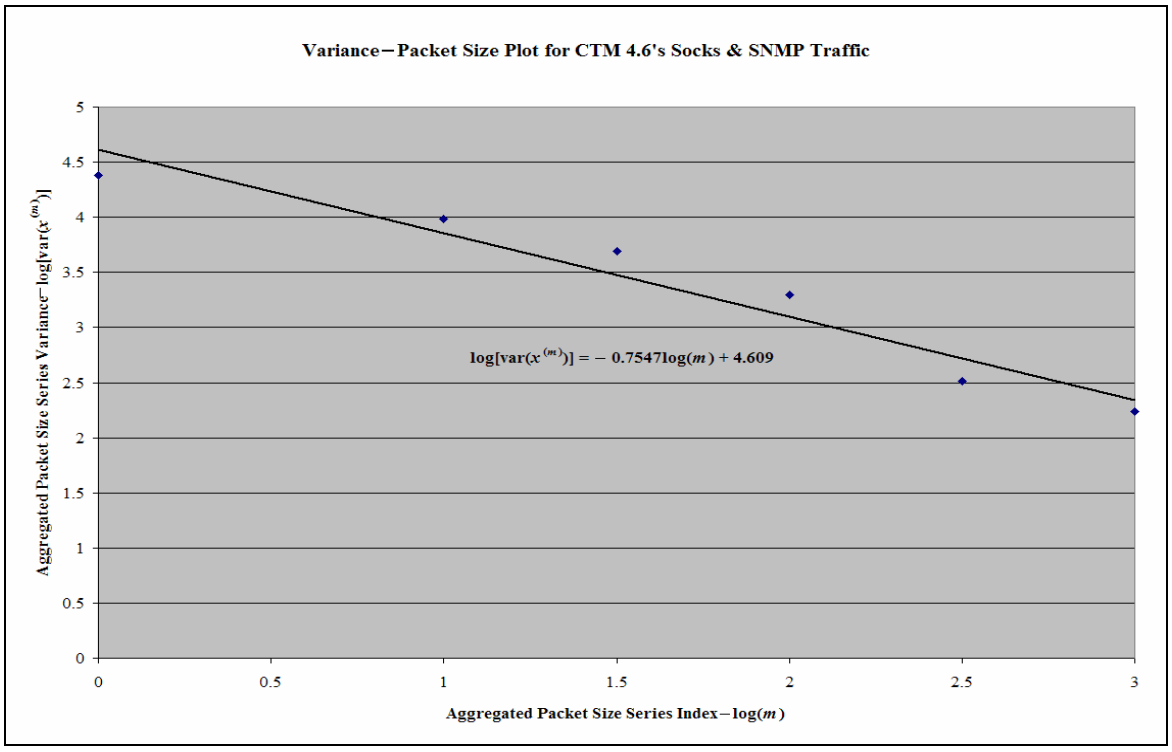


Figure 26. Variance–packet size plot for CTM 4.6's combined Socks & SNMP traffic

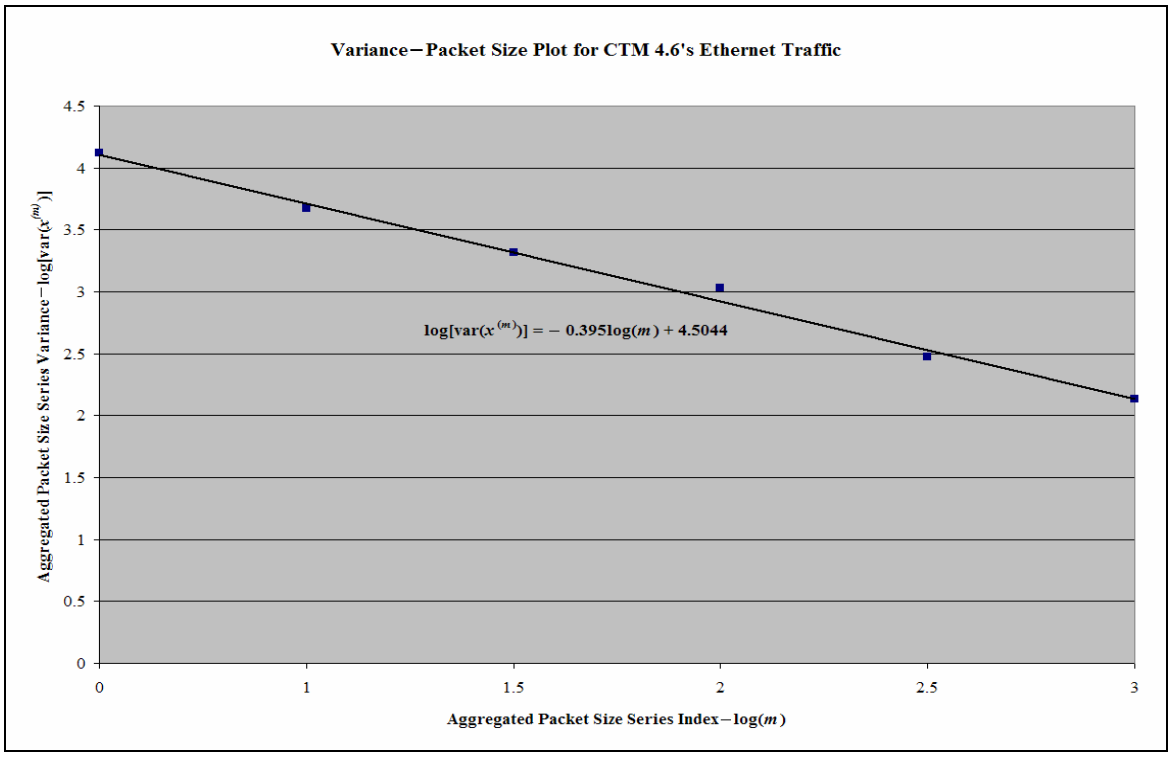


Figure 27. Variance–packet size plot for CTM 4.6's Ethernet traffic

Type of Traffic	β	H
CTC's Socks Traffic (Interarrival Time)	0.1731	0.9135
CTC's Socks Traffic (Packet Size)	0.143	0.9285
CTM 4.6's Socks Traffic (Interarrival Time)	0.99	0.505
CTM 4.6's Socks Traffic (Packet Size)	0.8867	0.5567
CTM 4.6's SNMP Traffic (Interarrival Time)	0.5952	0.7024
CTM 4.6's SNMP Traffic (Packet Size)	0.1869	0.9066
CTM 4.6's Combined Socks & SNMP Traffic (Interarrival Time)	0.9785	0.5108
CTM 4.6's Combined Socks & SNMP Traffic (Packet Size)	0.7547	0.6227
CTM 4.6's Ethernet Traffic (Interarrival Time)	0.6324	0.6838
CTM 4.6's Ethernet Traffic (Packet Size)	0.395	0.8025

Table 10. Tabulated values for β and H

From the values of H obtained in Table 10, it can be seen that with the exception of the CTM 4.6's Socks and the CTM 4.6's combined Socks and SNMP traffic that have values of H near to 0.5, thus less self–similar, the rest have a high degree of self–similarity. The high values of H also suggest that the CTC's Socks traffic, the CTM 4.6's SNMP traffic and the CTM 4.6's Ethernet traffic are bursty. This matches the results obtained earlier in the distributions plots. In the next subsection, the impact of traffic burstiness on the network utilization is examined.

5. Effects of Self–similarity on Queue Depth

Figures 28 to 30 show plots of the mean utilization of the network, ρ, versus the queue depth, q, in Equation (4.24) for the values of H in Table 10, using different scales for q.

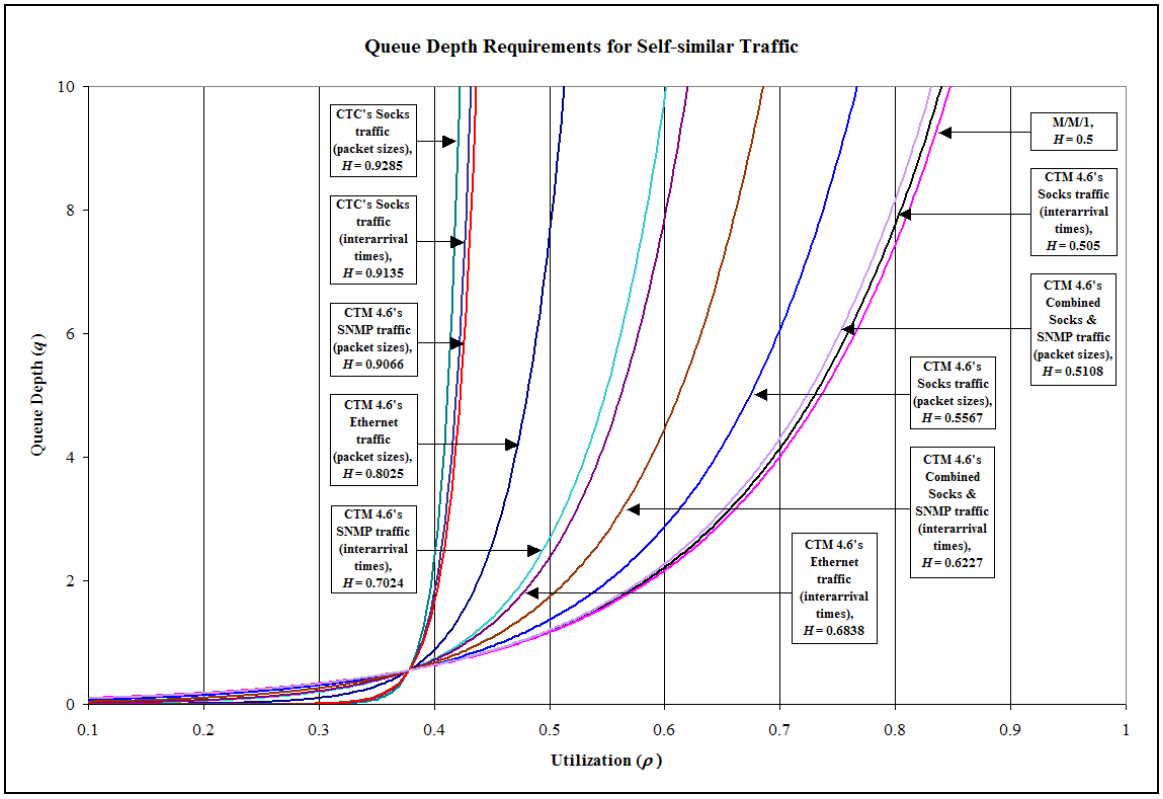


Figure 28. Plot of utilization, ρ, versus queue depth, q, (scale to q = 10)

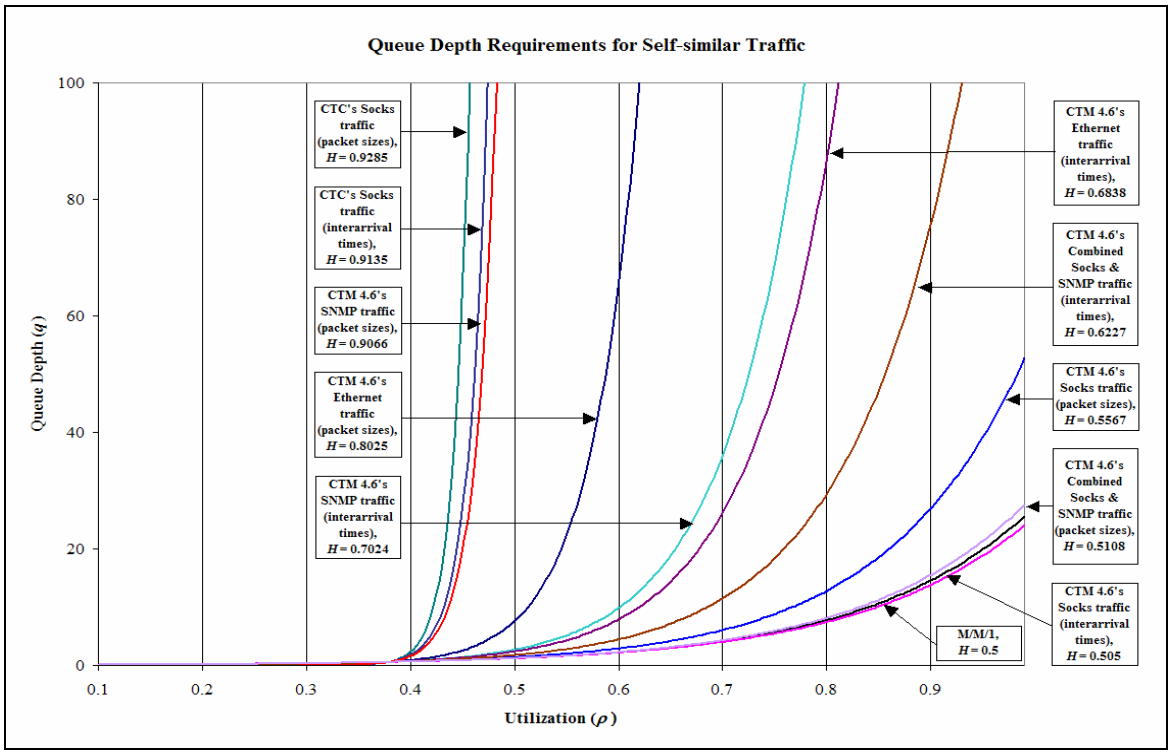


Figure 29. Plot of utilization, ρ, versus queue depth, q, (scale to q = 100)

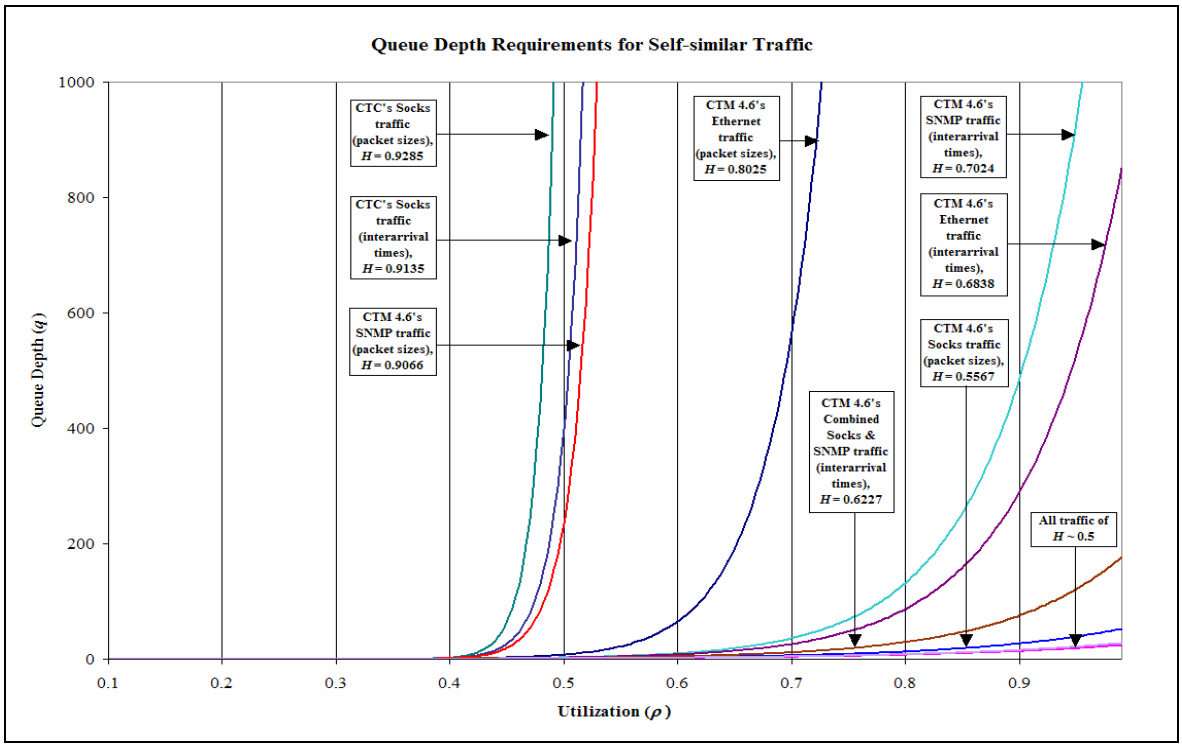


Figure 30. Plot of utilization, ρ, versus queue depth, q, (scale to q = 1000)

From Figure 28, it can be seen that for $\rho \leq 0.38$, $q \leq 1$ for all traffic. The maximum number of NEs required to obtain a utilization of 0.38 for the various kind of traffic are computed in Table 11, which confirms the earlier conclusion (based on first–order statistics) that the CTM 4.6's Ethernet traffic does not create any significant impact on the Ethernet network.

Type of Traffic	Number of NEs
CTC's Socks Traffic	1109
CTM 4.6's Socks Traffic	1142
CTM 4.6's SNMP Traffic	9620
CTM 4.6's Combined Socks & SNMP Traffic	1027
CTM 4.6's Ethernet Traffic	360,000

Table 11. Maximum number of NEs required to obtain a utilization of 0.38

It is observed from Figure 28 that when operating the CTC at $\rho > 0.38$, the requirement for q increases steeply. Figure 30 also shows that if q is increased from 1 to 1000 to accommodate the burstiness of the CTC's Socks traffic (for packet size), ρ only increases by 10% to 0.49, which translates to the ability to manage 1430 NEs. Nevertheless, the CTC's specification is only to manage up to 50 NEs with a utilization of 0.0171, which is significantly below 0.38. Therefore, although the traffic is self–similar and bursty, the low utilization ensures a low requirement for q.

As mentioned earlier, the operation of the CTM 4.6 requires both the CTM 4.6's Socks and SNMP traffic, and Table 9 shows that when managing 2500 NEs, the utilization for the CTM 4.6's combined Socks and SNMP traffic will reach 0.926. On the other hand, Figure 29 shows that when operating at $\rho = 0.926$, it would require $q = 100$ (approximately 15 kB based on the mean packet size of combined Socks and SNMP traffic) in order to accommodate the CTM 4.6's combined Socks and SNMP traffic (interarrival time). Nevertheless, if the CTM 4.6 is operating with $p = 0.67$ (which translates to man-

aging 1800 NEs) the requirement for q is reduced by a factor of 10. Table 11 also shows that the requirement for q is further reduced to 1, if it is managing only 1027 NEs.

Therefore, depending on the queuing buffer available, it is possible but not advisable to use the CTM 4.6 for managing 2500 NEs as claimed in its specifications. For safe operation, it is recommended that the CTM 4.6 be used to manage not more than 1027 NEs.

E. SUMMARY

In this chapter, the captured traffic was first analyzed using Ethereal to determine the protocols used by the CTC and the CTM 4.6. Next the chapter briefly described the data pruning process. Then the traffic was further analyzed using statistical tools mentioned in Chapter IV. Finally, the results of the analysis were discussed and the effects of the self–similar nature of the traffic were briefly illustrated.

The next chapter summarizes the entire study and discusses some avenues for further research into the management tools's characteristics.

THIS PAGE IS INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND FUTHER RESEARCH AREAS

A. CHAPTER OVERVIEW

The first part of this chapter summarizes the work done and concludes this study. The second part of this chapter discusses some areas which were identified during the course of this work for further study.

B. CONCLUSION

This study began with preliminary market research on SONET management tools available in the market for use with the Cisco ONS 15454. It had been found that most SONET/SDH equipment manufacturers also build their own EMS to support their own products and that few third–party EMSs exist that can interface with multi–vendor's products. Therefore, for the purpose of this study two Cisco's EMSs, the CTC and the CTM 4.6 are deployed onto the SONET network (consisting of four ONS 15454s) in the Advanced Networking Laboratory. Subsequently, packet analyzers are deployed to passively capture the network traffic for analysis.

Using Ethereal, it was revealed that the CTC communicates with the NEs through a connection to TCP Port 1080. This connection uses a proprietary Socks protocol that incorporated GIOP. Similarly, the CTM 4.6 also uses the same Socks protocol (as its main communication tool) in addition to using SNMP. The captured traffic was thus divided into five categories: CTC's Socks traffic, CTM 4.6's Socks traffic, CTM 4.6's SNMP traffic, CTM 4.6's Socks and SNMP traffic, and CTM 4.6's Ethernet traffic.

Analyzing the interarrival time distributions and packet size distributions of the five kinds of traffic showed that the interarrival time distributions of all the traffic resemble that of the exponential distribution with a low decay rate (<1). While only the packet size distributions of the CTM's 4.6 Socks traffic, CTM 4.6's Socks and SNMP traffic, and the CTM 4.6's Ethernet traffic resemble the exponential distribution. In addition, the interarrival time distributions of the CTC's Socks traffic and the CTM 4.6's SNMP traffic

and the packet size distributions of the CTC's Socks traffic and the CTM 4.6's SNMP traffic appear to exhibit self–similarity characteristics.

Thus higher–orders statistics are used to estimate the Hurst parameter of the various distributions. It was found that the CTC's Socks traffic, the CTM 4.6's SNMP traffic, and the CTM 4.6's Ethernet traffic are self–similar with high values for the Hurst parameter. On the other hand, the CTM 4.6's Socks traffic and the CTM 4.6's combined Socks and SNMP traffic have Hurst parameter values closer to 0.5, which is the Hurst parameter value for M/M/1 traffic.

From the first–order statistics of the interarrival time distributions and packet size distributions, the link utilizations of the five categories of traffic were computed and linearly extrapolated to obtain the link utilizations for 50 NEs (the CTC's capacity) and 2500 NEs (the CTM 4.6's capacity). Looking at the low link utilization of 0.171 for the CTC's traffic when the CTC is used to manage 50 NEs, it can be concluded that even with a high Hurst parameter value, the CTC still would not have any problem in managing 50 NEs concurrently. Similarly, the low link utilization for the CTM 4.6's SNMP traffic and CTM 4.6's Ethernet traffic would not pose any problem for the CTM 4.6, even with high Hurst parameter values. However, the CTM 4.6's combined Socks and SNMP traffic would have a high utilization of 0.926 when the CTM 4.6 is used to manage 2500 NEs.

Through the plot of the mean network utilization versus the queue depth for the estimated Hurst parameters, it can be seen that, in order to accommodate the burstiness of the CTM 4.6's Socks and SNMP traffic (packet size distribution), a large queuing buffer is required. Thus to prevent queuing buffer overflow, it is recommended that the CTM 4.6 be used to manage up to a maximum of 1027 NEs, operating within a utilization of 0.38.

In conclusion, this study provided a great opportunity for the author to investigate and understand Cisco SONET equipment and EMSs. It is hoped that the results obtained herein are useful to telecommunications network service providers that are using Cisco equipment.

C. FURTHER RESEARCH AREAS

In the course of working on this thesis, a number of areas were not investigated further due to either a lack of required resources or time. In this subsection, those areas are briefly discussed.

1. Varying the Number of NEs

In this study, only the traffic of a SONET ring with four NEs was captured. The utilization of the network was assumed to be linearly proportional to the number of NEs and the Hurst parameter was assumed to be constant regardless of the number of NEs. Due to time and equipment constraints, it was not possible to vary the number of NEs on the ring and to capture the traffic for verification. In this respect, it would be good to acquire two more NEs for capturing the traffic of three, five, and six NEs on the SONET ring. The utilization of the network and the Hurst parameter can then be obtained for the different number of NEs on the SONET ring and can verify if the assumptions made in this study are valid.

2. Investigating the Traffic on the SDCC

Again, in this study, the network traffic was captured on the IP network. Although the captured traffic is representative of the traffic that traverses on the SDCC, there maybe some traffic overhead introduced by the IP network that can potentially cause the results obtained in this study to be inaccurate. This was not investigated further as the equipment for capturing the traffic on the SDCC was not ready during the course of this study. Hopefully, this area can be examined further with the equipment built by Lieutenant Matthew Klobukowski and Lieutenant Commander Britt Talbert for their theses.

3. Use of Cross–vendor's EMS

As mentioned in Chapter II, the SONET equipment builders supply most of the EMSs available in the market, mainly for managing their products. There is no known case of anyone using a cross–vendor EMS. Nevertheless, SONET and the management protocols are open standards. There is no reason why a cross–vendor EMS cannot be de-

ployed onto the SONET equipment. Therefore, it would be good if EMSs built by other vendors can be acquired and deployed in the Advanced Networking Laboratory for testing with the Cisco equipment. A similar study can also be done to compare the performance of cross–vendor EMSs against that of Cisco's EMSs.

4. Use of Production Network Traffic

The laboratory traffic that was captured and studied does not contain user–command related traffic, as it is difficult to simulate user–commands in the laboratory. The impact of user–command related traffic was thus not studied. In addition, production network traffic that covers the different exceptions, faults, and alarms, etc., cannot be simulated under laboratory conditions. Therefore, it would be beneficial if production network traffic can be acquired and studied. This would enable a more accurate analysis to be performed. Furthermore, a better understanding of the management traffic can be achieved.

LIST OF REFERENCES

1. "Alcatel: Optical Networks Tutorial," Technical Report, IEC Web ProForum, June 1998, *http://www.urec.cnrs.fr/hd/DWDM/ALCATEL/optical_network.pdf*, last accessed July 2004.
2. "SDH/SONET: History, QUB," Technical Report, Parallel Computer Center, *http://www.pcc.qub.ac.uk/tec/courses/network/SDH-SONET/sdh-SONETV1.1a_1.html*, last accessed July 2004.
3. "SONET/SDH Technical Summary," Technical Report, TechFest, *http://www.techfest.com/networking/wan/SONET.htm*, last accessed July 2004.
4. Antonio Liotta, George Pavlou and Graham Knight, "Exploiting Agent Mobility for Large-Scale Network Monitoring," *IEEE Network*, Volume 16, Issue 3, pp. 7-15, May/June 2002, *http://www.ee.surrey.ac.uk/Personal/A.Liotta/Publications/liotta-02a.pdf*, last accessed July 2004.
5. Kok Seng Lim, *Analysis of Network Management Protocols in Optical Networks*, Master's thesis, Naval Postgraduate School, Monterey, California, Mar 2004.
6. Walter Goralski, *SONET/SDH,* 3rd Edition, McGraw Hill/Osborne, Berkeley, California, 2002.
7. "Element Management Systems (EMSs)," Technical Report, IEC Web ProForum, *http://www.iec.org/online/tutorials/acrobat/ems.pdf*, last accessed July 2004.
8. "Alcatel 1353 Generic Element Manager – Datasheet," Technical Report, Alcatel, *http://www.alcatel.com/doctypes/opgdatasheet/pdf/1353_gem_ds_10_31_03.pdf*, last accessed July 2004.
9. "Services and Products –Telecommunications," Technical Report, Fujitsu, *http://www.fujitsu.com/us/services/Telecom/ByAppl/NetworkMgmt/index.html*, last accessed July 2004.
10. "Navis® Optical Element Management System," Technical Report, Lucent, *http://www.lucent.com/livelink/0900940380001dd8c_Brochure_datasheet.pdf*, last accessed July 2004.
11. Kazuhiro Hara, Email Correspondence, NEC Corporation, 21 April 2004.
12. "Tellabs 7190 Element Manager," Technical Report, Tellabs, *http://www.tellabs.com/products/7000/tellabs7190.shtml*, last accessed July 2004.
13. "Alcatel 1350 Management Suite," Technical Report, Alcatel, *http://www.alcatel.com/products/productsummary.jhtml?relativePath=/x/opgproduct/a1350_ms.jhtml*, last accessed July 2004.
14. "Navis® Optical Network Management System (NMS)," Technical Report, Lucent, *http://www.lucent.com/products/solution/0,,CTID+2018-STID+10145-SOID+750-LOCL+1,00.html*, last accessed July 2004.
15. Herbert B. Shulman, Email Correspondence, AT&T, 13 April 2004.
16. Heinz-Gerd Hegering, Sebastian Abeck and Bernhard Neumair, *Integrated Management of Networked Systems: Concepts, Architectures, and Their Operational Application*, Morgan Kaufmann, San Francisco, California, 1999.

17. "Cisco Transport Manager Gateway/CORBA User Guide and Programmer Manual: For Cisco Transport Manager Release 4.6," Technical Report, Cisco, 21 January 2004, *http://www.cisco.com/application/pdf/en/us/guest/products/ps5565/c1674/ccmigration_09186a00801eb02b.pdf*, last accessed September 2004.
18. "Maximizing Business Performance and Resilience with Managed Multiservice Optical Networking," Technical Report, Cisco, *http://www.cisco.com/en/US/products/hw/optical/ps2006/products_white_paper0900aecd800fa597.shtml*, last accessed July 2004.
19. "Cisco ONS 15454 Product Overview, Release 4.0," Technical Report, Cisco, *http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_architecture09186a0080173e5a.html#1007974*, last accessed July 2004.
20. "Cisco Transport Manager Data Sheet 4.6," Technical Report, Cisco, *http://www.cisco.com/en/US/products/sw/opticsw/ps2204/products_data_sheet09186a00801fae55.html*, last accessed July 2004.
21. William Stallings, *High–Speed Networks and Internets: Performance and Quality of Service*, 2nd Edition, Prentice Hall, Upper Saddle River, New Jersey, 2002.
22. Will E. Leland, Murad S. Taqqu, Walter Willinger and Daniel V. Wilson, "On the Self–Similar Nature of Ethernet Traffic (Extended Version)," *IEEE/ACM Transactions on Networking*, Volume 2, Issue 1, pp. 1-15, February 1994, *http://delivery.acm.org/10.1145/180000/178222/p1-leland.pdf?key1=178222&key2=5817401901&coll=portal&dl=ACM&CFID=24844189&CFTOKEN=18213357*, last accessed July 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Chairman, Code EC
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

4. Ms. Rosemary Wenchel
   Chief Scientist, Naval Security Group Command
   Fort Meade, Maryland

5. Lieutenant Michael Herlands
   Naval Security Group Command
   Fort Meade, Maryland

6. Ms. Becky Ankrom
   Laboratory for Telecommunication Science
   Fort Meade, Maryland

7. Professor John C. McEachen
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

8. Professor Randy L. Borchardt
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California