NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ANALYSIS OF NETWORK MANAGEMENT PROTOCOLS IN OPTICAL NETWORKS

by

Kok Seng Lim

March 2004

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

Approved for public release, distribution is unlimited

THIS PAGE 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** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Analysis of Network Management Protocols in Optical Networks			**5. FUNDING NUMBERS**
6. AUTHOR(S) Kok Seng, Lim			
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)

In this thesis, the scalability issues of Simple Network Management Protocol (SNMP) in optical network management are explored. It is important to understand the effect of varying the number of nodes, the request inter-arrival times and the polling interval on the performance of SNMP and the number of nodes that can be effectively managed. The current study explored the effect of varying these parameters in a controlled test environment using the OPNET simulation package. In addition, traffic analysis was performed on measured SNMP traffic and statistics were developed from the traffic analysis. With this understanding of SNMP traffic, an SNMPv1 model was defined and integrated into an OPNET network model to study the performance of SNMP. The simulation results obtained were useful in providing needed insight into the allowable number of nodes an optical network management system can effectively manage.

14. SUBJECT TERMS Network Management Protocols, SNMP, CMIP, SONET, Optical Networks, Data Communication Channels, Scalability Issues, Traffic Analysis and OPNET Simulation.			**15. NUMBER OF PAGES** 89
			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 INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ANALYSIS OF NETWORK MANAGEMENT PROTOCOLS IN OPTICAL NETWORKS

Kok Seng Lim
Civilian, Ministry of Defense, Singapore
Bachelor of Engineering (Hons), Nanyang Technological University, Singapore, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author: Kok Seng Lim

Approved by: John C. McEachen
Thesis Advisor

Randy L. Borchardt
Second Reader

John P. Powers
Chairman, Department of Electrical Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this thesis, the scalability issues of Simple Network Management Protocol (SNMP) in optical network management are explored. It is important to understand the effect of varying the number of nodes, the request inter-arrival times and the polling interval on the performance of SNMP and number of nodes that can be effectively managed. The current study explored the effect of varying these parameters in a controlled test environment using the OPNET simulation package. In addition, traffic analysis was performed on measured SNMP traffic and statistics were developed from the traffic analysis. With this understanding of SNMP traffic, an SNMPv1 model was defined and integrated into an OPNET network model to study the performance of SNMP. The simulation results obtained were useful in providing needed insight into the allowable number of nodes an optical network management system can effectively manage.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would first like to thank my wife Amanda for all of her support during the past one and a half years. Without her help and understanding regarding my late hours at work, this would have been a much more difficult ordeal. I would like to express my most sincere gratitude to Prof. John McEachen for his guidance and providing me with the resources necessary to conduct this study as effectively as possible. He has never failed to stop whatever work he is doing to attend to my questions and I really appreciate it.

I would also like to thank Prof. Randy Borchardt for agreeing to be my second reader to this thesis and also providing support and guidance.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Optical networks are in a period of transition when it comes to network management issues. At the present time, optical network management is still a young discipline and considerable development is required before it can be deployed to manage large optical networks. Introduced in 1988 to provide management capability for TCP/IP-based networks, SNMP rapidly became the most widely used standardized network management tool. SNMP is designed according to a centralized network management paradigm characterized by a low degree of flexibility and re-configurability. This centralized approach is known to present severe efficiency and scalability limitations: the process of data collection and analysis typically involve massive transfers of management data causing strain on network throughput and processing bottlenecks at the manager host. The problems of efficiency and scalability become an issue with the increase of management data.

Until now, however, no exploration had been conducted on the scalability of SNMP. It is important to understand the effect of varying the number of nodes, the request inter-arrival times and the polling interval on the performance of SNMP and the number of nodes that could be effectively managed. Thus the current study explores the effect of varying these parameters in a controlled test environment using the OPNET simulation package. The main thrust of the study was to explore these parameters to gain needed insight into the number of nodes a network management station can effectively manage and to develop notions for properly specifying the request inter-arrival time to avoid potential processing bottlenecks and network congestion.

The first part of this study involved performing a traffic analysis on real, operational SNMP traffic. Statistics were developed from the traffic analysis. This analysis was necessary in order to understand traffic parameters, such as polling interval, request inter-arrival times, request packet size, etc., of actual SNMP traffic. With this understanding, a SNMPv1 model was defined and integrated into an OPNET network model to study the scalability issues of SNMP-based polling. Subsequently, various test scenarios were generated and simulated. The performance of SNMP, constrained by the bandwidth of man-

agement channels in optical networks, was studied with respect to the effect of varying the number of nodes and request inter-arrival times, and obtaining an optimum number of nodes for a specified polling interval.

In exploring the effect of varying the number of nodes (from 50 to 250 nodes) to be managed by the NMS, it was determined that for a given request inter-arrival time, the link utilization and link throughput would increase with an increase in the number of nodes to be managed. From the simulation results, potential bottleneck and the level of congestion in the network could be determined. Hence, the allowable number of nodes that could be effectively managed by a NMS at a specific request inter-arrival time could be determined from the results obtained.

In exploring the effect of varying the request inter-arrival time (from $2\,\mu s$ to $5000\,\mu s$), it was determined that for a given number of nodes, the link utilization and link throughput would decrease for an increase in request inter-arrival time. From the simulation results, given the number of nodes to be managed, appropriate request inter-arrival time could be determined.

Additionally, for a given polling interval, results were obtained on determining the optimum number of nodes that a NMS can effectively manage for different request inter-arrival time without any significant bottleneck or network congestion. From this analysis, the “bottleneck zone” and “non-congestion zone” were defined. In the “bottleneck zone”, the number of nodes that could be managed was significantly lower than those in the “non-congestion zone”. However, in the “non-congestion zone” the number of nodes that could be managed was limited by the polling interval.

LIST OF SYMBOLS, ACRONYMS, AND/OR ABBREVIATIONS

ASN.1	Abstract Syntax Notation One
CMIP	Common Management Information Protocol
CMISE	Common Management Information Service Element
DARPA	Defense Advanced Research Project Agency
DCN	Data Communication Network
DES	Data Encryption Standard
EMS	Element Management Systems
IAB	Internet Activities Board
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IM	Information Model
IP	Internet Protocol
ISO	International Standard Organization
ITU-T	International Telecommunication Standardization Sector
kbps	kilo bits per seconds
MD5	Message Digest 5
MIB	Management Information Base
μs	microsecond
ms	millisecond
MONET	Multi-wavelength Optical Networking
NEs	Network Elements
NMSs	Network Management Systems

NOC	Network Operations Center
NPS	Naval Postgraduate School
OADMs	Optical Add/Drop Multiplexers
OXCs	Optical Crossconnects
OLTs	Optical Line Terminals
OPNET	Optimized Network Engineering Tool
OSC	Optical Supervisory Channel
OSI	Open Systems Interconnection
OSS	Operations Support System
PDU	Protocol Data Unit
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USM	User-Based Security Model
VACM	View-based Access Control Model

I. INTRODUCTION

A. MOTIVATION

Networks have grown from the connection of a few computer systems located in the same office using a small number of simple protocols to the interconnection of several widely dispersed and highly complex computing facilities, communicating with a mixture of protocols. This growth has made network management an essential and critical function. To maintain the network, network managers must control the operation of each attached component. The combination of network size, equipment complexity and number of protocols would make this nearly an impossible task if each device had to be configured manually [1]. While management functions are now built into the various network elements, these must be interoperable with the management systems used within the network in order to be useful. Additionally, the recurring costs associated with the management of a large network can be much higher than the acquisition costs of the equipment [2].

Network management in SONET/SDH (Synchronous Optical Network / Synchronous Digital Hierarchy) networks is in a period of transition. For a number of years, the International Standard Organization (ISO) and International Telecommunication Union Telecommunication Standardization Sector (ITU-T) have been working to develop several open systems interconnection (OSI) network management standards. The proposed standards are based on the common management information service element (CMISE), which defines both the network management applications and the common management information protocol (CMIP). However, when SONET was deployed, neither CMISE nor CMIP had sufficient maturity to be integrated into production equipment and networks due to their complexity [3].

In the mid-1980s, the simple network management protocol (SNMP) was developed by Internet Engineering Task Force (IETF) to provide simple and effective management of LAN-based internetworking products such as bridges and routers. While SNMP centralizes and reduces the complexity of managing common network resources, SNMP provides the flexibility to manage vendor-specific information and configurations.

SNMP has continued to evolve and is currently supported by almost every enterprise network equipment manufacturer worldwide [1,4]. Due to its ease of implementation and simplicity, SNMP is now widely used as a network management standard.

B. OBJECTIVE OF THESIS

The primary objective of this thesis was to study the performance of the SNMP in optical networks and to carry out an analysis on its performance using an Optimized Network Engineering Tool (OPNET) simulation. In particular, we looked into the scalability of SNMP and the performance of the SNMP operations. We explored the effect of varying the number of nodes to be managed, as well as the effect of varying the request inter-arrival time. Additionally, we also explored the effect of polling interval on the optimum number of devices that a network management system (NMS) can effectively manage using SNMP. The main thrust of the study was to explore these parameters to gain needed insight into the number of nodes a NMS can effectively manage and to properly specify the request inter-arrival time to avoid potential bottleneck and network congestion.

C. RELATED WORK

Over the last few years, with the development of new technologies the capacity of optical transport networks has increased rapidly. This increase in capacity has created an issue in the management and control of the optical networks. Performance-related issues of network management, such as efficiency, scalability, flexibility and re-configurability, have been the focus of much research. Virtually all current network management systems are designed using a centralized network management approach [5]. There is also a moving trend towards distributed network management. New enabling technologies, such as mobile agents, web-based network management and Java-based network management, have been developed for distributed network management [6].To prove the commercial viability of optical network management, considerable research effort will be required in the area of network management and control [7]. In recent years, numerous papers on network management and control have been published. The Multi-wavelength Optical Networking (MONET) program [8], mobile agent technology in network management

[5,9] and enabling technologies for distributed network management [6] are some of the examples on research work done in the area of network management and control. The MONET program, sponsored by the Defense Advanced Research Project Agency (DARPA), brought together resources from leading telecommunication companies and several government agencies to develop technologies needed for a high-capacity, high-performance, and national-scale optical network based on the multi-wavelength fiber-optic technology [8]. A more detailed description of the program can be found in Reference [8].

D. SUMMARY

In today's increasingly expanding optical networks, problems of scalability and efficiency become an issue with the increase of management data. Hence, in order to ensure that networks are properly monitored and maintained, there is a need to study and analyze the performance of the commonly used network management protocol, i.e., SNMP.

The thesis is organized as follows: Chapter II presents an overview on the management of a typical optical network. It also provides an overview on the in-band data communication channels, which are used to transport management data in a SONET networks. Chapter III presents the comparisons between the two main network management protocols, CMIP and SNMP, along with their respective advantages and disadvantages. Chapter IV reviews the key concepts of SNMP and describes the SNMP protocol operations and message formats for the three versions of SNMP. Chapter V presents the traffic analysis performed on measured SNMP traffic and the statistics developed from the traffic analysis. Chapter VI describes the modeling of SNMP, including the simulation module, simulation parameters and test scenarios used in the study. It also discusses the simulation results obtained with respect to the scalability of SNMP in a typical optical network. Chapter VII presents a summary of the thesis and suggestions for follow-on work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MANAGEMENT OF SONET NETWORK

A. CHAPTER OVERVIEW

This chapter presents an overview of network management in a typical optical network. The management framework, the management information model and two main network management protocols are discussed. The chapter also reviews the data communication channels that are used by the SONET network to exchange management messages between devices.

B. MANAGEMENT FRAMEWORK

Besides monitoring and controlling network elements (NEs), network management is also concerned with planning and accounting for the use of NEs and their activities. As mentioned earlier, the size and the diversity of different networks led to considerable complexity in network management applications. Different vendors normally developed their own proprietary network management systems (NMS). Hence, each NE relied on its own unique NMS for management purposes, causing interoperability issues to arise [10].

Figure 1 shows the implementation of key network management functions on a typical optical network. Typically, network management is centralized and may involve multiple management systems deployed in a hierarchical manner [2].

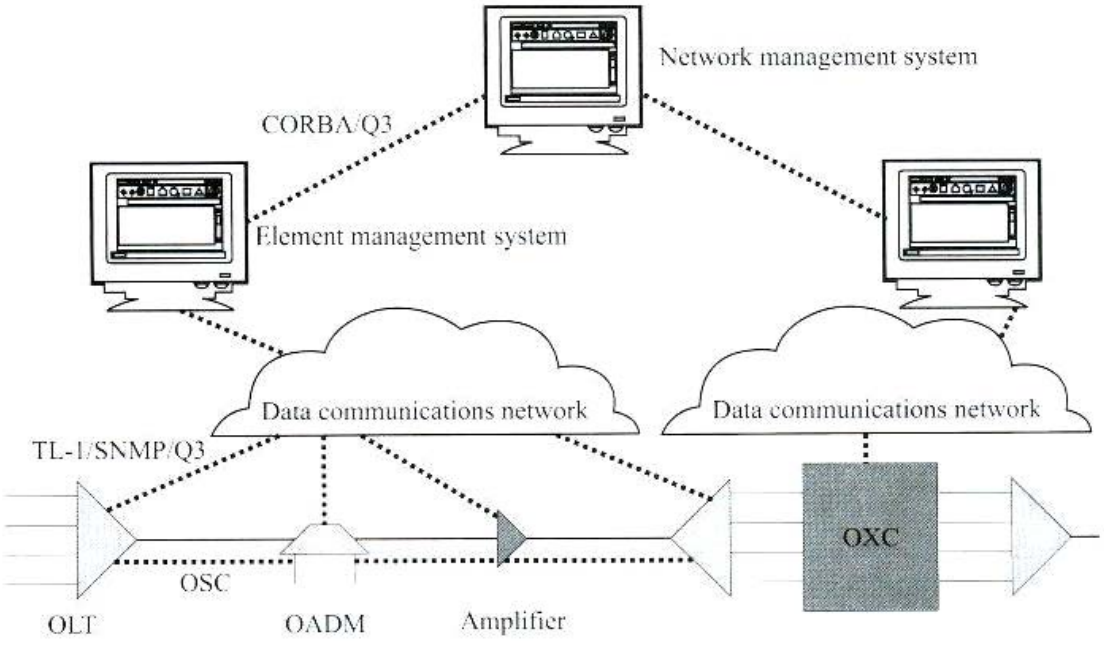


Figure 1 Overview of network management functions of a typical optical network (From Ref. [2].)

Optical line terminals (OLTs), optical add/drop multiplexers (OADMs), optical amplifiers, and optical crossconnects (OXCs), as shown in Figure 1, are examples of NEs that may be managed in the network by the NMS. Each NE is managed by its element management systems (EMSs). Communication with the EMS over the data communication network (DCN) is made possible by a built-in agent implemented in software. While multiple NEs may be connected to an EMS, each EMS typically manages NEs from only one vendor and can view only one NE at a time. Thus, an EMS probably will not have a complete view of the entire network. A fast signaling channel, such as an optical supervisory channel (OSC), as shown in Figure 1, is also required for the exchange of real-time information to control protection switching and other functions. In some cases, multiple EMSs may be used to manage the overall network. In larger networks, the EMSs communicate over a management network with a NMS, also known as an operations support system (OSS). The NMS has a complete view of the entire network and may manage different types of NEs from various vendors. In a multi-tiered management hierarchy, mul-

tiple OSSs may be used to perform different functions, such as fault management and provisioning circuits [2].

C. DATA COMMUNICATION CHANNELS

Each SONET frame has two in-band Data Communication Channels (DCC), namely the Section DCC and the Line DCC. Both are used to convey network management messages between NMS and NEs. Use of these in-band data communication channels preclude the requirement for expensive out-of-band management communications [11].

Table 1 shows the section and line overhead in the transport overhead of a SONET Synchronous Transport Signal "1" (STS-1) frame. Three bytes in the section overhead, bytes D1, D2 and D3, form the Section DCC, a 192 kbps channel that transfers operations, administration, maintenance, and provisioning (OAM&P) information between section-terminating equipment. Nine bytes from the line overhead, bytes D4 through D12, form the Line DCC, a 576 kbps channel for OAM&P (alarms, control, maintenance, remote provisioning, monitoring, administration, other communication needs) messages between line entities [11,12]. As such in SONET, the DCCs are dedicated for the exchange of management traffic.

Section Overhead	A1	A2	J0/Z0
	B1	E1	F1
	D1	D2	D3
Line Overhead	H1	H2	H3
	B2	K1	K2
	D4	D5	D6
	D7	D8	D9
	D10	D11	D12
	S1/Z1	M0 or M1/Z2	E2

Table 1 Transport Overhead in a SONET STS-1 frame (After Ref. [11].)

D. INFORMATION MODEL

An information model (IM) provides a standardized way of representing information to be managed by each NE. Implemented in software within the NE, EMS and NMS using an object-oriented programming language, the IM specifies the attributes, activities, characteristics and external behavior of the network device to be managed [2].

E. MANAGEMENT PROTOCOLS

Most network management systems are based on a centralized, client-server relationship between a manager (central station or client) and the agents (servers) it controls. When the manager needs to read or retrieve the status of the parameters in the NE, it polls the agent, also known as the "get operation". To write or modify values in the NE, the manager will use the "set operation". The agent can also send notifications to its manager when significant events occur. Upon detecting a problem within the NE, the agent can alert its manager via a notification message or an alarm if the condition is serious. These notifications are also known as "traps" [2].

There are multiple standards relating to network management and the two main network management protocols, SNMP and CMIP. The Internet approach, designed to be simple, is based on SNMP. The OSI approach, designed to provide a common, flexible

and robust protocol to provide solution to overcome all problems of network management, is based on CMIP. The simplicity and the ease of implementation of the SNMP, resulted in its rapid design and deployment. These features also solved the immediate problem of managing the Internet, as well as network management related issues in other networking environments. On the other hand, CMIP took longer to design, and its implementation in enterprise network equipment was slowed both by its inherent complexity and the popularity of the SNMP. Despite the shortcomings of both SNMP and CMIP technologies, they will likely be deployed in future enterprise network management products [10].

F. SUMMARY

This chapter presented an overview of how network management functions are implemented on a typical network. It also discussed the management framework, the management information model and the two main network management protocols. An overview of the DCC, which is a SONET in-band communication channel for the exchange of the management messages, is also presented.

The next chapter presents a comparison between SNMP and CMIP, including the advantages and disadvantages of each protocol.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SNMP VERSUS CMIP

A. CHAPTER OVERVIEW

This chapter presents a comparison between CMIP and SNMP. Both the advantages and disadvantages of each protocol are presented. It also discusses why SNMP is the most popular network management solution in use today.

B. INTRODUCTION

SNMP and CMIP are the two prevalent network management protocols in use today. The use of either network management protocols depends on a wide range of factors and both have their advantages and disadvantages (to be discussed in detail later). It is important to understand that SNMP and CMIP are based on different assumptions [10]:

1. In SNMP, the User Datagram Protocol (UDP) is used as the transport protocol for the exchange of the network management messages between the manager and the agent. UDP is a connectionless transport protocol, which does not guarantee the delivery of the messages. Hence, each request and response between the manager and the agent is a separate transaction. On the other hand, in CMIP, the exchange of the requests and responses uses an OSI connection-oriented transport protocol, which provides sequencing of messages as well as guaranteed delivery [10].
2. In SNMP, an agent does not perform analysis on the information it retrieves or modifies. Only the manager is capable of performing an analysis task. In CMIP, some manager functions are transferred to the agent, which are capable of performing some analysis tasks [10].

C. SNMP

1. Advantages of SNMP

The main advantage of SNMP is its ease of implementation due to its simple design. The number of messages required for each request and response is small and, as such, SNMP does not consume many system resources. In addition, due to its simple design, the variables that are to be monitored can be programmed easily. The net result of SNMP's simplicity is a network manager that is inexpensive, easy to install and use effectively, and has minimal impact on the existing network [10].

Another advantage of SNMP is its widespread popularity [13]. It quickly became the de facto network management standard for a wide range of applications. Almost all major vendors of network equipment design their products to support SNMP. Currently, there is no development underway for a network management protocol to replace SNMP. As such, SNMP will continue its stronghold as the most popular network management protocols [14,15].

Expandability is another advantage of SNMP. Due to its simple design, it allows enhancements to be added easily to meet users' demands. Various new features have been added to SNMP over the past few years and different versions had been created. The different versions and enhancements added will be examined later on in this thesis [14].

2. Disadvantages of SNMP

Like any system, SNMP has its faults; however, due to its clever design most of these faults have workarounds. The major disadvantage encountered by most SNMP is weak security: network management data is vulnerable to threats such as: modification of management information during transit between the manager and agent, disclosure of management information to unauthorized users, and disruption of service through equipment shutdown [1,14]. Security features have been added in the latest release of SNMP, called SNMPv3, in the form of encryption, authentication and access control. These security features were added to protect privacy of data (to prevent management information from being eavesdropped, modified, reordered and copied during its transit between the

manager and agent), prevent masquerading and to restrict access of management information to certain group of users [1,14].

Some consider SNMP unsuitable for management of large networks as polling by SNMP managers affect network performance. In addition, critical messages concerning errors within network devices sent by the agents are not guaranteed to reach the NMS. This is because the connectionless transport protocol UDP is used to exchange messages and, as such, the traps sent will not be acknowledged [10].

Further, in every SNMP message, bandwidth is wasted with unnecessary information, such as SNMP version and multiple length and data descriptors (example, describing the type of PDU sends). In addition, substantial amount of bandwidth is being consumed by the needlessly large data handles: SNMP variables are defined as byte strings, each corresponding to a particular managed object. Therefore, SNMP is not a very efficient protocol [13].

The most significant problem with SNMP is that it is so simple that it cannot handle large and expanding networks [14]. The short design time of SNMP did not allow sufficient consideration of the large amount of data that would be in exchanged in future expanding networks. SNMP was not designed to lead network management into the 21st century [14]. New enhancements have been included in SNMPv2 to fix this problem. This new version allows for more in-detail specification of variables, including easier retrieval of large blocks of data. This resulted in two new protocol data units being defined for manipulating the tabled objects [14].

D. CMIP

CMIP was initially designed to replace and overcome the deficiencies in SNMP. It is a more robust, organized and detailed network manager than SNMP. Hence, CMIP is more complex requiring a large amount of system resources. In addition, CMIP has sophisticated data structures with many attributes. These variables properties include:

1. Variable attributes which represent the variable's characteristics, including attributes such as whether it can be readable or writable.
2. Variable behaviors which indicate the type of tasks the variable can perform.
3. Notifications or asynchronous reports generated by the variable in the event of an unusual network conditions, such as an error in a network device.

It is noted that SNMP's variables possess only property one and three as stated above [14].

1. Advantages of CMIP

The major advantage of CMIP over SNMP is that its variables, besides capable of relaying information, can be used to perform tasks. This is impossible under SNMP [14]. For example, when CMIP is used, it can notify the appropriate personnel whenever a client cannot reach a server after pre-determined number of attempts. However, with SNMP, a user must explicitly monitor the number of unsuccessful tries the client has made to reach the server. Hence, CMIP is a more efficient network management protocol as compared to SNMP, as the above task can be automated [14].

Another advantage of CMIP is that it has inherent security features that address the security deficiencies of SNMP [14]. CMIP has built-in security features that support authentication, access control and security logs. Hence, CMIP is an inherently safer system than SNMP and does not require for security upgrades, unlike SNMP [14].

2. Disadvantages of CMIP

Based on CMIP's superior features, one might question why CMIP has not been implemented already; after all, it has been in development for about ten years. The main reason is that the CMIP protocol takes more system resources than SNMP by a factor of ten [14]. In other words, only large systems would be able to handle a full implementation of CMIP, resulting in very few NE implementations. The only way to overcome this disadvantage is to redefine the protocol specifications. Over the past few years, researchers have developed several protocols to adapt CMIP to TCP/IP based networking environments. However, none of these new enabling technologies has gathered sufficient wide spread popularity to replace SNMP as the de facto network management standard [14].

Another disadvantage of CMIP is that it is very complex, hence very difficult to program its variables. Programmers need to undergo specialized training to be able to develop and maintain applications and operate CMIP-based NMS [14].

E. CONCLUSION

The above discussion has presented the advantages and disadvantages of SNMP and CMIP. Based on the above comparison between them, the choice between these network management systems depends largely on its implementation. Even though, CMIP it is superior to SNMP (v1, and v2) in design and operation, current available systems are realistically unable to support CMIP-based NMS due to its requirement for large system resources to support the CMIP model [14].

Initially, SNMP was designed to be a temporary solution and stop-gap measure for network management until a better method could be developed. However, SNMP continued to evolve and is currently supported by almost every enterprise network equipment manufacturer worldwide [1,4]. Due to SNMP's simple design, modular nature and the addition of security features in SNMPv3, it has continued to be the de facto network management standard. [1].

In the next chapter, a brief overview of the key concepts of SNMP which includes the key components of SNMP, the information model used in SNMP, and SNMP data

representation is presented. In addition, the SNMP operations, message format and descriptions of the SNMPv1, SNMPv2 and SNMPv3 protocol operations are covered.

IV. SIMPLE NETWORK MANAGEMENT PROTOCOL

A. CHAPTER OVERVIEW

This chapter provides a brief overview of the key concepts of SNMP. This includes the key components of SNMP, the information model used in SNMP, and SNMP data representation. In addition, it also covers the SNMP operations and message format and provides descriptions of the SNMPv1, SNMPv2 and SNMPv3 protocol operations.

B. INTRODUCTION

SNMP is an application layer protocol based on the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite which offers network management services for monitoring and control of network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. SNMP is a network management tool that allows network administrator to perform monitoring, control and planning tasks on the network to be managed [16].

There are currently three versions of SNMP: SNMPv1, SNMPv2 and SNMPv3. The modular design of SNMP is shown in the consistency of the architecture, structure, and framework of all three versions; this aides gradual evolution of protocol enhancements. Though SNMPv1 was effective and easy to implement, it had its problems and limitations. Enhancements to SNMPv1, resulted in a new SNMP version, SNMPv2, which also corrected the bugs and limitations in SNMPv1. However, these new enhancements did not address security deficiencies, such as privacy of data, masquerading and unauthorized disclosure of data. Subsequently, SNMPv3 was then developed to address these security deficiencies: SNMPv3 added security features, such as access control, authentication, and encryption of management data [1] (see Figure 2, [15]). The SNMPv3 specifications were approved by the Internet Engineering Steering Group (IESG) as full Internet Standard in March 2002, and vendors have begun to support SNMPv3 in their products.

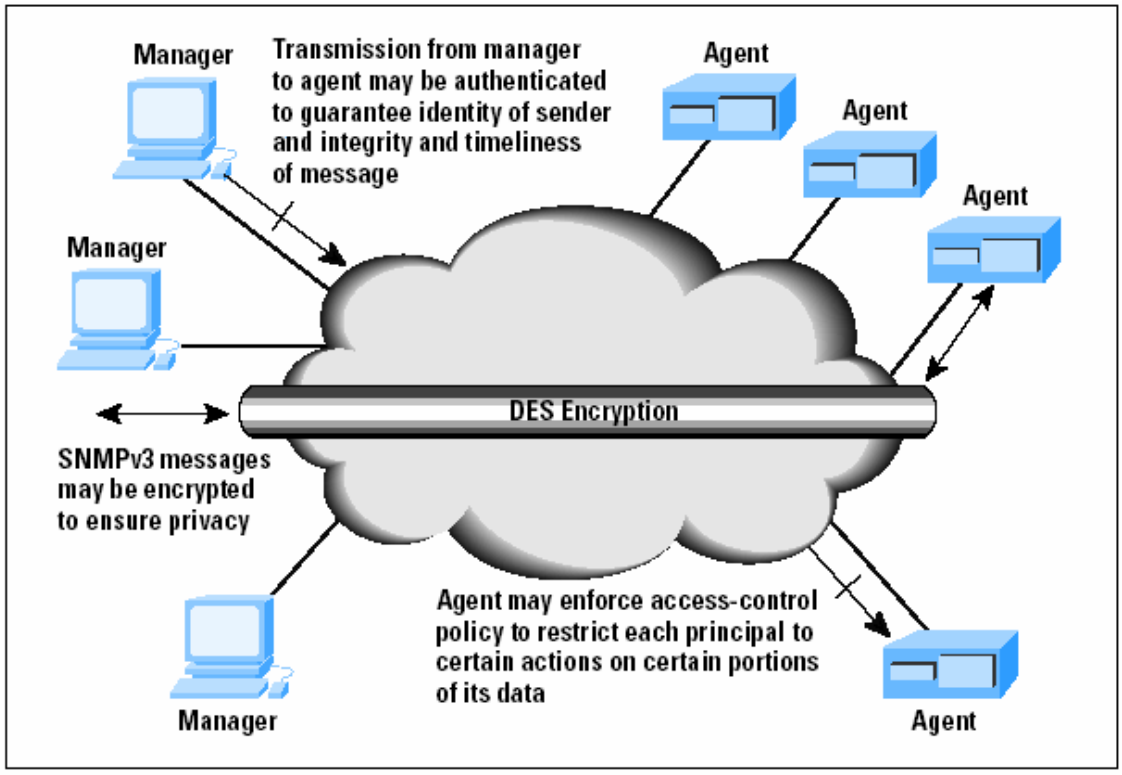


Figure 2 Highlights of SNMPv3 Security Features (From Ref. [15].)

C. SNMP BASIC COMPONENTS

The three key components of a SNMP-based network device are managed devices, agents, and network management systems (NMSs).

A managed device, also known as a network element (NE), has a built-in SNMP agent and resides on a managed network. The managed device collects and stores management information, such as network statistics and traffic information, so that this information can be made available to NMSs whenever it is requested. Optical line terminals (OLTs), optical add/drop multiplexers (OADMs), optical amplifiers, and optical cross-connects (OXCs) are some examples managed devices in optical networks. An agent, residing in a managed device, is a software-based network-management module that translates available local knowledge of management information into a format compatible with SNMP [16].

A NMS is like the "brain" of network management, it executes network management applications that initiate requests to read and write to the NEs; the NMS also provides most of the processing capability as well as memory resources. In order to effectively manage a network, one or more NMSs must coexist together to manage the entire network. The relationships of these three components are shown in Figure 3 [16].

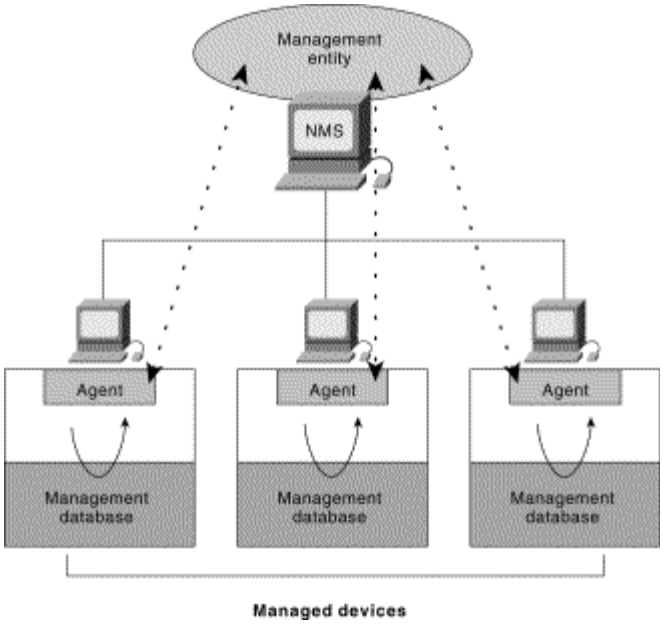


Figure 3 A SNMP-Managed Network Consists of Managed Devices, Agents, and NMSs (From Ref. [16].)

D. SNMP MANAGEMENT INFORMATION BASE

The information model in SNMP is called Management Information Base (MIB). A MIB is a collection of all objects which can be managed by SNMP. Each object is identified by a unique object identifier (or object ID). A MIB is organized in a hierarchical or tree structure and is accessible using a network-management protocol such as SNMP.

A managed object (sometimes called a MIB object, an object, or a MIB) represents a specific characteristic, activity or related information of a managed device. There are two types of managed objects, scalar and tabular. Managed objects with a single ob-

ject instance, i.e., variable, are called scalar objects; managed objects with multiple related object instances, grouped in MIB tables, are called tabular objects.

An object identifier is a unique identifier for a particular object type in the MIB tree structure. All logically related objects are grouped together in the tree structure with a nameless root. Figure 4 illustrates the MIB tree. Object identifiers at each level of the MIB tree structure are assigned by different organizations; the different standards organizations control the top-level MIB object identifiers, while their associated organizations allocate identifiers at the lower-levels. The managed objects in the private branch, as shown in Figure 4, are defined by vendors for their own products. The experimental branch is typically used to identify those non-standardized MIBs [16].

A managed object can be identified either by the object name or object descriptor. For example, the managed object atInput can be uniquely identified either by the object name—iso.identified-organization.dod.internet.private.enterprise.cisco.temporary variables.AppleTalk.atInput—or by the equivalent object descriptor, 1.3.6.1.4.1.9.3.3.1 (see Figure 4) [16].

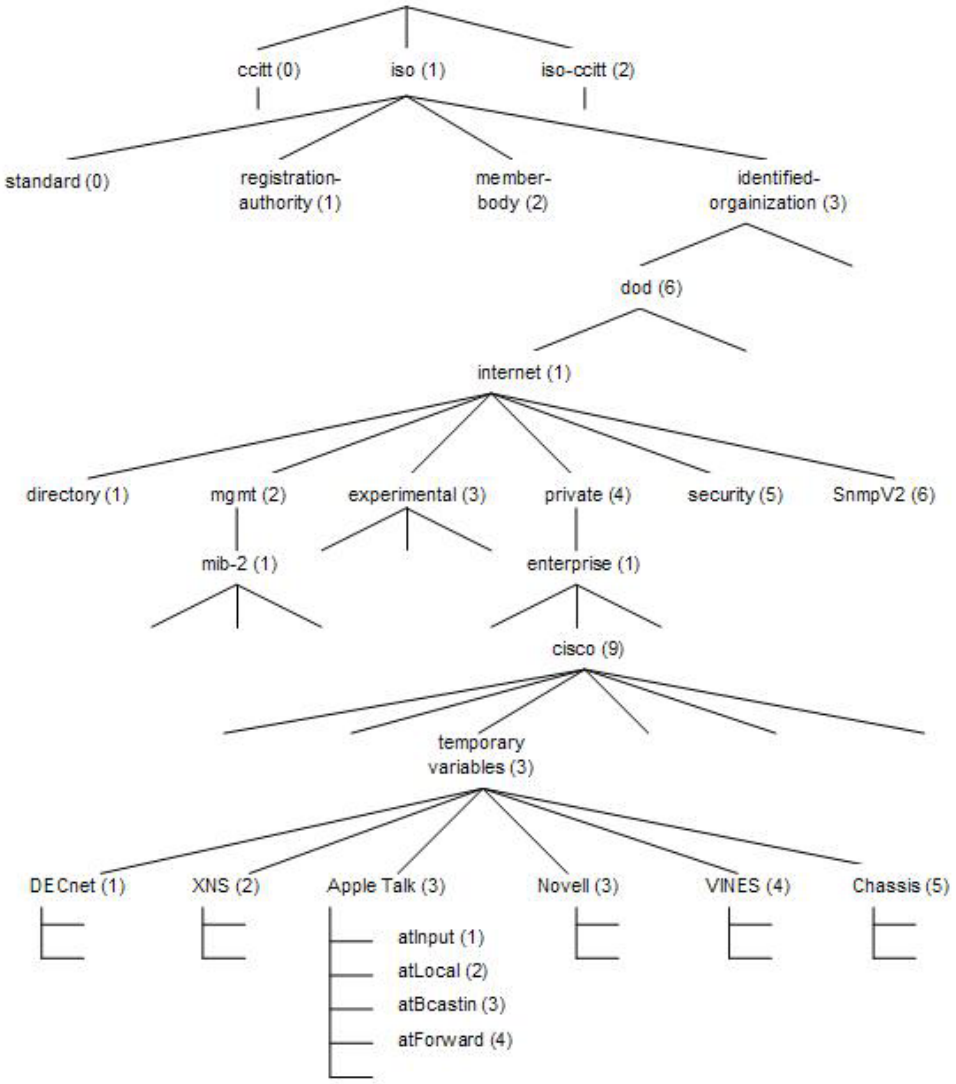


Figure 4 The MIB Tree Illustrates the Various Hierarchies Assigned by Different Organizations (From Ref. [16].)

E. SNMP AND DATA REPRESENTATION

SNMP is responsible for translating different data representation techniques that are used by different networking computing devices into a common data representation language. The difference in data-type definition language between managed devices can compromise the capability of SNMP to exchange information between managed devices. SNMP overcomes these incompatibilities between diverse systems by using a subset of Abstract Syntax Notation One (ASN.1). ASN.1 provides a standardized way to represent data to allow for interoperability [16].

F. PARTIES

SNMPv3 introduces the concept of a "party", which is a logical SNMPv3 entity that can request or receive SNMPv3 communication between two parties. Each SNMPv3 party is defined as a single, unique party identity, a logical network location, a single authentication protocol, and a single privacy protocol. However, a SNMPv3 entity can also be defined as multiple parties, but with different parameters, i.e., having different authentication and/or privacy protocols [17].

G. SNMP OPERATIONS

1. SNMPv1 Protocol Operations

SNMP is a simple request/response protocol that communicates management information between the NMS and managed devices. Typically, when a NMS initiates a request to retrieve or modify management information, such as a network statistic, the managed device will return a response. There are four different protocol operations that allow the implementation of the above behavior: "Get", "GetNext", "Set", and "Trap". The NMS uses the Get operation to retrieve the value of one or more object instances from an agent. The agent will not provide any values in its response if any of the object instances in a list is not successfully found and retrieved. Rather, if the retrieval is unsuccessful, the appropriate error is sent in the response. If the NMS does not know the next object instance from a known managed object instance, it will use the GetNext operation to retrieve the value of the next object instance in a table or a list within an agent. In order to modify the values of object instances within an agent, the NMS uses the Set operation. When a significant event occurs, the agents use the Trap operation to send an unsolicited notification to the NMS [16]. Figure 5 shows the architecture of SNMPv1, which details the various protocol operations between a NMS and a managed device [4].

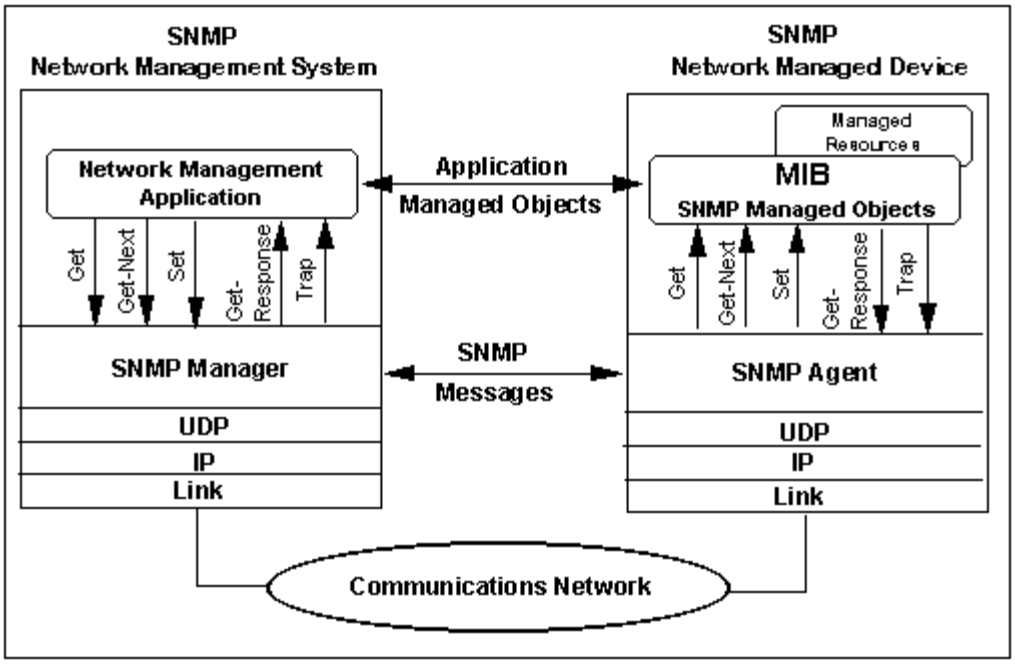


Figure 5 SNMPv1 Architecture (From Ref. [4].)

2. SNMPv2 Protocol Operations

In SNMPv2, the Get, GetNext, and Set operations are exactly the same as in SNMPv1. However, SNMPv2 adds two new protocol operations and enhances the Trap operations. The only difference between the SNMPv2 Trap operation and that used in SNMPv1 is the message format; otherwise, both serve same function.

The two new protocols operations as defined in SNMPv2 are GetBulk and Inform. The GetBulk operation provides efficient bulk retrieval for large blocks of data in multiple rows of a table, allowing the NMS to retrieve as much data as possible in a single operation. The amount of data being retrieved is dependent on the size of a response message. In SNMPv2, the agent responding to GetBulk operations will provide partial retrieval even if some of the variables in a list are not successfully found and retrieved. The other new protocol operation is the Inform operation; it allows trap information to be communicated between two NMSs [16].

3. SNMPv3 Protocol Operations

Due to the modular nature of SNMP, SNMPv3 is designed to be backward compatible with SNMP versions 1 and 2. SNMPv3 is essentially, SNMPv2 with the addition of three important security features: access control, authentication, and encryption, along with other enhancements. Thus, SNMPv3 is based upon the protocol operations and data types from SNMPv2.

Two key significant additions provided by SNMPv3 are the User-based Security Model (USM) and View-based Access Control Model (VACM). The USM of SNMPv3 defines mechanisms for providing authentication and privacy for message-level security in SNMP implementations. The VACM of SNMPv3 defines mechanisms for providing access control facility for providing different levels of access control (read, write, notify) to each piece of management information for different users [1].

H. SNMPV1 MESSAGE FORMATS

The SNMPv1 messages, defined in ASN.1 format, are organized into two main parts, a message header and a protocol data unit (PDU). Figure 6 illustrates the basic format of a SNMPv1 message. The message header contains a *version* and a *community name*. The PDU contains the actual SNMP PDU. It specifies one of the SNMPv1 protocol operations ("Get," "Set," and etc.) and the object instances involved in the operation [16,17].

Figure 6 SNMPv1 Message Format (From Ref. [16].)

1. SNMPv1 Message Header

There are two fields in the SNMPv1 message header, Version Number and Community Name. The version field is used for SNMP compatibility. This is to ensure that the software used by all NEs is of the same SNMP version. The community name is used as a weak form of authentication because devices that do not know the valid community strings will ignore the SNMP request. Therefore, a predefined set of NMSs having the same community name are said to exist within the same administrative domain [17].

2. SNMP Protocol Data Unit

SNMPv1 PDUs contain information such as the type of SNMPv1 protocols operations ("Get", "Set", and etc.), message sequencing, error status and condition, and object instances involved in the operation. The length of SNMPv1 PDU field is dependent on the list of object instances specified; hence its length is variable. Figure 7 illustrates the fields of the SNMPv1 Get, GetNext, Response, and Set PDUs transactions and Table 2 below provides a summary of the descriptions of the fields [16].

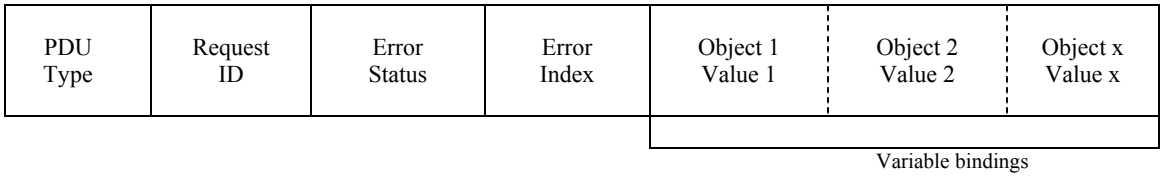


Figure 7 SNMPv1 Get, GetNext, Response, and Set PDUs Contain the Same Fields (From Ref. [16].)

Field	Description
PDU type	Specifies the type of PDU transmitted.
Request ID	Associates SNMP requests with responses.
Error status	Indicates one of a number of errors and error types. Only the response operation sets this field. Other operations set this field to zero. In SNMPv2 and SNMPv3 GetBulk operations, this field becomes a Non-Repeaters field.
Error index	Associates an error with a particular object instance. Only the response operation sets this field. Other operations set this field to zero. In SNMPv2 and SNMPv3 GetBulk operations, this field becomes a Max Repetitions field.
Variable bindings	Serves as the data field of the SNMP PDU. Each variable binding associates a particular object instance with its current value.

Table 2 Summary of SNMPv1 Get, GetNext, Response, and Set PDUs fields description (After Ref. [16].)

3. Trap PDU Format

Figure 8 illustrates the fields of the SNMPv1 Trap PDU and Table 3 below provides a summary of the descriptions of the fields.

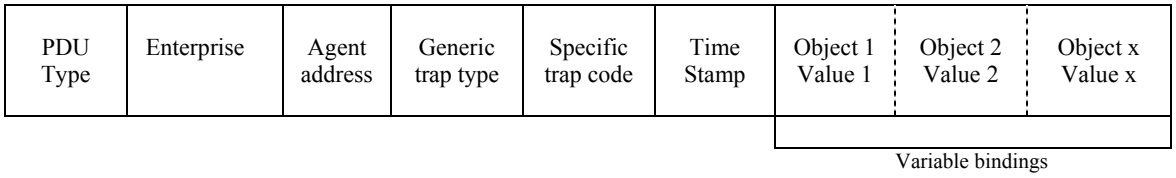


Figure 8 SNMPv1 Trap PDU (After Ref. [16].)

Field	Description
Enterprise	Identifies the type of managed object generating the trap.
Agent address	Provides the address of the managed object generating the trap
Generic trap type	Indicates one of a number of generic trap types.
Specific trap code	Indicates one of a number of specific trap codes.
Time stamp	Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.
Variable bindings	The data field of the SNMPv1 Trap PDU. Each variable binding associates a particular object instance with its current value.

Table 3 Summary of SNMPv1 Trap PDU fields description (After Ref. [16].)

I. SNMPV2 MESSAGE FORMAT

SNMPv2 messages, defined in ASN.1 format, are virtually identical to that of SNMPv1 messages (see the previous description of an SNMP PDU for differences). Depending on the SNMP protocol operation, the SNMPv2 PDU formats may differ. SNMPv2 PDU fields are also variable in length [16,17].

Figure 9 illustrates the fields of the SNMPv2 Get, GetNext, Inform, Response, Set, and Trap PDUs. The fields descriptions illustrated in Figure 9 are identical to that of a SNMPv1 Get, GetNext, Response, and Set PDUs.

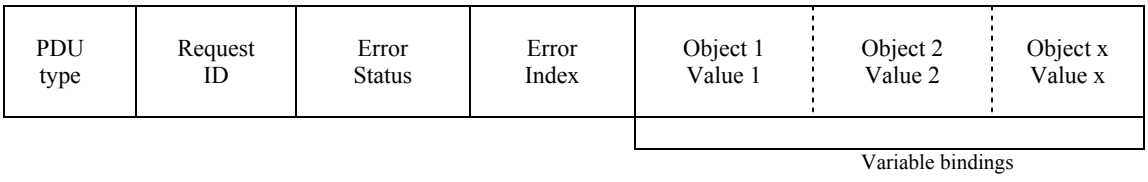


Figure 9 SNMPv2 Get, GetNext, Inform, Response, Set, and Trap PDUs Contain the Same Fields (From Ref. [16].)

Figure 10 illustrates the fields of the SNMPv2 GetBulk PDU. Within this PDU, the fields Non repeaters and Max repetitions replace the Error status and Error index fields shown in Figure 7. The GetBulk operation uses the Non repeaters and Max repetitions fields to specify how much information is retrieved. Non repeaters specify the number of object instances in the variable bindings field that should be retrieved once (typically for scalar objects with only one variable) from the beginning of the request. Max repetitions define the maximum number of times that other variables, other than those specified by the Non repeaters field should be retrieved [16].

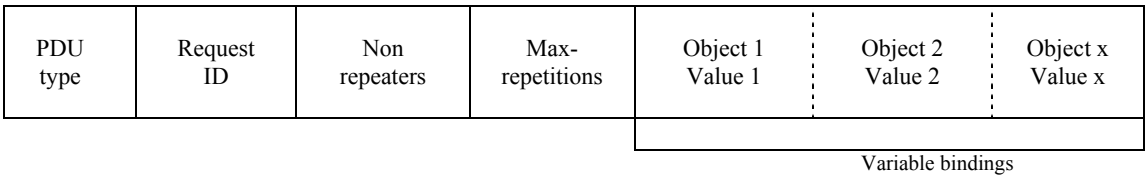


Figure 10 SNMPv2 GetBulk PDU (After Ref. [16].)

J. SNMPV3 MESSAGE FORMAT

Like SNMPv2 messages, SNMPv3 messages (shown in Figure 11) contain two parts. The second part of the SNMPv3 message (the PDU) is identical to that of a SNMPv2 message. The main difference between SNMPv2 and SNMPv3 is on the first part of the SNMPv3 message.

Figure 11 SNMPv3 Message Format (From Ref. [17].)

The wrapper forms the first part of a SNMPv3 message. It contains authentication and privacy information that are defined in the destination and source parties (see Section F for more detailed explanation about a party). In addition to a destination and a source party, a context, which specifies the managed objects involve in an operation, is defined in the wrapper [17].

The authentication protocol is designed to ensure that a received message was, in fact, transmitted by the originating SNMPv3 party. It consists of authentication information required to support the authentication protocol used. The privacy protocol is designed to prevent eavesdropping by unauthorized users. In order for the message to be protected from disclosure, the message must also be authenticated [17].

There are two primary security protocols that are defined in the SNMPv3 specifications, the Digest Authentication Protocol, designed for authentication purposes, and the Symmetric Privacy Protocol, designed to ensure message privacy [17].

The Digest Authentication Protocol verifies that the message received is, in fact, from the original sender. This is to ensure data integrity and prevents masquerading. A 128-bit message digest is calculated using the Message Digest 5 (MD5) algorithm at the sender to protect data integrity. The algorithm produces an authentication value and encloses it within the SNMPv3 message. The receiver applies the same MD5 algorithm and verifies the digest. After the message integrity is verified, a secret key known only to the sender and the receiver and prefixed to the message is used to verify the message's origin [17].

The Symmetric Privacy Protocol is used to ensure message privacy by encrypting the message with Data Encryption Standard (DES) algorithm. When this encrypted message is sent or received, both the sender and receiver of the message must have the same secret encryption key, known only to both of them. [17]. This is to prevent eavesdropping and ensure privacy of management information.

K. SUMMARY

This chapter provided a brief overview of the key concepts of SNMP. This included the key components of SNMP, the information model used in SNMP, and SNMP data representation. It also presented the evolution and features of the three different versions of SNMP. In addition, it also covered the SNMP protocol operations in each SNMP versions, as well as each message format.

In the next chapter, traffic analysis is performed on real, operational SNMP traffic and statistics are developed from the SNMP traffic.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TRAFFIC ANALYSIS OF SNMP TRAFFIC

A. CHAPTER OVERVIEW

This chapter presents traffic analysis performed on SNMP traffic collected by the Naval Postgraduate School (NPS) Network Operations Center (NOC). This analysis was necessary in understanding the traffic parameters, such as polling interval, request inter-arrival time, request packet size, etc., of actual SNMP traffic. From this traffic analysis, statistics for the packet size and inter-arrival time of the Get request and the Get response messages with respect to a NMS and an agent are developed.

B. INTRODUCTION

The objective of this traffic analysis is to determine the packet size of each request/response, number of packets per request/response, request/response inter-arrival times and polling interval. With the understanding of the SNMP traffic, statistics were developed and these statistics were used to specify a SNMPv1 definition in OPNET. Subsequently, the SNMPv1 definition was integrated into an OPNET network model to study the scalability issues of SNMP-based polling in an optical network.

C. TRAFFIC MEASUREMENTS

The measurement of the SNMP traffic was collected from NPS campus network via the NOC. The measured SNMP traffic was the management data that is used to monitor the network status of infrastructure devices throughput the NPS campus. In this traffic analysis, the SNMP traffic was captured using Etherpeek (packet sniffer). From the SNMP message header, the SNMP version could be determined and it was found that the measured SNMP traffic was SNMPv1. Based on the measured SNMP traffic, it was found that the SNMP polling interval for the collection of the management data statistics was approximately five seconds. The SNMP protocol operations in the measured SNMP traffic consist of SNMPv1 Get and Trap messages. As observed from the measured SNMP traffic, SNMP-defined traps are significantly less frequent compared to the SNMP Get request-responses. Furthermore, proprietary traps frequently are not understood by

network management stations from other vendors. Thus, virtually all required information that is needed by the management station is gathered by polling (Get Request). In this study, we only looked at the Get messages. Figure 12 shows the screen shot of an Etherpeek capture of a typical SNMP Get request packet behavior between NMS and agent. Initially, fifteen thousand packets of traffic were captured. However, in this study, we were only interested in the SNMP traffic originating from the NMS, i.e., Get request, and the SNMP traffic originating from a frequently polled agent, i.e., Get response. Therefore, after filtering those traffic sources irrelevant to our study, approximately eight thousand packets were left. This traffic sample size was still considered large enough to perform a rough but meaningful statistical traffic analysis. These results were later compared with a four-hour study and found to be consistent. There were a total of 29 different agents, i.e., the NMS was monitoring 29 different NEs. However, in this study, we only performed analysis on the SNMP traffic between the NMS and the frequently polled agent.

A	B	C	D	E	F	G	H
Packet	Source	Destination	Size	Delta Time	Relative Time	Protocol	Summary
1	IP-131.120.33.37	IP-131.120.0.1	88		0	SNMP	Src= 1093,Dst= 161 ,L= 42
2	IP-131.120.33.37	IP-131.120.0.1	88	0.000682	0.000682	SNMP	Src= 1093,Dst= 161 ,L= 42
3	IP-131.120.33.37	IP-131.120.248.1	88	0.000712	0.001394	SNMP	Src= 1093,Dst= 161 ,L= 42
4	IP-131.120.33.37	IP-131.120.248.1	88	0.000764	0.002158	SNMP	Src= 1093,Dst= 161 ,L= 42
5	IP-131.120.33.37	IP-140.32.132.65	89	0.000701	0.002859	SNMP	Src= 1093,Dst= 161 ,L= 43
6	IP-131.120.33.37	IP-140.32.132.65	89	0.000535	0.003394	SNMP	Src= 1093,Dst= 161 ,L= 43
7	IP-131.120.0.1	IP-131.120.33.37	92	0.001339	0.004733	SNMP	Src= 161,Dst= 1093 ,L= 46
8	IP-140.32.132.65	IP-131.120.33.37	93	0.001598	0.006331	SNMP	Src= 161,Dst= 1093 ,L= 47
9	IP-131.120.0.1	IP-131.120.33.37	93	0.0005	0.006831	SNMP	Src= 161,Dst= 1093 ,L= 47
10	IP-131.120.248.1	IP-131.120.33.37	93	0.00213	0.008961	SNMP	Src= 161,Dst= 1093 ,L= 47

Figure 12 Screen shot of an Etherpeek capture showing a typical SNMP Get request packet between NMS and agent.

D. TRAFFIC ANALYSES AND RESULTS

Analyses were performed separately on the filtered SNMP traffic: one for the Get request from the NMS to the agent and the other for the Get response from agent to NMS. Various statistics, including maximum, minimum, mean and variance of packet sizes, and request and response inter-arrival times, were collected. Table 4 shows the statistics associated with the filtered SNMP traffic.

1. Packet Sizes of SNMP Traffic

From the filtered SNMP traffic data, the statistics of the packet sizes of Get request and Get response with respect to the NMS and the agent were computed (see Table 4). Based on the measured SNMP traffic, it was observed that one packet is sent for every Get request or Get response message. Each Get request packet size was almost the same, approximately 88 bytes. However, based on the measured SNMP traffic, it was observed that each Get response packet size varied and was dependent on the type of NE that the NMS was managing as well as the MIB that was being requested by the NMS. As a result, there was a large variance in the Get response packet sizes as compared to the Get request packet sizes. Hence, based on the measured SNMP traffic, the average Get request and Get response packet size was approximately 88 bytes and 93 bytes respectively.

	Average (bytes)	Variance (bytes)	Minimum (bytes)	Maximum (bytes)
Get request	88.73	0.4186	86	89
Get response	93.48	37.74	86	206

Table 4 Statistics of Get request and Get response packet sizes from filtered SNMP traffic data

2. Inter-arrival Times of SNMP Traffic

From the filtered SNMP traffic data, the statistics of the Get request and Get response inter-arrival times with respect to the NMS and the agent were computed (see Table 5). To obtain more accurate statistics of the actual Get request inter-arrival times, analysis was also performed on the inter-arrival times from the original measured SNMP traffic, i.e. unfiltered, and the statistics were also computed (Table 5). Besides polling the most frequently polled agent, the NMS also polled the other agents. Consequently, the average Get request inter-arrival time obtained from the filtered SNMP traffic represents the time in between polls of a specific agent. As might be expected, this was higher than the Get request inter-arrival time obtained from the original measured SNMP traffic.

Hence, the average Get request inter-arrival times were 56 ms and 276 ms as obtained from the original measured SNMP traffic and the filtered SNMP traffic respectively.

The average Get response inter-arrival time was 210 μs. This represents the time it took an agent to respond to a Get request.

	Average (s)	Variance (s)	Minimum (s)	Maximum (s)
Get request (filtered)	0.276	2.64	0.733×10^{-3}	26.0007
Get request (unfiltered)	0.056	0.1024	0.468×10^{-3}	4.62
Get response (filtered)	0.21×10^{-3}	10.34×10^{-9}	0.077×10^{-3}	2.25×10^{-3}

Table 5 Statistics of Get request/response inter-arrival times

E. CONCLUSIONS

Based on the above traffic analysis, the measured SNMP traffic has an average Get request packet size of 88 and Get response packet size of 93. The average Get request inter-arrival time was 56 ms from the original measured SNMP traffic and average Get response inter-arrival time was 210 μs, with a polling interval of 5 s. We used these statistics to model the SNMP traffic in OPNET and subsequently evaluated how well SNMP scales in an optical network.

In the next chapter, the modeling of SNMP, including the simulation module, simulation parameters and test scenarios used in the study are discussed. The simulation results obtained with respect to the scalability of SNMP in a typical optical network is also discussed.

VI MODELING OF SNMP USING OPNET

A. CHAPTER OVERVIEW

This chapter describes the modeling of SNMP, including the simulation module, simulation parameters and test scenarios used in the study. The test scenarios explored the effect of varying the number of nodes and the request inter-arrival times and determine the optimum number of nodes to be managed for a specified polling interval. It also discusses the simulation results obtained with respect to the scalability of SNMP in a typical optical network.

B. SIMULATION MODULE

In this study, OPNET IT Guru 10.0 [18] was used as a modeling and simulation tool to analyze the performance of SNMP behavior in an optical network. OPNET is a modeling and simulation tool that provides an environment for analysis of communication networks. However, OPNET does not have a SNMP model in its standard model library. Therefore, in order to represent and study the behavior of SNMP traffic in the network management system, a simulation module called SNMP Module was developed. The most commonly used version of SNMP is version 1 (SNMPv1); therefore, in this study SNMPv1 was modeled in OPNET. With information regarding SNMP fundamentals and concepts, as well as the statistics obtained from the traffic analysis, the SNMPv1 model can be defined and developed using the custom application model. Hence, a representation of the expected behavior of the SNMPv1 NMS-agent relationship was created in OPNET and integrated into an OPNET network model to study scalability issues of SNMP-based polling.

C. SIMULATION PARAMETERS

The network configuration for this study consists of a NMS, a router and a node, where the agent resides (Figure 13). The data rate of the duplex link connecting these NEs is 768 kbps (simulating the data rate of DCC in the SONET frame, see Chapter II, Section C). As explained in Chapter II Section C, the DCC carries only the management

data traffic. As such the communication between NMS and the agent is for network management purpose only (i.e., SNMP traffic only).

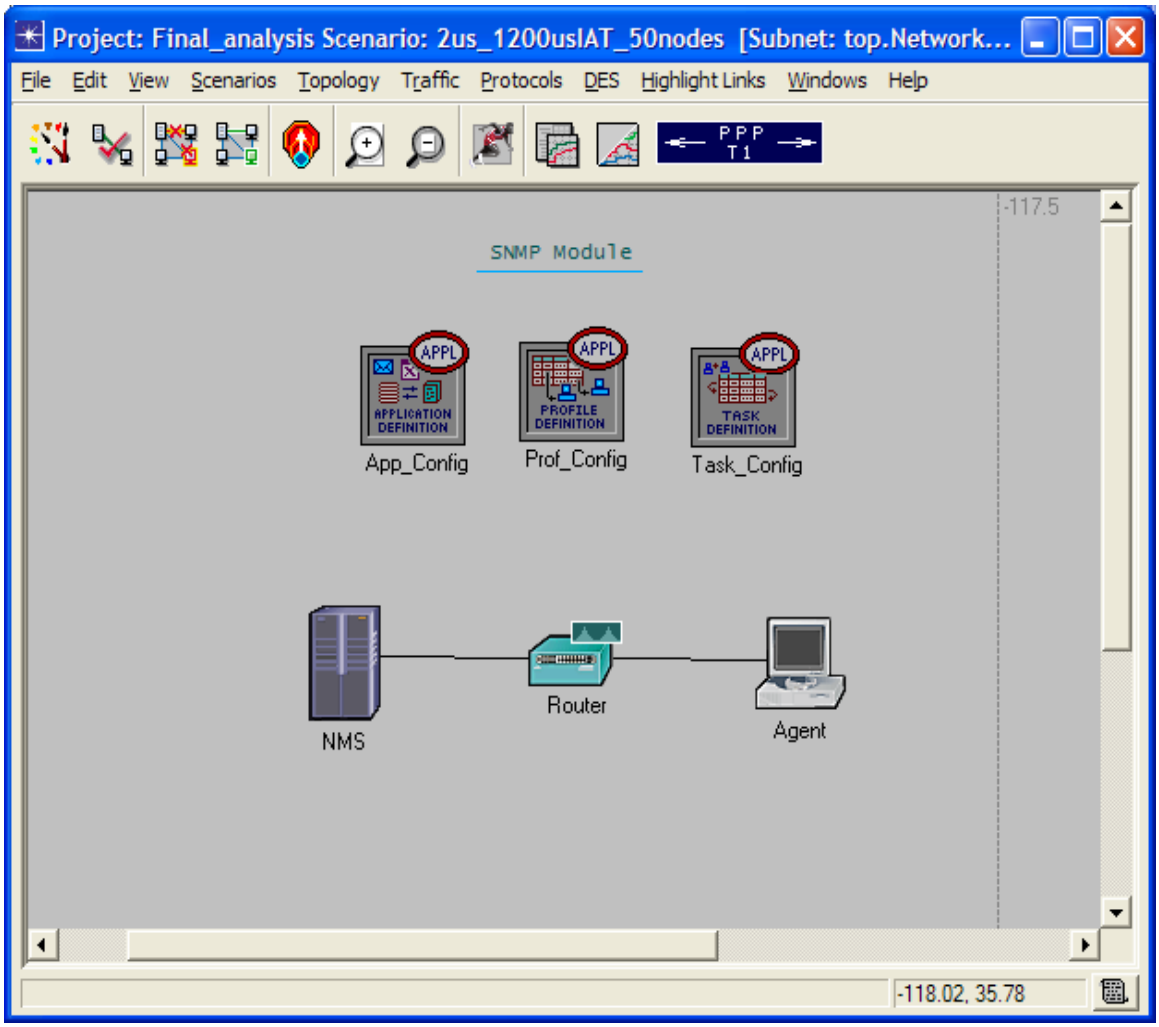


Figure 13 The SNMP Module as modeled in OPNET

The SNMP traffic characteristics can be modeled by defining the following attributes (Table 6) into the Application, Profile and Task configuration of the OPNET custom application.

Attribute	Value	Object
Link rate	768 kbps	Link
Transport Protocol	UDP	App Config
Request packet size (bytes)	scripted	Task Config
Request inter-arrival time	varies	Profile Config
Number of nodes	varies	Profile Config

Table 6 Attributes set in the SNMP application

SNMPv1 was modeled as a custom application in OPNET and was defined in the 'App_Config' object in OPNET, whereby the transport protocol is also defined, i.e., UDP. The modeling of the custom application is broken down into task and phase under the 'Task_Config' object in OPNET. The task will be the SNMPv1 Get operation and the phase will be the Get request that is sent from the NMS to the agent. The Get request traffic parameters are set in the traffic attribute under the phase in the 'Task Config' object (see Figure 14). As discussed earlier in Chapter V (traffic analysis), there is only one packet sent per Get request. Since the pre-defined distributions in OPNET for the request packet size in bytes do not fit into our modeling requirements, a "scripted file" was created. The "scripted file" was generated by entering all request packet sizes, as obtained from the measured SNMP traffic, on each line (representing an outcome for a particular attribute) of the text editor. Once this file is created, it must be saved under the ".csv" or ".gdf" extension so that the data can be read and replayed line by line. In this study, the "scripted" filename for the request packet size was "NMS181Req_pktsize_dist.csv".

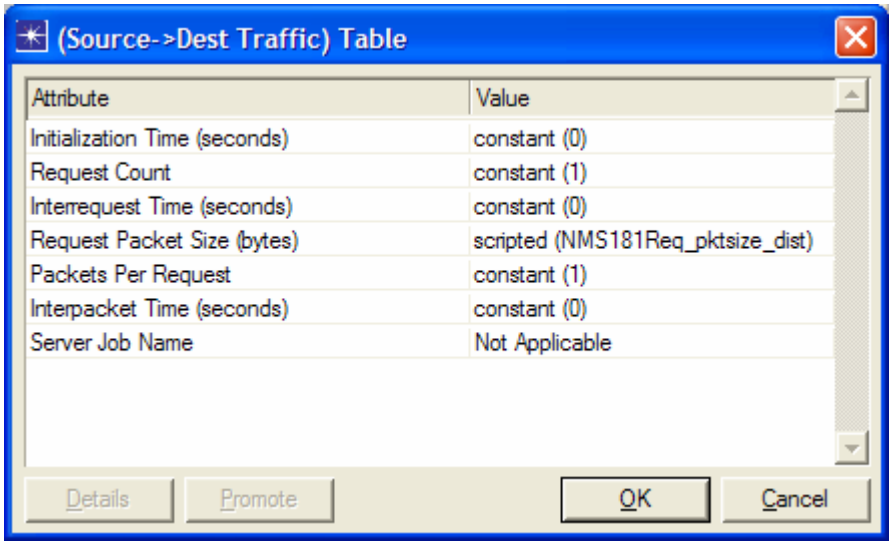


Figure 14 Definition of Get request traffic parameters in 'Task Config' object

The Get request inter-arrival time and the number of nodes are defined under the 'inter-repetition time' and 'number of repetitions' attributes, respectively (Figure 15), under the 'Profile Config' object in OPNET. As for setting the required number of nodes, for example, to poll 50 nodes, the number of repetitions is set to 49.

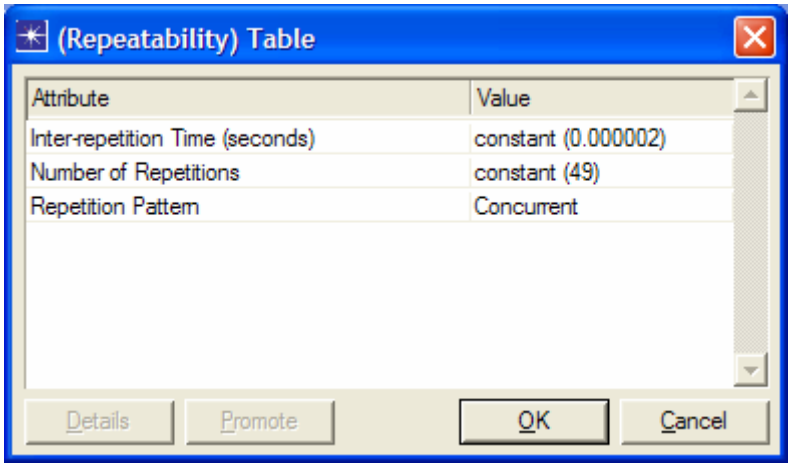


Figure 15 Definition of Get request inter-arrival time and number of nodes parameters in 'Profile Config' object

The start time of the first SNMP Get request is set at 30 s. This is to allow sufficient time to elapse for dynamic routing protocol to build the routing table. This is defined in the 'Start Time Offset' under the applications in the 'Profile Config' object (Figure 16).

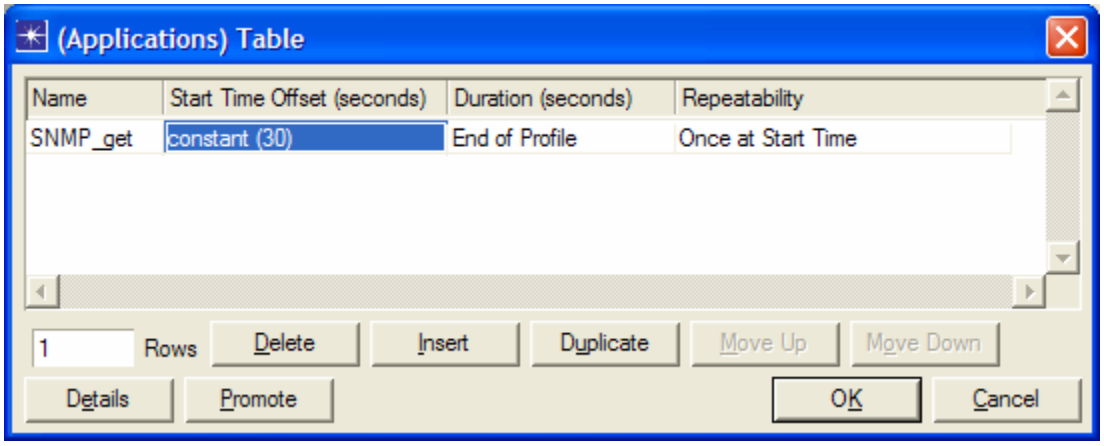


Figure 16 Definition of SNMP Get request start time in 'Profile Config' object

With the above attributes set, the SNMP behavior can be simulated using OPNET. Different SNMPv1 network management test scenarios can be generated by varying the Get request inter-arrival time and number of nodes to be managed.

The simulation technique that is used in this study is called the Discrete-event simulation (DES). DES models a system dynamically and each packet data transfer is modeled as a discrete event. It enables the simulation of the specific application transactions, reproduces the exact network as well as the detailed protocol behavior. Hence, it allows the evaluation of the network and application characteristics and studies the various sources of delay that could be experience in the actual production network. Accurate results can be obtained from this technique but it is time consuming and a large memory will be required [19]. In this study, the number of nodes required for simulation can approach tens of thousands; therefore it is impractical to physically create that large number of nodes in the network configuration as shown in Figure 13. To simplify the modeling and reduce the simulation run-times, the number of nodes was simulated by sending mul-

tiple Get requests to a single node (Figure 13) rather than sending each request to the actual number of nodes.

D. TEST SCENARIOS

In order to check the scalability issues of SNMP polling, various test scenarios are created by varying the number of nodes and the request inter-arrival times. All test scenarios were performed using the network configuration as in Figure 13. The objective of each test scenario was to evaluate the performance metrics, such as link throughput, link utilization, and queuing delay, collected after the simulation.

These performance metrics were studied because throughput provides a good measure for projected demand and potential performance-related problems. On the other hand, utilization indicates the percentage of loading on the link capacity over a specified period of time. Link utilization is defined as the ratio of link throughput over link data rate. When fine granularity is required, utilization will be studied instead of throughput.

Utilization is an important performance metric because it is closely related to network congestion and response time. Typically, utilization is a good indication for potential bottlenecks and area of congestion. In addition, when the utilization increases, the response time will usually increase exponentially. Due to this exponential behavior, it is important to determine potential network congestion before it gets out of control [20]. Similarly, queuing delay also provides a good indication of potential bottlenecks and area of congestion.

E. DISCUSSION OF SIMULATION RESULTS

The test scenarios vary the number of nodes and the request inter-arrival time, and determine the optimum number of nodes for a given polling interval (Figure 17). The performance metrics studied were the link utilization, link throughput and queuing delay.

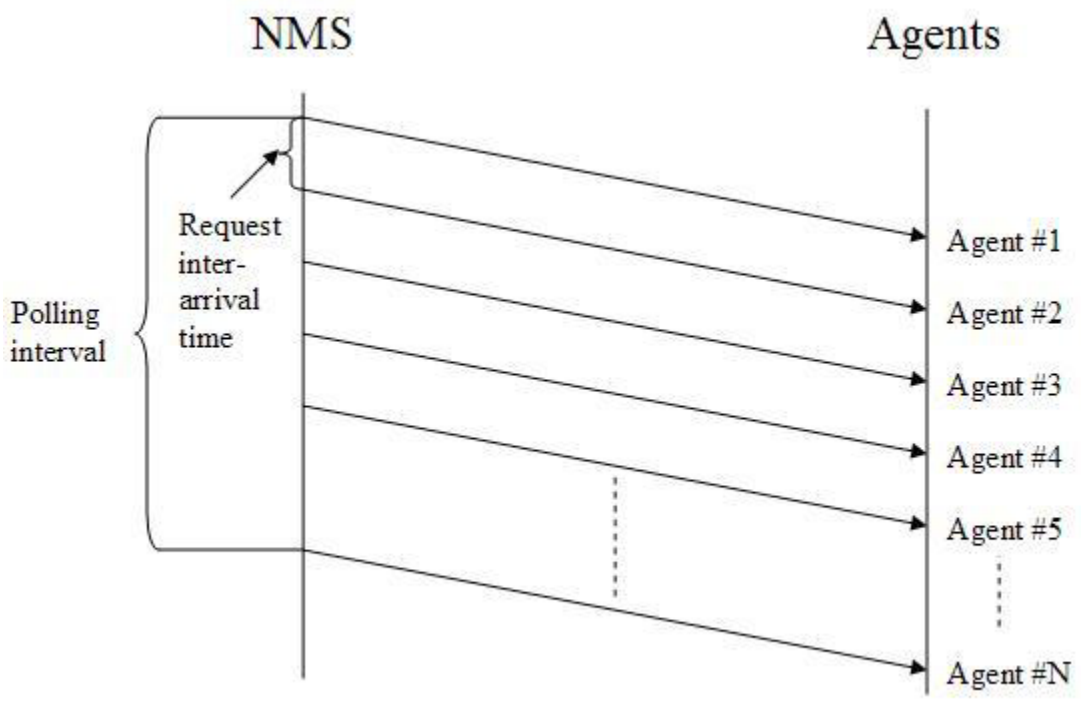


Figure 17 SNMP polling showing polling interval, request inter-arrival time and number of agents

1. Effect of Varying the Number of Nodes

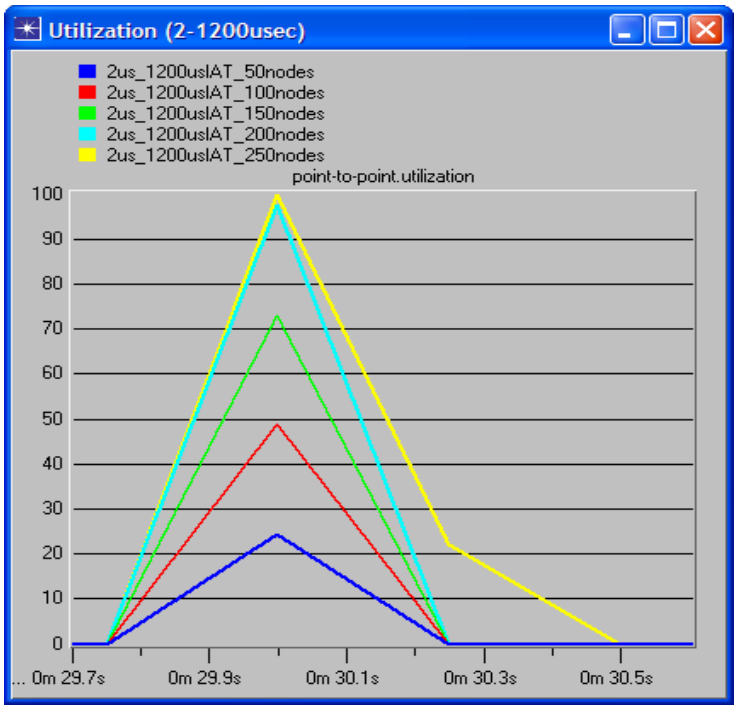
This experiment was designed to explore the effects of varying the number of nodes for a given request inter-arrival time. The request inter-arrival time that is used in each scenario and the corresponding figures depicting results for each run of the experiment are outlined in Table 7.

Test scenarios no.	Request inter-arrival time (μs)	Figures depicting results
1	2–1200	18(a) & (b)
2	2000	19(a) & (b)
3	3000	20(a) & (b)
4	4000	21(a) & (b)
5	5000	22(a) & (b)

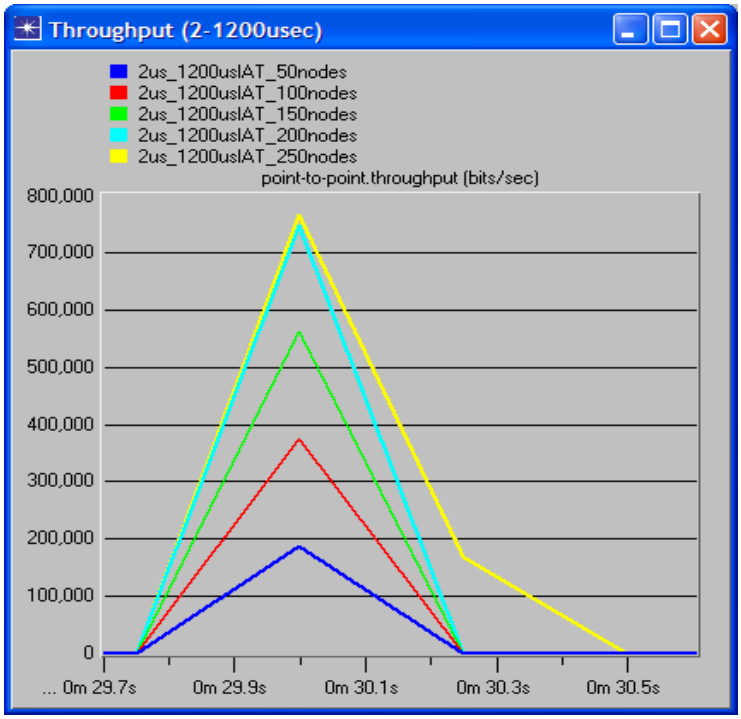
Table 7 The request inter-arrival time used to study the effect of varying the number of nodes

Figures 18 to 22 show the link utilization and link throughput respectively obtained due to the effect of varying the number of nodes to be managed by NMS at a given request inter-arrival time. Each figure consists of a pair of graphs. The first graph shows the plot of link utilization against time taken to poll the specific number of nodes; the second graph shows the plot of link throughput against time taken to poll the specific number of nodes. When the link utilization is more than 80% or the link throughput is more than 80% of the link rate, (as mentioned in Chapter VI, Section C, link rate is 768 kbps, i.e., the theoretical maximum), processing bottlenecks and network congestion will likely occur. The link utilization and link throughput is measured on the link between the NMS and router. The link utilization and link throughput results obtained from the five different test scenarios are tabulated in Table 8 and 9. From numerous simulations, it is found that for a given number of nodes and for any request inter-arrival times of between 2 μs and 1200 μs, the link utilization and link throughput shows identical results. As such, analysis of request inter-arrival time of between 2 μs and 1200 μs is considered together. It is observed that all plots start at approximately 30 s, this is expected as the start time of the first Get request begins only 30 s after the simulation starts (as explained earlier in Section C of this chapter).

In general, link utilization and link throughput increase with an increase in the number of nodes at a given request inter-arrival time. The experiment results are as expected, given that with more nodes to be managed more packets will be sent. Comparing the results obtained for the five different test scenarios, it is observed the link utilization will only reach 100% or link throughput will equal link data rate if the request inter-arrival time is between 2 μs and 1200 μs. This will mean that if the request inter-arrival time is between 2 μs and 1200 μs, the DCC will likely experience bottleneck or network congestion if the NMS is to manage 200 or more nodes. This will likely affect the proper operation of network management function of the NMS.

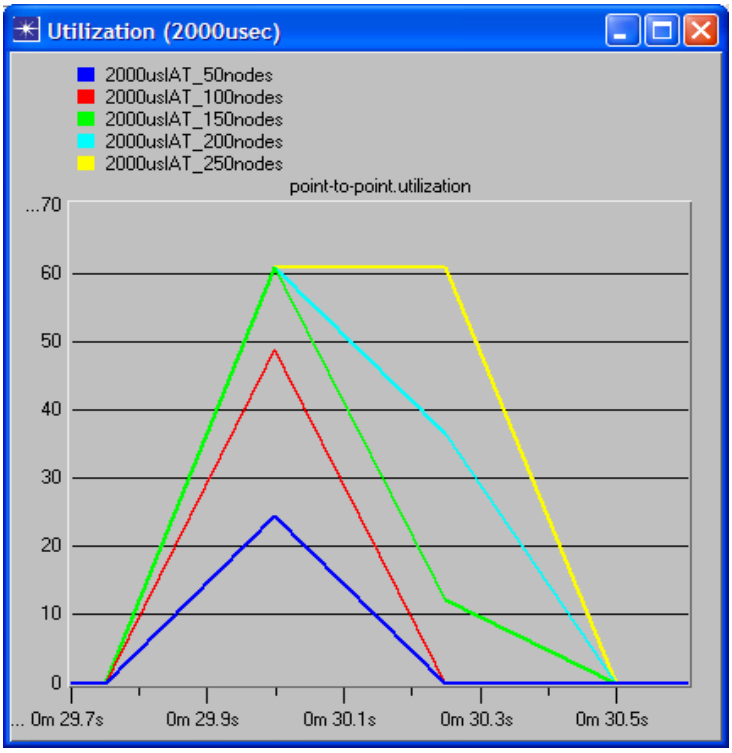


(a)

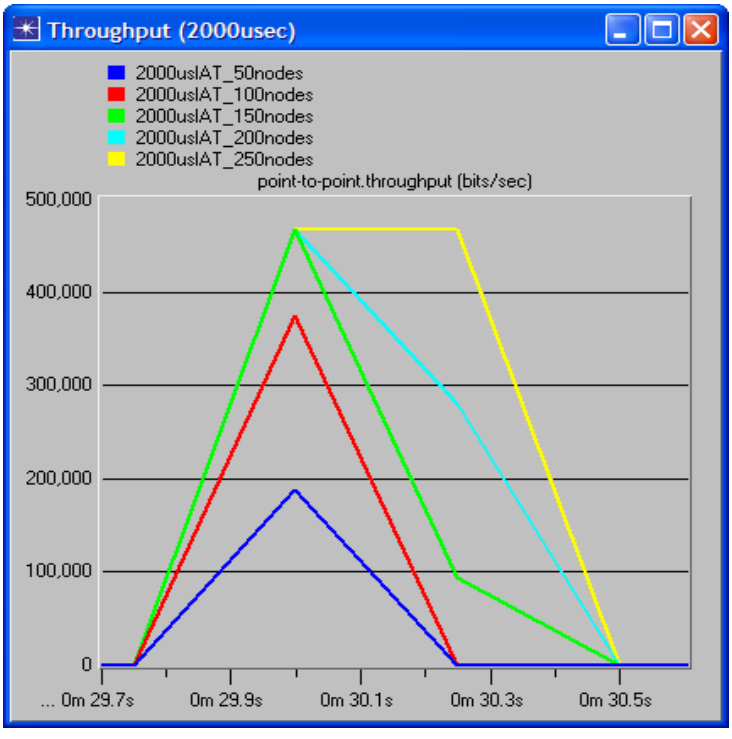


(b)

Figure 18 Screen shot of (a) link utilization and (b) link throughput depicting the effect of varying the number of nodes for any request inter-arrival times of between 2 μs to 1200 μs.

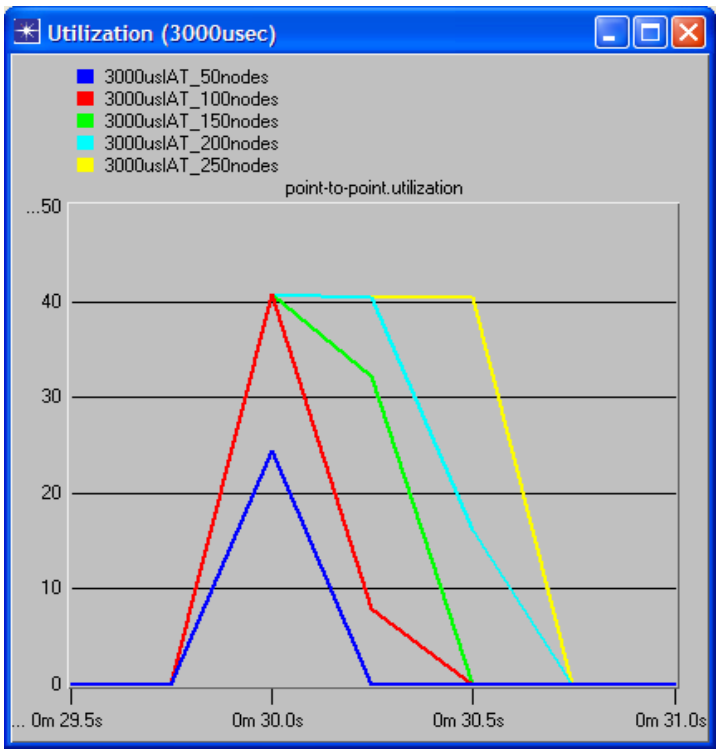


(a)

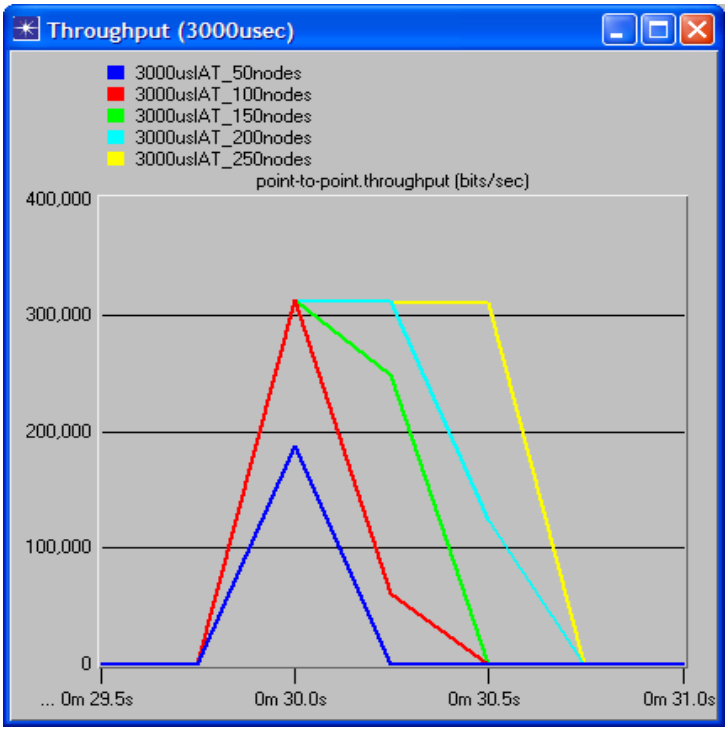


(b)

Figure 19 Screen shot of (a) link utilization and (b) link throughput depicting the effect of varying the number of nodes for request inter-arrival times of 2000 µs.

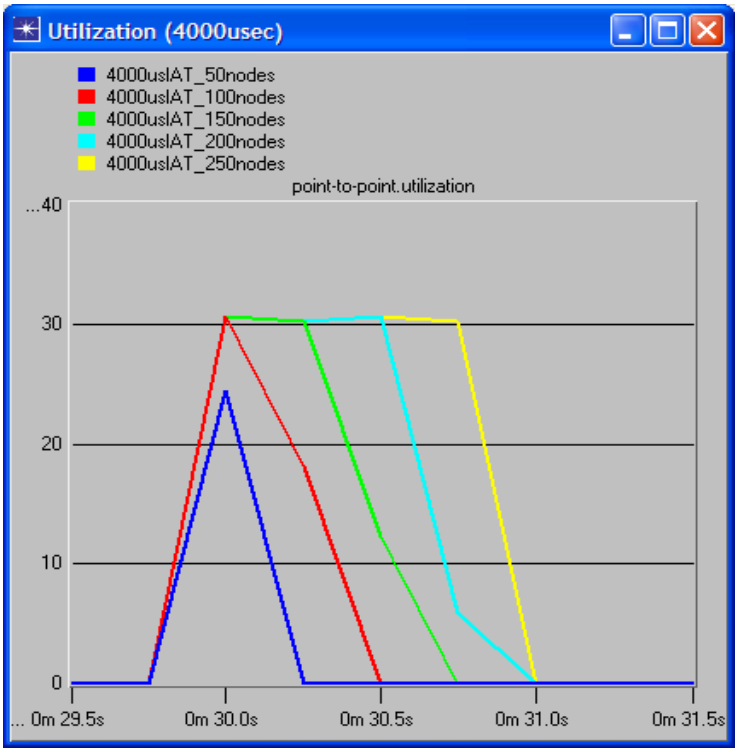


(a)

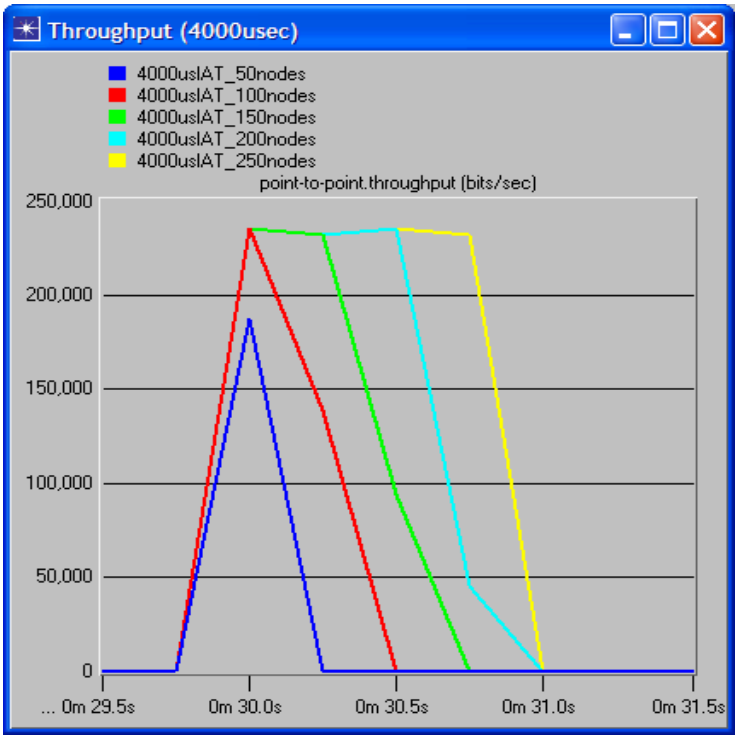


(b)

Figure 20 Screen shot of (a) link utilization and (b) link throughput depicting the effect of varying the number of nodes for request inter-arrival times of 3000 μs.

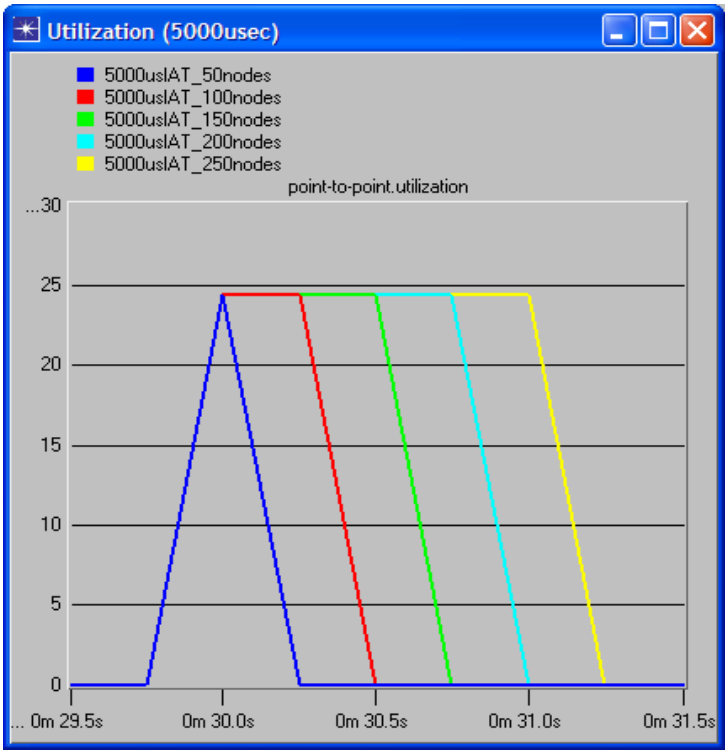


(a)

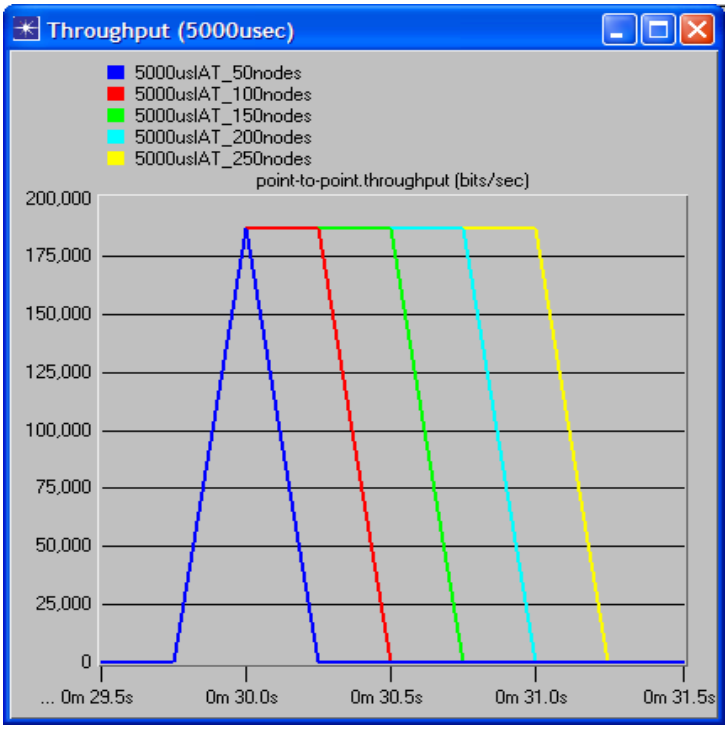


(b)

Figure 21 Screen shot of (a) link utilization and (b) link throughput depicting the effect of varying the number of nodes for request inter-arrival times of 4000 μs.



(a)



(b)

Figure 22 Screen shot of (a) link utilization and (b) link throughput depicting the effect of varying the number of nodes for request inter-arrival times of 5000 μs.

No. of Nodes	Link Utilization (%) for different request inter-arrival time				
	2–1200 µs	2000 µs	3000 µs	4000 µs	5000 µs
50	24.38	24.38	24.38	24.38	24.38
100	48.75	48.75	40.85	30.71	24.38
150	73.13	60.94	40.85	30.71	24.38
200	97.50	60.94	40.85	30.71	24.38
250	100	60.94	40.85	30.71	24.38

Table 8 Link utilization due to the effect of varying the number of nodes to be managed at a given request inter-arrival times

No. of Nodes	Link Throughput (kbps) for different request inter-arrival time				
	2–1200 µs	2000 µs	3000 µs	4000 µs	5000 µs
50	187.2	187.2	187.2	187.2	187.2
100	374.4	374.4	313.8	235.9	187.2
150	561.6	468	313.8	235.9	187.2
200	748.8	468	313.8	235.9	187.2
250	768	468	313.8	235.9	187.2

Table 9 Link throughput due to the effect of varying the number of nodes to be managed at a given request inter-arrival times

The corresponding queuing delay is shown in Figure 23. This figure shows that the queuing delay for 200 or more nodes is at least 121.5 ms and will increase with an increase in the number of nodes. This result is expected because the packets at the router will build up much more quickly when there are many packets being sent within a short inter-arrival time. In other words, for a request inter-arrival time of between 2 μs and 1200 μs, in order to avoid a bottleneck, it is necessary for the NMS to manage not more than 200 nodes.

Based on the link utilization or link throughput results, for request inter-arrival times of above 2000 μs, the link utilization is less than 50%. Hence, the number of nodes to be managed by the NMS will not be constrained by queuing delay or network congestion.

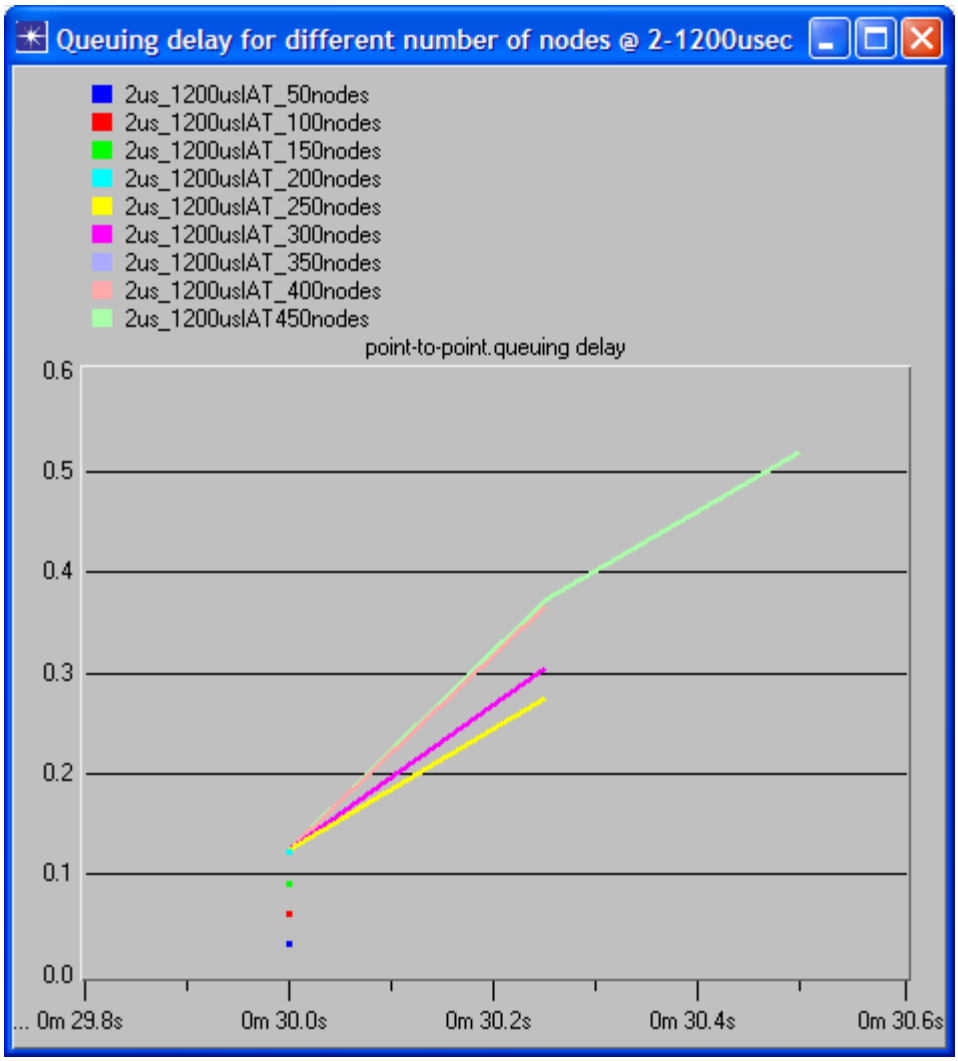


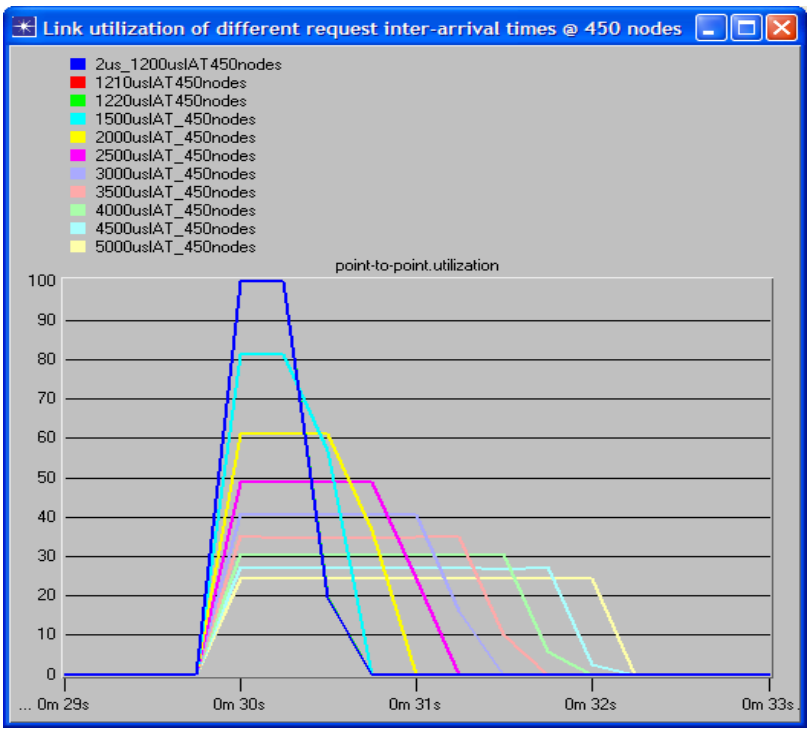
Figure 23 Screen shot of queuing delay depicting the effect of varying the number of nodes for any request inter-arrival times of between 2 µs to 1200 µs.

2. Variation of Request Inter-arrival Times

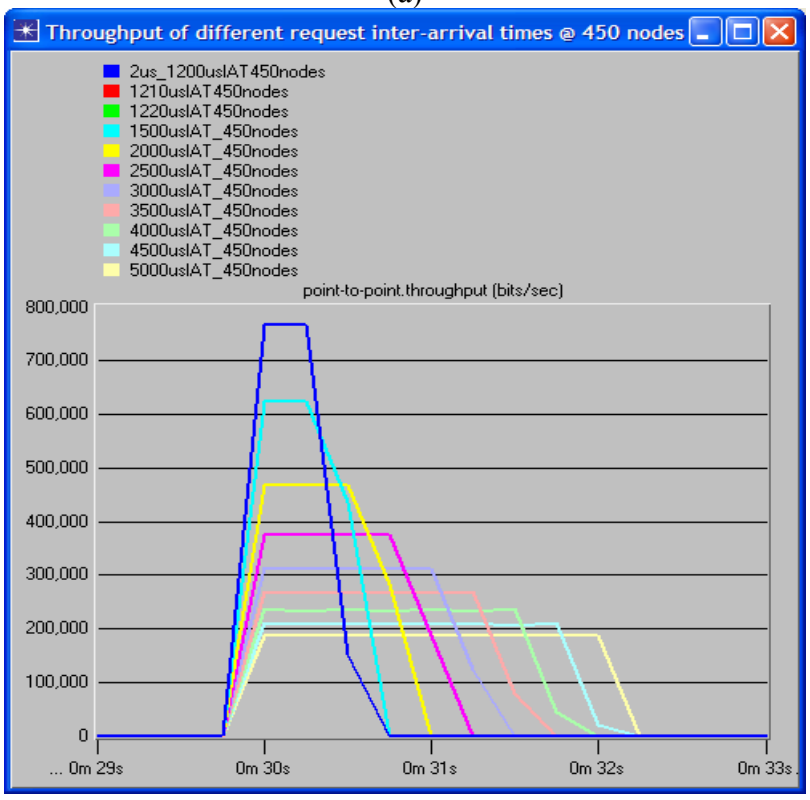
This experiment was designed to explore the effects of varying the request inter-arrival time (from 2 µs to 5000 µs) for a given number of nodes to be managed by the NMS. The assumption made in this experiment is that the minimum request inter-arrival time will not be less than 2 µs and the maximum request inter-arrival time will not exceed 5000 µs. In this experiment, we assume that 450 nodes are to be managed by the NMS.

Figures 24 (a) and (b) show the link utilization and link throughput respectively obtained due to the effect of varying the request inter-arrival time when 450 nodes are being managed by NMS. The link utilization and link throughput results obtained from this test scenario are tabulated in Table 10.

In general, to manage 450 nodes, link utilization decreases with an increase in the request inter-arrival time. The experimental results are as expected, given that with the higher request inter-arrival time, more time is given to the router to process each packet sent, hence the chance of bottleneck or network congestion is reduced. This can be seen in Table 10 where the link utilization is lower for request inter-arrival times of above $1220\,\mu s$ because the request inter-arrival time is large enough for the router to process the incoming packets before the queue build up. Based on numerous simulations, it was found that the link utilization and link throughput for the different request inter-arrival times as listed in Table 10 are the maximum achievable value. In addition, it can be seen from Table 8 and 9 that, in fact, this maximum value will be reached when the NMS is to manage 250 nodes. Table 10 shows that for a link utilization of less than 80%, it is better to use a request inter-arrival time of more than $1500\,\mu s$ in order to effectively manage 450 nodes.



(a)



(b)

Figure 24 Screen shot of (a) link utilization and (b) link throughput depicting the effect of varying the request inter-arrival times when managing 450 nodes.

Request inter-arrival times (μs)	Link Utilization (%)	Link Throughput (kbps)
2–1200	100	768
1210	100	768
1220	99.90	767.2
1500	81.32	624.5
2000	60.94	468
2500	48.75	374.4
3000	40.85	313.8
3500	35.10	269.6
4000	30.71	235.9
4500	27.30	209.7
5000	24.38	187.2

Table 10 Link utilization and throughput against different request inter-arrival times when managing 450 nodes.

Figure 25 shows for a request inter-arrival time of 1210 μs, with 450 nodes to be managed, the queuing delay is increasing at a much slower rate as compared to the queuing delay for any request inter-arrival times of between 2 μs to 1200 μs. However, for any request inter-arrival time of 1220 μs and above, the queuing delay is constant at 1.22 ms and is negligible. Therefore, for any request inter-arrival times of 1220 μs and above, the number of nodes that can be managed will only be limited by the polling interval instead of constrained by the bottleneck or congestion level in the network (this will be explained in more detail later). Since all plots for a request inter-arrival time of 1220 μs and above have the same queuing delay and the first poll starts at 30s for all simulations, plots

for request inter-arrival time of 1220 µs and above, depending on the inter-arrival time, will either fully or partially overlap the previous plot, as shown in Figure 25.

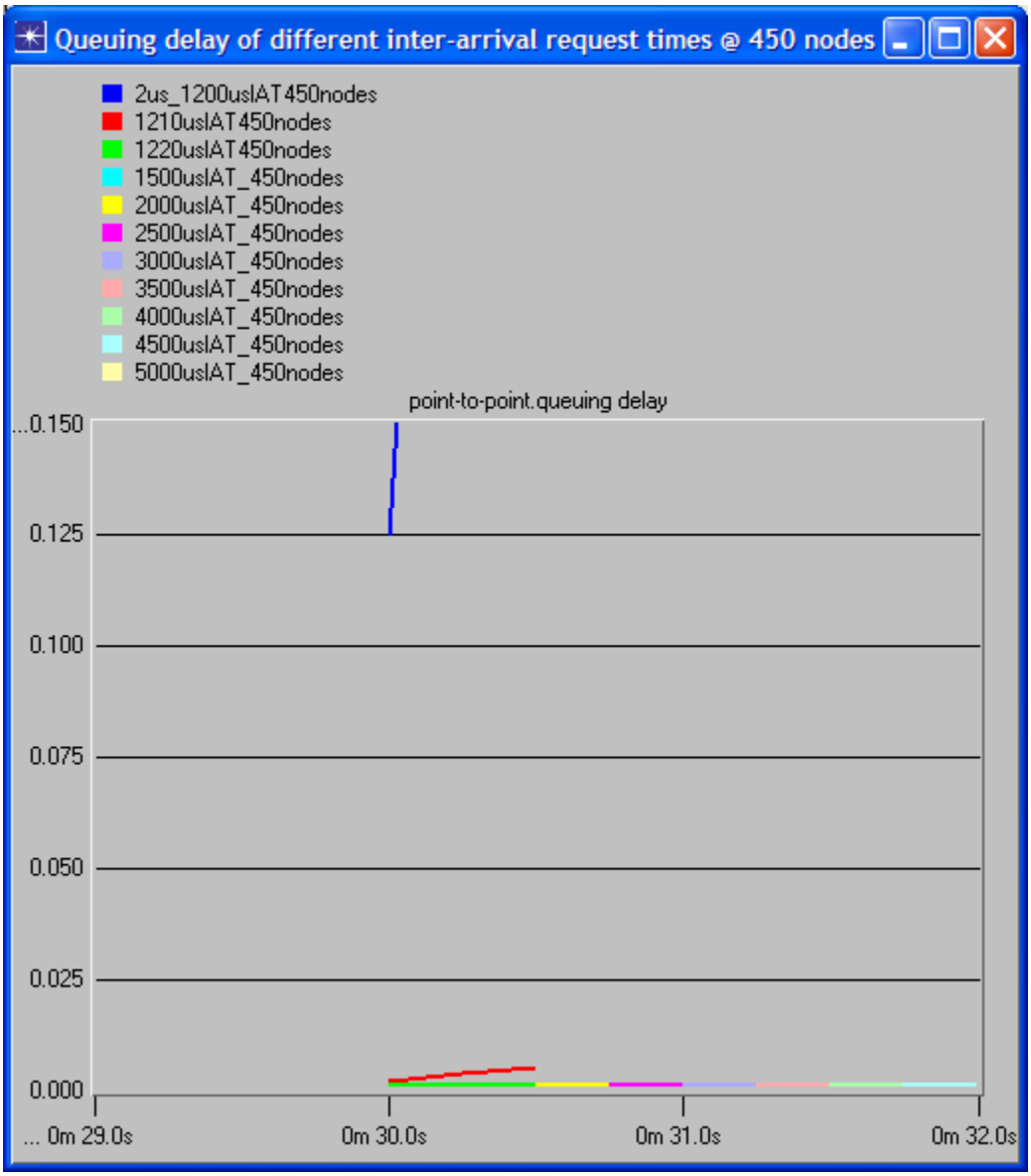


Figure 25 Screen shot of queuing delay depicting the effect of varying the request inter-arrival times when managing 450 nodes.

3. Polling Interval

The polling interval is an important parameter as it determines how often the management station will have an up-to-date view of the network. As such, some form of policy must be in place to determine the frequency with which the management station polls. Though performance is dependent on the processing power in the management station, level of congestion, and other performance-related factors, the main deciding factor on the specification of the polling interval is the size of the network. In other words, it is the number of agents that are to be effectively managed by the management station will directly affect the polling interval specified. In order to provide a quick indication on the maximum number of agents a network can support, some simple formulas must be created. This problem can be simplified by considering that only one agent can be managed by the management station at a time and the management station is engaged full-time in polling. The poll may involve either one or more Get transactions. Based on the above assumptions, the following equation is generated [20].

$$N \leq \frac{T}{\Delta} \tag{6.1}$$

where

N = Number of agents,

T = Polling interval, and

Δ = processing time to generate a request.

The above equation is a slight modification of a similar formula as specified in Reference [20]. In Reference [20], the author considers the processing time for both request and response; in our case, we only assume the processing time for the request, which is the request inter-arrival time.

Assuming a polling interval of 30 s and using the minimum request inter-arrival time of 733 μs (worst case) obtained from the traffic analysis, the theoretical maximum number of agents that the NMS can manage is $N \leq 41{,}000$. Hence, as discussed in the

Sub-section 1 of this section (effect of variation of number of nodes), for a request inter-arrival time of 733 μs, the number of nodes that the NMS can effectively manage should not exceed 200 nodes. In addition, as observed from the traffic analysis, the NMS can poll a single agent multiple times within a polling interval for different statistics. Therefore, the effective number of nodes that can be managed will be lower.

4. Optimum Number of Nodes for a Given Polling Interval

This experiment is based on the assumption that the polling interval is 30 s and an acceptable maximum queuing delay is 135 ms. For plot with a request inter-arrival time of 1210 μs and different number of nodes, the queuing delay is increasing at the same rate. Since the first poll starts at 30 s for all simulations, plots for request inter-arrival time of 1210 μs with different number of nodes will partially overlap by the previous plot, as shown in Figure 26. Based on the earlier simulation results when the number of nodes is varied, the maximum number of nodes that can be managed without experiencing significant bottleneck for any request inter-arrival times of between 2 μs to 1200 μs is approximately 200 nodes. This will give a queuing delay of approximately 121.5 ms. Figure 26 shows that the queuing delay goes up to approximately 132.4 ms when the number of nodes is increased to 15,000 nodes at a request inter-arrival time of 1210 μs. As such, based on the acceptable maximum queuing delay assumed, the optimum number of nodes for a request inter-arrival time of 1210 μs is approximately 15,000 nodes. Beyond a request inter-arrival time of 1210 μs, the maximum possible queuing delay is approximately 1.22 ms and is negligible; as such, the optimum number of nodes is determined by using Equation (6.1).

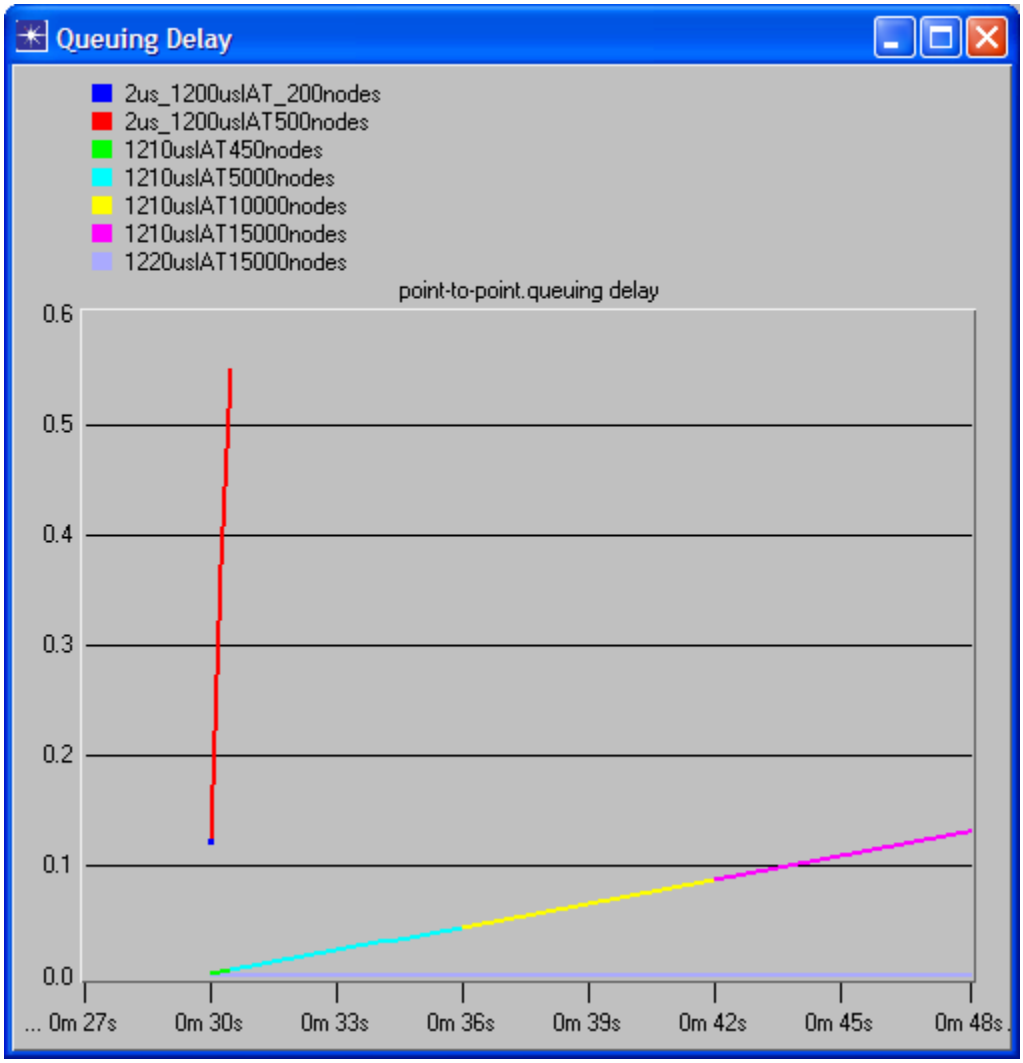


Figure 26 Screen shot of queuing delay for different request inter-arrival time and different number of nodes

Based on the above, the optimum number of nodes for different request inter-arrival times is tabulated in Table 11. These data points are plotted in Figure 27 and these data points are merely joined up by a straight line. Figure 27 can be divided into 2 zones, the “bottleneck zone” and the “non-congestion zone”.

Optimum number of nodes	Request inter-arrival time (μs)
200	2–1200
15000	1210
24590	1220
23077	1300
20000	1500
15000	2000
6000	5000

Table 11 Optimum number of nodes for different request inter-arrival times with a polling interval of 30 s and a maximum acceptable queuing delay of 135 ms

a. "Bottleneck Zone"

This zone is defined between request inter-arrival times of 2 μs to 1210 μs. In this zone, a bottleneck will be experienced due to the high rate of requests being sent, especially for a large number of nodes. Hence in this zone, the optimum number of nodes that the NMS can effectively manage depends largely on the acceptable queuing delay or acceptable congestion level of the network. Figure 27 shows that the number of nodes that can be managed is constant from 2 μs to 1200 μs. However, there is a sharp increase in the number of nodes that can be managed from 1200 μs to 1210 μs. This increase is dependent on the queuing delay that one specifies or can tolerate. If a higher queuing delay can be tolerated, the curve will increase more gradually from a request inter-arrival time starting from 2 μs.

b. "Non-congestion Zone"

This zone is defined for a request inter-arrival time of more than 1210 µs. In this zone the optimum number of nodes that the NMS can effectively manage is constrained by the polling interval specified. For a request inter-arrival time of 1210 µs and below, the optimum number of nodes is not dependent on the polling interval. On the other hand, for a request inter-arrival time of above 1210 µs, the optimum number of nodes will increase with an increase in the polling interval as seen from Equation (6.1).

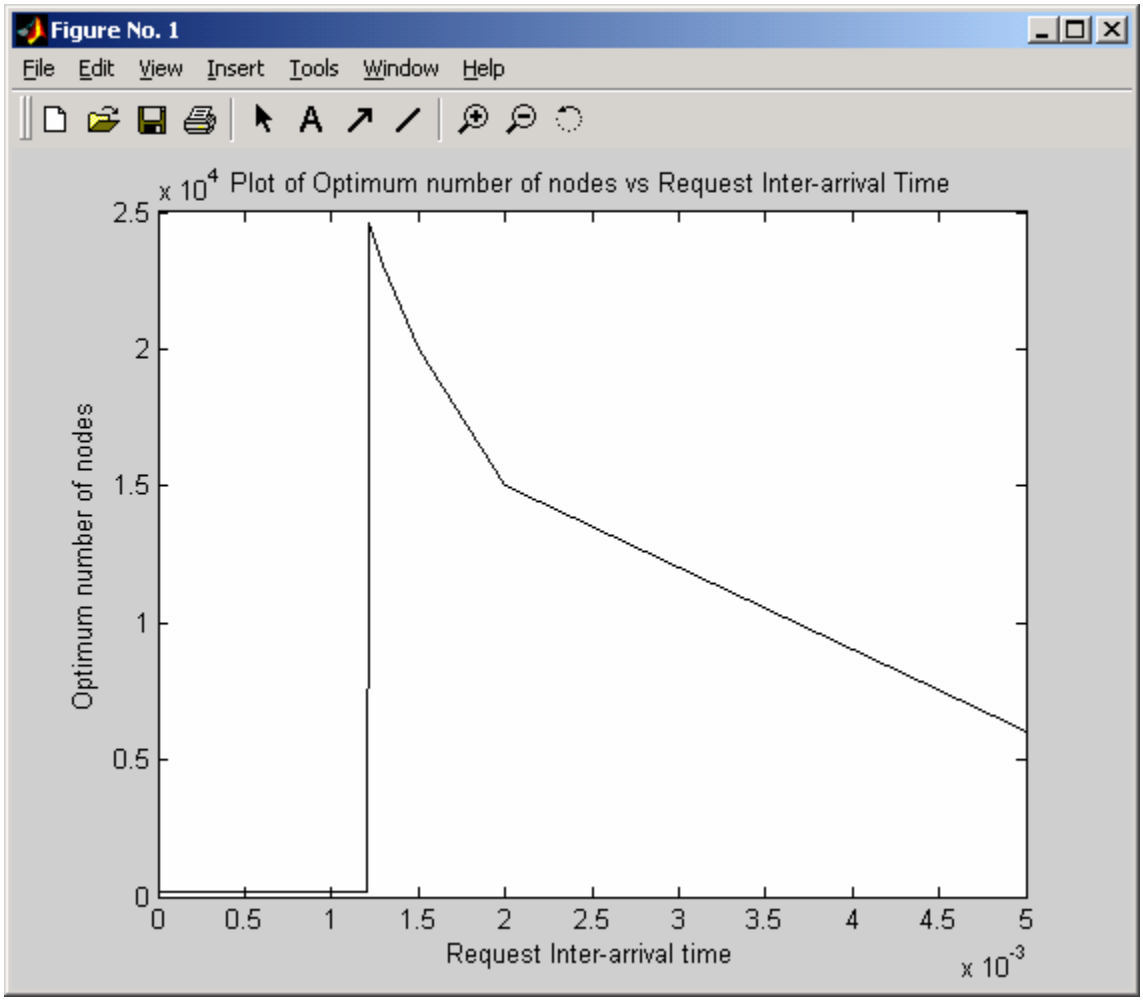


Figure 27 Optimum number of nodes to be effectively managed for different request inter-arrival times with a polling interval of 30 s and a maximum acceptable queuing delay of 135 ms.

F. CONCLUSIONS

This chapter presented the modeling of SNMP using OPNET, based on the statistics obtained from the traffic analysis on the measured SNMP traffic fitted to the constraints of an optical network management channel. It outlined the test scenarios used for the simulation. This chapter looked at the effects of altering the SNMP traffic parameters. There were three sets of experiments conducted – the effect of varying the number of nodes and request inter-arrival times, and finding the optimum number of nodes to be managed for a specified polling interval were explored. The simulation results were presented and discussed for the study of the scalability issues of SNMP-based polling over SONET/SDH networks.

The next chapter summarizes the findings from this study and presents possible areas for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

VII SUMMARY AND FUTURE WORK

A. CHAPTER OVERVIEW

This chapter provides a summary of the findings of this study. Included in the summary are conclusions from observations made during the execution of this study. Suggestions for future and follow-on work are also presented.

B. SUMMARY

Undertaking this thesis project has provided the author with many learning opportunities regarding the network management and its associated technologies. The first part of this study involved performing a traffic analysis on measured SNMP traffic to develop statistics needed to model the traffic. This analysis is necessary in understanding the traffic parameters, such as polling interval, request inter-arrival times, request packet size, etc., of an actual SNMP traffic. With the understanding of the SNMP traffic, SNMPv1 model was defined and integrated into an OPNET network model to study the scalability issues of SNMP-based polling.

Subsequently, various test scenarios are generated and simulated. The performance of SNMP was studied with respect to the effect of varying the number of nodes and request inter-arrival times, and obtaining an optimum number of nodes for a specified polling interval.

In exploring the effect of varying the number of nodes to be managed by the NMS, it was determined that, for a given request inter-arrival time, the link utilization and link throughput would increase with an increase in the number of nodes to be managed. From the simulation results, potential bottlenecks and the level of congestion in the network could be determined. Hence, the allowable number of nodes that could be effectively managed by a NMS at a specific request inter-arrival time could be determined from the results obtained.

In exploring the effect of varying the request inter-arrival time, it was determined that, for a given number of nodes, the link utilization and link throughput would decrease for an increase in request inter-arrival time. From the simulation results, given the num-

ber of nodes to be managed, an appropriate request inter-arrival time could be determined.

Additionally, for a given polling interval, results were obtained on determining the optimum number of nodes that a NMS can effectively manage for different request inter-arrival time without any significant bottleneck or network congestion. From this analysis, two different zones, i.e., the "bottleneck zone" and the "non-congestion zone", were defined. In the "bottleneck zone", the number of nodes that could be managed was significantly lower than those in the "non-congestion zone". However, in the "non-congestion zone" the number of nodes that could be managed was limited by the polling interval.

B. FUTURE WORK

Throughout this study, a number of possible directions have been identified for future work and they are as follows:

1. OPNET Modeler

In the OPNET IT GURU, a virtual network environment is created from the information one has; coarse granularity (minimum detail) is required for the modeling. In this study, the OPNET IT GURU is sufficient to provide us a quick estimate on the performance of SNMP in an optical network with respect to its scalability. In order to obtain a more exact result, SNMP can be modeled more exactly by using the OPNET Modeler. In the OPNET Modeler, fine granularity (more detail) is required to allow greater precision; hence this will require more complex development. With the OPNET Modeler, one can reproduce the SNMP traffic behavior exactly and the protocol specifications can be defined and created in OPNET Modeler.

2. Generate Real SNMP Traffic in Network Testbed

A test network can be setup in the laboratory and the network management tool can be installed into the network testbed to provide realistic SNMP traffic. The test scenarios generated in this study could be reproduced and results obtained from the network testbed compared with the OPNET analysis performed in this study.

3. Security Issues in SNMP

Security is a major concern in most networks. With the development of SNMPv3, security features such as authentication, access control and encryption were added to SNMPv3. With this new development, a study could be conducted to verify the robustness of these security features and how secure management data can be in network with the implementation of SNMPv3. In addition, a study could also look at other possible security-related issues even with the implementation of SNMPv3.

4. Using a Mobile Agent for Distributed Network Management

There are numerous problems that a centralized client-server based network management frameworks have suffered such as insufficient scalability, interoperability, reliability and low flexibility. As such, there is a moving trend towards distributed network management, i.e. to disperse or distribute centralized network management. Today's rapidly changing distributed network environment has caused network management to become a critical issue . Since then, several new enabling technologies for distributed network management have been developed and one such technology is the Mobile agent. It is a rapidly developing area of research in the fields of network management. In order to handle today's rapidly changing and complex networks, mobile agents are used in the management of network systems to enhance management distribution and distribute the management functionality throughout the network [5,9]. Hence, it may be useful to study the performance of network management using mobile agent.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1 "SNMPv3 - Simple Network Management Protocol," Technical Report, Alcatel e-Briefing, February 2003, http://www.ind.alcatel.com/library/e-briefing/eBrief_SNMPv3.pdf, last accessed 29 January 2004.

2 Rajiv Ramaswami and Kumar N. Sivarajan, *Optical Networks - A Practical Perspective*, 2nd Edition, Morgan Kaufmann, San Francisco CA, 2002.

3 Walter Goralski, *SONET/SDH,* 3rd Edition, McGraw Hill/Osborne, Berkeley CA, 2002.

4 "Simple Network Management Protocol," Technical Report, Carnegie Mellon Software Engineering Institute, 3 September 2003, http://www.sei.cmu.edu/str/descriptions/snmp_body.html, last accessed 4 November 2003.

5 Tarag Fahad, Sufian Yousef and Caroline Strange, "A study of the behavior of the Mobile Agent in the network management systems," *Proc. Of PG Net 2003*, 16-17 June 2003, http://www.cms.livjm.ac.uk/pgnet2003/submissions/Paper-02.PDF, last accessed on 5 January 2004.

6 Raouf Boutaba and Jin Xiao, "Network management: state of the art," *Proc. Of IFIP 17th World Computer Congress – TC6 stream on communication systems*, Volume 220, pp. 127-146, August 25-30 2002.

7 Mari W. Maeda, "Management and control of transparent optical networks," *IEEE Journal on Selected Areas in Communications*, Volume 16, Number 7, pp. 1008-1023, September 1998.

8 Brian J. Wilson, Ned G. Stoffel, Jorge L. Pastor, Mike J. Post, Kevin H. Liu, Tsanchi Li, Kenneth A. Walsh, John Wei and Yukun Tsai, "Multiwavelength optical networking management and control," *Journal of Lightwave Technology,* Volume 18, Number 12, pp. 2038-2057, December 2000.

9 Chi-Yu Huang and Colin Pattison, "Using mobile agent techniques for distributed manufacturing network management," *Proc. of PG Net 2001*, 18-19 June 2001, http://www.cms.livjm.ac.uk/pgnet2001/papers/CYHuang.pdf, last accessed on 5 January 2004.

10 Ashraf M. Koth, Ahmed El-Sherbini and Tarek Kamel, "A new interoperable management model for IP and OSI architectures," *Proc. Of IEEE AFRICON 4th*, Vol. 2, pp. 944-949, 24-27 September 1996.

11 "DCC Solutions for SONET/SDH Systems," Technical Report, OpenCon systems, Inc., Version 1.0, October 2003, http://www.opencon.com/dcc/DCC-white-paper-Rev2.pdf, last accessed 29 January 2004.

12 "SONET Telecommunications Standard," Technical Report, Tektronix, *http://www.tek.com/Measurement/App_Notes/SONET/overheads.pdf*, last accessed 29 January 2004.

13 "What is SNMP?," Technical Report, Williams Technology Consulting Services, *http://www.snmp4tpc.com/snmp.htm*, last accessed 3 Mar 2004.

14 "An Introduction to Network Management," Technical Report, *http://www.geocities.com/SiliconValley/Horizon/4519/work.html#Summary*, last accessed 10 January 2004.

15 William Stallings, "Security comes to SNMP: the new SNMPv3 proposed internet standards," *The Internet Protocol Journal*, Volume 1, Number 3, pp. 1-12, December 1998.

16 "Simple Network Management Protocol (SNMP)," Cisco Documentation, Internetworking Technology Handbook, Chapter 56, pp. 1-12, 20 Feb 2002, *http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm*, last accessed 11 January 2004.

17 "Cisco – Simple Network Management Protocol (SNMP)," Technical Report, Cisco, *http://www.cisco.com/warp/public/535/3.html*, last accessed 11 January 2004.

18 OPNET Technologies Inc., *http://www.opnet.com*, last accessed 3 February 2004.

19 "Representing Network Traffic," Technical Report, OPNET Technologies Inc., 14 August 2003.

20 William Stallings, *SNMP, SNMPv2, SNMPv3, and RMON1 and 2,* 3rd Edition, Addison Wesley, Reading MA, 1999.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. 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. Mr. Bryan Haas
   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