

**A FRAMEWORK FOR POLICY-BASED QUALITY OF SERVICE  
FOR FIXED BROADBAND WIRELESS NETWORKS**

Rangaprabhu Parthasarathy

Thesis submitted to the Faculty of the  
Virginia Polytechnic Institute and State University  
in partial fulfillment of the requirements for the degree of

Master of Science  
in  
Electrical Engineering

Charles W. Bostian, Chair  
Scott F. Midkiff  
Luiz A. DaSilva  
Timothy M. Callahan

June 9, 2003  
Blacksburg, Virginia

Keywords: Local Multipoint Distribution Service (LMDS), Network Management, SNMP, Quality of Service (QoS), Wireless, Broadband, Policy-based Networking

# **A FRAMEWORK FOR POLICY-BASED QUALITY OF SERVICE FOR FIXED BROADBAND WIRELESS NETWORKS**

**Rangaprabhu Parthasarathy**

**Electrical Engineering**

**Virginia Polytechnic Institute and State University**

## **Abstract**

This thesis describes an architecture for policy-based quality of service (QoS) for fixed broadband wireless systems. An implementation of the proposed architecture for the Local Multipoint Distribution Service (LMDS) wireless network in Blacksburg, Virginia is described in detail. The focus of the research work was to enable simpler management of the LMDS system and to design and enable network QoS.

The thesis examines various means to provide QoS in the network. It highlights issues related to enabling QoS in the VT-LMDS network, like prioritized access, resource management, service differentiation, and lack of predictability in network performance. Quality of service assumes a definition based on the context and application of interest. This research focuses on enabling service differentiation and intelligent resource management based on network conditions and link utilization.

A software application that serves as a model of the described architecture was developed using the C++ programming language. The tool uses the Simple Network Management Protocol (SNMP) for the network management operations. The design, implementation issues and the advantages and shortcomings of the tool are outlined and a short primer on the use of the tool is provided.

Finally, possibilities for future work in this area especially towards enabling the tool to work with other vendor-specific LMDS systems and non-LMDS fixed broadband wireless systems are examined and the issues in implementing one such system are described.

## ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Dr. Charles W. Bostian for his excellent guidance and wholehearted support for this research. His encouragement has been the guiding force for my research work at the Center for Wireless Telecommunications culminating in this thesis.

Timothy M. Callahan has been more than just an advisory committee member. As the hands-on person with experience on the LMDS network operations, administration and maintenance, Tim provided tremendous insight into the working of the system that helped towards developing the LMDS QoS application. His mentorship and support have helped me guide the project and my graduate research through very rough days. Any amount of thanks would fall short of how much I owe this thesis to his efforts.

I would like to thank Dr. Scott F. Midkiff for his keen insight into the networking aspects of the project and also providing me with very valuable tips along the development of the project. I would like to thank Dr. Luiz A. DaSilva for inspiring me to look at quality of service as more than just a theoretical concept but a real-world necessity. His classes and subsequent guidance in the development of the thesis proved to be invaluable.

The Research and Development group at Virginia Tech's Communication Network Services (CNS) helped me a great deal towards testing the application and solving a few critical problems on the way.

The staff at the CWT, especially Shelley Johnson, has helped me tide many a logistical nightmare with their calm efficiency. My heartfelt thanks to all of them.

A special note of thanks to Ms. Cortney Martin who made me believe in LMDS.

Finally I would like to thank my family and friends without whom things would have been very unpleasantly different.

A lot of people have made my graduate studies at Virginia Tech and research at CWT and CNS a wonderful experience. My thanks to all those who made a difference, but did not find a mention in this space. You are always remembered.

# TABLE OF CONTENTS

**Abstract**

**Acknowledgements**

**Table of Contents**

**List of Tables and Figures**

<b>1. Introduction</b> .....	1
1.1. Background .....	1
1.2. Need for Quality of Service.....	2
1.3. Need for LMDS QoS tool.....	3
1.4. Related Work.....	4
1.5. Description of Results.....	5
1.6. Organization of Thesis.....	5
1.7. Significance of Thesis.....	6
1.8. Chapter Summary.....	7
<b>2. Blacksburg LMDS Deployment</b> .....	8
2.1. LMDS Network Architecture.....	9
2.2. Advantages.....	9
2.3. Disadvantages .....	10
2.4. LMDS Deployment in Blacksburg.....	11
2.4.1. Limitations of Current Deployment.....	13
2.5. Chapter Summary.....	14
<b>3. Policy-based QoS for the Blacksburg LMDS Network</b> .....	15
3.1. Design Issues.....	15
3.1.1. Priority Access.....	15
3.1.2. Provisioning for Additional Customers.....	16
3.1.3. Efficient Resource Allocation.....	16
3.2. Resource Management Model.....	16
3.3. Policy-based Network Management.....	18
3.4. Proposed Architecture.....	20
3.5. Policy Description.....	22
3.6. Simple Network Management Protocol.....	23

3.7. System Reactivity.....	24
3.8. Chapter Summary.....	24
<b>4. Implementation of the LMDS QoS Tool.....</b>	<b>25</b>
4.1. Implementation Issues.....	25
4.1.1. Delay.....	25
4.1.2. SNMP Related Issues.....	26
4.2. Implementation Tools.....	27
4.2.1. SNMP++.....	28
4.2.2. Expect.....	29
4.3. User Interaction.....	30
4.3.1. Current Settings.....	32
4.3.2. Network Conditions.....	33
4.3.3. AutoManage.....	35
4.3.3.1. Link Utilization.....	37
4.3.4. QoSManagement.....	38
4.3.5. Additional Features.....	42
4.3.5.1. Authentication Module.....	42
4.3.5.2. Help Windows.....	43
4.4. Chapter Summary.....	44
<b>5. Conclusions.....</b>	<b>45</b>
5.1. Results.....	45
5.2. Applications of LMDS QoS Tool.....	47
5.3. Limitations of LMDS QoS Tool.....	48
5.4. Areas for Future Work.....	49
5.4.1. Providing Priority Access.....	49
5.4.2. Allowing More Customers per Radio.....	50
5.4.3. Extending the LMDS QoS Tool.....	50
5.5. The LMDS QoS Tool and IEEE 802.16.....	52
<b>References.....</b>	<b>54</b>
<b>Vita.....</b>	<b>58</b>

# LIST OF TABLES AND FIGURES

## Tables

5.1. Performance of LMDS QoS Tool.....	46
--	----

## Formulae

4.1. Input Link Utilization Formula.....	37
4.2. Output Link Utilization Formula.....	37

## Figures

2.1. LMDS Network Architecture.....	9
2.2. LMDS Deployment at Virginia Tech.....	12
3.1. Architecture of proposed PBNM system.....	20
3.2. Architecture of the Policy Manager.....	21
3.3. Sample Policy.....	22
4.1. Snapshot of LMDS QoS Manager Primary Menu .....	32
4.2. Snapshot of the Current Settings Window.....	33
4.3. Snapshot of the Network Conditions Window.....	34
4.4. Snapshot of the AutoManage Window.....	34
4.5. Sample of Log File.....	36
4.6. Snapshot of QoSManagement Window.....	39
4.7. Script for Coarse-grained Resource Management.....	41
4.8. Snapshot of Rate-limit Operation from Router CLI.....	42
4.9. Snapshot of Authentication Dialog.....	43
4.10. Snapshot of QoSManagement Help Window.....	44

# 1. INTRODUCTION

Fiber technologies have enabled high-speed data communications all over the world. But the benefits of high-speed Internet access have still eluded many places not served by fiber. The “last mile” bottleneck has created a digital divide between the fiber “haves and have-nots.” Many solutions, both wired and wireless, have been proposed to alleviate this problem. While wired last mile solutions such as Digital Subscriber Line (DSL) and cable modems have met with a reasonable amount of success, there is an imposed need for existing infrastructure and a minimum number of subscribers to make these services feasible. As a consequence, there are still many places without affordable high-speed connectivity. Local Multipoint Distribution Service (LMDS) is a last mile wireless technology that can serve speeds up to 1 Gigabits per second on a point-to-point or point-to-multipoint basis [10].

LMDS is a wireless technology that operates in various blocks of frequencies from 28 to 31 GigaHertz in the United States and 38 GHz in few other countries [24]. It provides symmetric or asymmetric wireless broadband service [1] to remote customers within a 5 miles radius from a hub unit. LMDS can operate in a point-point or point-multipoint configuration, based on customer requirements and total network capacity. It is also possible and viable to use LMDS as a backbone technology from which other wired or wireless techniques like IEEE 802.11b wireless local area networks or conventional Ethernet would provide final connectivity. LMDS can itself be used as the last mile solution for apartment complexes, community centers, and small and medium businesses. The applications that can be used over LMDS include real-time video services, interactive conferencing, multimedia applications, and high-speed data communications.

## 1.1. Background

LMDS operates in licensed bands between 28 and 31 GHz. Virginia Tech is the only university in the world to hold LMDS licenses to provide service and use it for research. The Virginia Tech Basic Trading Areas (BTAs) comprise of much of southwest and



southern Virginia and parts of North Carolina and Tennessee [2]. In 1999, Wavtrace Corporation (now Harris Corporation) donated LMDS equipment for deployment in Blacksburg, Virginia. A test network is currently operational providing service to a few non-paying customers. The Blacksburg LMDS testbed is currently being used for multidisciplinary research in areas such as teleradiology, enabling of services for rural communities and testing of broadband wireless equipment. The research project described in this thesis is one such activity that aims to enhance the economic viability of the network by providing various levels of network quality of service for customers. Further details on LMDS deployment at Virginia Tech are provided in Chapter 2.

## **1.2. Need for Quality of Service**

The last few years has seen a widespread increase in the use of interactive and multimedia rich content for web sites and web-based applications. This has resulted in a greater need for higher capacity with reliable and predictable service in the network. While the Internet Protocol (IP) provides best effort service that attempts to deliver a packet to its destination, there is no onus on the timely delivery of packets and, thereby, the quality of the complete transmission. This problem becomes more acute in the case of voice and video applications, where delay beyond a minimum limit is often unacceptable [3]. As more and more interactive web applications evolve, the need for bandwidth and reliability will only increase. Providing more bandwidth for the application to use does not necessarily solve the problem. Even with additional resources, the applications would find means to make use of all of it and request more. There is a lot of ongoing research to address this issue of maintaining acceptable and minimum levels of quality of service in the network at all times and to provide guaranteed service [4][5]. Differentiated Services and Integrated Services are two popular approaches at various stages of standardization and widespread acceptance that address the problem of providing QoS in packet networks. Variants and combinations of the two approaches have also been studied extensively. IP differentiated services which treat traffic on a per-aggregate basis seem to be more popular in terms of vendor acceptance and are expected to be implemented extensively in the near future.

One of the means to manage network resources and create a certain degree of dependability in network service is by the use of network policies. This method of controlling a network's resources and behavior in response to various conditions or actions in the network is called policy-based network management. Network policies help in abstracting QoS decisions and business choices on how and where resources can be and should be used to simple rules. These rules are translated by policy-based network management systems to network configuration changes and traffic regulation. By definition, policy-based network management is a mechanism where the configuration and service levels of the network are governed by a set of rules defined and implemented by the network administrator. The set of rules that are enforced on the network constitute a *policy*. Each policy is essentially a collection of “*if...then*” statements that are dependent on various parameters like time of the day, organizational hierarchy, or existing configuration and performance [6].

### **1.3. Need for LMDS QoS Tool**

The work presented in this thesis aimed at developing a framework for policy-based quality of service for fixed broadband wireless networks. An application that would implement the principles outlined in the framework was designed and implemented. This tool, *LMDS QoS*, has two main purposes. The first and foremost purpose is to serve as a proof of concept for the policy-based QoS framework. The second is to simplify LMDS network management and facilitate easier configuration and maintenance of the network.

The Virginia Tech LMDS network equipment has its share of limitations. The important limitations are highlighted in Chapter 2. These exist because the network is implemented on a test basis with limited resources and the equipment is a first-generation LMDS system. While the system does provide dedicated T1 and Ethernet service to customers in and around the Virginia Tech campus, it does little to offer built-in service differentiation mechanisms or QoS enabling features. In many instances, the system facilitates only sub-optimal use of resources. The system is not flexible for experimenting with new configurations and innovative designs.

For an effective business case to be made out of the network, SLA enforcement for current and future services assumes a lot of importance. Hence, there is a need for a tool that enables optimization of network performance and use of resources. There is also a need for a tool that simplifies the complex management of day-to-day operations of the network.

#### **1.4. Related Work**

There is limited or no work recorded in the area of providing quality of service for legacy LMDS systems. There have been a handful of proposals at various forums for quality of service for multichannel multipoint distribution service (MMDS). A proposal for the Singapore Government by erstwhile Newbridge Networks discusses the feasibility of a broadband fixed-wireless network for Singapore encompassing LMDS, MMDS and other fixed wireless technologies [25]. A few fixed-wireless vendors in various parts of the United States claim that they offer class of service (CoS) options for their full and fractional-T1 services with “five nines” (99.999%) reliability. But the vendors do not indicate that they use a common tool for enabling the CoS. They seem to be using their own custom-developed management applications that are specific to their equipment and systems [26].

A proposal for QoS for systems based on IEEE 802.16 standards establishes the need for different traffic-based classes of service. The proposal recommends various classes of service that can and should be supported by IEEE 802.16 standard-compliant systems. This approach does not address the problem at a macroscopic level of enabling QoS in a network by means of providing a better resource management system and service differentiation based on a unique mixture of operations. It rather looks at addressing QoS on an application level and offering varying treatment for video and audio and other types of traffic [27]. The IEEE 802.16 standard specifies that QoS be treated as an integral part of the standard and that it be a necessary part of the service offering. The IEEE 802.16 standard describes the various levels at which QoS needs to be assured ranging from the application level for various CoS to the physical layer level QoS assurances [28]. This set of specifications seems to be more applicable towards systems that would be designed

and created hereon as IEEE 802.16-compliant. It does not address the means of QoS-enabling existing systems that lie within the IEEE 802.16 frequency domain, but were designed and deployed before the standards procedure was initiated.

This research would definitely be unique in it proposing an architecture for quality of service for fixed wireless networks, especially LMDS systems, and in extending the design of the proposed management tool to multi-vendor fixed-wireless equipment.

### **1.5. Description of Results**

The LMDS QoS tool enables monitoring the performance of the LMDS network. Instantaneous polling of the network using SNMP can monitor vital parameters like carrier-to-noise ratio (CNR), bit error rate (BER) and received signal strength indication (RSSI). The tool allows for automatic resource management of multiple T1 circuits based on the utilization of the individual remote units. Apart from allowing the administrator to configure resources for each remote unit, the tool also allows changing their modulation type. The tool allows the administrator to provision arbitrary data rates to individual remotes units using scripts to enable rate-limited operations in the router at the network ingress. These operations are described in detail in Chapter 4 along with a simple primer on the use of the tool. The time-savings obtained as a result of using the LMDS QoS tool in lieu of the OpenView interface to manage the LMDS network is presented in chapter 5 along with other advantages of using the LMDS QoS tool.

### **1.6. Organization of this Thesis**

The rest of the thesis is organized as follows. Chapter 2 gives an overview of the LMDS Network Architecture, LMDS deployment at Blacksburg and the limitations of the current network. Chapter 3 gives an outline of policy-based quality of service concepts and how it can be utilized for enabling QoS in the Blacksburg LMDS network. Chapter 3 also covers the design of the LMDS QoS application. Chapter 4 provides a detailed discussion on the implementation of the application. A short primer on usage of the LMDS QoS tool is also provided in Chapter 4. Chapter 5 presents conclusions of the research work and outlines the possible areas for future work. Chapter 5 also gives a brief

outlook on the compatibility of the tool with multi-vendor LMDS equipment and non-LMDS fixed broadband wireless equipment like those of MMDS and UNII. Portions of the thesis are taken from a paper authored by the student and his advisory committee [8].

### **1.7. Significance of Thesis**

The LMDS QoS tool demonstrates a practical implementation of quality of service on a legacy broadband wireless network. It demonstrates an implementation of service differentiation and utilization-based network resource management in an existing network with no apparent provision for any such mechanism. It demonstrates a simple mechanism to provide better services to the customer without significant expenditure in terms of equipment or manpower. It enhances the business prospects and economic viability of the LMDS system and serves as a model for future projects in similar scenarios.

The LMDS QoS tool does not result in tremendous savings for the service provider. Instead it tries to improve upon existing equipment and configuration short-comings and offer the best possible service and options with the current infrastructure. It does more with what is currently available and, thereby, enhances the viability of the technology and the existing equipment. The resource allocation and control mechanism ensures service level agreement (SLA) enforcement which ensures that the business case be more robust when presented to potential customers. The LMDS QoS tool demonstrates a unique implementation of policy-based network QoS concepts. It is not a faithful implementation of the various models recommended as policy-based network QoS. Instead, it is a hybrid of useful and practical tenets from policy-based network management and related principles.

The LMDS QoS tool is a completely unique solution for providing network QoS and efficient network management for the Virginia Tech LMDS fixed broadband wireless network. It includes customization to suit the design of the Virginia Tech campus network. It requires varying levels of modification to be used with LMDS equipment from multiple vendors and for non-LMDS fixed broadband wireless technologies. But the

underlying architecture and design serves as a common model for network QoS implementation for most fixed broadband wireless technology implementations.

### **1.8. Chapter Summary**

This chapter outlined the motivation for the development of the LMDS QoS tool and a QoS mechanism for the Blacksburg LMDS system. It described the organization of the thesis and the contribution of this work. The next chapter explains, in detail, the Blacksburg LMDS deployment highlighting the unique features of the existing LMDS system and its shortfalls that led to the design and development of the LMDS QoS tool.

## **2. BLACKSBURG LMDS DEPLOYMENT**

This chapter gives an overview of the LMDS architecture, discusses the advantages and disadvantages of the technology and provides a background on the Blacksburg LMDS deployment. The last section in the chapter outlines the limitations of the current equipment, which serves as one of the motivations for the LMDS QoS tool.

### **2.1. LMDS Network Architecture**

LMDS operates under two basic configurations, point-to-point and point-to-multipoint. The former is used in cases where a single customer is in need of more than 10 Mbps of capacity and is willing to pay for it. The latter is the more commonly used architecture with multiple customers being serviced by a single hub radio. The Blacksburg LMDS deployment uses the point-multipoint configuration. Figure 2.1 illustrates how an LMDS hub radio provides service to multiple remotes and the various services that can be offered to the customer [9].

Figure 2.1 shows that the LMDS network can be coupled with an asynchronous transfer mode (ATM) and/or IP infrastructure based on whatever is in use at the hub location. A typical fiber backbone would be interfaced through SONET OCn (n=3, 12 currently), DS-3 links to the LMDS indoor unit. Interfaces in the LMDS hub indoor unit can also be made to support broadcast video services whereby non-data applications can be served to customers by the network. Switched circuit services like basic telephony can also be enabled over the LMDS network as is evident from Figure 2.1.

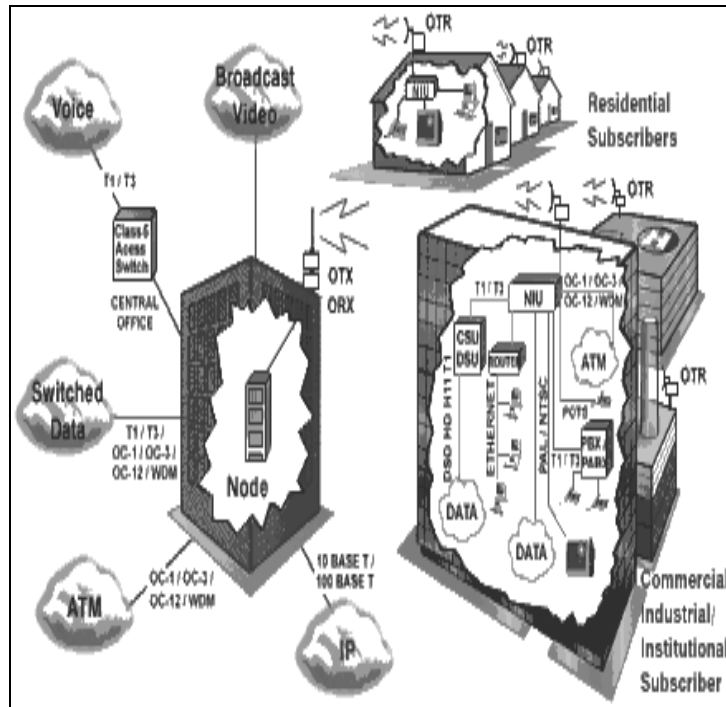


Figure 2.1. LMDS Network Architecture [9]

## 2.2. Advantages

The advantages of LMDS are as follows:

- LMDS offers the maximum bandwidth among all wireless technologies currently in use. With 850 MHz of bandwidth in a single band and a total of 1300 MHz between the A and B LMDS bands, it is the single largest allocation for any particular wireless technology.
- With adequate support from the wireline network, LMDS can offer data rates of 1 Gbps and more. This has the potential to provide an array of voice, video and data services to customers.
- The deployment time for an LMDS network is short and can typically be completed within a couple of days, if a fiber connection to the wired network is available.
- The initial cost of deployment is high, but expansion can be realized in a phased manner based on the growth of the network and addition of new subscribers.



Unlike fiber, there is not a high fixed cost required to connect the entire region. An LMDS network can be set up with a hub unit and one remote and then the number of remotes can be increased gradually according on demand.

- The major advantage of LMDS is that it can be used as a last mile service enabler and also as a backbone technology from which other wired and wireless technologies can serve the end-points.

### **2.3. Disadvantages**

The disadvantages of using LMDS are as follows:

- LMDS is a line of sight technology. This means that the hub antenna and remote antennas have to be within sight of each other. Obtaining spots for hub and remote units, which are within sight of each other, can be a difficulty, especially in hilly areas and cities with many high-rise buildings.
- In areas already served by fiber, LMDS is not cost competitive because of the initial cost required to set up an LMDS wireless network is higher compared to the cost of providing existing fiber access to a location. Unless there is a lack of existing fiber infrastructure and presence of an LMDS network in the vicinity, fiber access is cheaper when compared to LMDS.
- While the average cost per subscriber scales down as the number of subscribers increases, the initial deployment costs can be prohibitive. In rural areas where fiber has not made inroads, LMDS deployment, though advantageous, could also prove expensive.
- At the frequency of operation of LMDS (28 GHz), the distance that can be covered by the millimeter wave antennas is very limited. This is because the costs of covered by high power transmitters and low noise receivers is not much. LMDS coverage regions typically lie within 3 to 5 miles from the hub radio. At LMDS frequencies, economic considerations i.e. the cost of transmitter power amplifiers and receiver low noise amplifiers, limit path lengths to 5 miles.
- Due to its operation at millimeter wave frequencies, LMDS is prone to rain fades. Rain rates up to 3 inches/hour would not typically hamper service, but heavier

rains could induce outages in the network. While the outages can be reduced to an extent by having the remotes closer to the hub radio, it does not make economic sense, given that one would like to cover as large a region as possible with a single hub unit and not have multiple hub units at different geographic locations.

- The cost of customer premises equipment (CPE) is high when compared to those of DSL or cable modem service. While there is an ongoing initiative among many LMDS vendors to reduce the cost of the LMDS CPE [24], it will be a while before the costs are brought to more affordable levels.

#### **2.4. LMDS Deployment in Blacksburg**

The Blacksburg LMDS network serves multiple customers in and around the Virginia Tech campus. The current equipment from Harris Corporation [10] can support up to 32 remote sites. This is made possible by using the three radios at the hub unit in Slusher Tower. Each radio can support a maximum of eight airlinks, four each on the uplink and downlink, and can provide service for a maximum of four remote sites. Based on the architecture, namely point-to-multipoint or point-to-point, each customer can receive from 1.5 Mbps to 12 Mbps of capacity from the Hub unit. This means that, at any time, each remote can be allocated up to 8 T1s worth of resources. These T1s can be allocated in the form of conventional DS1 circuits or as an Ethernet bridge service. The hub indoor unit has an OC3 interface and an Ethernet 10BaseT interface fed from the campus network. The remote indoor units have multiple DS1 interfaces and a single 10BaseT interface.

The DS1 traffic to and from all remotes is concentrated at the hub unit by an OC3 interface, allowing a current theoretical maximum capacity of 155 Mbps [8]. The equipment supports a variable index quadrature amplitude modulation (QAM) scheme whereby each remote can use a different modulation type (4, 16 or 64 QAM). Support for variable index QAM enables remotes at different distances from the hub unit to receive acceptable service and throughput based on the appropriate choice of the modulation scheme [10].

Time division duplexing (TDD) is the access scheme used by the Harris LMDS system. This mechanism consists of allocating predetermined and fixed slots to each of the active remotes serviced by the hub. There are a total of four time-slots for the uplink channel and four time-slots for the downlink channel with two timeslots for control information.

Figure 2.2 shows an overview of the Blacksburg LMDS network. As seen in the figure, the LMDS hub is fed by an OC3 connection from Virginia Tech’s Multiple Service Access Point (MSAP) router and also an Ethernet switch. The LMDS hub equipment consists of an indoor unit, radio equipment and an outdoor distribution box (ODB). The ODB distributes the available resources to the various remotes as provisioned. Each hub antenna serves a 30-degree sector. Therefore, a maximum of four remote units can be serviced within a 30-degree sector.

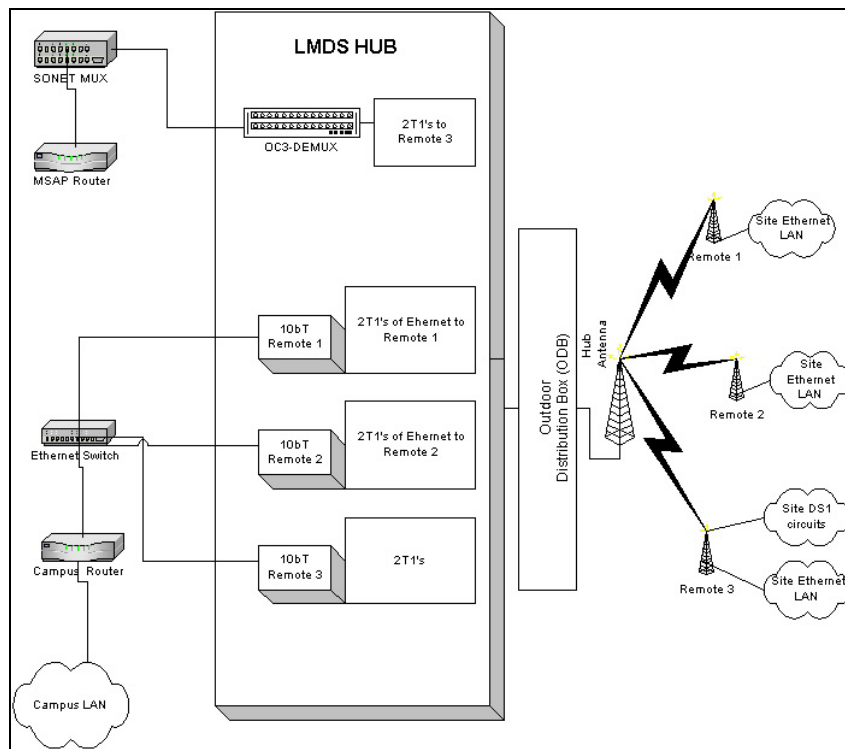


Figure 2.2. LMDS Deployment at Virginia Tech [8]

### **2.4.1. Limitations of Current Deployment**

The Virginia Tech LMDS deployment has its share of limitations because the equipment is first-generation equipment. The system was the first of its kind and the technology has evolved considerably.

Some of the limitations are as follows:

1. The allocation of time-slots and the order in which the remotes are serviced is determined by the system. Timeslot allocation is not manually configurable and hence implementing any kind of priority in servicing remotes is extremely difficult.
2. The system is not upgradeable in terms of increasing system capacity beyond OC3 speeds (155 Mbps). Hence, a complete rollout utilizing all the remote units would result in restricting individual remotes to not more than two DS1s' worth of resources.
3. The total number of remotes that can be serviced by each hub radio is fixed at four. In case of demand for additional remotes within a 30 degree sector beyond the basic four, two hub radios would have to be utilized in an overlapped configuration that would result in a waste of resources and decreased coverage for the network. At any point of time, increasing the number of remotes serviced by a single hub radio beyond four is not possible.
4. Fractional or sub-T1 provisioning to remote units is not possible. If a remote customer requires only 256 Kbps, the customer would have to be allocated at least one T1. There is a resultant waste of resources in areas where remote units require lower data rates than 1.5 Mbps. Since pricing of service is usually data rate dependent, it does not help the business case of the service provider. Even if a customer is offered fractional T1 packages, there is no mechanism in place to ensure that the customer does not violate his SLA and use the higher integral multiple T1s worth of resources allocated to him.
5. There is a 12 Mbps limit on the maximum data rate that can be provided to a single user. While it is theoretically possible to have two hub radios and two remote units for the same user and enhance the maximum data rate to 24 Mbps or

more, such point-point design rarely make economic sense, unless the user is ready to pay a lot.

Given these limitations, we envisaged and designed a quality of service framework for the LMDS system that would enhance the viability of the network in spite of the drawbacks and would position the service to be on par with other commercial high-speed Internet access technologies. The next two chapters describe in detail how the *LMDS QoS* tool attempts to overcome a few of these limitations indirectly and provide network quality of service.

## **2.5. Chapter Summary**

The basic LMDS network architecture in use was illustrated in this chapter. The advantages and disadvantages of LMDS and the Blacksburg LMDS deployment were then described in detail. Finally, the limitations of the existing LMDS network were listed. The next chapter discusses the limitations of the current system that can potentially be addressed. It describes policy-based network management techniques and how that can be used to provide QoS in the Blacksburg LMDS network.

### **3. POLICY-BASED QUALITY OF SERVICE FOR THE BLACKSBURG LMDS NETWORK**

The proposed QoS system is a hybrid model that takes its roots from policy-based network management concepts and adapts them in a manner that suits the system under study. The model does not completely adhere to any one particular policy-based network management model or implementation but is an amalgamation of basic ideas from many such systems and, also, some ideas unique to this particular implementation [8].

This chapter details the motivation for the LMDS quality of service tool, the issues that need to be addressed in the proposed system and the design of the system. The following section describes the possible areas that can be addressed.

#### **3.1. Design Issues**

##### **3.1.1. Priority Access**

Preferential service to customers can be offered by implementing priority-based access to the radio medium. This could be implemented at the medium access control (MAC) layer by reserving slots. The current generation of LMDS equipment is based mostly on a fixed slot assignment scheme if using time division duplexing (TDD) for medium access, or fixed frequency allocation if using frequency division duplexing (FDD). In the case of TDD, the system does not allow the administrator to control the allocation of timeslots to various users. Instead, at initialization, all valid remotes using an air link are allocated a fixed timeslot for the uplink channel and one for the downlink channel and that arrangement is maintained throughout the time that remote is active. This means that, at any time, zero to four slots can be active. This wastes timeslots in airlinks with fewer than four remotes and effectively decreases system throughput [8]. Since the LMDS hub decides and allocates the slots, and this mechanism is embedded in the system, it would not be possible to provide priority access to customers.

The next generation of equipment from the vendor is expected to provide dynamic slot allocation based on requirements of individual remotes [10]. This would enable priority access to radio resources.

### **3.1.2. Provisioning for Additional Customers**

One drawback of the current system is that it does not allow for over-subscription of capacity in a single airlink sector. This means that even if there are unused slots in a link, there can be no more than four remote units provisioned per link. Timeslots are allocated for a maximum of four remotes in the hub based on their remote unit IDs.

To allow for provisioning additional remotes in the link, the hub software could service up to four remotes in any one cycle, but could allocate timeslots to different nodes in different cycles. While this approach is theoretically possible, it requires changes to the operating system software and, perhaps, to system hardware. Moreover, next generation equipment is expected to provide dynamic timeslot allocation, that will alleviate this problem [10]. Therefore, provisioning for additional customers was not considered to be of paramount importance in this project.

### **3.1.3. Efficient Resource Allocation**

One of the most important aspects of QoS assurance is efficient resource management. Hence, it is also one of the core focus areas of this research. On a simple level, resource management means efficient, fair and consistent capacity allocation based on requirements and the SLA in effect. The current system allocates capacity in terms of a discrete number of T1's. Ethernet interfaces present capacity that is a multiple of a T1's capacity. There is also a theoretical maximum limit of 12 Mbps or eight T1's that can be allocated to a single remote, although the actual limit is typically about seven T1s or approximately 10 Mbps.

## **3.2. Resource Management Model**

Given the restrictions in resource allocation, we can distribute the available bandwidth using a coarse or a fine-grained resource allocation scheme. In the coarse-grained

mechanism, the allocation and regulation of resources is in terms of discrete T1s. The main advantage of such an implementation is its simplicity. The main disadvantage of this scheme is that it may waste significant amounts of capacity by offering discrete T1s instead of more efficient fractional T1 allocations.

The *coarse resource allocation* scheme can be enforced either in a static or a dynamic manner. With the currently used static scheme, the administrator selects the allocation in terms of discrete T1s to a particular remote and enforces it. No change is made to that allocation subsequently based on the link utilization. It is easy to implement, but does not result in an intelligent management of resources.

In the dynamic scheme, the administrator specifies the utilization levels which will be used to regulate the resources made available to the user. The AutoManage module of the LMDS QoS tool explained in detail in the next chapter aids the administrator in specifying an upper and lower link utilization limit for each remote. If and when the utilization in that link falls below the lower utilization level or goes beyond the upper utilization level over an interval of time, the automatic resource management mechanism kicks in. If the utilization exceeds the defined upper threshold, an additional T1 is allocated to the remote based on availability. Similarly, if utilization over a period of polling is below a lower threshold, the number of T1s allocated to the remote is reduced by 1. The polling interval based over which the utilization is computed should be chosen such that it is representative of the general behavior of the remote unit over a larger period of time. This allows for a more efficient management of resources at the cost of increased implementation complexity.

An alternative *fine-grained approach* is to regulate the traffic at the hub and the remote before transmission by the respective radios. This can be implemented through appropriate scheduling mechanisms at the router at the ingress points of the hub and remote. This enables finer-grained control over the capacity allocated to the users and also allows for statistical multiplexing gains in the airlink by sharing the available bandwidth.



Requirements of a single user can exceed 12 Mbps, which is the theoretical maximum that can be allocated. When single user requirements are equal to maximum radio capacity, point-to-point links are required to be established between that remote user and the hub. When environmental conditions degrade link performance, the permissible throughput can be reduced to account for the use of more error correction bits.

### **3.3. Policy-based Network Management**

Policies provide means to simplify management of complex networks comprised of a multitude of heterogeneous devices. Verma states that, “A network policy is a statement defining which traffic should be treated differently in the network, and how so” [6].

Policies define the actions of the network under varying conditions based on key parameters that are defined by the administrator. These parameters depend on the goals of the organization and the particular network. For example, allocating different access permissions to network services in an organization based on the user’s position in the company would constitute a policy. A more complex policy would couple the organizational hierarchy, time of day, and importance of the request to provide service to the user.

To offer differentiation in service to the customer, network policies must be implemented. These policies are simple rules that typically authenticate and authorize users and keep an account of their usage based on service level agreements [11]. On an extended basis, a policy performs admission control based on criteria such as available and requested capacity, acceptable and deliverable throughput, and priority rules.

A network using a policy-based management system typically has a centralized architecture. The *policy management tool (PMT)* decides on the appropriate policy to implement. The selected policy and other policies are stored in a repository called the *policy repository*. The repository refers to a database of all the policies for the network. The edge devices where the policies are applied are called *policy enforcement points (PEP)*. Routers, switches, hubs, and other network devices may act as PEPs. *Policy*

*decision points (PDP)* relay policies to the appropriate PEP. The intelligence of the PDP and PEP could be embedded in the same device. This is usually the case in simple networks where there is not much complexity involved in relaying the policies to various segments of the network. In this project, the policy rules have been designed on a simple level to reflect the external factors that affect performance of an LMDS system.

As an example, weather is a critical component in the performance of an LMDS system [9]. Since LMDS is a millimeter wave technology, it is prone to rain fades and even outages under heavy rain conditions. The policy should directly or indirectly take into consideration the effect of such channel impairments and ensure that there is maintenance of service levels or, at the least, a graceful degradation of service.

The policy decisions are based on a set of rules governed by the SLA of that particular customer, the customer's current usage, and channel performance metrics. The channel performance metrics are, in turn, determined to a large extent by the rain rate and other environmental conditions. The system has a built-in algorithm to compute the required error correction coding rate for a given raw channel loss rate. It will have a set of rules that monitor the bit error rate (BER) and make decisions based on that value. For example, a high BER implies that the medium is noisy and that a higher level of error correction coding is needed to compensate for the errors. Under such circumstances, it makes sense to regulate the sending rate at the transmitter by controlling the traffic leaving the routers.

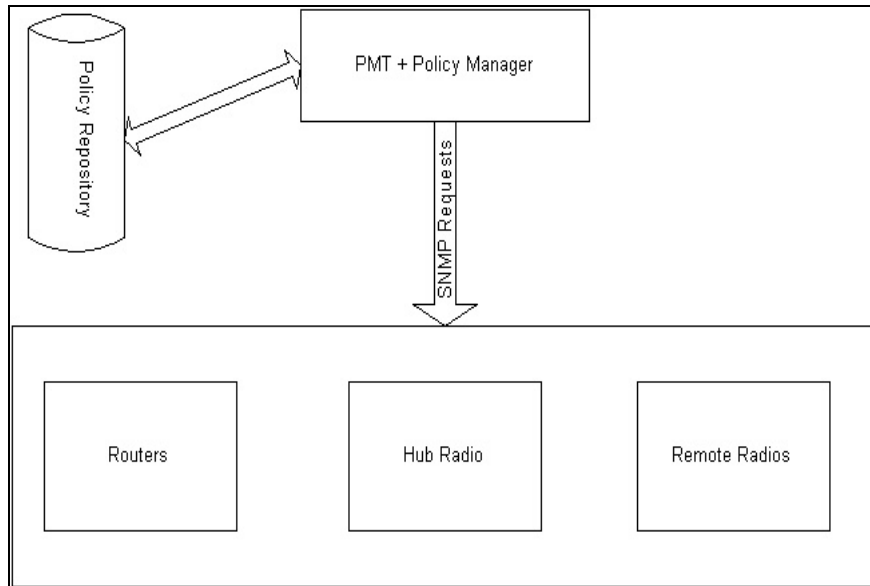


Figure. 3.1. Architecture of the Proposed PBNM System [11] [14]

### 3.4. Proposed Architecture

The architecture of the system proposed in this thesis is shown in Figure 3.1. The terminology used in the figure is similar to that used by Verma [7] and Phanse, et al. [11]. In this case, the Policy Manager and the Policy Repository are all parts of the same physical entity. Also, there is no use of the Lightweight Directory Access Protocol (LDAP) to move the policy information between a specific directory server and the Policy Manager or the Managed Agents. Instead, the architecture is centralized and concentrated at the Management Station, which functions as the policy management tool (PMT) [6], Policy Manager and the Policy Repository. There is no problem of additional overhead due to a centralized management system because signaling overhead does not tend to be a limiting factor in broadband wireless systems.

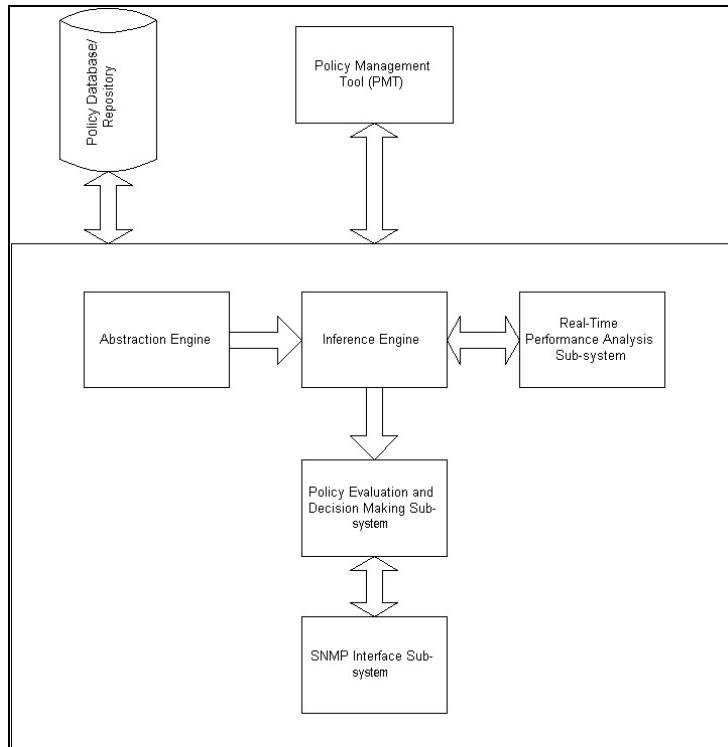


Figure. 3.2. Architecture of the Policy Manager

The policy management tool (PMT) offers the user or administrator a high-level decision making interface where rules are abstracted for convenience and usability. The Abstraction and Interpretation Engine at the management station runs on the back-end of the PMT and extracts node-level policy information that is then distributed using SNMP to the managed devices.

The functional architecture of the Policy Manager is shown in Figure 3.2. There is close interaction between the Abstraction Engine, which essentially abstracts policy related information from the user inputs in the PMT, the Inference Engine, which interprets the data from the Abstraction Engine to obtain actual device-level instructions to be distributed, and the Performance Monitoring Subsystem, which provides the Abstraction and Inference Engine with current network statistics to enable effective policy decisions.

### 3.5. Policy Description

To illustrate the idea of a policy within the framework of LMDS wireless networks, a sample policy is given in Figure 3.3.

```
if (Remote_Id = 1000) //User A's Remote Unit Id
{
  if (Post_BER <= 10-7) //Acceptable post corrected BER
  {
    if (Average_Rate <= 1Mbps) {
      reprovision_0.5Mbps; //Utilize spare BW
    }
  }
  else if (Post_BER > 10-6) // Bad medium conditions
  {
    if (Average_Rate >= 0.8Mbps)
    {
      if (SLA_T1 > 1) {
        provision_additional_T1;
      }
      else {
        regulate_sending_rate;
      }
    }
  }
};
```

Figure. 3.3. Sample Policy [8]

The example policy is designed for the unit with Remote\_Id=1000. The policy checks to see whether the post-correction BER is greater than the defined acceptable threshold. If it is, then the rule checks the utilization. If the average rate is less than a particular predefined value, the spare capacity is re-provisioned. In this case, the predefined capacity threshold is 1 Mbps. The constructs of the policy rule are based on common policy terminologies [7] [12] [13] [14].

For a 28-GHz broadband wireless network, the acceptable post-correction bit error rates are between  $10^{-7}$  and  $10^{-12}$ . For this example, let there exist a customer, User A, with Remote\_Id = 1000 whose average requirement is 2.25 Mbps with rare peak utilization of 3 Mbps. A sample policy rule can then be represented as shown in Figure 3.3. If the post-corrected BER is found to improve and fall within the acceptable limits, checks are performed on the utilization and if it's found to be more than a particular value, then

additional T1(s) are provisioned to the particular remote. This is done only when the SLA with User A is for more than one T1. If User A's SLA requires only one T1, then a process to reduce the sending rate is initiated.

### **3.6. Simple Network Management Protocol**

The simple network management protocol (SNMP) is a protocol used for transferring management information on IP networks. SNMP provides users with a set of operations to remotely manage devices in a network. The devices that can be managed range from simple printers and servers in the office to complex routers in large-scale networks. SNMP allows for network monitoring and, also, making changes in the configuration of the SNMP-aware devices in the network. The managing device that sends SNMP instructions and receives updates from devices is called the *Manager*. The software that runs in the devices that helps in collecting statistics about the device and sends it to the Manager is called the *Agent*. A database of managed objects which an agent tracks is called the management information base (MIB). All agents are composed of general MIBs common to that type of device and defined in RFC 1213 [21] as MIB II. In addition, each vendor defines its own set of MIBs for the device. The managed objects are arranged in a tree-like hierarchy. Individual objects are uniquely named and identified by their position in the tree. The numerical dot separated identifier for each object is its Object Identifier (OID). In addition, the objects also have a plain English name that is long and difficult to remember. So for convenience purposes, the OID is used to identify each managed object. SNMP uses user datagram protocol (UDP) for communication between the manager and agents. SNMP uses UDP ports 161 and 162 for communication, although vendors are allowed to define their own ports for SNMP operations [15].

We use the SNMP to carry the policy decision from the management station to the policy enforcement points. Although the Common Open Policy Service (COPS) protocol has been found to distribute policies more efficiently than SNMP [11] [13] [16], SNMP has its own advantages. With SNMP it is possible to distribute policies to multiple devices. This is unlike COPS, which is limited to one distribution at a time due to the limits of

transmission control protocol (TCP), which is used as the transport layer protocol with COPS. Moreover, the current network operations and management of the LMDS system is performed using SNMP. This makes SNMP the protocol of choice for the work reported here.

### **3.7. System Reactivity**

The proposed architecture consists of two levels of policy specification and enforcement. The first level of policy specification is driven by user preferences as indicated via the PMT to the management station. The system reacts to policy decisions that are then translated into device-specific instructions and sent via SNMP to the devices. Once a policy is enforced in a device, the policy conditions are repeatedly checked to ensure that the right policy is in place at the devices. For example, changes in weather could result in the worsening of medium conditions. In such a case, the system is proactive and, expecting that a threshold level can be reached soon, would implement a different policy. For this purpose, alarm management can be performed with alarms triggered when BER rises above acceptable levels. Such a dual system with a reactive approach to user inputs and proactive approach to predefined threshold levels yields a robust QoS system that ensures that an appropriate policy is enacted at the right place and time [8].

### **3.8. Chapter Summary**

This chapter outlined the basic concepts of policy-based network management and how it can be used to provide QoS in the Blacksburg LMDS network. The proposed policy manager was illustrated with a discussion on its design choices and potential issues. The proposed architecture for implementation was discussed with sample policies for better understanding. Also, the reason for using SNMP to transfer management information and how it is proposed to be used was described.

The next chapter discusses in detail the issues in implementing the LMDS QoS tool and the tools used for implementation. It further explains the individual components on the LMDS QoS tool in detail with the help of snapshots from the operation of the tool.

## **4. IMPLEMENTATION OF THE LMDS QoS TOOL**

The design of the policy-based QoS framework for the LMDS network was discussed in Chapter 3. In this chapter we describe the various issues in implementation and their proposed solutions. We also provide a detailed description of the LMDS QoS tool, its operation, and, finally, its limitations.

### **4.1. Implementation Issues**

#### **4.1.1. Delay**

One of the possible implementation issues is delay. The delay in implementing a particular policy could be significant if the network is congested or if the policy requires multiple device-specific commands to be executed in the hub and/or remote units. Since the policies are implemented by SNMP requests sent to the hub or remote radios, there is a possibility that the number of SNMP requests required to implement a complete policy might be considerable, which can result in substantial delays. The delays could be even more significant if the SNMP requests are sent one at a time. This can, to some extent, be overcome by coupling multiple SNMP requests together. Unfortunately the hub does not accept multiple SNMP requests simultaneously. It expects the requests to arrive sequentially, and one at a time. If one of the SNMP Set operations fails, the hub does not accept the remaining instructions in that operation.

Executing multiple commands requires that the resulting latency be taken into consideration in the application design. This problem can be further complicated by repeated policy changes at the hub unit. A mechanism to regulate the frequency of policy changes needs to be in place to minimize system complexity and overhead. Fortunately most of the operations performed by the LMDS QoS tool do not extend beyond a few seconds. Compared to the time taken when performing the same operations with HP OpenView, it is trivial. This delay metric is acceptable for the hub and, hence, does not create any problems. In the future, if link activation is included as a part of the application, it can be expected to take a few minutes and could create potential problems in the case of any outages during that time. But as of the current version, the LMDS QoS



tool does not support new link creation and hence the major delays due to implementation are not an issue.

An issue related to delay is the possibility of having outages due to system re-initialization during policy implementation. This occurs when there are major changes in the functioning of the hub or remotes. Most of the operations performed in the process of policy distribution and enforcement do not require changes that to cause or force re-initializations or a system reboot. Such a situation is not ruled out, however, and provision can be made in those circumstances to maintain policy information so that it is not lost due to the re-initialization.

The LMDS QoS tool is designed to perform operations on the network completely from scratch. This means that all the operations of the LMDS QoS tool assume and expect the system to be in an idle state. So if due to an outage, an operation is only partly completed, the next time, the changes already introduced are overwritten with the same values again and then the tool proceeds to make the remaining modifications. A message box that indicates success or failure in completion of tasks is used as one of the mechanisms to indicate the result of the task to the administrator. This can be used as an indicator to let the administrator know whether the operation needs to be executed again or has been completed successfully. Extreme environmental conditions might force an outage in one or more of the remote units. This is indicated in the monitoring part of the tool and would alert the administrator of the impending problems. Upon reboot, the original configuration is restored. The possibilities of such environment or external factor-induced outages can be incorporated into the service level agreement (SLA) and alternate provisions arranged by means of wired Ethernet or dial-up connectivity to restore basic network services to the customer.

#### **4.1.2. SNMP Related Issues**

The process of coupling multiple SNMP requests and distributing them to devices could pose problems at run-time that would need to be resolved for efficient functioning of the system. For the initial version, the number of policy changes that can be performed is

limited to reduce the possibility of failure of the existing system. This is particularly important because the system serves regular customers who cannot afford to have repeated or long system outages.

Routers typically do not allow SNMP Set operations to be performed on them. Moreover, the tasks to be implemented by the router cannot be enforced or issued by means of SNMP operations. Such operations would need to be performed at the command line interface (CLI) using Cisco's Internetworking Operating System (IOS). It is not possible to manually login to the device every time a new policy is being enforced. This would compromise the security of the router by requiring that the password be made public to all the users. Instead, a script that automatically logs into the router at run-time and issues the appropriate IOS commands is used. The router enable passwords would be hard coded in the program and the release version of the software would not permit unauthorized users to view the router passwords. *Expect* is a tcl extension that helps in automating interactive programs. Expect allows us to create scripts in tcl and embed them in any common programming language and then login to remote devices and execute commands in that device [18]. More information on Expect and how it is used in this particular application is provided later in the chapter.

The authentication mechanism of the LMDS QoS tool, discussed in later chapters, offers a first level of defense for the tool against unauthorized users. The SNMP operations are also tied to the authentication module in such a way that Guest level users are not permitted to perform the SNMP set operations. Only the SNMP get operations that are used in current settings and network conditions dialog boxes are permitted to be exercised for the Guest level of users. This ensures that there is a dual level of security for the LMDS QoS tool.

## **4.2. Implementation Tools**

This section briefly describes the two major tools that were used to achieve the desired operations for the LMDS QoS tool. They are SNMP++ and Expect.

#### 4.2.1. SNMP++

The HP OpenView tool currently used requires the administrator to perform all the SNMP operations individually in sequence to achieve the desired result. This procedure takes time and also a certain level of understanding on the tool and the system it manages. While performance monitoring and statistical data collection can be automated by creating small OpenView applications, the decision making required for the bandwidth management and resource management operations cannot be automated using OpenView. There was a need for a tool that would allow us to easily develop the LMDS QoS application with the desired logic and decision making in place along with the facilities offered by OpenView. For this purpose, HP SNMP++ classes, which actually was used for the development of HP OpenView was used. This allows us to make full use of the application programmer interface (API) that is used by HP OpenView and at the same time, provide the application with the required intelligence as per the design.

SNMP++ is a set of C++ classes that provide SNMP services to a network management application developer [19]. SNMP++ offers an object-oriented approach to develop SNMP based applications. SNMP++ does not constitute a new layer or wrapper over current SNMP engines like WinSNMP. Instead, it uses the existing SNMP provisions of various operating systems to provide the developer with a simple API to develop network management applications. Some of the advantages of using SNMP++ are as follows [19].

- It provides a simple interface for SNMP based application development.
- It provides support for SNMPv1 and SNMPv2.
- It does not modify lower layer SNMP implementation.
- It provides developers with the choice of bypassing the object oriented higher-level SNMP++ API and utilize lower layer SNMP programming implementations like WinSNMP.
- It provides a portable API that operates over different operating systems and different network layer protocols.
- It provides an automatic memory management mechanism to free memory used by various SNMP related structures and resources when the object is destroyed or is out of scope.

- It provides provision for notifications, time-outs and retries.
- It supports SNMP Get, Get Next, Set, Get Bulk, Trap, and Inform operations

Some of the classes provided to simplify the creation of SNMP applications include [19]:

- Oid (Object identifier) class,
- IPAddress (Internet Protocol Address) class,
- Vb (Variable Binding) class,
- Pdu (protocol data unit) class,
- Snmp (Simple Network Management Protocol session) class, and
- CTarget (Community based targets) class.

Hewlett Packard released an implementation of SNMP++ in 1997. The HP SNMP++ API is open source and available for download at [19]. This package was used for the development of the LMDS QoS application development. Simple C++ programs were created using the package to interact with the LMDS hub unit and Cisco Catalyst 1924 switch and effectively manage the network.

#### **4.2.2. Expect**

*Expect* is a tool that allows the user to automate interactions with applications. Expect is primarily used in conjunction with tcl and can be used to simplify and automate extremely complex interactive procedures. Within a Tcl script, the “expect” command waits for a particular pattern in the output of the interactive host program. When that pattern or word is encountered, any sequence of operations defined by the user can be executed. Expect can interact with multiple programs at the same time and can also be run as a background process. The three essential Expect commands that help in the process of automating interactions are expect, send and spawn. While “expect” waits for the pattern input from the application, “send” is used to send the response to a process and “spawn” is used to start other programs [18]. While there are many other commands in Expect, these three commands form the major portion of the Expect script.

To illustrate the use of Expect, let us consider any common login process. The host machine would prompt the user to input the user name and return. He would then be prompted to enter the password. This process of being prompted for username and password can be automated whereby a tcl script would wait for the host to prompt for a Username and then submit the username and subsequently the password. For this purpose, the script uses the Expect syntax of expecting a particular pattern of characters from the host, in this case “Username:”. The script then *sends* the username followed by the ASCII representation for return key. The client script now waits for the “Password:” pattern and responds with the actual password followed by a return key. This way, the user does not have to manually enter the username and password every time he or she is required to interact with the host.

In this application, an Expect code snippet embedded in a tcl script is used to interact with the Cisco router at the ingress of the LMDS network. Details of the Expect script and how it serves the purpose are provided in following sections.

### **4.3. User Interaction**

The LMDS QoS application can be installed on a Microsoft Windows-based management station. The application on the management station serves to control the LMDS network by a series of menu driven options, part manual and part automatic. These menus and buttons help the administrator to decide on the policy to be implemented. These policies can be completely based on predefined rules or can be a mixture of interactive user choices and existing policy definitions. These policies are then enforced at various policy enforcement points in the network, including routers and LMDS equipment. The front-end is a graphical user interface with menus for creating, editing and deleting policies. The existing tool to perform network management operations in the LMDS network is Hewlett-Packard Open View. It is expected that the LMDS QoS tool would someday, replace the OpenView management interface. For now it serves to simplify most but not all of the tasks currently performed using OpenView.

The policy management tool implementation is in C++ so that the front-end application can seamlessly interface with the Policy Manager and the Policy Database. Since the APIs are in the form of classes, the C++ implementation makes things simpler. For example, the SNMP operations are abstracted into sessions that are described by the methods of the Snmp class. The CTarget class allows us to define the target device that is to be configured or managed. The Oid class helps describe the exact OID of the device that is going to be modified. The Vb class serves as the entity which carries the OID to be modified and the actual modification. The developer is required to know only the methods of the various classes described above and their exact purpose. This simplifies the operations considerably

The LMDS QoS tool offers a Graphical User Interface (GUI) for the administrator to manage the LMDS network. An authentication module enables only valid users to use the tool. The tool has four main dialogs for easy navigation and management of tasks. They are as follows:

1. Current Settings,
2. Network Conditions,
3. AutoManage, and
4. QoSManagement.

The parameters selected as metrics of interest in the wireless network are bit error rate (BER), carrier to noise ratio (CNR) and received signal strength indication (RSSI). These parameters can be monitored for both the uplink and downlink channels of the network. In addition, threshold levels can be specified for these parameters. If the performance of the remote unit exceeds the threshold, alarms are generated and stored for later viewing. Figure 4.1 shows a snapshot of the Primary Menu with all the four dialog options.

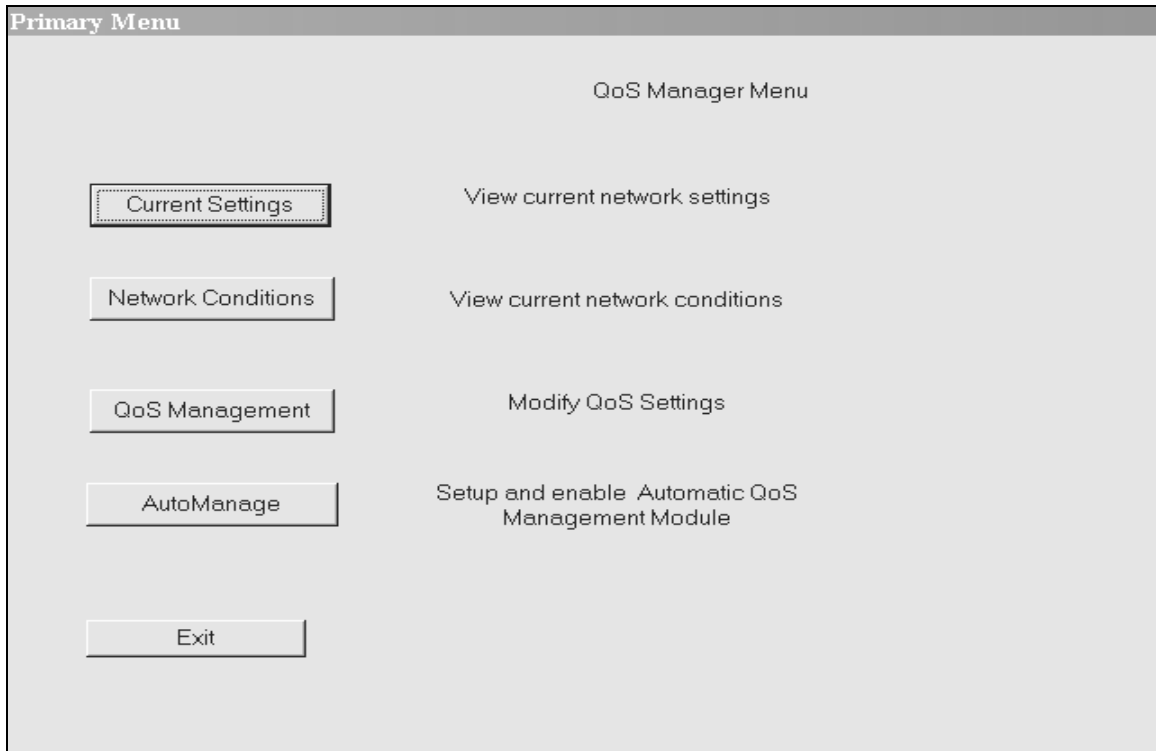


Figure 4.1. Snapshot of LMDS QoS Manager Primary Menu

The interface and operations of the LMDS QoS tool can be described based on the member dialogs and their purpose. The following section explains the usage and purpose of each of the four dialog windows.

#### 4.3.1. Current Settings

The current settings dialog, as the name implies, displays the current configuration of the network. When the user clicks on the current settings link, the application polls the network and obtains the latest configuration details from the hub. This is then displayed appropriately in a user-friendly format. The parameters that are displayed include the active remotes with their identification numbers, location description as input during the creation of the link, airlink class, which specifies a unique number that denotes the number of T1 circuits allocated to the remote at a particular modulation type, modulation type and the number of T1s currently active at that remote. Figure 4.2 is a snapshot of the Current Settings dialog. The purpose of the Current Settings window is primarily as a view to the accurate and on-the minute network configuration and to help in making

subsequent configuration choices. Changes made thus using the QoS Management or AutoManage module can be verified using the Current Settings window.

The screenshot shows a window titled "Current Settings" with a sub-header "Current Network Settings". It contains a table with five columns: "I.D", "Description", "AirLink Class", "Modulation", and "T1's". There are four rows of input fields corresponding to "Remote 1 ID" through "Remote 4 ID".

	I.D	Description	AirLink Class	Modulation	T1's
Remote 1 ID :	581	BTC	0	4 QAM	1
Remote 2 ID :	593	VTMNH	5	16 QAM	2
Remote 3 ID :					
Remote 4 ID :					

Below the table is a "Help on Current Settings" button. At the bottom of the window are five menu buttons: "Network Conditions", "QoS Management", "AutoManage", "Primary Menu", and "Exit".

Figure 4.2. Snapshot of the Current Settings Window

### 4.3.2. Network Conditions

The network conditions dialog allows the user to view network performance metrics like the bit error rate, signal to noise ratio and received signal strength indication. The values are polled at run-time from the LMDS hub unit and provided to the user. Both the hub side (downlink) and remote side (uplink) statistics are displayed for each active remote. Figure 4.3 shows a snapshot of the network conditions dialog.



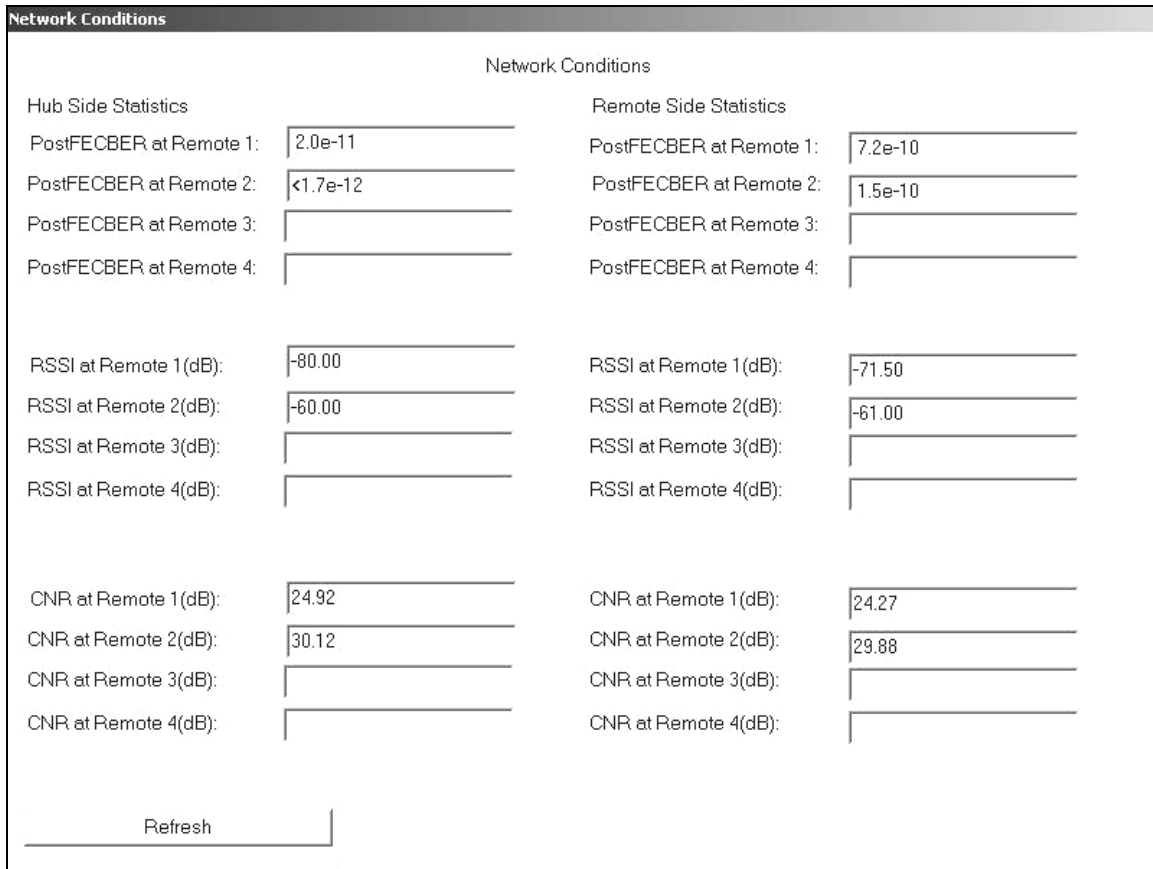


Figure 4.3. Snapshot of the Network Conditions Window

To ensure that the statistics are current, there is a provision to refresh the values of the parameters when the user desires. Like the Current Settings window, the Network Conditions window primarily serves as a decision making tool for policy choice. In addition, the Network Conditions module serves as a useful tool for researchers and customers to view real-time airlink performance metrics. It aids in observing the impact of changing environmental conditions on the medium characteristics. It also helps in estimating the impact of the error correction mechanism at various levels of medium degradation or improvement. It is expected that this module would be used to provide researchers with real-time statistics to augment the theoretical models of 28GHz channels and enable fine-tuning and better understanding of the medium.

### 4.3.3. AutoManage

The AutoManage module is used to enable the automatic recording of system alarms and also to enable the resource allocation to individual remotes based on their respective utilization levels. Figure 4.4 illustrates a snapshot of the AutoManage dialog window.

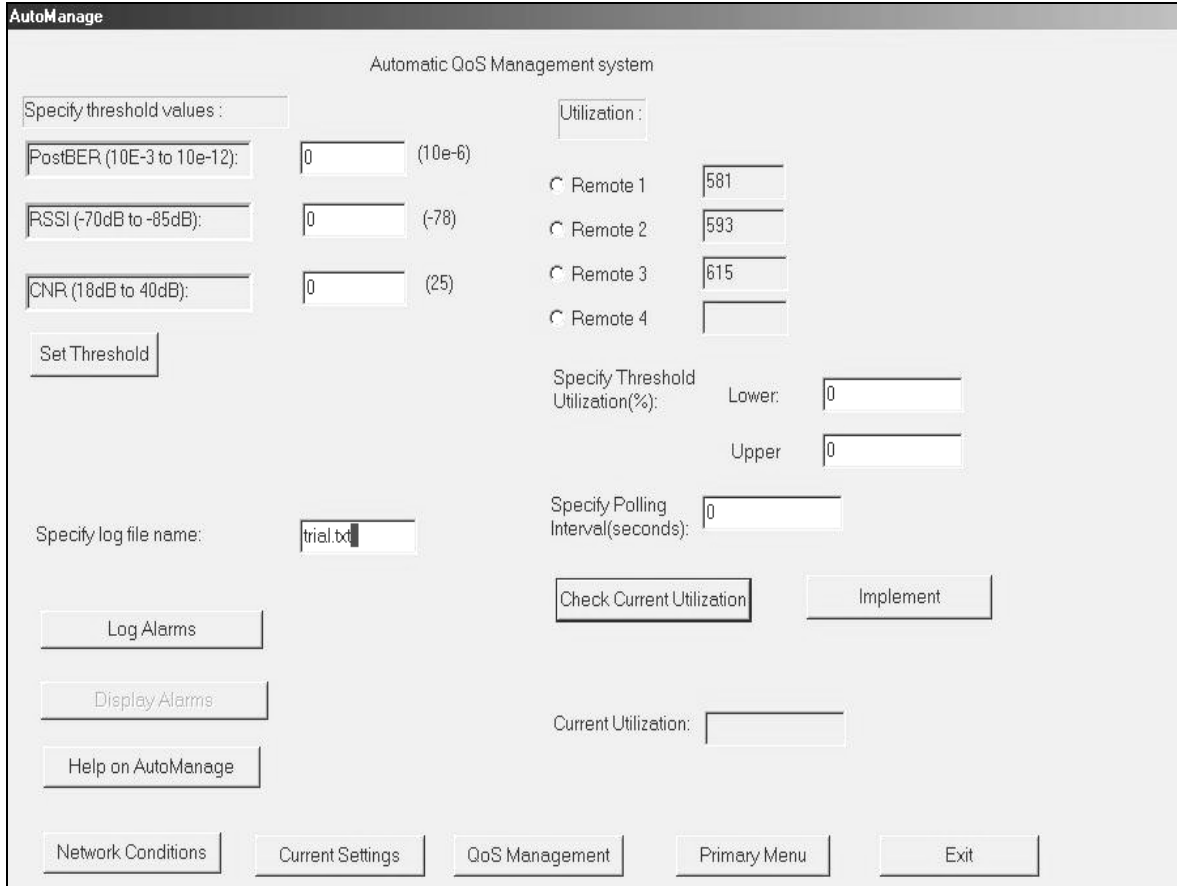


Figure 4.4. Snapshot of AutoManage Window

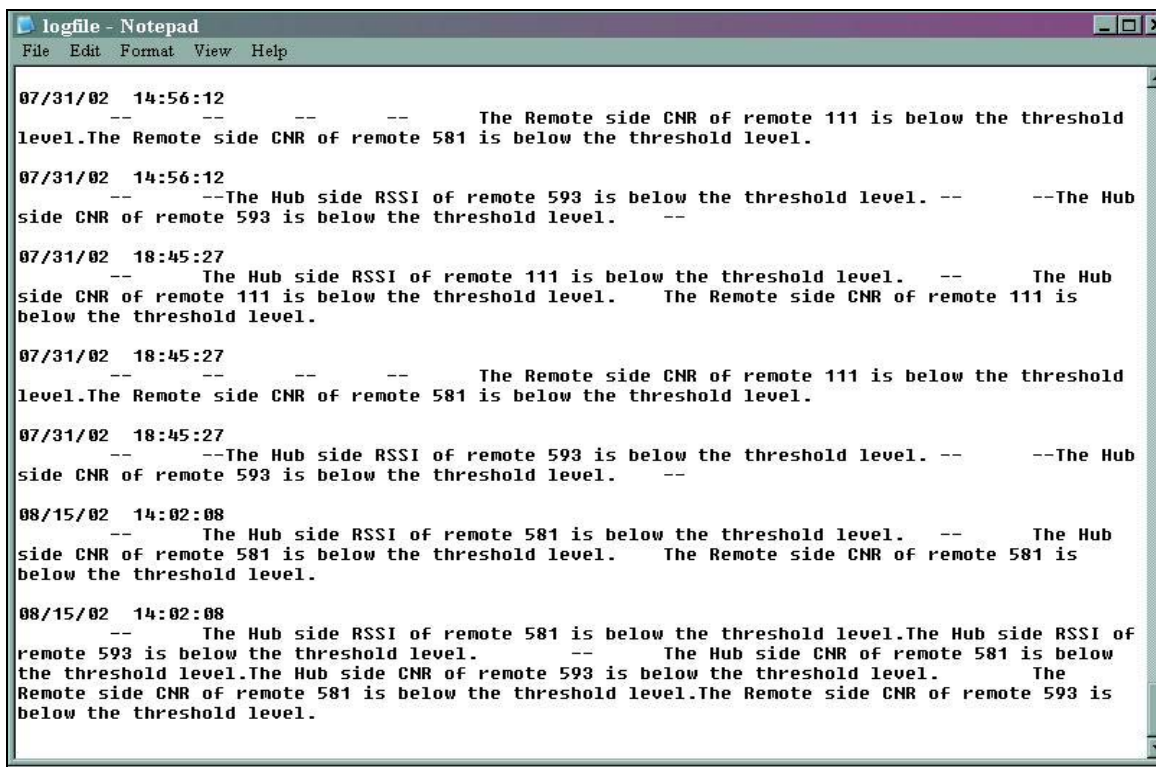
The alarm logging mechanism is flexible in terms of allowing the user to define his or her own alarm values for BER, RSSI and CNR. This allows for a better management mechanism based on specific network requirements. Alarm logging also allows for collection of statistical data on the network stability and performance over a period of time with respect to the alarms generated by the system and estimate future dependability levels to the customer. Predefined values of CNR, RSSI and BER used as default threshold are 30 dB, -78 dB and  $10^{-6}$ , respectively. The user can set his desired range of threshold values.

The ranges permissible are as follows:

- CNR: 18 to 40 dB
- RSSI: -85 to -70 dB
- BER:  $10^{-12}$  to  $10^{-3}$

These values are based on acceptable levels of the parameters in consideration, as recommended by the equipment vendor.

When the user wants to log the alarms, he or she can click on the Log Alarms button in the window. The application checks the values of all the above-mentioned parameters for the uplink and downlink channel by instantaneous polling. It then logs the parameters exceeding the threshold value in a log file whose name can be specified by the user. The default log file name is logfile.txt. A snapshot of the log file is presented in Figure 4.5.



```
logfile - Notepad
File Edit Format View Help

07/31/02 14:56:12
-- -- -- -- The Remote side CNR of remote 111 is below the threshold
level.The Remote side CNR of remote 581 is below the threshold level.

07/31/02 14:56:12
-- --The Hub side RSSI of remote 593 is below the threshold level. -- --The Hub
side CNR of remote 593 is below the threshold level. --

07/31/02 18:45:27
-- The Hub side RSSI of remote 111 is below the threshold level. -- The Hub
side CNR of remote 111 is below the threshold level. The Remote side CNR of remote 111 is
below the threshold level.

07/31/02 18:45:27
-- -- -- -- The Remote side CNR of remote 111 is below the threshold
level.The Remote side CNR of remote 581 is below the threshold level.

07/31/02 18:45:27
-- --The Hub side RSSI of remote 593 is below the threshold level. -- --The Hub
side CNR of remote 593 is below the threshold level. --

08/15/02 14:02:08
-- The Hub side RSSI of remote 581 is below the threshold level. -- The Hub
side CNR of remote 581 is below the threshold level. The Remote side CNR of remote 581 is
below the threshold level.

08/15/02 14:02:08
-- The Hub side RSSI of remote 581 is below the threshold level.The Hub side RSSI of
remote 593 is below the threshold level. -- The Hub side CNR of remote 581 is below
the threshold level.The Hub side CNR of remote 593 is below the threshold level. The
Remote side CNR of remote 581 is below the threshold level.The Remote side CNR of remote 593 is
below the threshold level.
```

Figure 4.5. Sample of Log File

### 4.3.3.1. Link Utilization

The AutoManage module also has a mechanism to automatically regulate the resources allocated to each remote unit. As shown in Figure 4.4, the ‘Check Current Utilization’ button, when clicked after selecting a particular remote obtains the interface input and output octets for that remote unit from the router present at the ingress of the hub and computes the link utilization from the values. The formulae used to compute the link utilization are given by Equations 4.1 and 4.2 [21].

$$Input\ Utilization = \frac{\Delta ifInOctets * 8 * 100}{(number\ of\ seconds\ in\ \Delta) * ifSpeed} \quad (4.1)$$

$$Output\ Utilization = \frac{\Delta ifOutOctets * 8 * 100}{(number\ of\ seconds\ in\ \Delta) * ifSpeed} \quad (4.2)$$

Since the utilization at the ingress of the router is being computed, the Input Utilization is considered for all practical purposes as the utilization of the link. These formulae do not take into account the overhead involved due to the protocol. The MIB variables used in these formulae are ifInOctets, ifOutOctets and ifSpeed. These variables are described in detail in RFC 1213 [22]. They are common interface parameters, which are made use of by the formulae as specified in RFC 1757 [21] [23]. A brief description of the interface parameters are provided below.

*ifInOctets:*

OID: .1.3.6.1.2.1.2.2.1.10

Description: “The total number of octets received on the interface, including framing characters”

*ifOutOctets:*

OID: .1.3.6.1.2.1.2.2.1.16

Description: “The total number of octets transmitted out of the interface, including framing characters”

*ifSpeed:*

OID: .1.3.6.1.2.1.2.2.1.5

Description: “An estimate of the interface’s current bandwidth in bits per second”

Once the link utilization of the selected remote is computed, the user can specify the minimum and maximum threshold levels for the utilization. By clicking the ‘Implement’ button, the user enables the T1 regulation mechanism. The application checks whether the utilization is below the lower threshold level. If it is, then the number of T1s allocated to the remote is reduced by one, if it is possible to do so. The application also checks whether the utilization is above the upper threshold level. If the utilization exceeds the upper limit, the application assumes that the remote is experiencing heavy traffic and provisions an additional T1 to the remote if available.

The critical factor in this operation is the time-range for which the network is polled to compute the utilization. A small polling interval is not sufficient to make a decision in terms of allocating or de-allocating a T1 to the remote. At the same time, too long an interval would mean that spikes in utilization are missed by the application and instantaneous values would determine the outcome. Hence, it is at the discretion of the user to specify a good time interval to poll the network and compute the utilization, which hopefully would result in a fair choice for regulation of resources. It is recommended that a polling interval of not more than twenty minutes and not less than ten minutes be used as it would serve as a suitable duration to capture the traffic levels realistically.

#### **4.3.4. QoSManagement**

The QoSManagement module in many ways is the most important component of the LMDS QoS tool. It allows the administrator to make critical changes in the configuration

of the system and, in effect, the performance of the network. Figure 4.6 illustrates a snapshot of the QoSManagement dialog.

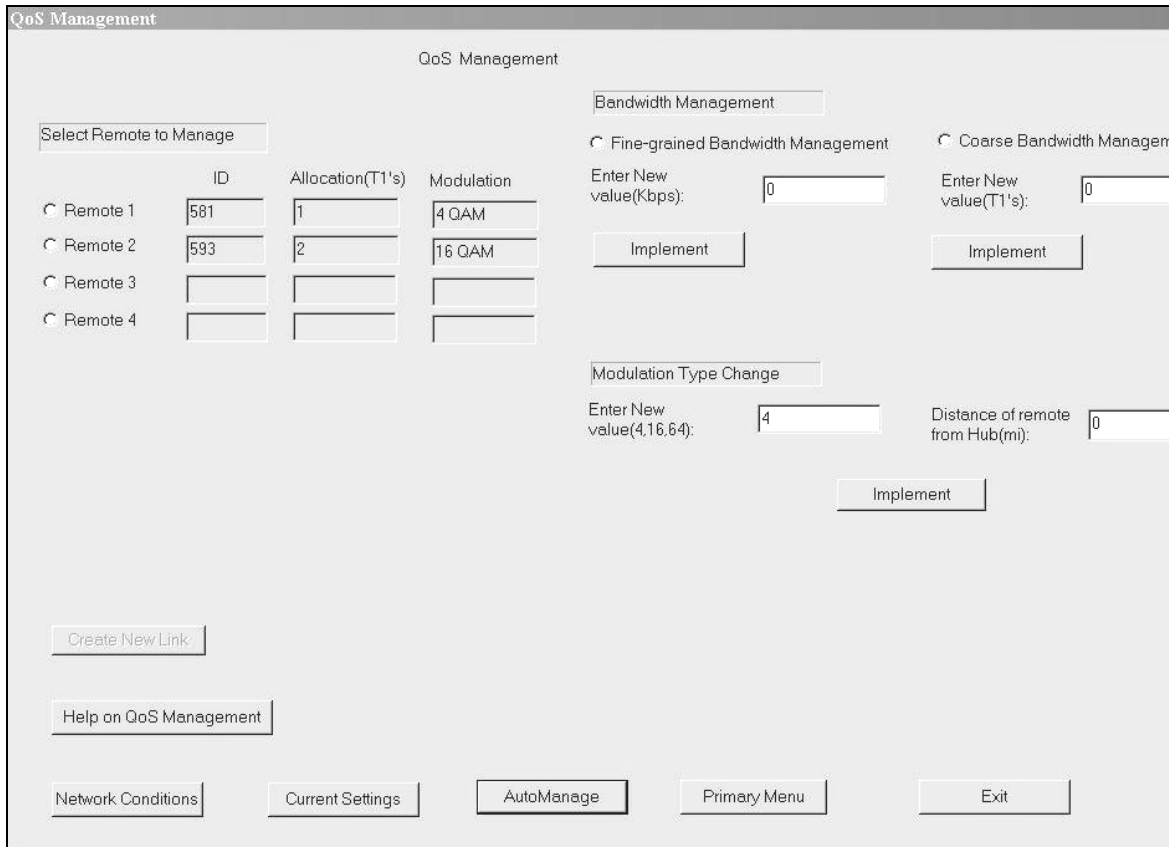


Figure 4.6. Snapshot of QoSManagement Window

The QoSManagement module has a simple interface that allows the user to first specify the remote unit to manage by selecting a radio button. To simplify the choice making process, basic configuration details of the remotes are displayed alongside the remote IDs. The major sub-modules in QoSManagement are as follows:

- coarse-grained bandwidth management,
- fine-grained bandwidth management, and
- modulation type management.

Coarse-grained bandwidth management allows the user to allocate and change the resource allocation to remotes in terms of discrete T1 circuits. Since there is a maximum limit of 8 circuits that can be provisioned for each hub radio, there is an accounting mechanism in place to ensure that there is no over-subscription of T1 circuits. The hub system computes the number of symbols allocated to each remote and compares it with a preset maximum value to determine whether the allocation for a radio link has reached its possible maximum. The number of symbols depends on the modulation type and number of T1s allocated to each remote. The equipment vendor provides the symbol count table.

The fine-grained bandwidth management module is more complicated in terms of implementation than the coarse-grained module. Since the Blacksburg LMDS system permits only T1 circuits over the air channel, there is very little granularity possible for allocation. For an Ethernet overlay over a T1, the allocations are still in terms of T1 circuits and fractional resource allocations are not possible. This serves as a disadvantage for customers who have sub or fractional-T1 requirements like 128 Kbps or 256 Kbps.

To address this issue, the LMDS QoS tool provides a mechanism to restrict the traffic to a user to arbitrary rates that are not necessarily integer T1 values. This does not translate to any savings in resources but it allows for service differentiation and the ability to reach a wider target audience than the existing system. For this purpose, a script written in Expect is executed at run-time. The script automatically logs in to the Cisco 2511 router at the ingress of the LMDS network and enforces a rate-limit at the interface to which the remote unit in consideration is connected. This ensures that the administrator does not need to know the IOS commands for enforcing the rate-limit and also ensures that the security of the router is not compromised. Figure 4.7 illustrates the router script used for the operation.

```
 routerscript - Notepad
File Edit Format View Help
package require expect 5.21
# to extract the router_ip,router interface number and rate limit bandwidth from cmd line
arguments
# overall usage is tc1sh80 scriptname router_ip router interface,rate limit value

set router_ip [lindex $argv 0]
#interface number in router where managed remote is connected
set interf [lindex $argv 1]
#specify the interface to manage
set band [lindex $argv 2]
#rate to which interface has to be limited
set burst_normal [lindex $argv 2]
#burst size
set burst_max [lindex $argv 2]
#burst- max

spawn telnet $router_ip
exp_internal 0
set timeout 200

expect ">"
send "enab\r"
expect "Password: "
send "*****\r"
expect "#"
send "config term\r"
expect "(config)#"
send "interface e0/$interf\r"
expect "(config-if)#"
send "rate-limit input $band $burst_normal $burst_max conform-action transmit exceed-action drop"
send "exit\r"
send "logout\r"
```

Figure 4.7. Script for Coarse-grained Resource Management

It can be noted in the example of Figure 4.8 that the password is been hidden from the reader. While the actual script does have the password in place, it has been hidden here for security reasons. It can also be observed that all the parameters required for the execution, namely the command line arguments of the script are assembled at run-time by the application. This is to simplify the task of the administrator and also to avoid tampering of valuable information by the customer or user.

A fine-grained bandwidth management operation was carried out to test the validity of the script and the router output is illustrated in Figure 4.8. The snapshot is captured from a telnet session with the router after the policy enforcement. The *show interfaces rate-limit* command displays all the rate limit operations performed on the selected interface. Here, Ethernet interfaces 1 and 0 have a rate limit of 256 Kbps and 128 Kbps respectively enforced on them.



```
ca\ Telnet 198.82.245.12
heron#show interfaces rate-limit
Ethernet0/0
  Input
  matches: all traffic
  params: 256000 bps, 128000 limit, 256000 extended limit
  conformed 0 packets, 0 bytes; action: transmit
  exceeded 0 packets, 0 bytes; action: drop
  last packet: 85246784ms ago, current burst: 0 bytes
  last cleared 00:00:35 ago, conformed 0 bps, exceeded 0 bps
Ethernet0/1
  Input
  matches: all traffic
  params: 128000 bps, 64000 limit, 128000 extended limit
  conformed 0 packets, 0 bytes; action: transmit
  exceeded 0 packets, 0 bytes; action: drop
  last packet: 85250214ms ago, current burst: 0 bytes
  last cleared 22:38:59 ago, conformed 0 bps, exceeded 0 bps
heron#
heron#
heron#
heron#
heron#
heron#
```

Figure 4.8. Snapshot of rate-limit operation from Router command line interface

### 4.3.5. Additional Features

#### 4.3.5.1. Authentication Module

The application has a simple authentication module that permits only valid users to access the application. Two levels of users are permitted to access the application.

*Guest level:* The Guest level users are allowed to view all sections of the application but not perform any critical operations that could jeopardize the network. The QoSManagement and AutoManage modules are blocked for the Guest level users.

*Administrator level:* The Administrator level users are expected to be those who are responsible for the operations of the LMDS network. Personnel of this level are permitted to perform all possible operations using the LMDS QoS tool. This includes access to the AutoManage and the QoSManagement sections.

A snapshot of the Authentication module is provided in Figure 4.9. This dialog box pops up immediately after the welcome window.

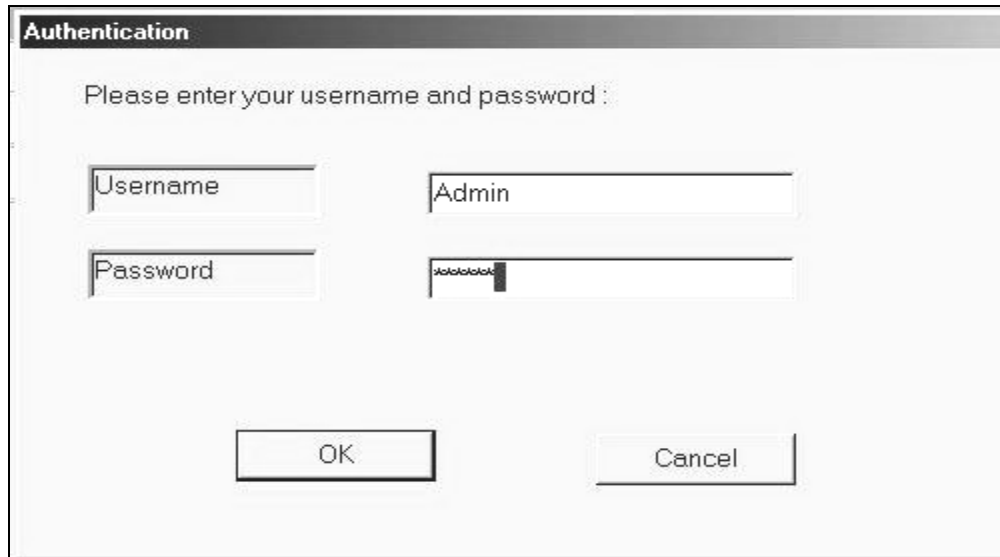


Figure 4.9. Snapshot of Authentication Dialog

It is expected that the authentication module would be tied into the Virginia Tech authentication server to allow administrator privileges to a selected set of users using their VT PID and password. This would ensure a dual level of security with the SNMP access regulations for Guest level users explained earlier and the VT PID authentication module and maintain the integrity of the network.

#### 4.3.5.2. Help Windows

The major operations performed using the LMDS QoS tool via their respective interfaces requires initial guidance for the novice user. Help windows are provided to facilitate understanding of each of the possible operations performed by the four major modules of the LMDS QoS tool. Figure 4.10 shows one such Help window. It is expected that a section of the documentation from this thesis would be included as a Help manual for users. The content in the respective Help menus are restricted to explaining the purpose of that particular dialog and potential ramifications, if any, on the operation of the network.

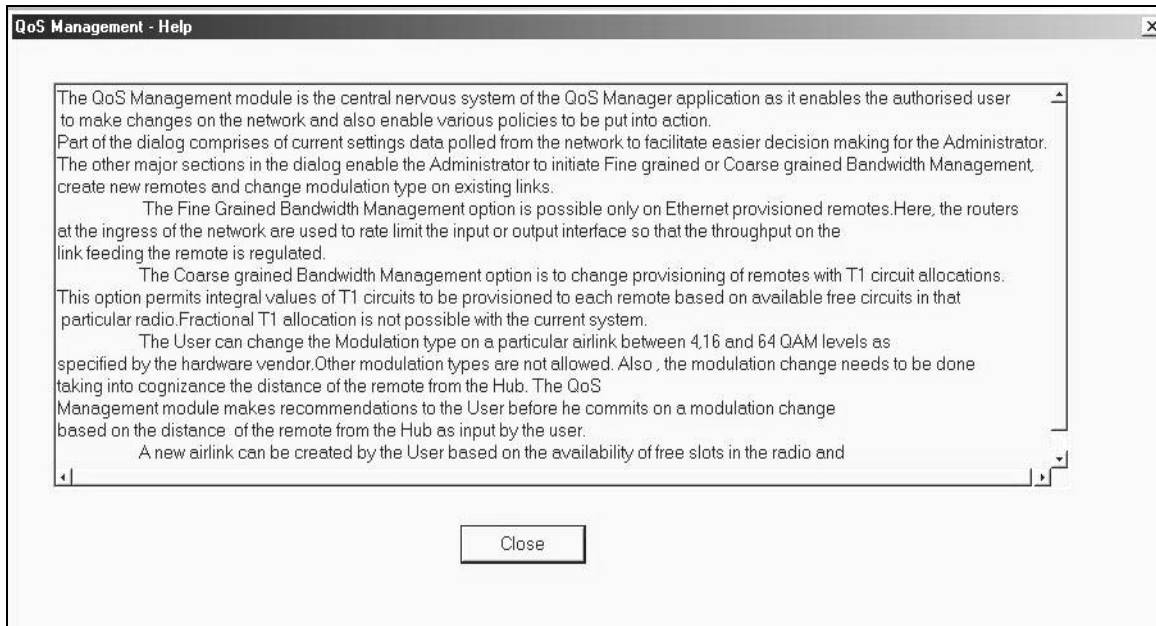


Figure 4.10. Snapshot of QoSManagement Help Window

#### 4.4. Chapter Summary

In this chapter, the potential issues in implementing the LMDS QoS tool were outlined and a short note on the tools that were used to develop LMDS QoS was provided. The operations and LMDS QoS tool was described in detail. The individual dialog boxes and their functions were explained along with the brief note on the additional features of the LMDS QoS tool. The concluding chapter describes the results and benefits of using the LMDS QoS tool. It outlines the areas not addressed by the tool and the potential for future work.

## 5. CONCLUSIONS

This concluding chapter summarizes the salient features of the LMDS QoS tool and outlines possible applications. The interoperability of the tool with LMDS equipment from different vendors and also for non-LMDS fixed broadband wireless technologies like MMDS and UNII is examined. The last section outlines the compatibility of the tool with systems based on the IEEE 802.16 Wireless MAN standards that are currently in development and expected to be available for commercial use in the near future.

### 5.1. Results

The LMDS QoS tool was designed to provide a simple and efficient mechanism to manage and utilize the Blacksburg LMDS network. It was also designed as an application to demonstrate a few possible ways to enable network QoS in legacy wireless systems. The application was implemented successfully and found to simplify network management for the broadband wireless network. The simplification was evident by the ease of managing the network with the tool in addition to the resource and management mechanisms provided by the tool. It was also found to be a useful tool for network performance monitoring by abstracting just the critical parameters and presenting them to the user in the Network Conditions window. The tool enabled the network administrator to provide service differentiation in the network and offer customers multiple packages with pricing based on requested capacity. The tool also allowed the administrator to specify utilization levels on the airlinks that could trigger allocation of additional resources or de-allocation of resources to a particular customer. This feature acts as a means to regulate resource allocation and ensure better service and use of network resources. Finally the LMDS QoS tool serves as a simple aid for students and researchers to understand the intricacies of wireless network configuration and the network performance from their desks without the network administrator having to compromise the security of the network or his or her availability for guidance. Currently, the network management station with HP OpenView software is single unit based at the administrator's office. Security constraints do not allow the software or any other network configuration and performance viewing mechanism to be made available to the

research community and potential customers. The LMDS QoS tool can be installed in multiple computers at various locations and with Guest level access, used to view network configuration and performance metrics.

On an elementary level the LMDS QoS tool has reduced the overall time involved in performing various configuration operations on the network. While the LMDS QoS tool does not seek to replace the HP OpenView management environment on an overall basis, it allows the administrator to perform part of the operations, like modifying modulation type, changing resource allocation to users without QoS enabling the link in consideration and, observing key performance metrics over time. The tool also allows the administrator to collect alarms over a period of time and analyze them to obtain key results on the network performance and response to various changes in the configuration and other external factors. Table 5.1 illustrates the approximate time savings due to using the LMDS QoS tool in comparison with the current HP OpenView method. The results are approximate and could vary with every attempt. The presented value ranges are averaged over four attempts at doing the same operation. The time values are also based on the fact that the user is equally familiar with performing the same set of operations with both the tools. The network conditions and current settings polling statistics are not presented since they could be simplified in HP Open View by creating specific tables to collect current values of just the required objects.

Table 5.1. Performance of LMDS QoS Tool versus HP Open View

<b>Operation</b>	<b>Time taken – HP Open View (s)</b>	<b>Time taken – LMDS QoS tool (s)</b>
Modulation type change	80-90	15-20
Coarse Bandwidth change	80-90	20-25
Fine bandwidth change	NA	30
Utilization Computation	NA	5 (based on polling interval selected)

## **5.2. Applications of the LMDS QoS Tool**

The LMDS QoS tool is a network management tool for LMDS and other similar fixed broadband wireless networks that uses a menu-driven graphical user interface. The tool acts as an intuitive interface for the management of the Blacksburg LMDS network. It reduces configuration time and simplifies the process of managing a complex wireless network. It enables the network administrator to perform complex procedures, like changing modulation type and re-provisioning links, in a matter of few minutes.

The tool acts in a proactive manner to compute the utilization in a particular airlink and re-provisions the resources for that link based on its usage. This conserves resources and uses them only when necessary. The LMDS QoS tool enables fine-grained bandwidth management, an option not directly provided by the vendor. Although there is no conservation of bandwidth on allocation in using a finer granularity, there is a possibility for service differentiation in the network. This allows the service provider to deliver multi-service offerings to the customer with pricing based on usage and QoS requirements. The customer neither pays more or less for his or her service. He or she pays only for the level and quantum of service he or she desires. This allows the service provider to reach out to a wider customer base with diverse requirements ranging from a few hundred kilobits per second bps to a capacity equivalent of few T1s.

As a result of managing the LMDS network using the LMDS QoS tool, there is considerable decentralization of network monitoring operations. The tool can be distributed to a wider audience with limited capabilities that do not include making any configuration changes in the network. It would assist in better understanding the network under diverse operating conditions. It would also enable non-technical staff and decision makers to understand the operations and management of the wireless network.

The LMDS QoS tool is extensible. It has the potential be used to operate with LMDS equipment from vendors other than Harris Corporation with limited changes. With proper changes especially in the handling of dynamic slot allocation, the tool can also be a

candidate for managing and providing QoS IEEE 802.16 networks. The interoperability and extensibility of the LMDS QoS tool is described in further sections of this chapter. The tool serves as a proof of concept demonstration of quality of service in legacy wireless networks with no provision or documentation for providing varying service levels to the customer.

### **5.3. Limitations of the LMDS QoS Tool**

The LMDS QoS tool does not provide the option of creating or activating a new customer service access point. While it is possible to add it as a part of the capabilities of the tool, the complexities involved in selection of appropriate tower, frame and sector and then provisioning the air-channel allows for the possible introduction of many errors. This could make the system unstable for regular operations. Also, the creation of a node involves decisions to be made at every step that is unique to the particular remote in consideration. By automating such a process, the inherent flexibility in resource allocation and service provisioning for the node by a manual procedure is compromised. Hence, it is left to the network administrator to configure the remote using the HP OpenView management software and the remote unit serial port CLI interface.

While fine-grained bandwidth management is possible using the LMDS QoS tool, there is no actual savings in terms of network resources. If a user decides to opt for a 128 Kbps link, the application, while making it possible, still needs to provision a T1 to the remote. Although the actual data rate allowed to the customer is 128 Kbps, the system still uses up a T1 for the link. Hence, service differentiation is provided, but at no saving to the service provider. This is due to a design decision on the part of the LMDS equipment vendor to allocate bandwidth to all remote units in terms of an integral number of T1s over the air interface.

The LMDS QoS tool presently does not have a web interface. Hence, if one needs to use it, the application needs to be installed in his or her machine. While this is feasible for a limited number of users, it does not scale well in terms of multiple users in geographically different locations. This design choice is driven more by security concerns

than any other. There is a possibility of compromising network security by allowing web access to certain sections of the network directly or indirectly.

The use of the LMDS QoS tool is restricted to the Harris Corporation PTM 1000 family of LMDS equipment. While it can be modified to work with other LMDS and non-LMDS systems as explained in earlier and forthcoming sections, it has been designed with the PTM 1000 family in consideration. Since most vendors require a non-disclosure agreement to release their private MIBs, there was no possibility of designing a more general tool that would seamlessly merge and operate with multiple LMDS systems. While fixed-slot TDMA is used in many first-generation LMDS systems, a more dynamic approach to slot allocation is being adopted by next generation equipment scheduled to be introduced in the near future. The long-term applicability of the LMDS QoS tool can be determined only when one such system is installed and the MIBs and features are analyzed.

#### **5.4. Areas for Future Work**

This section describes a few of the areas where there is potential for future work and improvement in the LMDS QoS tool.

##### **5.4.1. Providing Priority Access**

The LMDS QoS tool currently does not provide priority access to the network for any remote subscriber, even if he or she is willing to pay for it. While priority access is being addressed by the next generation equipment partly by means of dynamic TDMA and partly by certain proprietary mechanisms [10], it is theoretically possible to enable it in the current system itself. This would involve the router at the ingress of the hub acting effectively as the medium access controller and providing prioritized traffic to the hub. This would not involve any changes in the way the hub operates, but would only require scripts to enable prioritization at the router. By prioritization, we mean that the router would temporarily block traffic destined to the lower priority remote for one timeslot and provide the hub with only traffic for the high-priority remote. The problem with such an implementation is that if all or many remotes have traffic to send, it could result in a



waste of timeslots for prioritization purposes. This would have the negative effect of wasting precious network resources. Hence, prioritization of service can be enabled, but at the cost of using additional network resources and depriving more customers of the service.

#### **5.4.2. Allowing More Customers per Radio**

The current hardware limits the number of remotes units per hub radio to four. This implies that not more than four physical locations can be served by each hub radio. This is a limitation that is reflected by the fact that there are only four timeslots per cycle and an additional remote would not be served by the hub radio. Even if there are physically five remote units within the 30-degree sector of a hub radio, the first four remote units provisioned would only be served on a first-installed, first-served basis.

While the timeslot allocation is static and cannot be changed, the router at the ingress of the network can be manipulated to serve more customers than what is expected. This can be made possible by enabling the router to route traffic to the hub from four remotes every cycle with the actual set of four remotes differing with each cycle. For example, if remotes A, B, C and D are served in first cycle, the router would have access lists to block traffic to A for the next cycle and offer service to B, C, D, and E in the second cycle. The third cycle would then consist of traffic to C, D, E, A and so on. This approach is not without its flaws. The ability of the router to discern between consecutive hub cycles and service times for individual remotes is a critical issue in achieving the goal of serving additional customers with the same network resources. When traffic to a new remote is presented to the hub, the configuration details of the remote need to exist in the hub database and the hub should consider the remote in its “active service” list. This is not possible in the case of additional remotes as the hub does not allow the administrator to provision five or more remotes in a single sector. If a solution to this handicap is devised, additional customers can be served with the existing hub radios, thereby, increasing the revenue potential of the network.

### **5.4.3. Extending the LMDS QoS Tool**

The LMDS QoS tool is designed to work with all fixed broadband wireless systems that use TDMA and a fixed slot allocation method. The SNMP MIB used is Harris Corporation's private extensions for the PTM 1000 family. These MIBs are specific to the Harris PTM 1000 product. So, if the LMDS QoS application is to be required to be used with other vendor equipment, the SNMP Object Identifiers would differ.

The fixed slot assignment mechanism of the Harris PTM 1000 equipment was taken into cognizance while designing the LMDS QoS tool. So, if the tool were to be used with any system that has a dynamic slot assignment system or uses FDMA, then parts of the tool would have to be redesigned.

Currently, all the device-specific MIB data are stored in header files and can be replaced with alternate headers for other devices. But, one other important issue to be considered is the sequence of SNMP operations that have to be performed to achieve a desired task. For example, to change the modulation type for a particular remote, a sequence of eight individual SNMP Set operations have to be performed in a particular order. This order would not be the same for all wireless devices or equipment that operates at LMDS frequencies. While the operations that need to be achieved would theoretically be the same, the way they are programmed in the system and the sequence are rarely, if not ever, the same. As technology evolves, the complexity of performing individual operations is expected to reduce. With this assumption, expecting a change in modulation to have the same long sequence of operations in all LMDS equipment in the future does not make sense. On a positive note, the basic framework and design of the LMDS QoS tool would definitely be applicable for any fixed wireless system that uses SNMP for managing the network. Although individual implementations might differ, the overall objective is the same. A thorough understanding of the device in question and the design of the LMDS QoS tool would likely allow a simple and efficient way to modify the application for use with any fixed broadband wireless system.

The LMDS QoS tool can be used for a mobile wireless network, too. Apart from the previously mentioned issues, the most critical concern in a mobile network, namely mobility management, is not addressed by the application. Hence, the LMDS QoS tool would need extensive revising before being used for mobile broadband wireless networks like IEEE 802.11b or third-generation wireless systems like universal mobile telecommunication systems (UMTS) or code division multiple access release 2000 (CDMA2000).

### **5.5. The LMDS QoS Tool and IEEE 802.16**

The IEEE 802.16 working group is defining the WirelessMAN standard for broadband wireless access for metropolitan area networks (MAN). The standard currently encompasses wireless systems operating from 10 to 66 GHz and is soon expected to cover systems operating in the 2 to 11 GHz range. The air interface standardization is expected to pioneer the deployment of wireless access systems in wide-area networks as a viable alternative to Digital Subscriber Line and cable modem service for high-speed Internet access. Wireless technologies like multichannel multipoint distribution service (MMDS) and LMDS are expected to reach a wider audience with the release of the IEEE 802.16 standards [17].

The IEEE 802.16 standards do not specify conditions for resource allocation and scheduling. Quality of service mechanisms are described extensively in the standards with support for legacy time division multiplexing (TDM), ATM and IP connectivity. The standards allow for a dynamic request-based slot allocation for the remote units to receive service from the base station or hub. This is meant to enable efficient management of resources and delay in service [17]. The LMDS QoS tool is designed to work with fixed slot allocation-based systems. While it could still be used to manage the network and monitor the performance of the network, the resource management mechanisms implemented in the system would be controlled by the hub unit by means of the dynamic slot allocation scheme. The cost of having the LMDS QoS tool manage the resources of the network would now include polling the hub unit for every frame so that the QoS manager module knows which remote is being serviced by the hub. Since, in a

dynamic system, the remotes serviced in each cycle are possibly different, polling at regular intervals is necessary. This would result in an additional load on the network for SNMP requests and responses and, also, an additional processor load on the management station. Hence, it is recommended that for IEEE 802.16 standards-based systems, the LMDS QoS tool be used as a monitoring and configuration tool only and not for any resource management.

## REFERENCES

- [1] A. Khobare, "Simulation Study of Local Multipoint Distribution Service," Master's Thesis, Virginia Polytechnic Institute and State University, July 20, 2000.
- [2] LMDS at Virginia Polytechnic Institute and State University  
<http://www.lmds.vt.edu> (current April 4, 2002)
- [3] G. Armitage, *Quality of Service in IP Networks: Foundations for a Multi-service Internet*, Macmillan Technical Publishing, April 2000.
- [4] Differentiated Services charter:  
<http://qos.internet2.edu/wg/charter.shtml> (current February 13, 2001)
- [5] Integrated Services charter:  
<http://www.ietf.org/html.charters/intserv-charter.html> (current September 5, 2000)
- [6] D. Verma, *Policy Based Networking: Architecture and Algorithms*, New Riders Publishing, 2000.
- [7] D. Verma, "Simplifying Network Administration Using Policy-based Management," *IEEE Network*, vol. 16, no. 2, pp. 20-26, March-April 2002.
- [8] R. Parthasarathy, C. W. Bostian, L. A. DaSilva, S. F. Midkiff, T. Callahan, "A framework for policy-based Quality of Service (QoS) in an LMDS Wireless network," *Wireless and Optical Communications '2002*, pp. 398-404, July 2002.
- [9] International Engineering Consortium, "Local Multipoint Distribution System,"  
<http://www.iec.org/online/tutorials/lmds/> (current June 11, 2003)

- [10] Harris Corporation, "ClearBurst Family," <http://www.microwave.harris.com/products/clearburst/> (current June 11, 2003)
- [11] K. S. Phanse, L. A. DaSilva and S. F. Midkiff, "A Taxonomy and Experimental Evaluation of Policy Architectures for Bandwidth-constrained Networks," Technical Report, Virginia Polytechnic Institute and State University, 2002.
- [12] Y. Kanada, "Rule-based Modular Representation of QoS policies," *10th Networking Architecture Workshop*, pp. 106-113, Oct. 2000.
- [13] A. Pras, "Internet management: Where we are and Where we go," *High Speed Networking Workshop*, pp. 11-12, May 2000.
- [14] F. Straub, "Concept of a Script MIB Based Policy Management System," Technical Report, <http://www.ibr.cs.tu-bs.de/projects/jasmin/policy-concept.pdf>, May 2001.
- [15] D. R. Mauro, K. J. Schmidt, *Essential SNMP*, O'Reilly & Associates, 2001.
- [16] S. Boros, "Policy-based Network Management with SNMP," *EUNICE 2000 Summer School*, University of Twente, Netherlands, pp. 1-3, September 2000.
- [17] R. Marks, "IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband wireless access," IEEE 802.16 Broadband Wireless Access Working Group, April 6, 2002.
- [18] D. Libes, *Exploring Expect: A Tcl-Based Toolkit for Automating Interactive Programs*, O'Reilly & Associates, 1995.
- [19] P. E. Mellquist, *SNMP++: An Object Oriented Approach to Developing Network Management Applications*, Hewlett Packard Professional Books, March 1997.

- [19] SNMP++ v3.2:  
[http://www.agentpp.com/snmp\\_pp3\\_x/snmp\\_pp3\\_x.html](http://www.agentpp.com/snmp_pp3_x/snmp_pp3_x.html) (current June 11, 2003)
- [20] Cisco Systems, “How to calculate bandwidth utilization using SNMP”:  
[http://www.cisco.com/warp/public/477/SNMP/calculate\\_bandwidth\\_snmp.html](http://www.cisco.com/warp/public/477/SNMP/calculate_bandwidth_snmp.html) (current October 31, 2002)
- [21] RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II:  
<http://www.ietf.org/rfc/rfc1213.txt> (current March 1991)
- [22] RFC 1757, Remote Network Monitoring Management Information Base:  
<http://www.ietf.org/rfc/rfc1757.txt> (current February 1995)
- [23] Radiant Networks:  
<http://www.radiantnetworks.com> (current June 11, 2003)
- [24] FCC LMDS Band plan:  
<http://wireless.fcc.gov/auctions/data/bandplans/lmds.pdf> (current June 11, 2003)
- [25] Newbridge Networks, “Proposed Approach to Fixed-Wireless Broadband Network Deployment and Service Provisioning in Singapore,” March 2000.
- [26] A. Menezes, “Case Study: Setting Fixed Wireless in Motion,” *Wireless Future Magazine*, <http://www.wirelessfuturemagazine.com/fixedwireless.html>, September-October 2002.
- [27] A. V. Arunachalam, “Quality of Service (QoS) Classes for BWA,” IEEE 802.16 Broadband Wireless Access Working Group, July 22, 2002.

[28] G. Fishel, "Summary of IEEE 802.16 System Requirements," IEEE 802.16 Broadband Wireless Access Working Group, April 11, 1999.



## VITA

Rangaprabhu Parthasarathy (“Prabhu”) hails from Coimbatore, a city in Southern part of India. He graduated with distinction in 2000 with a Bachelor of Engineering degree in Electronics and Communication Engineering from PSG College of Technology, Coimbatore. He joined the graduate program in Electrical Engineering at Virginia Tech in 2000 and will be graduating in June 2003. While a graduate student at Virginia Tech, he worked as a research associate with the Center for Wireless Telecommunications (CWT) and Virginia Tech’s Communication Network Services (CNS). He is currently on a temporary assignment with Interdigital Communications Corporation in King of Prussia, PA, developing a protocol stack for third-generation wireless systems.

### **Publication:**

R. Parthasarathy, C. W. Bostian, L. A. DaSilva, S. F. Midkiff, T. Callahan, “A framework for policy-based Quality of Service (QoS) in an LMDS Wireless network,” *Wireless and Optical Communications* ‘2002, pp. 398-404, July 2002.