Int. J. Engng Ed. Vol. 22, No. 4, pp. 896–905, 2006
Printed in Great Britain.

0949-149X/91 $3.00+0.00

Telecommunications Network Management Applications in an Educational Environment*

IBRAHIM RAAD, PETER VIAL, WALID RAAD and KENI POPOVSKI
University of Wollongong, School of Electrical, Computer and Telecommunications Engineering, Australia
E-mail: ibrahim@uow.edu.au

Network management and the application of the different components have become an important part of networks in industry. Therefore, it has become important to teach network management to potential employees of companies which have come to rely on large networks. One of the more important network management protocols is known as Simple Network Management Protocol. This paper presents, in some detail, a new development of an SNMP laboratory for a specialisation subject in Telecommunications engineering based on this protocol. Other aspects of this laboratory include three other types of network management applications: Nagios, TKINED and a remote monitor known as RMON probe. Encryption and decryption are also introduced and studied in depth for security aspects of network management. The students are required to complete the laboratory tasks in six weeks and are required to submit reports based on this work demonstrated in the laboratory.

Keywords: SNMP; Nagios; TKINED; RMON; Network; Security; DES

INTRODUCTION

MANAGEMENT PROTOCOLS used to monitor networks like that shown in Fig. 1, such as Simple Network Management Protocol (SNMP), depicted in Figs. 2 and 4, are widely used in the monitoring of devices. Together with management tools such as TKINED, Nagios and remote monitoring (RMON) probes, local area networks may be statistically analysed, mapped, and queried for various properties.

These tools may also be applied to more complex networks. More sophisticated software may be required when considering monitoring software for networks which incorporate modern voice, video and data services. However, SNMP is commonly found in complex network configurations, such as in the management of Ethernet switches.

Security is a vital feature in all systems. Many algorithms, including 'Data Encryption Standard' (DES), with its block diagram (depicted in Fig. 4), have been devised to encrypt data. All are designed in order to maintain user confidentiality and privacy.

Due to the large-scale application of network management tools such as those mentioned above, and with the security 'issue' being more important than ever in communications, it was decided that a course would be offered in the fourth and final year of the Telecommunications Engineering degree at the University of Wollongong (UOW) that would give students an insight into the number of network management tools that are available. This course is an elective subject and is also available to other students within the School of Electrical, Computer and Telecommunications Engineering (SECTE).

While the subject itself has been available for some time, it did not have a laboratory to supplement the theoretical content, which has been presented in the lecture theatre. So the laboratory is new and has become an integral part of the Telecommunications Network Management course at SECTE.

What makes this laboratory's experiments unique is that, rather than concentrating merely on one networking management tool (as is usually the case when teaching this course), it introduces and allows the students to use four different applications of networking management, which will in turn allow them to compare and experience the different applications in preparation for working in the industry. It enables the students to obtain a deeper understanding of security in network management by allowing them to develop (using MATLAB programming language) the encryption and decryption of DES, which has now become the fundamental building block of SNMP security. By the end of the six experiments, the students have gained a good understanding of network management, an appreciation that there are different tools with which this can be done and a clear working example in security for SNMP and its applications in networks and network management.

So the reader, by the end of this paper, should have discovered a new way of educating engineering students in telecommunications network

* Accepted 8 May 2005.

management, which has been successfully tested at UOW (through surveys of students in a class of over 60) and does not require large sums of money to build and set up. Nagios, TKINED and AdventNet are free downloads. JoeSNMP, depicted in Fig. 2, was developed at SECTE and is discussed in [11]. Programming of DES is carried out using a MATLAB student version which is widely available at a number of universities. Finally, the RMON probe was also developed at SECTE and is discussed in [15].

MANAGEMENT PROTOCOLS AND SOFTWARE

Simple network management protocol

Simple network management protocol software is used to monitor any network device which has the SNMP agent software installed [1]. The SNMP agent interacts with other management software, transferring information regarding network status between monitored devices, applications, and management systems [2]. Each agent maintains a database known as a 'management information base' (MIB), which contains configuration and traffic information about the device [3]. An example of this device is the Tiny Internet Interface (TINI) board, depicted without casing in Fig. 3. The TINI is used in this lab to act as a node on the network, which has the MIB installed, collecting data. Other devices in the network include PCs, bridges and remote monitors. Using a variety of nodes rather than PCs allows students to understand that network management is used to manage any device that can be connected to a network, not just a standard PC. The general idea behind this is to show that any device which has an MIB (i.e. can collect and report information about the network) can be managed using the appropriate tools.

A software example which utilises SNMP is 'AdventNet' [14], depicted in Fig. 4, a package which can be used to browse the MIB of a network node. Various aspects of the device can be obtained, such as the services it offers, the limit on the total number of TCP connections the entity can sustain, and the physical location of the device. Entries which may be set by the software include the name of the managed device and contact details of the manager. SNMP software such as this may be used within local area networks (LANs), allowing administrators to examine network nodes and manage their operation.

SNMP offers many features related to network management. One such feature is the TRAP function. This feature enables agents to notify management stations of significant events, such as a reboot of the device. This is depicted in Figs. 10 and 11, which are screen shots from the laboratory, explained in detail in the section below on laboratory experiments. The students are taught about the TRAP feature of SNMP (which is a notification mechanism of the agent to the station manager) by simulating a trap that is sent and captured, respectively.

Network management tools

Numerous tools exist which aid in the management of network devices, including TKINED, Nagios, and remote monitoring (RMON) probes.

TKINED is an interactive editor for creating and maintaining network maps [4]. The package contains applications to discover IP networks, to obtain MIBs for network nodes, and to monitor network status using SNMP. This is depicted in Fig. 8. This software allows the student to enter an IP address of a network, resulting in the 'mapped network' shown in Fig. 9. This shows PCs with their IP addresses below them, to indicate which nodes in the mapped network are active and which are not. The inactive nodes are highlighted in red. Due to these features, this software may be used with LANs to obtain data about network nodes, and also to observe their 'reachability'. For example, if a node which was previously detected was disconnected from the network, its icon would flash red until it was reconnected. By this means, a network manager may be quickly alerted to problematic nodes and seek repair.

Nagios is a host and service monitor which informs users of various network problems. Regular checks are conducted on hosts and services, reporting information such as status of nodes and historical logs. Its various methods of displaying statistics allow network managers to observe status data about device groups and individual nodes in a graphical or tabulated manner. 3D maps of reachable networks may also be created.

RMON, which is depicted in Fig. 12, is utilised to monitor sections of a network and gather statistics. Essentially, it is a node which gathers information about the network and stores it locally. This may be configured to notify network managers of exceeded thresholds using SNMP. RMON may be used to overcome some of the limitations of SNMP, such as the traffic incurred by the continual polling of agents, since it stores data locally, resulting in less management traffic over the links. The Internet Engineering Task Force (IETF) remote network monitoring management information base (RMON MIB) specification adds an extra MIB for defining managed objects. It diagnoses events on network segments and also reports on error conditions [5], which is useful in network management.

APPLICATION TO LARGER NETWORKS

Management protocols

Relative to LANs, larger networks are more difficult to monitor. Administrators within small networks may be able to visually monitor the entire network, while more complex systems require software such as SNMP for remote monitoring from a single workstation.

Another protocol which has been developed to overcome the shortcomings of SNMP and allow larger networks to be more easily monitored is Common Management Information Protocol (CMIP). While it consumes more resources and is designed to run with the Open Systems Interconnection (OSI) stack, it allows an agent to perform tasks or trigger events based upon certain variables or conditions [6]. For example, when a computer cannot communicate with a fileserver, an event can be triggered to notify managers. Within SNMP, this task would require user intervention, since SNMP agents do not analyse data [6].

Management tools

Network mapping through TKINED and obtaining statistical data through Nagios are not viable candidates for complex network mapping. However, there are various tools which are equipped to deal with larger-sized networks. One example is HP OpenView Node Manager, which is based upon SNMP. It allows the creation of multi-level maps and remote management, and also features an event correlation engine which can locate the root cause of mass network failure [7].

The original RMON standard only permitted the monitoring of traffic through the data link layer of the OSI model, and did not identify hosts beyond routers [5]. The RMON 2 standard is better equipped to monitor medium-sized networks, allowing viewing of complete network traffic and increased management capacity. Unfortunately, it does not function over all layers of the model and does not support high-speed topologies or switched LANs. Frontier Software developed a variation of RMON 2, dubbed EnterpriseRMON, which overcomes the limitations of RMON 2 and works over all layers of the OSI model [5]. These RMON developments make it more suitable for complex network structures and allow the management of network segments to occur remotely, and without generating excessive traffic.

Example of management in a complex network

The Cisco 1548M Micro Switch 10/100 is an eight-port managed switch with 10/100 Ethernet ports. Through SNMP and RMON, the switch is fully configurable and allows management and monitoring for each port [8].

Fig. 1 shows the use of the switch within a backbone network for a small to medium-sized network. Being critical to the network, proper management and monitoring through SNMP and RMON allows for optimal performance through statistical trend analysis and remote monitoring.

SECURITY ISSUES

Security within all networks is of paramount importance, particularly within larger networks which are connected to a global information infrastructure such as the Internet. The initial design of SNMP did not incorporate complex security, resulting in remote configurations usually being avoided due to fear of unauthorised entry [6]. Hence, new developments to the protocol were initiated. SNMPv2u supported standardisation of security features, but it was SNMPv2* which guaranteed that security design addressed issues of proxy, traps, and remote configurations, thus enabling efficient management of medium to large-sized networks [9]. The current standard, SNMPv3, utilises security based upon SNMPv2u and SNMPv2*.

A common encryption algorithm, now considered insecure, is the Data Encryption Standard (DES), which is shown in Fig. 5. It was designed by IBM in 1975 and, after being accepted as an official standard in the USA in 1976, was used internationally [10]. It uses a block size of 64 bits and key of 56 bits, and is based upon the Feistel structure.

Unfortunately, due to it being susceptible to attack and having a small key size, it is being replaced by other algorithms. One common encryption is Triple DES, which involves applying DES three times with different keys. Another method is the Advanced Encryption Standard (AES), which has a fixed block size of 128 bits, key lengths of 128, 192 or 256 bits, and is based upon a substitution–permutation network.

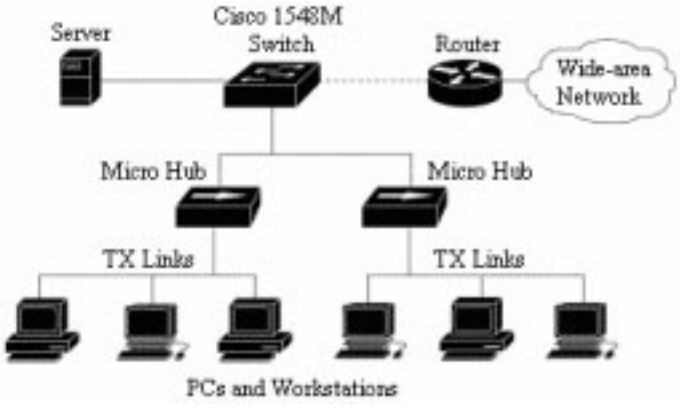

Fig. 1. Use of Cisco 1548M Switch in a backbone network [8].

Since the later encryption algorithms are based on the concept of DES, DES is taught to students as a building block to other more secure algorithms. Thus, knowing the building block of the other algorithms helps students in their study of the more complicated and more advanced encryption and decryption procedures.

LABORATORY EXPERIMENTS

The laboratory class that has been developed presents six experiments that students undertake throughout the course. This is done to aid students in further understanding the material presented in the field of network management. Each experiment discusses a different aspect of network management.

Experiment one introduces SNMP and its main functionality using a package called AdventNet [14], depicted in Fig. 4, with Internet-embedded devices such as the TINI, depicted in Fig. 3. Students are required to use AdventNet to connect to the TINI boards through their IP addresses and obtain information available from the MIB tree on the agent. This introduces the GET function of SNMP, while at the same time introducing the class to network management by allowing them to retrieve data from agents in the network.

Experiment two again focuses on SNMP basics, this time using JoeSNMP, depicted in Fig. 2, such as the SET and GET functions. However, in this situation the experiment allows the students to manage an entire network. The SET function is used by the students to set values of network devices into the MIBs, for example the threshold of the number of packets at a particular node which instructs the agent to send a notice to the manager when this point has been reached. The devices that are utilised for this experimental network include work stations, hubs, printers and bridges. Again, the students are required to obtain information stored on these 'snmpable' devices and to analyse them.

Experiment three introduces the TKINED SNMP manager to the students. This manager allows the user to 'map' the entire network. By mapping the entire network students are taught an important lesson in system administration; i.e. how to analyse and monitor the network that is under their control. Fig. 8 depicts the tool that the students use for mapping the entire network. Fig. 9 depicts the mapped network, showing all nodes that are present and operating in the network. If one of the nodes is switched off—for example, if the power has failed—then this is shown on this page by the symbol and IP address for this node flashing in red.

Experiment four introduces the TRAP function, which is another feature that is used when managing a network using SNMP. This experiment uses the package developed in [11]. It simulates the agent sending data (a trap) to the manager and the manager using the trap viewer to view and analyse this data (depicted in Figs. 10 and 11, respectively).

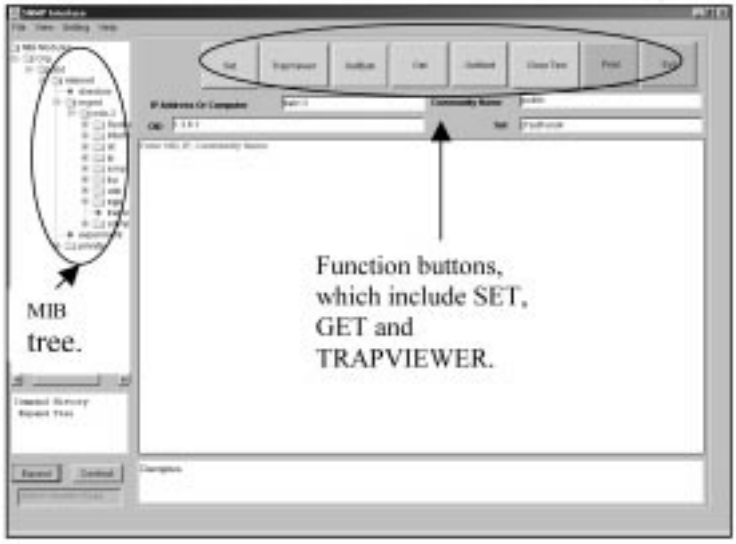

Fig. 2. GUI of JoeSNMP, developed for the network management lab [11]/

Fig. 3. TINI board without casing used as a node within the experimental network [13].

This is done from one PC and the simulated trap can be sent to a number of other machines, where the trap can be viewed and analysed by the manager. The trap viewer lists the different traps it has received from various agents.

Security using encryption and decryption (presented in the block diagram in Fig. 5) is undertaken in experiment five. As discussed earlier in this paper, security has become a very significant issue in networking today, so students are given an opportunity to program—using encryption and decryption—in MATLAB a key word unique to each student. Since DES forms the basis of all the new forms of security, the students are taught this. The students then demonstrate their work to the laboratory demonstrator.

Finally, experiment six uses the remote monitor that is also known as RMON probe. This is based on [15] and is depicted in Fig. 12. It allows the students to statistically analyse the network traffic, since this is what remote monitors actually do. A GUI that has been developed in-house is used to allow students to interface to the RMON probe [15].

WEBCT QUIZ

Online quizzes were given to students based on the material presented and demonstrated during the six weeks of the laboratory section of the subject. In total, two quizzes (worth 10% of the total mark) had to be completed at the end of the fourth and sixth experiment, respectively.

The first quiz concentrated mainly on the basics of SNMP, Nagios and TKINED—testing the students on such topics as the GET, SET and TRAP functionality of SNMP. The second quiz concentrated on the final two experiments—testing the students on DES and the RMON probe. Samples are depicted in Figs. 6 and 7.

The main reason behind this is to reinforce the material taught and connect the information taught in the lecture and demonstrated in the laboratory. This also serves as a monitoring tool of the progress of students during the session before the final exam. A practical exam was not used, since this is a six-week course and, with six experiments presented one per week, this was not a practical option.

REPORT ON EXPERIMENTS

After completing the six experiments and two quizzes, the students were required to write a paper of two pages in length on the application of such telecommunications network management tools in a scaleable network environment and discuss their feasibility. This is worth 20%, in total, which allows students to exhibit their theoretical knowledge, based on their practical experience of network management in a real-time environment. This paper is then used by the lecturer to assess the students' overall understanding of the material presented in the lecture room and to make any necessary adjustments for the following year's class based on these results.

SURVEY

To ensure that the material presented to students in lectures and laboratories remains the focal point in the study of network management, student surveys were carried out for feedback from

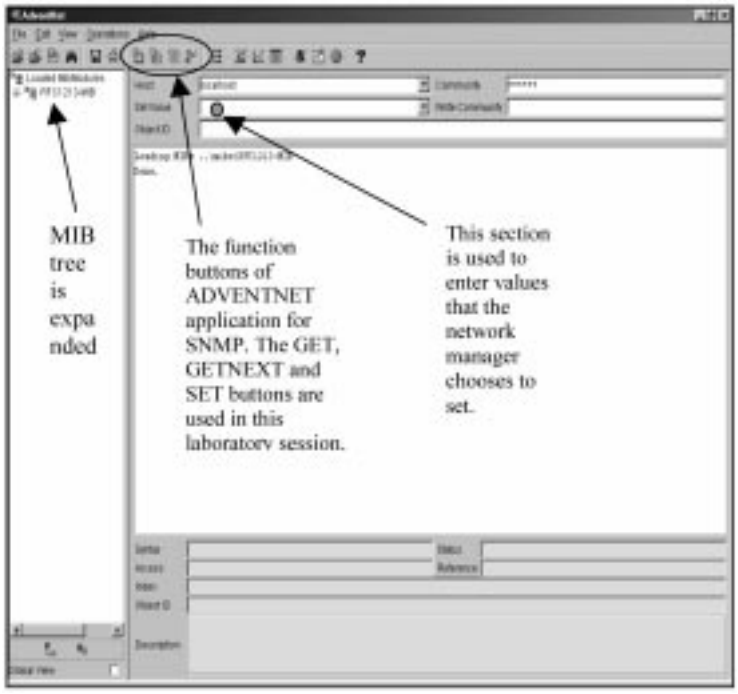

Fig. 4. AdventNet interface for SNMP [14].

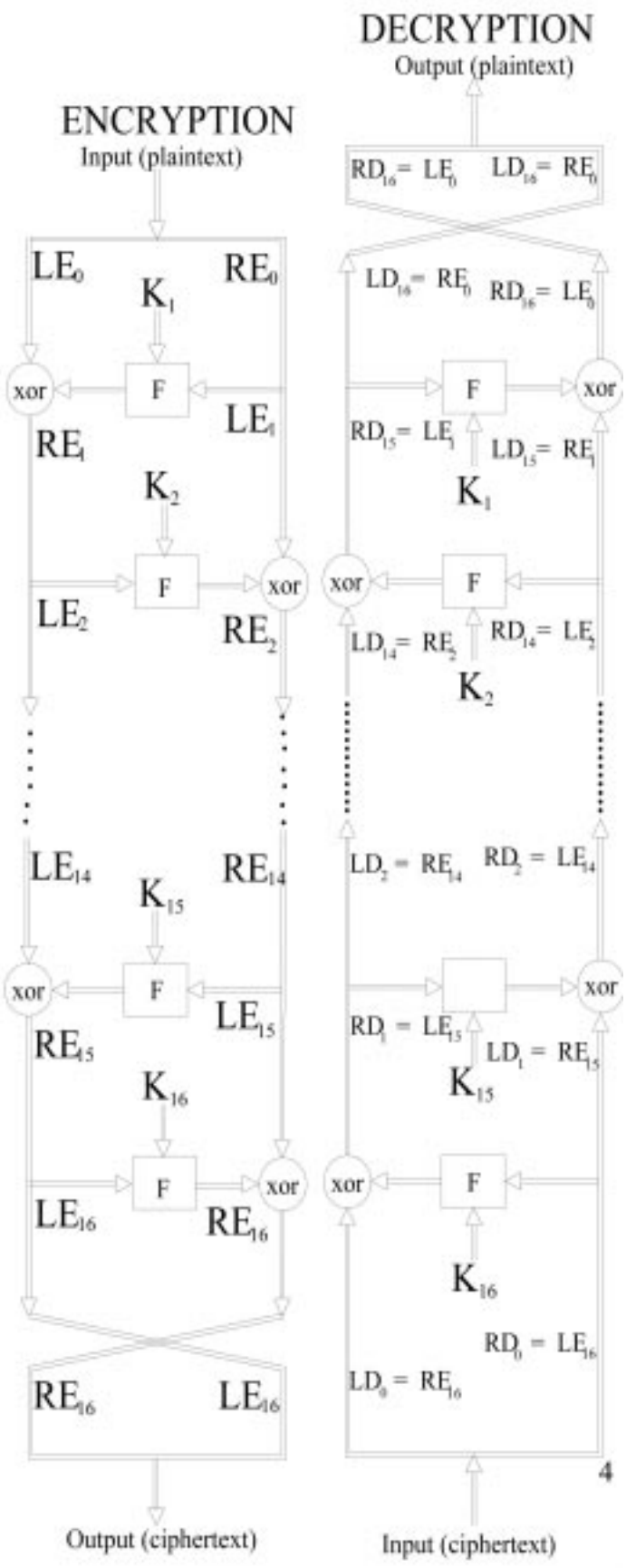

Fig. 5. Block diagram of the Feistel Encryption and Decryption [10].

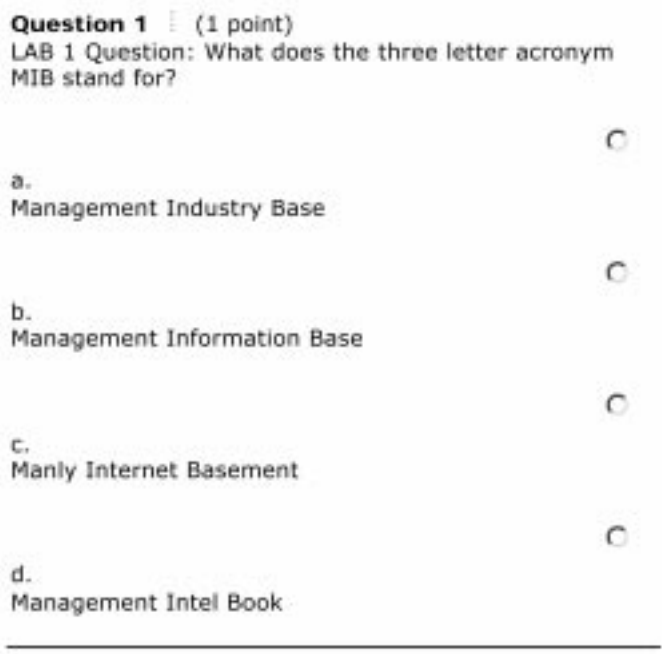

Fig. 6. Sample from quiz one, based on the basics of SNMP [16].

Fig. 7. Sample from quiz two, based on the last two experiments [16].

the 60 students enrolled in the subject. This feedback is then used to identify any weaknesses within the subject. The survey showed that 82.6% of the students enrolled in this subject strongly agreed or agreed that the subject matter covered in the course was clearly presented. Furthermore, 73.9% of students agreed that this laboratory stimulated them to think about the subject. Finally, 79.1% of the students agreed that the activities and tasks undertaken in this subject make it a worthwhile learning experience. Thus the survey showed that students had a positive reaction to the course.

Fig. 8. TKINED, which allows the user to map the entire network.

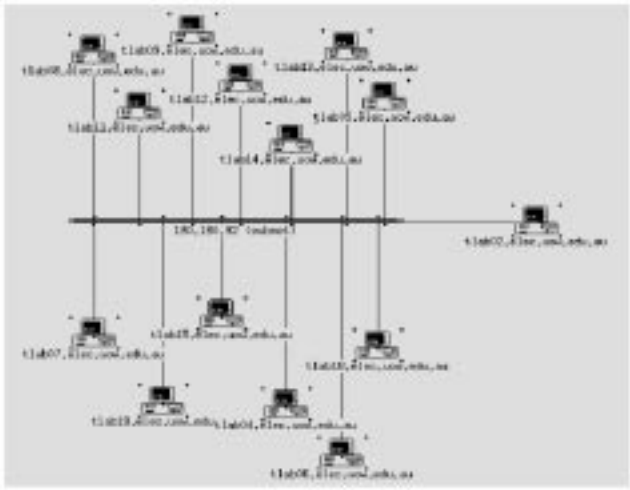

Fig. 9. The mapped network using TKINED, which allows the user to monitor the entire network.

Fig. 10. Trap generator used to simulate a TRAP message [11].

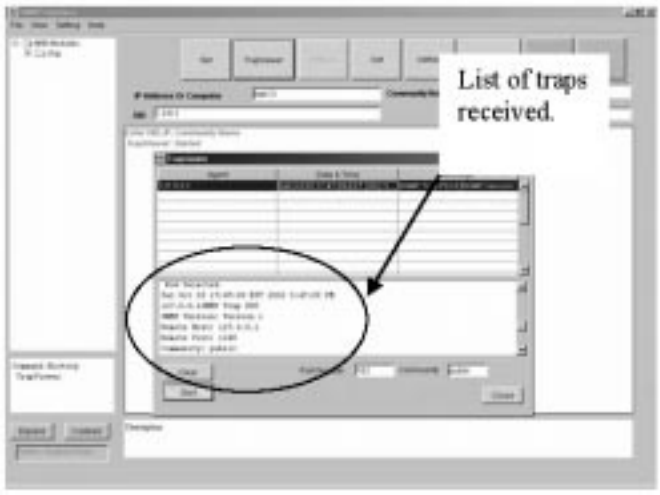

Fig. 11. Trap viewer used by manager to view and analyse a TRAP message sent by the agent [11].

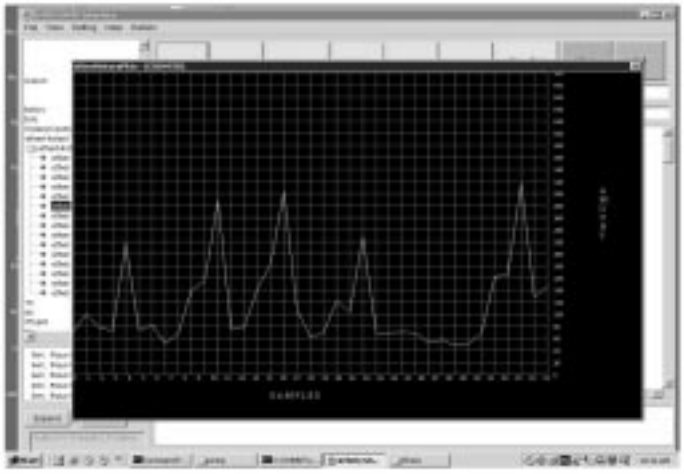

Fig. 12. Plot of *EtherHistoryPkts* from RMON probe using the RMON/SNMP interface [15].

CONCLUSION

With local area networks becoming increasingly popular and global connectivity becoming vital in many areas of modern businesses, network management and monitoring tools have become essential. While some are only suitable for use in small networks, other tools allow for management of larger, more complex, networks. SNMP is commonly used in small networks, while CMIP is more suited to a larger infrastructure.

Security is also crucial in modern communications, to ensure that all private data remains secure. Many algorithms have been developed, such as DES, although once they are perceived as having become insecure they must be replaced with more sophisticated algorithms. All management tools and security protocols are designed to ensure that networks remain functional, efficient, and protected. This paper has presented a description of a complete set of laboratory experiments for telecommunications engineering.

The educational network management laboratory presented here has proved to be an excellent supplement to the theoretical material taught in the lectures. It has also been demonstrated that it is not expensive to produce such a laboratory. SECTE had previously purchased a laboratory which cost $15,000, comprising Spectrum from Aprisma (formally Cabletron) and NMS from Novels. The majority of students agreed that this laboratory had the desired outcome in educational terms, teaching them the practical aspects of network management. This laboratory not only concentrated on the practical skills needed by network management engineers but also addressed their theoretical knowledge through quizzes and reports during the session. These quizzes and reports were used by the lecturer to monitor the progress of the students during the semester. Based on the six experiments presented in this paper, the authors recommend this approach to teaching network management, as it gives students a good balance between practical and theoretical knowledge and provides lecturers with a mechanism to monitor the progress of the students during the period of study.

REFERENCES

1. A. Leinwand and K. F. Conroy, *Network Management*, 2nd edition, Addison-Wesley (1996).
2. Microsoft, Windows Server 2003, accessed on 8 August 2004 (www.microsoft.com/resources/documentation/WindowsServ/2003/).
3. Alcatel, SNMPv3—Simple Network Management Protocol. Executive brief (February 2003) available at http://www.ind.alcatel.com/library/e-briefing/eBrief_SNMPv3.pdf.
4. J. Schoenwaelder, Guntram Hueske. Accessed on 6 August 2004 at http://wwwhome.cs.utwente.nl/~schoenw/scotty/man/tkined.html.
5. QUE, Managing Multivendor Networks. Accessed on 15 August 2004 at http://docs.rinet.ru/MuNet/ch11/ch11.htm.
6. Carnegie Mellon, SNMP. Accessed on 20 August 2004 at http://www.sei.cmu.edu/str/descriptions/snmp_body.html.
7. Agilent Technologies, Hewlett Packard, HP OpenView Node Manager. Accessed on 20 August 2004 at http://www.phoenixdatacom.com/hp/hp.html.
8. Cisco, Cisco 1548M Micro Switch. Accessed on 8 August 2004 at www.cisco.com/univercd/cc/td/doc/product/lan/ms1548m/icg/overview.htm.
9. D. Harrington, The Evolution of Architectural Concepts in the SNMPv3 Working Group. Accessed on 20 August 2004 at http://www.simple-times.org/pub/simple-times/issues/5–1.html#operations.
10. Wikipedia. accessed on 20/8/04 at http://en.wikipedia.org/wiki/DES.
11. I. Raad and P. Vial, Network Laboratory Management Laboratory, 1st International Conference on Information & Communication Technologies: From Theory to Applications—IEEE-ICTTA'04. April 19–23 2004, Damascus, Syria.
12. Ibutton. Accessed on 6 April 2005 at www.ibutton.com.
13. TINI image. Accessed on 6 April 2005 at http://www.smartsc.com/tini/tiniimage.html.
14. AdventNet—excellence matters. Accessed on 6 April 2005 at www.AdventNet.com.
15. I. Raad, P. J. Vial and P. Gallon, Graphical User Interface to Access RMON Probe in Java, 4th International Symposium on Communication Systems, Networks and Digital Signal Processing, School of Electrical, Electronics and Computer Engineering, University of Newcastle, UK, 20–22 July 2004.
16. Webct.uow.edu.au, Telecommunications Network Management home page.

Ibrahim Raad received his Bachelor of Engineering (Electrical) and Masters of Engineering (Research) from the University of Wollongong in 2002 and 2004, respectively. He is currently undertaking a PhD in the wireless communication field. His research interests include wireless communications (multi-user systems), error correction codes and engineering education.

Peter Vial is a lecturer in the School of Electrical Computer and Telecommunications Engineering, where he has taught since September 1992 up to the present day, first as a Teaching Fellow, then as an Associate Lecturer and, since January 2004, as a Lecturer. His interests lie mainly in the area of telecommunications, but his foundation degree is in Electrical Engineering and he has a Masters in telecommunications as well as a diploma in Education (Mathematics, Secondary Education), all awarded by the University of Wollongong. His main areas of interest are packet networks (Frame Relay), network management, and wireless communications, in which he is doing a doctorate studying the use of Space Time Spreading. He has been teaching network management since 2000 and is keenly interested in developing appropriate material for the network management strand within the telecommunications course. He was instrumental in developing the laboratory experiments for network management laboratories, along with his thesis students (in particular Mr Ibrahim Raad).

Walid Raad is a student who graduated from the University of Wollongong in Electrical Engineering and is currently undertaking a PhD in Wireless Communications at the University of Wollongong.

Keni Popovski is a student who graduated from the University of Wollongong in Telecommunications Engineering and is currently undertaking a PhD in Wireless Communications at the University of Wollongong.